National Centre of Excellence
for Cybersecurity Technology
Development & Entrepreneurship

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

सत्यमेव जयते
Ministry of Electronics &
Information Technology
Government of India

PRESENTS AT

AISS 2020
NASSCOM-DSCI
ANNUAL INFORMATION
SECURITY SUMMIT

OUR PARTNERS

IEEE
BANGALORE SECTION

futureskills prime
A MeitY - NASSCOM Digital Skilling Initiative

SERI

Security Education, Research, & Innovation Conference

Promoting Cybersecurity Education, Research and Innovation

SERI Conference Proceedings

SHORTLISTED PAPERS

THEME	AUTHORS	INSTITUTE/ ORGANIZATION
Data Privacy Considerations during Requirements Phase of IoT Product Development	HARSHA BANAVARA	Signify North America Corporation, Burlington, MA USA
ASTRA: A Post Exploitation Red Teaming tool	AKSHAY JAIN DR. BHUVNA J SUBARNA PANDA	Jain University, Bengaluru
New Space and New Threats	RAMESH KUMAR V PRASANNA PHANINDRAN	zSpaze Technologies, Bengaluru Easwari Engineering College, Chennai
Cross-Channel Scripting Attacks (XCS) in Web Applications	SHASHIDHAR R	Bennett University
Quantum Cryptography and Use Cases: A Short Survey Paper	SANCHALI KSHIRSAGAR DR. SANJYA PAWAR SHRAVANI SHAHAPURE	UMIT SNDT Women's University, Mumbai NCoE-DSCI, New Delhi
Securing IoT using Permissioned Blockchain	SHALINI DHULL	Tata Advanced System Limited, Noida
An Analysis of Internet of Things(IoT) Architecture	YASSIR FAROOQUI DR. KIRIT MODI	Parul University, Vadodara Sankalchand Patel University, Visnagar
Cyber Security-Modern Era Challenge to Human Race and it's impact on COVID-19	DR. SUMANTA BHATTACHARYA BHAVNEET KAUR SACHDEV	Zonal advisory at Consumer Rights Organization Indian Institute of Human

Data Privacy Considerations during Requirements Phase of IoT Product Development

HARSHA BANAVARA

Data Privacy Considerations during Requirements Phase of IoT Product Development

Harsha Banavara
Signify North America Corporation
Burlington, MA USA

***Abstract*—This paper addresses the continuing issues of comprehensive consideration and integration of data privacy into product and solution development to enable compliance to applicable standards, rules and regulations. The data privacy landscape is in continuous flux with more countries and regional entities placing increased importance and rigor upon the handling of specific categories of *people* data: personally identifiable information (PII) or personal data, protected health information (PHI), and sensitive information (SI). A process is offered which promotes early consideration of what kinds of data need to be collected, processed, and stored; determination of the implications based upon intended geographic locations of sales or services; and concluding with generation of comprehensive security requirements.**

***Keywords*—data privacy, security requirements, standards and regulations, product development lifecycle**

I. Introduction

The ever-expanding desire to collect information on anything and everything has resulted in an enormous amount of collected, manipulated, and stored data; data gleaned from machines, processes, and most importantly from people [1]. In this paper the authors will bring into discussion the terms of data privacy and security; how they interrelate and are connected is at the core of the presented concepts. Privacy within the context of data privacy "refers to keeping information confidential;" that is, allowing it to be viewed by only authenticated and authorized individuals and processes. Typically, information within Data Privacy involves PII, PHI, and SI [2]. To ensure the confidentiality of these data types requires application of security practices and policies, e.g. authentication, authorization, encryption at rest and in motion [3].

This paper will discuss issues and consequences associated with data collection, processing, and retention - steps that need to be considered during the early stages of product and solution development to minimize organizational exposure relative to data collection and use legislation and regulation [4].

A process is offered to address data decisions early-on in development activities to allow lowest costs and highest integration in solutions [5]. The authors' experience in concert with referenced contemporary sources provide an unbiased and objective approach to this growing issue.

II. Data Classification

A. Personally Identifiable Information

The definition of personal data or Personally Identifiable Information (PII) varies from one country to another. The authors in [6] define PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual 's identity, such as name, social security number, date and place of birth, mother 's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information".

Some examples are:

- Name – e.g. full name, maiden name, alias
- Personal identification number – e.g. social security number (SSN), passport number, driver's license number, taxpayer identification number, financial account, credit card number
- Address information – e.g. street address, email address
- Personal characteristics – e.g. photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, other biometric data (e.g., retina scan, voice signature, facial geometry).

B. Protected Health Information

Protected Health Information (PHI) is a subset of PII. The definition of PHI is defined in the Privacy Rule published by United States Department of Health and Human Service to implement the requirement of Health Insurance Portability and Accountability Act (HIPAA) of 1996. PHI includes, but is not limited to, all information relative to the patient-practitioner relationship [7]:

- The individual's physical or mental health or condition (past, present or future)
- Services provided and diagnoses defined
- Associated payment information (past, present or future)
- Standard PII (name, address, government issued identification number, etc...

In jurisdictions other than the United States, PHI may not be a separate category but is rather included within the ambit of PII.

C. *Sensitive Information*

Sensitive Information (SI) is also a subset of PII. The definition of SI may vary by jurisdiction, however, some categories included are racial, ethnicity, political alliance, religion, philosophical beliefs, organizational memberships, health conditions, sexual orientation / preferences, geo-location [3].

III. CHALLENGES

Developers of products and solutions involving data collection, processing and storage are faced with many challenges. Among these are a constantly changing regulatory environment, cross-border data flow, data localization, and penalties for non-compliance:

A. *Regulatory Environments*

In 1973, Sweden passed the first national data protection law in the world. Since then we have come a long way; as of January 2020, approximately 132 countries (out of 194) have enacted data privacy laws with many under development by their governments. This means that countries without data privacy laws are now in the minority [8]. Some regulations can have a huge impact not only on a region but also globally; e.g. the European Union General Data Protection Regulation (EU GDPR). This legislation superseded the existing EU Data Protection Directive (DPD) of 1995, and was a dramatic paradigm shift [9]. In another 3 years we will be celebrating the 50th anniversary of the first national data protection law; by then we can expect more laws to be passed by countries, making data privacy compliance even more challenging.

B. *Cross-border Data Flow*

When considering transfer of personal data across geo-political borders caution should be taken due to the following concerns [3]:

- Some countries do not have data privacy laws
- Some countries have a very restrictive set of data privacy laws
- Some countries data privacy laws are ambiguous

C. *Data Localization*

Some countries are enforcing strict regulations on their citizen's personal data. This includes mandatory storage of the data on servers physically located within their country; restricted access to and use of the data from outside of their country; and penalties for non-compliance. Examples are China, Russia, etc. [10].

D. *Penalties for Non-compliance*

Failure to warn can also mean heavy penalty, fines and possibly even jail time. A recent survey published by the Data Protection Authority (DPA) of Hungary, reported the number of fines collected for data privacy infringements has increased over 100% YoY 2014 vs 2015 [11].

IV. A PROCESS

Introducing security-oriented features earlier in the product development cycle incurs less costs and improves integration versus later consideration [5]. In order to address this critical issue early on in the development lifecycle, it is important that we adopt a robust time-tested process. One such process is Microsoft's Security Development Lifecycle (SDL) developed in 2002 [12]. The process matured quickly and was opened to public use in 2004.

According to Microsoft "SDL is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.". Requirements within SDL is the second phase of seven, right after training. Building resilient products is like designing a house - both require a strong foundation; good security requirements help in reducing the ambiguity for developers [13].

The process of coming up with good security requirements can be divided into 3 stages:

1. Collection and harmonization stage
2. Filtering stage
3. Prioritization stage

In the first stage, understanding the product along with the market segments, regions and sectors into which it will be offered, is essential in determining the coverage of the standards. Sometimes, the target market can be a single country (e.g. China, Russia) and organizations can come up with a China for China or Russia for Russia strategy wherein they leverage the resources within those countries thereby eliminating complex supply chain issues. A plethora of standards, regulations exist and there needs to be a mechanism to filter out the ones that are required and the ones that are *nice to have*.

In the second stage, the Pareto principle can be used to narrow down the number of documents that need to be considered. For example, if a product is to be sold in 10 countries and 80% of the revenues is coming from just 20% of the countries (20% of 10 is 2), then the organization can concentrate its efforts primarily on those 2 countries.

Finally, in the third stage, after the requirements have been narrowed down, they must be prioritized by all the relevant stakeholders. Some considerations for prioritization may include the customer needs, time to market, return on investment, resources available.

Following the above three stages will set the stage for Design phase of the security development lifecycle during which Threat Model is conducted. The recommendations from the Threat Model can also be used as an input to the initial requirements from the previous step and there by serving as a master set of requirements which can be revised and/or revisited as deemed necessary.

It is always good practice to consider data privacy requirements along with other cyber security requirements as it eliminates redundancy or additional effort at a later point in time [5]. Governance, Risk and Compliance (GRC) tools, available in the market, can assist in coming up with robust cyber security requirements for the product, traceable to multiple standards and regulations.

Oftentimes, there are multiple standards applicable to a product. In such a scenario it is recommended to go with the most stringent criteria. This allows compliance to the strictest requirements while still addressing the less rigorous ones. At the end of this three-stage process one should have a requirement specification document containing both data security and data privacy requirements for the product [4].

V. RECOMMENDATIONS

The following recommendations provide a basic toolkit for addressing data privacy within product development.

A. *Basic Principles and Frameworks*

If the collection of PII, PHI, and/or SI data is part of a product, the development team should consider and accommodate some basic principles, in order to be compliant with many data privacy Acts and Laws (apart from GDPR). Although published in 1980, the following Organization for Economic Co-operation and Development (OECD) privacy principles are still valid today. These principles are [14]:

- Collection Limitation – limits on collection of personal data
- Data Quality – data collected should be relevant to the purpose
- Purpose Specification – purpose specified at the time of collection of data
- Use limitation – only use the data for the intended purpose
- Security safeguards – data should be properly protected in all states- rest, motion, process
- Openness – principles and/or policies should be transparent to the data subject
- Individual participation – data subject has right to view, modify, delete their data
- Accountability – data controller and processor are accountable for the above principles

These are also incorporated into the Fair Information Practice Principles (FIPPs) [4] and in the UK Data Protection Act [15].

Note: When deleting personal data, always use standard practices such as those mentioned in National Institute of Standards Technology Special Publication (NIST SP) 800-88 Rev.1 [16]

Some of the other frameworks worth evaluating and investigating are:

- The Fair Information Practice Principles (FIPPs), 1973
- The Generally Accepted Privacy principles (GAPP), 2009
- APEC Privacy Framework, 2005
- The OECD Privacy Framework, 2013
- NIST Privacy Framework ver 1.0, 2020

B. *Assessments*

An essential tool for determining potential risks to data privacy is a Privacy Impact Assessment (PIA) [7]. It consists of a checklist and questions which cover many of the basic principles previously cited. The PIA should be introduced to the development process prior to commencement of design and revisited if any major changes are made to data, architecture, and features [3].

C. *More is Not Always Better*

Be judicious in what you collect. Some data which may not be core or essential to your product can push you into highly restrictive territory (e.g. HIPAA, PCI-DSS) [3]. Knowing your end goals and customer needs will limit the variety and quantity of data, making the data privacy scope more limited and simplistic.

Once you have determined the type of data to be collected, how are you going to handle it in the most efficient and cost-effective manner? Sometimes organizations go overboard on application of security policies and practices by, for example, encrypting *all* data. Always remember to apply security wisely as it incurs costs in both money and resources to implement and maintain, e.g. only encrypt *sensitive* data [1].

D. *Morphing your Data*

Unless there is a clear need for attaching an individual to collected data, aggregation or anonymization of the data is preferred. This breaks the connection between data and a specific person and takes the information out of the realm of data privacy controls [3].

E. *Securing your Image*

An organization can build market goodwill and notoriety based upon their security efforts through communicating data privacy-oriented actions and demonstrating the company is committed to secure handling of its customers' personal data. A couple of suggested tactics are the use of Trust Seals on websites and publicizing establishment of a Binding Corporate Rules (BCR).

1) Trust Seals: Trust seals have been around for quite some time. We have seen them mainly being used in eCommerce websites. These seals are associated with Secure Socket Layer (SSL) and its endorsement on a website ensures that the website has safe and secure transmission of customer's payment card information to the vendor. The Privacy Trust Seal is issued to websites which handle customers' personal data in compliance with either FIPPs, OECD, GAPP, APEC, etc [3].

2) Binding Corporate Rules: The EU Commission defines BCR as "internal rules (such as a Code of Conduct) adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection" (mainly EU to non-EU). BCRs provide a sufficient level of protection to companies to get authorization of transfers by national data protection authorities (DPA) [17].

These recommendations provide a starting point and can help optimize results. All projects are unique, and applicability of these recommendations must be weighed for relevance, value-add, and suitability.

VI. CONCLUSION

This stated process will go a long way in bringing data considerations to the forefront of the conceptualization and development processes. Considerations that if ignored or glossed over could place organizations in non-compliance with regional and country-specific rules and regulations, thereby, exposing them to both sanctions and resultant reduced revenues from curtailed sales. Additionally, the earlier in the development cycle features and accommodations are incorporated, the less cost associated with the effort and the more integrated the solution[4]. Such an approach will address the immediate data privacy needs, however, the rapidly changing legislative landscape requires those tasked with remaining in compliance to stay current and informed. Products will surely need to evolve in this topical area, requiring organizations to plan for these changes in strategic roadmaps.

As people in the security realm are aware, there is no such thing as *absolute* security, only the pursuit of being more secure. Indeed, compliance does not guarantee security. Additionally, integration of security with data does not ensure data privacy but rather mitigates its loss; and in the end that is the most we can hope for.

REFERENCES

[1] S.H. Harris, "All in one CISSP exam guide" , 6th ed, McGraw Hill, New York, NY, 2013

[2] J.M. Stewart, M. Chapple and D. Gibson, "CISSP – Certified Information Security Professional (ISC)^2: Official Study Guide", 7th ed, John Wiley, Indianapolis, IN, 2015

[3] P.P. Swire and K. Ahmad, "Foundations of Information Privacy and Data Protection," IAPP Publication, Portsmouth, NH, 2012

[4] T. Breaux, "Introduction to IT Privacy: A handbook for technologists", IAPP Publication, Portsmouth, NH, 2014

[5] R. Kissel, et al, "Security considerations in the system development lifecycle", NIST SP 800-64 Rev.2, 2008

[6] E. McCallister, T. Grance, and K. Scarfone, "Guide to protecting the confidentiality of personally identifiable information (PII)", NIST SP 800-122, 2008.

[7] "Summary of the HIPAA Privacy Rule", OCR Privacy Brief, 2010 retrieved from http://www.helpingyoucare.com/wp-content/uploads/2010/10/Summary-of-the-HIPAA-Privacy-Rule-Office-For-Civil-Rights-Privacy-Brief.pdf.

[8] G. Greenleaf, ""133 Privacy Laws and Business International Report", UNSW, Australia, 2015.

[9] "Joint statement on the final adoption of the new EU rules for personal data protection", European Commission, 2016 retrieved from http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm.

[10] "Data Localization: A challenge to global commerce and the free flow of information", Albright Stonebridge Group, 2015 retrieved from http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf

[11] A. Liber, "Hungarian DPA's 2015 annual report and enforcement statistics indicate increased activity", Baker Inform, 2016 retrieved from http://www.bakerinform.com/home/2016/4/11/hungarian-dpas-2015-annual-report-and-enforcement-statistics-indicate-increased-activity

[12] M. Howard and S. Lipner, "Security development lifecycle", Microsoft Press, 2006

[13] "SDL: What is the Security Development Lifecycle", Microsoft, 2016 retrieved from : https://www.microsoft.com/en-us/sdl/

[14] "The OECD Privacy Framework", OECD, 2013 retrieved from http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[15] "Data controllers and data processors: What the difference is and what the governance implications are", ICO, UK, 2014 retrieved from www.ico.org.uk

[16] R. Kissel, A. Regenscheid, M. Scholl and K. Stine, "NIST SP 800-88 Rev.1: Guidelines for Media Sanitization", NIST, 2014 retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

[17] "Overview of Binding Corporate Rules", European Commission, 2016 retrieved from http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm

ASTRA: A Post Exploitation Red Teaming tool

AKSHAY JAIN
DR. BHUVNA J
SUBARNA PANDA

ASTRA: A Post Exploitation Red Teaming tool

Akshay Jain[1]
[1]MCA Scholar, *School of CS & IT, Department of MCA, Jain (Deemed-to-be) University,*
Bangalore, Karnataka, India

Dr. Bhuvana J[2]
[2]Associate Professor, *School of CS & IT, Department of MCA, Jain (Deemed-to-be) University,*
Bangalore, Karnataka, India

Subarna Panda[3]
[3]Associate Professor, *School of CS & IT, Department of MCA, Jain (Deemed-to-be) University,*
Bangalore, Karnataka, India

Abstract: Red teaming is the act of thoroughly testing plans, arrangements, frameworks and suppositions by receiving an ill-disposed methodology. A red group might be a contracted external gathering or an internal gathering that utilizes techniques to empower an outcast's perspective. Post-exploitation can be defined as any activities taken after a session is created and accessible. A session is an open shell connection from an exploit. A shell can be a Meterpreter or by using spawn function. In this research paper, a deliberate methodology is proposed and a prototype model created for the red teaming operation. In this case study, the programmed ASTRA red teaming tool is capable of creating an end to end shell connection with admin privileges and can perform other red teaming operation which play important role in an operation. This paper is a result of keen research on cyber-attacks emphasizing, Virtual machine detection and bypass, obfuscated payloads bypassing windows firewall, Anti-malware Scan Interface bypass, encrypting files and other post-exploitation behaviour.

I. INTRODUCTION

When doing a careful obscure objective data framework vulnerability test, i.e., a red team commitment, there are situations when basic organization correspondence conventions should be focused on and surveyed in a limited period of time which can open a network connection and the red teamer has a specific tasks that are important to be carried out in the operation so that the whole system can be compromised. Proper tools are required to allow testing or getting a reverse shell with minimum effort.

The fundamental objective of post–misuse is to discover the base worth and capacities of the casualties' undermined framework/gadget and to access all the territories of the focused target systems without even being detected. Raising an alarm can make everything in vain and all the efforts useless [4].

Exploit the necessary frameworks with an elevated level of covertness and investigate the estimation of the information that is available on the objective's device. If they deem the information to be of worth, at that point they can burrow considerably further to attempt to get more data. Notwithstanding breaking down the information, an infiltration analyser can likewise dissect vault settings, methods of correspondence, framework design settings, and network strategies by which gadgets are associated with a specific network.

Many application aims to utilise application layer protocols (e.g., FTP, HTTP, SSH), but are not concerned with the underlying transport and Internet layers, which are critical to ensure correct communications. The developed prototype is capable of creating a stealthy reverse shell connection to the attacker which is less "noisy" which is because of providing features for flexibility by implementing simple hardcoded port and socket bind, whilst striving to ensure a balanced simplicity of use. The implemented functionality allows ASTRA to establish a reverses shell connection its features are, pre-allocated port to bind, stealthy connection.

This paper addresses the identified drawbacks in open source tools for red team operation and provides the following contributions:

1) Creates a less noisy reverse shell connection
2) ASTRA can be used to deliver more powerful Third-party scripts
3) Can leverage privileges and create paths for further attack vectors

II. RELATED WORK

Closed source Red Team instruments (e.g., Cobalt strike) are pricey, and by and large not it isn't attainable for short discovery infiltration testing or impromptu red teaming commitment.

In such cases, the open-source panacea is investigated and adjusted to meet the testing prerequisites. No closed source apparatuses were surveyed since no preliminary renditions were made accessible or given upon creator's solicitation.

Acunetix isn't only a web weakness scanner. It is a finished web application security testing arrangement written in C++ that can be utilized both independently and as a major aspect of complex conditions.

It offers built-in vulnerability assessment and vulnerability management, just as numerous choices for combination with market-driving programming development instruments. By making Acunetix one of the safety measures, you can altogether expand your online protection position and wipe out numerous security chances at a low asset cost.

InvisiMole bunch is a threat actor operating since at least 2013, whose malware was first revealed by ESET in 2018 regarding focused on digital surveillance tasks in Ukraine and Russia. We recently archived its two component rich secondary passages, RC2CL and RC2FM that give broad undercover work abilities, for example, recording from the casualty's webcam and receiver following the geolocation of the people in question, and gathering as of late got to reports.

In late 2019, the InvisiMole bunch re-emerged with a refreshed toolset, focusing on a couple of prominent associations in the military area and conciliatory missions, both in Eastern Europe. ESET specialists directed an examination of these assaults in collaboration with the influenced associations and had the option to reveal the broad, complex toolset utilized for conveyance, sidelong development, and execution of InvisiMole indirect accesses—the missing bits of the riddle in our past exploration. The examination additionally revealed beforehand obscure participation between the InvisiMole gathering and Gama Redon, an exceptionally dynamic danger bunch likewise working since at any rate 2013, and fundamentally focusing on Ukrainian foundations.

Cyber espionage groups are the refined adversary group that leads to complex assault crusades against their objectives. As digital surveillance exercises increment, there will be an expanded tension on these gatherings to rapidly and successfully direct their digital tasks against their objectives. Utilizing open-source hacking instruments (Vault 7) can permit these gatherings to satisfy this need by bringing down assets that would somehow or another be utilized to create redid tooling. Utilizing a language, for example, PowerShell which is broadly accessible on track frameworks. Open source PowerShell-composed post-misuse structures permit cyberespionage gatherings to use open source tooling on the PowerShell stage. This makes an ideal assault stage to lead digital tasks. This paper subtleties digital reconnaissance bunches that utilization open-source PowerShell-composed post-abuse systems and portray how they are

The Metasploit is a tool written in Ruby language, secluded penetration testing stage that empowers you to compose, test, and execute misuse code. The Metasploit Framework contains a set-up of instruments that you can use to test security weaknesses, list organizations, execute assaults, and dodge identification. At its centre, the Metasploit Framework is an assortment of regularly utilized devices that give a total domain to entrance testing and adventure improvement.

Bloodhound is an application used to visualise active directory environments. The front-end is based on electron and the back-end is a Neo4j database, the information utilized is pulled from a progression of information gatherers additionally alluded to as ingestors which come in PowerShell and C# flavours.

It tends to be utilized on engagement to recognize diverse assault ways in Active Directory (AD), this incorporates access control records (ACLs), users, groups, trust relationships and unique AD objects. The apparatus can be utilized by both blue and red teams to discover various ways to targets. The subsections beneath clarify the distinction and how to appropriately use the diverse ingestors

Mimikatz, portrayed by the creator as only "a little device to play with Windows security," is an extraordinarily viable hostile security instrument created by Benjamin Delpy. It is utilized by infiltration analysers and malware creators the same. The dangerous 2017 NotPetya malware moved spilt NSA abuses like Eternal Blue along with Mimikatz to accomplish most extreme harm.

Mimikatz abuses Windows single sign-on (SSO) usefulness to gather accreditations. Until Windows 10, Windows as a matter, of course, utilized a component called WDigest that heaps encoded passwords into memory, yet in addition stacks the mystery key to decode them. WDigest has been a helpful component for confirming enormous quantities of clients on a venture or government organization, yet additionally lets Mimikatz abuse this element by unloading memory and separating the passwords.

III. Algorithm Performance Analysis

Numerous significant things should be dealt with, similar to ease of use, measured quality, security, practicality, and so on

One gullible method of doing this is – execute both the calculations and run the two projects on your PC for various sources of info and see which one takes less time. There are numerous issues with this methodology for investigation of calculations.

1) It may be conceivable that for certain information sources, the main calculation performs in a way that is better than the second. What's more, for certain data sources second performs better.

2) It may likewise be conceivable that for certain data sources, the main calculation performs better on one machine and the second works better on another machine for some different information sources.

Asymptotic Analysis is a major thought that handles the above issues in investigating calculations. In Asymptotic Analysis, we assess the exhibition of a calculation as far as info size (we don't gauge the real running time). We figure, how the time (or space) taken by a calculation increments with the info size.

Consider the below table where tools are compared with each other.

Function	Running time by ASTRA	Running time by Similar tools
Boot Time	3 seconds	45 or > Seconds
UI Load screen	2 Seconds	15 SECONDS
Stager response	1 time stable stager connection	Beaconing, unstable connection

IV. CORE CONCEPTS AND IMPLEMENTATION

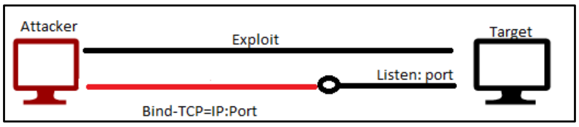
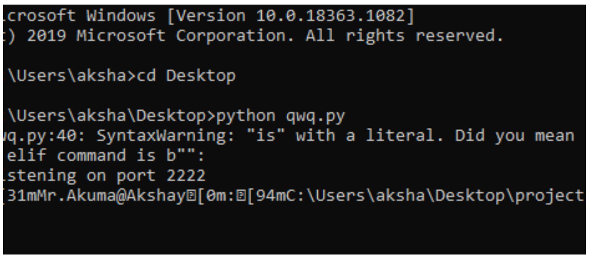


Fig: 1

In a red group activity, a straightforward device that gives outer component separated from making an opposite shell association are more utilize full as they can conceal and finish task under the same rooftop.



```
icrosoft Windows [Version 10.0.18363.1082]
:) 2019 Microsoft Corporation. All rights reserved.

\Users\aksha>cd Desktop

\Users\aksha\Desktop>python qwq.py
vq.py:40: SyntaxWarning: "is" with a literal. Did you mean
 elif command is b"":
istening on port 2222
[31mMr.Akuma@Akshay▯[0m:▯[94mC:\Users\aksha\Desktop\project
```

ASTRA is a prototype tool, which is developed using Python 3, using standard libraries, Cryptography classes and library with power-shell .net framework. ASTRA focuses on bringing a simple, stealthy and
Systematic attack vector in utilization: obtaining Reverse TCP-Bind Shell, defining the base connection for a port, describing the payload, accessing data and executing legacy commands, pivoting, lateral movement, and conducting logging, monitoring and tracking the state of the target. Systematic work-flow, disabling security mechanism, erasing the tracks using obfuscation. The Red Teamer, Pentester can interact with the system and post exploit according to the test plan.

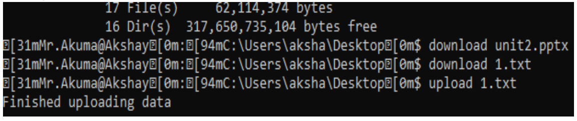
A. Sample Acquisition

In a Red Team operation, gaining control over the system is an important task for which proper Reconnaissance is important where in a Post Exploitation I any activity that can be carried out after a session is initiated and is accessible to perform an action. Here a session is referred to a shell which is opened after successful exploitation of service or brute-forcing into the network, during the assessment a shell can be spawned which can be a Meterpreter or a Standard shell [2].

ASTRA uses a TCP Bind Shell which have 2 modules namely listener and Server, listener module is the one that runs on the target end and the server is the one which is executed from the attacker machine, a TCP bind shell is a type of shell wherein the target machine opens up a communication port or a listener on the target machine and sits tight for an approaching connection. The attacker at that point associates with the target machine's listener which at that point prompts code or order execution on the server [3].

Fig: 2

ASTRA give the in manufactured element to download document and envelope in a simple way wherein the red teamer simply need to type download and the record name, this element gives the red tamer to look at critical records and besides can use to post abuse stage wherein the red teamer can use Process Doppelgänging or make a clone Trojan.



```
              17 File(s)     62,114,374 bytes
              16 Dir(s)  317,650,735,104 bytes free
▯[31mMr.Akuma@Akshay▯[0m:▯[94mC:\Users\aksha\Desktop▯[0m$ download unit2.pptx
▯[31mMr.Akuma@Akshay▯[0m:▯[94mC:\Users\aksha\Desktop▯[0m$ download 1.txt
▯[31mMr.Akuma@Akshay▯[0m:▯[94mC:\Users\aksha\Desktop▯[0m$ upload 1.txt
Finished uploading data
```

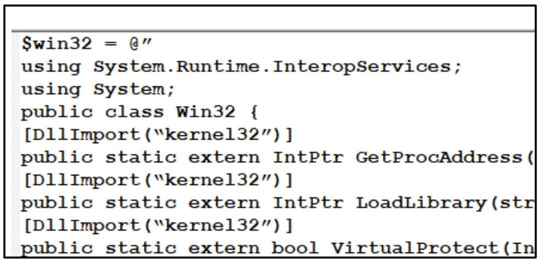
Fig: 3

ASTRA also supports uploading of files which is again an intense operation which can allow us to further exploit the system which can be informed of dumping SAM registry key content to admin password hash.

To run powerful third party scripts like Mimikatz, Mimikatz is an open-source application that permits clients to view and spare validation certifications like Kerberos tickets. Benjamin Delpy keeps on driving Mimikatz advancements, so the toolset works with the current arrival of Windows and incorporates the most exceptional assaults. Mimikatz initially showed how to abuse a solitary weakness in the Windows authentication framework. Presently the instrument exhibits a few various types of weaknesses. Mimikatz can perform accreditation gathering methods like Pass-the-Hash, Pass-the-Ticket, Golden Ticket, Silver Ticket, and Pass-the-Cache.

[1] The Antimalware Scan Interface (AMSI) helps antivirus programs in recognizing "script-based attacks" malicious PowerShell or Microsoft Office macros. Regardless of whether the content utilized were intensely obfuscated, there will come a point where the plain un-jumbled code must be provided to the scripting engine. In this occurrence, AMSI can be called upon to capture. AMSI is an interface on which applications or administrations (outsider included) can examine a content's substance for malignant utilization. On the off chance that a mark in the content is enlisted by the AMSI antimalware specialist co-op (Windows Defender of course), it will be obstructed. One way that appeared to be an instinctive method of avoiding AMSI was to fix out exported functions from AMSI.dll, the library liable for sticking together Defender and PowerShell. There is a strategy exhibited introduced by Tal Lieberman in his Blackhat talk "The Rise and Fall of AMSI". This strategy shows an elective way to deal with AMSI avoidance, and we will cover the basics here to give you a thought of exactly how this method can be applied.

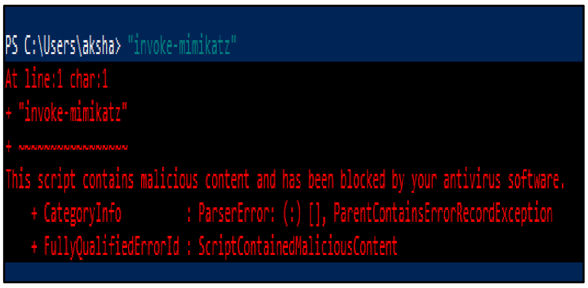
This strategy utilizes .NET's interop usefulness to fix "amsi.dll's" exported work "AmsiScanBuffer", which is conjured from PowerShell as an approach to check if a command is vindictive. By altering the capacity body by infusing gathering code, we can make a little stub which will consistently restore a code demonstrating that command is non-malicious. As the AMSI DLL is stacked into PowerShell's location space during execution, one just one to conjure the Win32 API's to supplant the function's body with the new stub which will return before the command is checked. Which will look like this:



```
$win32 = @"
using System.Runtime.InteropServices;
using System;
public class Win32 {
[DllImport("kernel32")]
public static extern IntPtr GetProcAddress(
[DllImport("kernel32")]
public static extern IntPtr LoadLibrary(str
[DllImport("kernel32")]
public static extern bool VirtualProtect(In
```

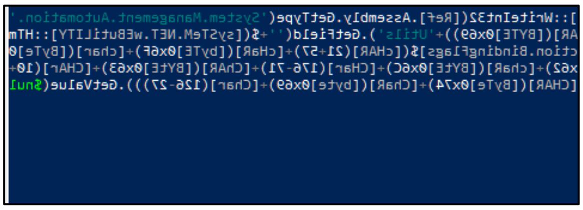
Fig: 4

[1]Utilizing "GetProcAddress", guaranteeing that we can keep in touch with the capacity body utilizing "VirtualProtect" by denoting the page as perused/compose/execute, and afterwards utilizing the "Duplicate" capacity to refresh the capacity with the new 7-byte stub with this one can bypass AMSI interface



```
PS C:\Users\aksha> "invoke-mimikatz"
At line:1 char:1
+ "invoke-mimikatz"
+ ~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
```

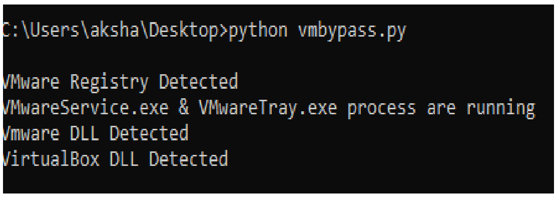
Fig: 5



```
]::WriteInt32([Ref].Assembly.GetType('System.Management.Automation.'
AR]([BYTE]0x69))+'Utils').GetField(''+$([sySTeM.NET.wEButiLITY]::HTm
ction.BindingFlags]$([cHAR](21+57)+[cHaR]([byTE]0x6F)+[char]([ByTe]0
x62)+[chaR]([BYtE]0x6C)+[CHar](176-71)+[ChAR]([BYtE]0x63)+[CHAr](10+
[CHAR]([ByTe]0x74)+[ChaR]([byte]0x69)+[Char](126-27))).GetValue($nul
```

Fig: 6

[8]Another feature of ASTRA is to detect any virtual instance running on the system which allows the red teamer and pentester to focus and look into other targets in the network, ASTRA can detect a running instance of Vmware, Virtual BOX, and Sandboxie. ASTRA uses DLL files, Registry key and process monitoring to detect if any VM instance is running on the target thus allows the pentester to shift the phase of the operation.



```
:\Users\aksha\Desktop>python vmbypass.py

Mware Registry Detected
MwareService.exe & VMwareTray.exe process are running
mware DLL Detected
irtualBox DLL Detected
```

Fig: 7

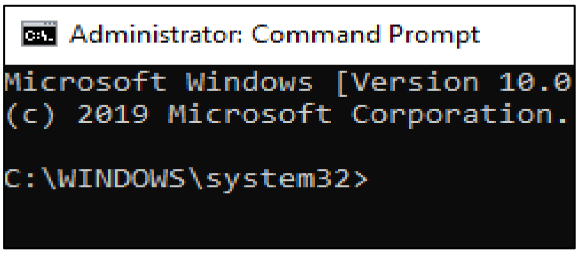
ASTRA is capable of spawning admin shell using task manager, an admin shell can be spawned without using admin prompt permission by scheduling a task with highest privileges and spawning it later, one can also automate this task using windows registry keys as shown below

```
Windows Registry Editor Version
5.00

[HKEY_CLASSES_ROOT\CLSID\{20D04FE0
-3AEA-1069-A2D8-
08002B30309D}\shell\runas]
@="Open Command Prompt
(Administrator)"

[HKEY_CLASSES_ROOT\CLSID\{20D04FE0
-3AEA-1069-A2D8-
08002B30309D}\shell\runas\command]
@="cmd.exe
```

Once the required conditions are met the admin shell task manager spawns the shell which has admin privileges [7].



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0
(c) 2019 Microsoft Corporation.

C:\WINDOWS\system32>
```

Fig: 8

CONCLUSIONS AND FUTURE WORK: In this paper, a structured approach to Red teaming and post-exploitation is discussed, with a tool (ASTRA) prototype implementation described and its applicability in real use cases for red team engagements. ASTRA is a planned red tool focuses on spawning a TCP Bind shell, Uploading scripts and third-party tools, downloading files, Binary, and directory, performing an operation to maintain persistence, disabling security operations (AMSI), Detecting virtual instance like Vmware, spawning an admin shell using task manager and obfuscating files. With all these features ASTRA is an ideal tool to be used in during a red team operation as it can complete multiple tasks without utilising multiple tools or application.

ACKNOWLEDGMENTS

[1] T. Nelson and H. Kettani, "Open Source PowerShell-Written Post Exploitation Frameworks Used by Cyber Espionage Groups," 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 2020, pp. 451-456, doi: 10.1109/ICICT50521.2020.00078.

[2] B. Blumbergs and R. Vaarandi, "Bbuzz: A bit-aware fuzzing framework for network protocol systematic reverse engineering and analysis," MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, 2017, pp. 707-712, doi: 10.1109/MILCOM.2017.8170785.

[3] S. Chaudhary, A. O'Brien and S. Xu, "Automated Post-Breach Penetration Testing through Reinforcement Learning," 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 2020, pp. 1-2, doi: 10.1109/CNS48642.2020.9162301.

[4] J. Decraene, M. Chandramohan, M. Y. H. Low and C. S. Choo, "Evolvable simulations applied to Automated Red Teaming: A preliminary study," Proceedings of the 2010 Winter Simulation Conference, Baltimore, MD, 2010, pp. 1444-1455, doi: 10.1109/WSC.2010.5679047.

[5] INVISIMOLE: THE HIDDEN PART OF THE STORY UNEARTHING INVISIMOLE'S ESPIONAGE TOOLSET AND STRATEGIC COOPERATIONS by Zuzana Hromcová Anton Cherepanov

[6] C. Liu, B. Xia, M. Yu and Y. Liu, "PSDEM: A Feasible De-Obfuscation Method for Malicious PowerShell Detection," 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, 2018, pp. 825-831, doi: 10.1109/ISCC.2018.8538691.

[7] C. Liu, B. Xia, M. Yu and Y. Liu, "PSDEM: A Feasible De-Obfuscation Method for Malicious PowerShell Detection," 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, 2018, pp. 825-831, doi: 10.1109/ISCC.2018.8538691.

[8] T. Li et al., "AClog: Attack Chain Construction Based on Log Correlation," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9013518.

[9] M. Lupascu, D. T. Gavrilut and D. Lucanu, "An Overview of Obfuscation Techniques used by Malware in Visual Basic for Application Scripts," 2018 20th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), Timisoara, Romania, 2018, pp. 280-287, doi: 10.1109/SYNASC.2018.00051.3

New Space and New Threats

RAMESH KUMAR V
PRASANNA PHANINDRAN

NewSpace and New threats

An overview of security threats facing the emerging newspace players and a generic framework to effectively analyse threats

Ramesh Kumar V, Grahaa Space, zSpaze Technologies Pvt. Ltd., Bangalore, India.
ramesh@grahaa.com;   ORCID :: 0000-0003-2665-5294

Prasanna Phanindran S, B.Tech (Information Technology), Easwari Engineering College, Chennai.
prasannaphanindran24@gmail.com

***Abstract*— Given the extent of utilisation of satellites for various earth based and space based applications, military recon missions, interplanetary missions and all other types of space exploration, we can comfortably say that we have officially entered the space age. Tremendous amount of technological developments, miniaturisation of systems and subsystems in the past decade have paved the way for increase in quantity and quality of space based systems thereby increasing the efficacy of space economy across the globe. Modern day satellites can be comfortably considered to be mini computers orbiting the earth with their own operating systems, customised softwares, navigation and processing units, in-built memory and other optical and communication capabilities. With the growing complexity of satellites, there have been multiple recorded instances of attacks that have happened on space based systems since the last three decades. So, it is ever more important that space agencies, commercial organisations and other new space startups take serious note of the new threats facing space based systems. This paper provides a brief overview of orbital and ground level security threats faced by space based and ground based systems, a brief on the methodology to assess the threats for various scenarios and risk mitigation approach.**

Keywords—New space, Space based systems, space security, space based threats, ground station related threats.

I. Introduction

During the second quarter of 2020, when the whole world was still uncovering the threats of the covid pandemic, the United States Air Force (USAF) was busy organising one of the world's largest hackathons[2] to do cyber threat assessments literally "out-of-the-world". It was called "Hack-a-Sat" wherein about two thousand teams consisting of around six thousand hackers took part in a series of virtual challenges of the security vulnerabilities of US military satellites. After filtering out from the larger pool, the top 8 teams were invited for DEF CON and they were challenged to hack into an actual US satellite in orbit[3]. The challenge was primarily intended to test the security framework and infrastructure in place for the US satellites. The one of a kind Hack-a-Sat contest shows us the importance that is being given to space security systems and the intention to make it more robust. This is indeed a very important lesson that every space faring nation needs to learn.

II. A Brief History of Space based systems

Upto the late 90's, satellites and space based systems were built, launched and accessed by the respective space agencies of the countries and a few commercial establishments that had due licenses to do so. Except for public utilities like television and telecommunication data obtained from such satellites and space based systems, every other data from such systems were strictly accessed by the Government and Government approved agencies for various purposes. Since the late 90's, after the internet became prevalent, the data was more and more easily available to the common public through various devices and portals.

Two decades into the twenty-first century, a lot of people across geographies are utilising satellites and space based systems for at least one or two purposes in their day-to-day life. Major applications include telecommunications, navigation (GPS), internet, television broadcast, weather forecasting and predictions. Thanks to the miniaturisation of the consumer electronics industry, reduction in cost of launch, innovation in deployment systems and generous support by public and private investors, a lot of commercial establishments and academic institutions have launched their satellites into space to carry out their commercial payloads and experiments respectively. What used to be a research driven public sector has transformed itself to a profit-driven commercial sector with strong applications and smaller and smarter agile teams managing them. Thus the "New Space" economy came into existence with the rapid commercialisation of the space sector.

The private production and launch capabilities have become so competent during this decade that, apart from space agencies, private companies like SpaceX and Blue Origin are able to build cost efficient and reusable rockets that can launch hundreds of satellites in a single launch. While India is yet to achieve the reusability factor, it has achieved the capability to launch more than hundred satellites in a single launch using its Polar Satellite Launch Vehicle (PSLV).

According to data released by the Union of Concerned Scientists (UCS), as of August 2020, there are about 2787 functional satellites actively orbiting the earth[20]. More than half of the satellites are owned by the United States of America. China owns about 382 satellites followed by Russia with 172 satellites in orbit. India has launched about 110 satellites into orbit since its very first mission in 1975. These functional satellites are serving a variety of applications like communications, earth observation, planetary observation, navigation and space sciences.

III. A Brief History of Space & Ground Based Threats

There are thousands of satellites planned to be launched every year within the next decade. With so many satellites and space based systems in orbit, the threats faced by such assets have been taken very seriously by countries owning the assets. This is not just a precautionary measure, but due to hard learnings of the past.

Back in 1986, the Galaxy I Satellite uplink was disrupted[15] by a suspicious person from Florida under the pseudonym Captain Midnight. This led to the HBO viewers on the US

East Coast seeing an alleged text message about the monthly subscription overlaid on top of the SMPTE color bars.

In 1997, some of the computers belonging to the X-ray Astrophysics section of Goddard Space Flight Center campus were compromised. It was reported later that a large amount of data related to design, testing and satellite command and control codes were stolen and transferred overseas through a sophisticated set of network protocols.

In 1998, ROSAT X-Ray satellite co-owned by the United States and Germany was hacked[17]. Control system computers at the Goddard Space Flight Center in Maryland were targeted for this attack. Once they took control of the computers, they instructed the satellite to direct its solar panels to point to the sun directly, thereby exposing the high resolution imager. In addition, the batteries were fried and the satellite became defunct in space. It continued to orbit the earth as a junk piece of metal till 2011 post which it crashed into earth due to orbital decay. During the same year, a hacking group under the name "Masters of Downloading" broke into the secure Pentagon network and compromised a classified software that could help them control a military satellite system. As per a media report, Pentagon officials had admitted in a classified hearing that a less-secure network has been compromised leading to theft of sensitive information.

Within a year, in 1999, one of the satellites from the military communication system Skynet - which was owned and operated by the UK's Royal Air Force was hacked[22]. The hackers then allegedly sent an email blackmailing the Defense Ministry to provide a ransom.

The Greek defense officials in the year 2000, assessed a malfunction in the GPS navigational systems [36] of British and US tanks that participated in one of the tank trials. The performance of both these tanks were below average despite state of the art GPS navigational equipment capable of utilising signals from multiple GPS satellites for on-ground precision. It was later discovered that a French security agency had allegedly commissioned and remotely activated GPS downlink signal jammers within the firing range.

In 2003, the uplink signals from the Telstar-12 - a commercial communications satellite over the eastern Atlantic, were jammed[37]. The attack was reportedly done to interrupt certain programming in support of propaganda by a specific group.

Libyan nationals in 2006 successfully jammed Thuraya mobile satellite communications over a period of six months to restrict communications to satellite phones used by smugglers[39]. During the same year, Israel intercepted ARABSAT thereby jamming the transmission of Al-Manar television channel during the peak of Israel-Lebanon war.

During a testimony before the House Armed Services Committee Strategic Forces Subcommittee in 2006, a US military official had highlighted the fact that, over 50 instances of jamming attacks had been documented to be interfering with the uplink military communications signals over the commercial SATCOM links. All these instances had taken place during the 16 month period of military operations in Iraq.

In 2007, Intelsat reported that the Liberation Tigers of Tamil Eelam (LTTE), a terrorist organisation fighting for the independence of Sri Lanka's north eastern parts, had been utilising one of the company's satellites in an unauthorised manner [30, 34]. Declared as a case of hijacking signal piracy, LTTE was utilising one of the satellites in Intelsat illegally to broadcast its propaganda channel called National Television of Tamil Eelam (NTT) in Europe and Asia.

According to a report by the US-China Economic and Security Review Commission, in October 2007 and in July 2008, two satellites that were owned by NASA were interfered[17] four or more times using a ground station based out of Norway. Both Landsat-7 and Terra AM-1 were earth observation satellites primarily used for climate and terrain monitoring purposes by the US Geological Survey.

In 2014, US weather monitoring satellite network NOAA was breached[17] by Chinese hackers leading to sealing off data related to aviation, shipping, disaster and emergency management.

A high-profile government video conference using a secure satellite link consisting of senior most officials from key sectors of Indian government was hacked in 2017 for a brief period of 4 to 5 minutes[14]. As per a media report, Indian cybersecurity team is said to have countered the attack immediately thereby neutralising the hack. In the same year, a media report noted that ISRO's Telemetry, Tracking and Command Networks (ISTRAC) were infected by XtremeRAT, a trojan malware. The infected computer is said to be connected to the main servers used for Tracking and Telecommand (TTC) of various launch vehicles. After the incident was reported by a French researcher, ISRO had taken the issue and resolved it later.

All the above mentioned examples indicate that hacking into a satellite or satellite based network seems to be easy. But in reality, it is much more difficult than hacking into normal ground based systems or networks. A hacker or the group involved need to know orbital mechanics, precise revisit times align with the latitude and longitude above which the passage of a particular satellite happens, functioning of control centers, radio frequency protocols and the overall system architecture. That is one of the primary reasons why ground based reception systems are more vulnerable to attacks and threats than the satellites and space based systems in orbit.

Given the past experiences, space faring nations have come out with a classification of the most common types of threats.

A. Threats for Space Segment

As mentioned earlier, the space segment is really a tough one to crack. It requires a lot of resources, knowledge of a variety of satellite systems and protocols and the necessary equipment to manipulate or mimic the system. Even if the adversary has required knowledge, it takes a variable combination of protocols in specific sequence in order to transmit command and code and take control of the satellite in orbit.

Space debris is a potential threat in the space segment. It can happen naturally with dead satellites in decaying orbits or can be created intentionally to attack a specific satellite. Apart from the 2787 functional satellites, there are literally double the amount of dead or lost satellites in various orbits. NASA and ESA keeps track of a wide variety of space objects of varying sizes and shapes. It is estimated that there are around 29000 of such debris that are larger than 10cm, 670,000 pieces of size larger than 1 cm and more than 170 million pieces of space debris larger than 1 mm are orbiting the earth at present. Collision of any of these debris with functional satellites can alter the natural working of such satellites, may destroy solar panels or systems and subsystems or even render them useless.

A relatively new type of threat is the Kinetic physical wherein, weapons launched from space or from the ground can physically attack the satellite in orbit. ASAT or Anti-satellite weapon [9, 11] is the common type of threat which is now being possessed by major space faring nations. An ASAT weapon is usually launched to attack the satellite directly or can carry a warhead that can be detonated near the satellite. This is usually done through precise calculation of the trajectory of the target satellite. The ASAT weapon can be launched during a calculated time frame from a ground based launch station or it can be launched into a parking orbit first to be launched in the future as per needs. The latter is termed as co-orbital ASAT. Usually co-orbital ASATs are launched into orbit and would stay dormant for a long period before it is actively utilised for attack.

Non-Kinetic physical threat is one that utilises high powered microwaves (HPM) or electromagnetic pulses (EMP) or high powered lasers [9, 11]. They are predominantly commissioned on the ground and are targeted towards the satellite based on the passage. HPMs can disrupt the satellite systems and subsystems, corrupt the electronic components, electrical circuits and processing units. HPM can be targeted towards the satellite antennas or through the gaps in the structure or shielding. To avoid atmospheric interferences, usage of HPM works best when it is beamed from an air-borne system or another satellite. High power lasers work in a very similar manner and can blind the satellite optical systems. But it requires a huge amount of power, advanced steering control to point the beam precisely and advanced optics for focussing it right. High power laser will not work unless it is in line of sight with the satellite.

All the above mentioned methods require a lot of resources. This complexity is one of the primary reasons why adversaries usually take control of the command and control center or the telemetry and telecommand center in order to hijack and take control of satellite or space based systems.

B. Threats for Ground based Segment

It is much easier to compromise a ground station when compared to space based systems. The adversary needs to gain access to the command and control servers in order to utilise the existing hardware, software and terrestrial systems. A wide variety of attacks are possible as mentioned below.

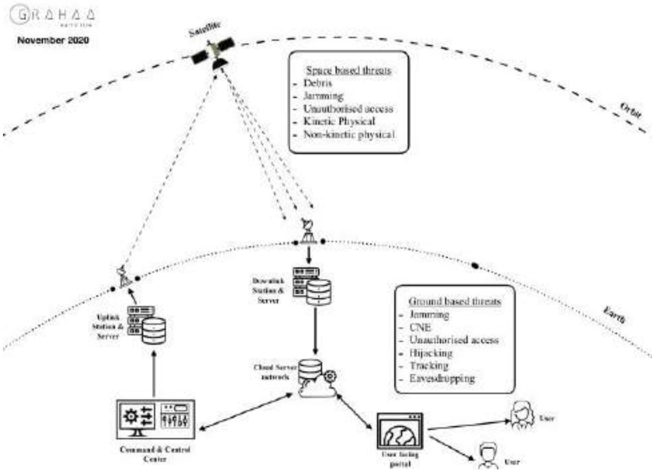


Figure :: Threats for space and ground segments

Jamming is a common practice of interfering with a legitimate transmission by overpowering a transmitter or a receiver. The transmitted signals are overpowered with the help of interference which results in the degradation of satellite services. Usually satellite jamming is used to tamper media for censorship purposes. There are two forms of satellite jamming - orbital and terrestrial. In the orbital Jamming, the adversary sends out a signal from an illegitimate uplink station by interfering with the correct ones. The signal sent by the adversary overpowers the transmission thereby blocking the recipient. In terrestrial jamming, the attacker transmits illegitimate frequencies to the ground satellite dishes. These frequencies are limited to a specific area and are capable of interfering with specific locations only.

Computer network exploitation is another common way of compromising an existing network. A poorly configured part of the network system or a stand alone unit can be exploited to gain access to the network. This can happen various ways like sending a phishing link, social engineering, sharing malicious security patches and upgrades and sometimes even tapping into the network cables to manipulate data traffic. Outdated softwares or open source softwares can also serve as a loophole in the system. Installation of cookies and malware in vulnerable systems can help adversaries record and track continuous activities of the ground segment. If the ground segment is connected with a third party centralised cloud infrastructure, then the adversaries can gain access anywhere in the cloud pipeline. It is easier and a regular task for hackers to gain access to any of the data processing systems, storage or any of the managed systems along the pipeline.

Tracking is basically the collection of user information from a website connected directly or indirectly to a ground station. Websites can collect information like location data, IP Address and other user information.. These are done with the help of cookies. Cookies are tiny bits of code stored in a computer when the user visits any website. There are two basic types of cookies - session cookies and persistent cookies. Session cookies help retain user login credentials, browsing and other activity information. These cookies will be deleted automatically once the user session ends. Secondly, the persistent cookies are ones that stay in the user's computer and track almost all the activities of the user.

These persistent cookies help in storing users data for long term and share it with the adversary. Another method of tracking is browser fingerprinting wherein, the adversary with the help of a code snippet can collect information on a wide variety of hardware, software, operating systems and security measures implemented in the specific system.

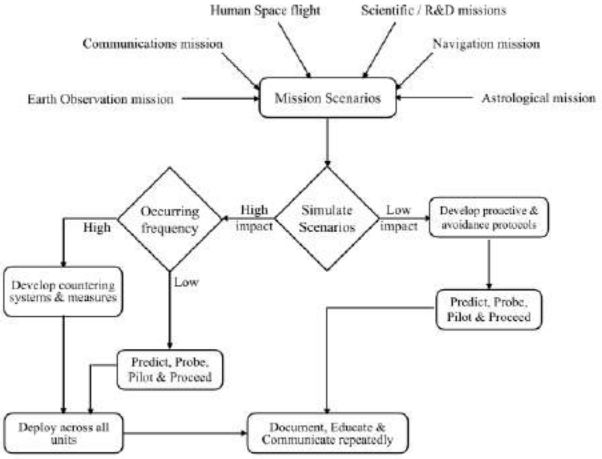
Eavesdropping is simply listening to communication without any authorization. Eavesdropping can be classified into two types - passive and active. Passive eavesdropping is where the adversary only listens to a specific communication. In active eavesdropping, the adversary modifies the communication in between. With the help of active eavesdropping, hackers can access the transmitted data from the satellites. Despite being encrypted these satellite communications can be intercepted with the help of sophisticated hardware.

Hijacking is seizing control of satellite transmission without any authorization. Hijacking also comes under active eavesdropping. This can be done by seizing control of a transmission or reception signals and replacing it with another one. Whenever a satellite is being hijacked, there is a high possibility that the adversary may take control of all the vital components of the satellite architecture.

Once the adversary has trespassed into the system, sensitive data and controls can be corrupted or altered or deleted. This can result in a wide variety of issues including transmission and reception failures, corruption of signals and data, failure of hardware, malfunctioning softwares or failure of a system in part or as a whole.

IV. THREAT ANALYSIS

Regardless of the type of the mission, it is essential to carry out threat analysis during the planning phase. Given in the figure below is a generic threat analysis framework that the emerging space economies can effectively utilise for their missions.



Human Space flight
Scientific / R&D missions
Communications mission
Navigation mission
Earth Observation mission
Mission Scenarios
Astrological mission
Occurring frequency
High impact
Simulate Scenarios
Low impact
Develop proactive & avoidance protocols
High
Develop countering systems & measures
Low
Predict, Probe, Pilot & Proceed
Predict, Probe, Pilot & Proceed
Deploy across all units
Document, Educate & Communicate repeatedly

Proposed generic threat analysis framework

This framework is mission agnostic and necessary steps can be included or modified based on specific missions.

As a first step, depending on the mission, a wide variety of scenarios are to be listed based on the nature, time frame and the budget allocated to the mission. Mission scenarios should consider variables like assets and its valuation, systems, subsystems, payloads and all the stakeholders involved. The intangible assets include pride of a specific country, international relations and various treaties that the country abides by. Based on these variables, the present and future implications of the mission has to be analysed. Wherever possible, a suitable monetary value can be included as a weighing factor.

Once this initial analysis is done, a well detailed use case scenario is to be thought through to simulate the circumstances and events. Including use case scenarios for a wide variety of threats can help in determining the impact factor for each of the assets involved. This leads to the classification of potential threats into high impact or low impact categories. If the threat has a high impact, then it has to be taken up seriously and the frequency of occurrence is calculated.

In case if the frequency of occurrence is really high, then it is very essential to have counter space systems and measures in place. The counter space systems have to be very effective and should be robust enough to mitigate the majority of the future recurrences. Suitable prototypes have to be developed, tested and qualified to tackle the future occurrences of the test scenarios. If the frequency of occurrence of a specific scenario is low, then all possible instances should be predicted through simulations and probed for intricate details. Based on the details, suitable prototypes are to be piloted and tested. Once a specific prototype turns out to be effective, then it can be deployed across all units.

If the threat has a low impact, then suitable protocols can be developed as a proactive measure. All future recurrences of the scenarios are to be accurately predicted and probed to obtain fine details. Based on the details evaluated, prototypes can be developed, piloted and tested.

The list of all high impact and low impact simulated scenarios are to be clearly documented throughout. Once the predictions are done and suitable prototypes are evaluated and qualified, all stakeholders involved in the mission should be educated.

All of these should happen during the planning and designing phase - to provide adequate time frame for testing the scenarios and evaluating the prototypes. Once the mission is on, these scenarios are to be verified against the actual mission data. This helps identify anomalies in the overall system and its functionality and take proactive measures and tackle expected threats.

This threat analysis methodology has a room for residual risk in terms of any abnormal astrological events. Such residual risk should also be documented and educated to all stakeholders. In addition to doing the threat analysis during the early stages of the mission, it is very essential that the potential risks are to be evaluated periodically through the mission life time. It is also imperative that all the stakeholders involved are to be clearly communicated about the normal routine of the mission as well as during the occurrence of threats throughout the course of the mission.

CONCLUDING REMARKS

Most of the developed space faring nations have counter space capabilities at present to tackle a wide variety of threats. On the other hand, countries like India, Iran, Australia, NewZealand and UAE, which are still new or emerging players in the newspace industry are still developing their systems to be robust enough to tackle space based and ground based threats. The threat analysis framework provided in this paper can be used as a stepping stone for deriving detailed processes and procedures. A unified cybersecurity standard for newspace vertical is imperative and the countries should have their own governing bodies to monitor, review and manage space based and ground based threats in future.

.

REFERENCES

[1] Nayef Al-Rodhan," Cyber security and space security" *The Space Review*, May 26,2020. [ONLINE]. Available: https://www.thespacereview.com/article/3950/1

[2] Brian Barrett, "The Air Force Will Let Hackers Try to Hijack an Orbiting Satellite" *Wired*, September 17,2019. [ONLINE]. Available: https://www.wired.com/story/air-force-defcon-satellite-hacking/

[3] Patrick Tucker, "The NSA Is Studying Satellite Hacking" *Defense one*, September 20, 2019. [ONLINE]. Available: https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/

[4] Max Eddy, "Want to Hack a Satellite? It Might Be Easier Than You Think" *PCMag*, March 7,2019. [ONLINE]. Available: https://uk.pcmag.com/news/119996/want-to-hack-a-satellite-it-might-be-easier-than-you-think

[5] Max Eddy, "Satellite Communications Hacks Are Real, And They're Terrifying" *PCMag*, August 9,2018. [ONLINE]. Available: https://uk.pcmag.com/blackhat/116815/satellite-communications-hacks-are-real-and-theyre-terrifying

[6] Max Eddy, "Hacking Airliners, Ships, and More Through Satellite Communications" *PCMag*, August 8,2014. [ONLINE]. Available: https://uk.pcmag.com/opinion/34795/hacking-airliners-ships-and-more-through-satellite-communications

[7] Mary Pat Flaherty , Jason Samenow and Lisa Rein, "Chinese hack U.S. weather systems, satellite network" *The Washington post*, November 12, 2014. [ONLINE]. Available: https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html

[8] NAYEF R.F. AL-RODHAN, *Meta-Geopolitics Of Outer Space: An Analysis Of Space Power, Security And Governance.* LONDON, CA: Palgrave Macmillan, 2012.

[9] Rajeswari Pillai Rajagopalan, *Electronic and Cyber Warfare in Outer Space*, MA: UNIDIR,2019. [EBOOK]. Available: https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf

[10] VAGO MURADIAN, "China Tried To Blind U.S. Sats With Laser" *AR15*, September 22,2006. [ONLINE]. Available: https://www.ar15.com/forums/general/Chi-na_Tried_To_Blind_U_S__Sats_With_Laser/5-501978/

[11] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar and A. Davis, "Cyber security in New Space" *Springer Link*, May 12,2020. [ONLINE]. Available: https://link.springer.com/article/10.1007/s10207-020-00503-w#ref-CR9

[12] Lorenzo Franceschi-Bicchierai, "This $1,000 Device Lets Hackers Hijack Satellite Communications" *Vice*, July 31,2015. [ONLINE]. Available: https://www.vice.com/en/article/xywjpa/this-1000-device-lets-hackers-hijack-satellite-communications

[13] MK Mithun, "ISRO computer had malware, could've been hacked, say researchers" *The New Indian Express*, March 12, 2018. [ONLINE]. Available: https://www.newindianexpress.com/cities/hyderabad/2018/mar/12/isro-computer-had-malware-couldve-been-hacked-say-researchers-1785758.html

[14] SANDHYA RAMESH, "China hacked Indian govt teleconference in 2017 — US think-tank reiterates old report" *The Print*, September 23,2020. [ONLINE]. Available: https://theprint.in/india/china-hacked-indian-govt-teleconference-in-2017-us-think-tank-reiterates-old-report/508801/

[15] Younis Dar, "Why Satellite Hacking Has Become The 'Biggest Global Threat' For Countries Like US, China, Russia & India?" *The EurAsian Times*, October 24,2020. [ONLINE]. Available: https://eurasiantimes.com/why-satellite-hacking-has-become-the-biggest-global-threat-for-countries-like-us-china-russia-india/

[16] Curtis Franklin Jr.," The Race to Hack a Satellite at DEF CON" *DARK Reading*, August 13,2020. [ONLINE]. Available: https://www.darkreading.com/application-security/the-race-to-hack-a-satellite-at-def-con/d/d-id/1338657

[17] William Akoto, "*Hackers could shut down satellites – or turn them into weapons*" *The Conversation*, February 13, 2020. [ONLINE]. Available: https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932

[18] "China-based hacking campaign is said to have breached satellite, defense companies" *CNBC*, June 19,2018. [ONLINE].Available: https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html

[19] Anusuya Datta, "How many satellites orbit Earth and why space traffic management is crucial" *GeoSpatial World*, August 23,2020. [ONLINE]. Available: https://www.geospatialworld.net/blogs/how-many-satellites-orbit-earth-and-why-space-traffic-management-is-crucial/#:~:text=According%20to%20the%20Union%20of,have%20had%20many%20more%20launches

[20] Union of Concerned Scientists, "UCS Satellite Database- In-depth details on the 2,787 satellites currently orbiting Earth, including their country of origin, purpose, and other operational details." *Union of Concerned Scientists*, December 8, 2005. Available: https://ucsusa.org/resources/satellite-database?_ga=2.206523283.1848871521.1598077135-464362950.1598077135

[21] Therese Wood, "Visualizing All of Earth's Satellites: Who Owns Our Orbit?" *Visual Capitalist*, October 20,2020. [ONLINE]. Available: https://www.visualcapitalist.com/visualizing-all-of-earths-satellites/

[22] "Satellite hack raises security questions" *Cnet*, January 2,2002. [ONLINE]. Available: https://www.cnet.com/news/satellite-hack-raises-security-questions/

[23] " ISRO CONFIRMS IT WAS ALERTED ABOUT DTRACK MALWARE DURING CHANDRAYAAN 2, SAYS IT HAD NO IMPACT" *TECH2*, November 10,2019. [ONINE]. Available: https://www.firstpost.com/tech/science/isro-confirms-it-was-alerted-about-dtrack-malware-during-chandrayaan-2-says-it-had-no-impact-7626131.html

[24] Amit Raja Naik, "ISRO, SEBI, Other Govt Email Accounts Breached In Hack", *Inc42*, January 26,2020. [ONLINE]. Available:

https://inc42.com/buzz/isro-sebi-other-govt-email-accounts-breached-in-hack/

[25] MATT LIEBOWITZ, “Hackers Interfered With 2 US Government Satellites”, *Space.com*, October 27,2011. [ONLINE]. Available: https://www.space.com/13423-hackers-government-satellites.html#:~:text=In%20October%202007%20and%20July,by%20the%20U.S.%2DChina%20Economic

[26] Jim Wolf, “China key suspect in U.S. satellite hacks: commission” *REUTERS*, October 28,2011. [ONLINE]. Available: https://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028

[27] Noah Shachtman, “Ukraine Big: We Can Spot Your Sats, Control Space” *Wired*, June 12,2007. [ONLINE]. Available: https://www.wired.com/2007/12/even-the-worlds/

[28] Noah Shachtman, “How China Loses the Coming Space War (Pt. 1)” *Wired*, October 1, 2008. [ONLINE]. Available: https://www.wired.com/2008/01/inside-the-chin/

[29] Nayef Al-Rodhan,” Quantum Computing and the New Space Race” *The National Interest*, June 20, 2018. [ONLINE]. Available: https://nationalinterest.org/feature/quantum-computing-the-new-space-race-26349?page=0%2C1

[30] James Middleton, “Tamil Tigers hack satellite”, *telecoms.com*, April 13,2007. [ONLINE]. Available: https://telecoms.com/6151/tamil-tigers-hack-satellite/

[31] ” Intelsat terminates use of its satellite by Tamil tigers” *Zee News*, April 25,2007. [ONLINE]. Available: https://zeenews.india.com/news/world/intelsat-terminates-use-of-its-satellite-by-tamil-tigers_367783.html

[32] “Sri Lanka's Tamil rebels using satellite illegally: Intelsat” *Spacedaily*, April 12,2007. [ONLINE]. Available: https://www.spacedaily.com/2006/070412031627.jt2jhcys.html

[33] “Intelsat removes Tiger TV” *BBC Sinhala.com*, April,2007. [ONLINE]. Available: https://www.bbc.com/sinhala/news/story/2007/04/printable/070425_intelsat

[34]” Intelsat stops Tamil Tiger satellite broadcasts” *REUTERS*, April 25,2007. [ONLINE]. Available: https://in.reuters.com/article/idUSN24434540

[35] “Pentagon 'at war' with computer hackers” *CNN.com*, March 5, 1999. [ONLINE]. Available: http://edition.cnn.com/TECH/computing/9903/05/pentagon.hackers/index.html

[36] Grau, Lester W., “GPS Signals Jammed during Tank Trials” *questia*, 2000. [ONLINE]. Available: https://www.questia.com/library/journal/1P3-70549841/gps-signals-jammed-during-tank-trials

[37] Robert Windrem, “U.S. satellite feeds to Iran jammed”, *NBC News*, October 24,2003. [ONLINE]. Available: https://www.nbcnews.com/id/wbna3340692

[38] MONTE MORIN AND JOEL RUBIN, “Cuba Jams Broadcasts to Iran, U.S. Says” *LOS ANGELS TIMES*, JULY 17, 2003. [ONLINE]. Available: https://www.latimes.com/archives/la-xpm-2003-jul-17-me-irantv17-story.html

[39] Peter B. de Selding, “Thuraya Accuses Libya of Jamming Satellite Signals” *SPACE NEWS*, February 25, 2011. [ONLINE]. Available: https://spacenews.com/thuraya-accuses-libya-jamming-satellite-signals/#:~:text=Thuraya%20suffered%20repeated%20jamming%20in,initiative%20successfully%20ended%20the%20jamming

Cross-Channel Scripting Attacks (XCS) in Web Applications

SHASHIDHAR R

Cross-Channel Scripting Attacks (XCS) in Web Applications

Shashidhara R
Department of Computer Science and Engineering, Bennett University,
Greater Noida, UP-India
eemailshashi@gmail.com

Abstract- XCS is one of the most common web application vulnerability, which is also known as Cross Channel Scripting. It's a variant of Cross-site Scripting (XSS), in this attack inoculation of a malicious vector is achieved via networking protocols and embedded devices have web interfaces like cameras, photo frames, routers etc. These devices permit the Web administrator to perform various activities from the browser to the server. XCS attacks are performed by injecting the malicious content in the embedded devices having the Web interface and this malicious code is exploited at the client browser. Further, the malicious content can be injected in the device through network protocols like File Transfer Protocol and Network File System. In this article, the analysis of scripting defending approaches at client-side and server-side has been discussed. In the literature, XCS vulnerability detection and mitigation are major extent covered by most of the studies. We have also conferred various state-of-art XCS techniques with their strengths, weakness and identified the research gaps.

Index Terms—XCS attack, Cross-site Scripting, JavaScript code injection, Network protocols, Sanitization.

1 INTRODUCTION

Presently, Web applications are convinced to be one of the excellence platform for presenting data over the Internet. The Web applications render approach to different online services like e-mail, social networking sites, e-commerce, net banking, etc, which make use of different Web technologies and components [1]. Although, variabilities between technologies and modules initiate a challenge to accomplish firm approaches for development of the applications on Web [2], [3].

The effortlessness of hold and wide availability of web attack toolkits are feeding the number of attacks in web applications, which doubled in 2018. Table 1 lists, classification of most frequently exploited websites in the recent years. According to Symantec's Internet Security Threat Report 2018, business and technology related sites were the frequently exploited websites. Technology sites were compromised almost twice as much as business related sites. Because, An adversary may pretend to be an employee by faking an identification card. The adversary obtains authorization to confined zones, thus providing furthermore chances for attacks. Therefore, the hackers are trying to target technology sites with maximum traffic are simply where malware distributors are focusing their attention at the moment. In XCS, a malevolent user makes use of simple network mail transfer protocol as an attack string. In a networked environment, there various embedded devices that allows user to store data through SMB protocol. Thus, the attacker can insert the malicious data, which contains malicious scripts [4].

1.1 Cross Channel Scripting

Cross Channel Scripting attacks are known as XCS attacks. It uses networking protocols and Web interfaces to inject attack vectors into the Web content, which is running in an independent security context. The attacker uses this scripting to send a malicious vector to the legitimate user. An overview of XCS attack is illustrated in Fig. 1. This attack consists of the following steps.

S1 An attacker makes use of SNMP or FTP, which are treated as non-web channels or other web-based networking protocol services to inject malevolent code on the web server.

S2 The malevolent code stored in the server is transferred to the victim's browser through web applications. Once the victim gains access to the malevolent web content by the browser, then malicious code execution is accomplished with his permissions [5].

XCS can be used to carry out numerous attacks. They are listed as follows:

1) Filtrating confidential data: This is also known as data extrusion. This is a security breach, where company's information is copied, transferred, or received from the system without proper validation.

2) Victim’s Redirecting: An attacker tricks the user to access his/her sensitive data by injecting the false login forms into the Website.

3) IP spoofing: If an attacker and the user share the same LAN, an attacker could target victim with Address Resolution Protocol (ARP) spoofing and launch a Man in the Middle (MITM) attack for all Internet communications.

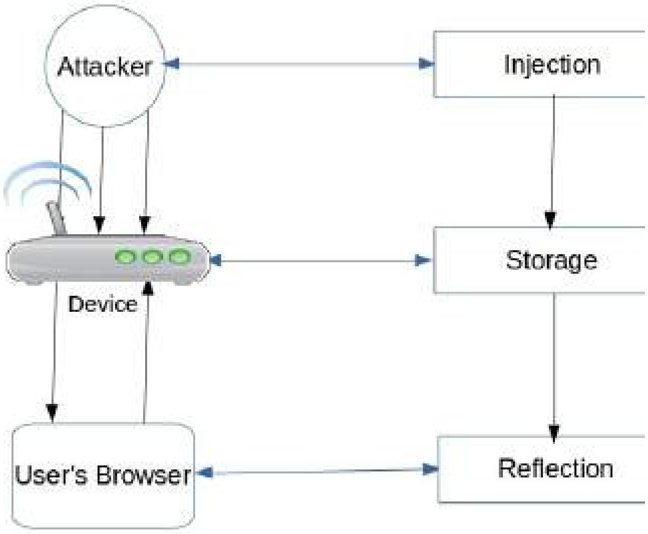


Fig. 1: XCS attack overview.

A homologous class of XCS attack in which the Web application attack vector is pre-owned to strike the web channel known as reverse XCS vulnerability [4]. Detection of reverse XCS vulnerability is tedious, in view of the fact that, XCS vulnerabilities mishandle the sessions with communication channel and the Web interface. XCS exploitation is a stepping stone in the direction of the massive attack vector on local area network that targets to break the network [6]. For example, the reverse cross channel scripting is used for rebooting the network switch thereafter shutting down an entire local area network.

1.2 Organization of the Paper

The rest of the paper is organized as follows: Section 2, presents motives of an attacker. Section 3, list the vulnerability classes. Section 4, describes XCS vulnerabilities found in embedded devices. Section 5, demonstrate Reverse Cross Channel Scripting (RXCS). Section 6, list the tools used to find XCS attacks. The XCS detection and mitigation techniques are presented in Section 7 and 8. Section 9, presents the concept of contextual fingerprints. Section 10, describes the Site Firewall. Section 11, presents result analysis. Section 12, describe other related works. Section 13 concludes the paper.

2 MOTIVES OF THE ATTACKER

This section describes motivations beyond XCS attacks:

- An adversary can obtain the leaked private information from compromised device such as wirless router in the network.
- The attacker can reveal sensitive information from the compromised printer that is configured with network. It share copies of all content it prints with the adversary [1].
- The attacker uses the embedded devices having the Web interfaces as resources to target remote-sites, instead of attacking the internal structure of the network.

3 VULNERABILITY CLASSES

In this section, we discuss the vulnerability classes in the web based management interfaces. During the evaluation of embedded devices, we find the following vulnerable classes in web applications.

1) XCS: These attacks are common in embedded devices since they reveal numerous services beyond HTTP. Cross-Channel Scripting bugs are very difficult to discover than CSRF (Cross-Site Request Forgeries) and XSS. Because they include several communication channels [7].

2) RXCS (Reverse Cross-Channel Scripting): The web interface/program is used as a benchmark to attack a further service on the network device is known as reverse cross-channel scripting. RXCS attacks are mainly used for unauthorized copying, transfer or retrieval of data that is protected by an access control.

3) CSRF (Cross-Site Request Forgeries): These vulnerabilities enable an adversary to reveal a information in the device by using a remote site as a stepping stone [8].

4) Cross-Site Scripting: These vulnerabilities are commonly found in web based applications, Most of the interfaces and devices are vulnerable to XSS, including those that perform some input checking [9].

5) File security: Devices like Samsung photo frame allows an adversary to interpret protected information without any authentication [7]. On this device, the web interface will be compromised by abusing the log file, even it’s protected by the password.

6) Authentication: Most of the devices authenticate users in clear text and without HTTPS [7]. This makes the security devices like cameras to be compromised.

3.1 Motivation and Contributions

Cross channel scripting attacks occur almost daily. Recently, the famous social networks like Twitter, Facebook,
Google etc, have become part of XCS vulnerabilities. In addition, XCS attack vectors found in the Yahoo, PayPal, Justin.tv, Orkut, Hotmail, universal search engine of UK parliament website and many more [2]. The contribution of this article includes:

- Exploiting and testing various XCS attacks by injecting real malicious attack vectors on the insecure web applications.
- This article presents a detail survey on discovery, identifying and mitigating of XCS attacks in web based and cloud based applications.

3.2 Research Gaps

The existing XCS defensive approaches have the following limitations:

1) Most of the existing XCS defensive approaches are unable to provide safe input handling and encoding mechanisms at client as well as server side of web based application [1].
2)) An automated process is essential to differentiate between JavaScript from the malicious script [10].
3) There is no proper defensive solution that capable to detect and prevent all XCS attacks like reflected, stored and encoding attacks.
4) A Secure XSS defensive algorithm needed to possess the list of malicious scripts and domains to decrease the rate of false positive and negatives.
5) In existing approaches effective policy checks are not implemented to increase XCS detection speed and mitigation process [11].

3.3 Attacks on Peer-to-Peer Channel [4]

Network-attached storage (NAS) server allows the Web client's to download Bit Torrent information via the embedded device. This device is configured by the Web based interface. A Bit Torrent file contains a file information with hash to track URLs. This helps attacker to find peer entities. The authors in [4] found many cross channel scripting attack vectors in Bit Torrent clients but an interesting fact is that an XCS attack vector results from a peer to peer (P2P) channel. Here, an attacker crafts the torrent data that behave as the malevolent content. When the Web client tries to obtain torrent information from the browser, the Web based interface notifies record indices and allows client browser to exploit malevolent payload present in the file. In more detail, the attack is illustrated in Fig. 2.

In peer-to-peer attack context, the web clients are not aware of the fact that the Bit Torrent has a malevolent content before the Bit Torrent is fetched. The P2P attack starts as soon as Bit Torrent is fetched.

3.4 Log-based XCS [5]

When the system software corrupted, admin of the system require local ingress to the console to reboot an operating system. These circumstances arise in the data centres, where the admin is able to diagnose it. The need of real involvement is problematic, in case of Service Level Agreement (SLA) since it increases the downtime drastically. To direct this problem, most of the vendors have designed firmware components known as LOM (Lights Out Management) modules, that can be externally acquired by an admin. Most of the Lights Out Management systems allow a web interface for the admin to remote accessing.

The Bojinov et al. [5] inspected the web interfaces on three commonly used Lights-out management modules like:

1) AMT (Active Management Technology) by the Intel
2) DRAC (Dell Remote Access Controller) by the Dell
3) Remote Supervisor Adapter (RSA) by the IBM

The researchers found some Cross-Channel Scripting vulnerabilities on these Lights-Out Management modules.

After that, the vendors of this module are taken several secure measures to prevent unauthorized login to the light-out management modules. These security measures involve several forms of user authentication, use of Secure Socket Layer to defence a range of network attacks, a substantial logging of user's activity. The researchers also examined that, this vulnerability implies to RSA and DRAC by accessing the interface of a web on the affected machine. This XCS attack makes use of log file to insert malicious script to the storage devices. This XCS vulnerability has been described by the following steps:

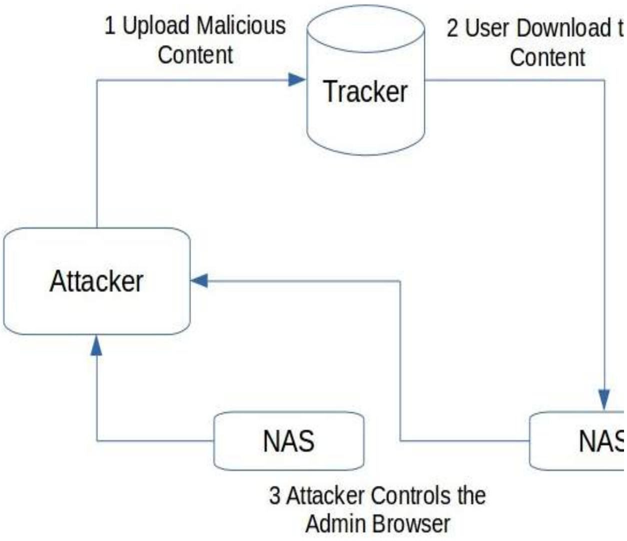

1 Upload Malicious Content
Tracker
2 User Download t Content
Attacker
NAS
NAS
3 Attacker Controls the Admin Browser

Fig. 2: Overview of P2P XCS attack.

S1: An adversary aims to login LOM device with a supervised system. Alternative of attempting to guess login credentials, an adversary enters a payload, which contains malicious code as the username.

S2: The logging system will capture and save these user credentials in log file of the LOM device. The login form present in the system does not escape the malicious information communicate to the log file to mitigate web based attacks.

S3: A malevolent code is accomplished by an admin browser of a LOM system when he/she views or interprets the log file. The malevolent code could be explored to append the rogue into the LOM. Accordingly, grant access to an adversary.

3.5 XCS Attack on Smartphone [2]

Mobile devices enable to download different application services through third-party vendors like commercial websites and Google play store. The source applications which are downloaded from third-party is problematic. Therefore, the mobile devices continousely in risk during installing malevolent applications, which gain authorization of the devices or steal sensitive data like browser cookies, passwords and credit/debit card numbers. Location based attacks, Bluetooth attacks, SMS based attacks, Spyware and Grayware are possible attacks in the mobile devices.

The mobile operating systems like Android and WebOS uses the Javascript code to develop the application services. This script code is more prone to cross-site scripting vulnerabilities. Recently, the authors in [12] verified few Smartphones that are developed using Javascript and demonstrated that cross site scripting attacks are still possible in the Smartphones. Further, a recent report describes about Palm Pre, which leads to cross channel scripting vector that inserts it’s malicious code via content [2].

3.6 XCS Attacks in Online Social Network (OSN)

Online Social Networks (OSN) are continuously suffering from the impact of XCS attacks [12]. Recently, the famous social networks like Twitter, Facebook and Google have become victim for the cross channel scripting attacks. Furthermore, cross-channel scripting attack vectors seized in UK parliament site, Yahoo website, PayPal, Hotmail, Justin.tv, Orkut website and many more [13].

4. RXCS:REVERSE CROSS CHANNEL SCRIPTING

Here, we outline RXCS attack, which uses the web interface to launch a series of problems on a Web channel. The main goal of this attack is the unauthorized transfer of users confidential information that should not be shared, since it’s guarded with access control technique [4]. Indeed, a popular web sites like Facebook, Google, Twitter and E-bay provides a Web based API of third-party applications, this leads to cross channel scripting attack opportunities. The application developer assumes that the cloud service provides safe and secure data by the third party applications. However, every cloud provider has its own sanitization mechanism, which is generally not explicitly documented. The unpredictability between supplied information and expected information can result in Reverse XCS [4].

4.1 RXCS Attack in Facebook [4]

In Facebook, the information furnished to third-party applications is not sanitized that is Facebook sanitize the information at display time. The terms of service and conditions of Facebook’s says that third party vendors applications are not meant to output the information fetched from the application programming interface directly. Correspondingly, Web applications not meant to keep user information. Although, some applications will store or display the information, even Facebook can monitors interface usage details to intercept terms of service violation.

Suppose we have the application to display the statistics of Facebook users like favourite pages, games, videos or movies, then it is enough to inject a malicious code in the favourite pages and eventually spammed to all users of the Facebook that views an application. In detail, a crafted attack vector would be injected in a viral page of the Facebook. The Facebook users who are clicking this malicious link would reflects the same code and then the user browser under attack. This compromised web page can be used to phishing attacks and malware spreading.

4.2 RXCS Attack in Twitter [7]

In Twitter, data sanitation will be completed at the input so all information given to third party vendor applications sanitized by HTML escaping mechanism. The filtering policy used in twitter is opposite compared to Facebook sanitation policy. The authors Bojinov et al.[4] describe that, if an application needs to manage with raw content, then it should be sanitized information. Suppose, an application wanted to outputs information, it should be re-escape an information. This re-escape, the un-escape process is error-prone and tedious, which leads to RXCS attacks.

The XCS attack vector mousing over the malicious link would results the pop up, which display the logged in user's cookies. The adversary later incorporated a reverse cross channel scripting component that forced Twitter users to retweet a piece of code.

4.3 Cookie Stealer Mechanism

The following steps describes how XCS attacks are performed by the adversary to steal victim's browser cookies.

1) The attacker crafts an URL of the Web with malicious content and then sends to the victim's Web Browser.
2) Victim's browser is misleads by the attacker and requesting Web server URL.
3) Further, Web server incorporate malicious attack vectors from URL in response message.
4) The clients execute malicious content inside HTTP response resulting, redirecting victim's cookies to an attacker's web server.

5. TOOLS USED

This section list the tools used in embedded devices to detect XCS vulnerabilities. The audit of each embedded device is done in 3 phases by researchers of stanford [4].

First, they performed a general analysis using the open source tool known as NMap (Network Mapper), it's a free utility for auditing and network discovery [14]. Further, Nessus scanner provides a Nessus Attack Scripting Language (NASL). This is a simple language to demonstrate individual threats and potential attacks [15]. Next,

they checked the capabilities of the web based management interfaces using Mozilla Firefox and its extensions

like Edit Cookies, Firebug and Tamper Data. Further, the researchers [14] come up with a custom tool for Cross-Site Request Forgeries inspection. In the final step the Stanford researchers Bojinov et al. tested for Cross Channel Scripting attacks using command line tools and handwritten scripts like smbclient [4]. Table 2 lists, the type of XCS vulnerability found for each embedded device. Further, the possible XCS attack vectors that can be injected into the vulnerable web applications and their patterns are listed in Table 3.

6. DEFENDING AGAINST XCS VULNERABILITIES

This section presents several XCS vulnerability detection and mitigation approaches.

6.1 Content Sanitization

This is a mechanism to keep confidential data safe in the non production databases. The content sanitization procedure is described through the following steps: [16]–[21]:

Step 1: XCS defense mechanism is to ensure that whether all information passed to the client browser is sanitized properly. To identify possible XCS vulnerabilities, static analyzers will perform flow analysis. This approach should track all web channels including persistent storage devices. After, this raises the alarm when tainted data presented on a Web without sanitization [4].

Step 2: This defense mechanism is to dis-infect all victims data before communicating to the storage devices at

the input. This approach not likely to sweeten XCS attack vectors since the malicious data is inserted through the Web channel. This cannot sanitize for web exploits.

6.2 Black-box Scanner [17]

This scanner is a better choice for identifying security vulnerabilities in applications through the automated fashion. The scanners mimic attacks from attackers, provide effective methods for identifying a range of XCS vulnerabilities. Few scanners like WVS (Web Vulnerability Scanner), Rational AppScan and webInspect. This scanners attempts to browse all possible paths in Web applications to get an HTML code. In this scanners to initiate the scanning session, an user should enter the web application URL and login details of the Web. Then, the user must specifies the detection approach used for scanning the profile before begining the scan. Afterwards, all scanners proceeds further scanning after choosing the profile of the Web. The black box scanning cycle consists of 3 significant components. One is crawling component, which attains to browse directories and all hyper links in the web based applications to retrieve HTML content. Secondly, the attack component, in which black-box scanners are attains to use hostile SQL vectors as inputs to mitigate vulnerabilities in an upcoming phases. Finally, the analysis component is used to scan the results returned by web applications to trace whether an attack is successful or not.

Most of the black-box scanners use automated approach, which targets to build a graph that represents a set of all navigations on a website. The building of a graph is dynamic in nature to identify several vulnerabilities. This automated approach proposed by Akrout et al. [22] for vulnerability identification as shown in Fig. 3. The eight black-box scanners with their manufacturer, version, scanning profiles used by each scanner and type of vulnerability detected are listed in Table 4. The scanners testbed found XCS vulnerabilities in Malicious File Upload, Header Injection, Cross-Frame Scripting, XPath injection, Open Redirects, Path Traversal, Server Side Includes, SMTP Injection and Flash Parameter Injection.

6.3 Client-side XCS Detection Mechanism

The authors in [23] present a novel solution to mitigate XCS web applications called Noxes, a web firewall. The novelity in Noxes is the first client solution to provide protection against XSS This mechanism supports the detection module that significantly eliminates the number of alert prompts and aslo it effectively mitigates XSS vulnerabilities where an adversary would target confidential data like session identifiers and browser cookies.

6.4 Server Side Approach (S2XS2) to Identify XCS Vulnerabilities

The authors in [24] developed an automated framework to identify XCS vulnerabilities in the server with policy generation and boundary injection. Further, they derived trusted features for dynamic information, which matched at response generation to identify vulnerabilities and introduced a system tool to automatically inject boundary and generates policy for JSP programs.

6.5 A Server Side Approach to Defend XCS Vulnerabilities Using XCS-SAFE

Gupta et al. [25] proposed a robust framework called XCS-SAFE, it is the server-side approach to mitigate XCS
attacks from malicious attack vectors. This framework is built on idea of inserting the features of script and sanitization routines in the code to eliminate the malign attack strings.

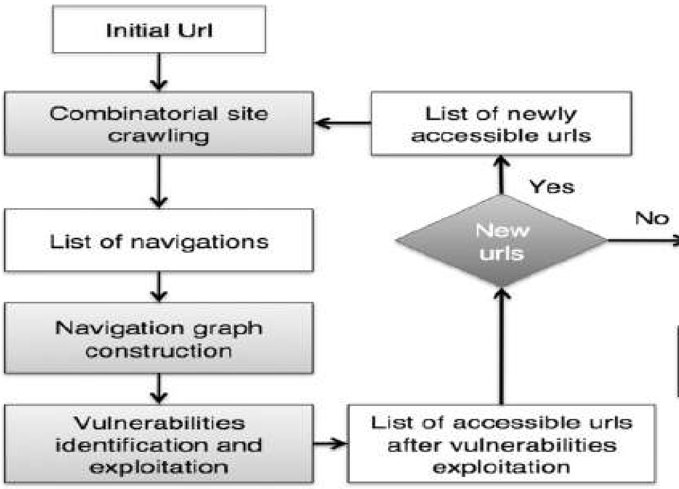

Initial Url
Combinatorial site crawling
List of newly accessible urls
Yes
No
New urls
List of navigations
Navigation graph construction
Vulnerabilities identification and exploitation
List of accessible urls after vulnerabilities exploitation

Fig. 3: XCS Vulnerabilities identification using Black-box scanners.

6.6 Secure Web Application Proxy

The authors in [26] describes an approach for XCS vulnerability mitigation known as Secure Web Application Proxy (SWAP). This approach recognize all static script calls within applications and encodes into invalid script elements. This proxy serves as a barrier between the Internet and the corporate applications. If no scripts elemets are found, then SWAP decodes all Javascript Identifiers, then restors all authentic vectors and transfers an HTML responses to the victim. Suppose, if the malevolent vector is identified by the script component, then after, instead of delivering responses, this approach alert an user for the cross channel scripting attack. Therefore SWAP techniques effectively mitigate XCS type of web attacks using a reverse proxy.

6.7 Server Side Mechanism to Mitigate XCS attacks [24]

In 2011, the authors in [24] presented the automated server cross channel scripting detection approach, which

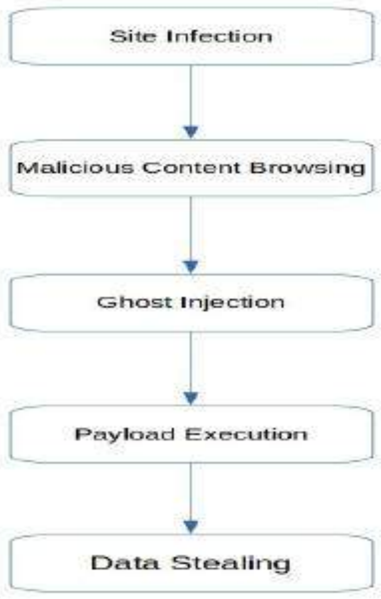


Fig. 4: Stages in the XCS attack.

is designed based on the boundaries insertion for generation of policies to validate the information. The boundary injection discovers probable javascript content, HTML tags and other expected features in web servers.

7. PREVENTION OF XCS ATTACKS

Here, we review the important stages of the cross channel scripting attack suggested by Bojinov et al. [4], the four stages of XCS attack is illustrated in Fig. 4. Furthermore, we discuss several prevention techniques that can be used to block XCS attacks [3], [4], [19], [23], [27]–[30].

1) **Site infection:** The most of the web based attacks begins with injecting the malicious web content into a website or web server through an embedded devices, communication protocols or through XCS exploit. The infected web can be a public-facing website or some management site an embedded device. In consideration of securing all existing as well as fortune web applications will not happen anytime soon, it’s well off annoying to obstruct subsequent phases of the attack.

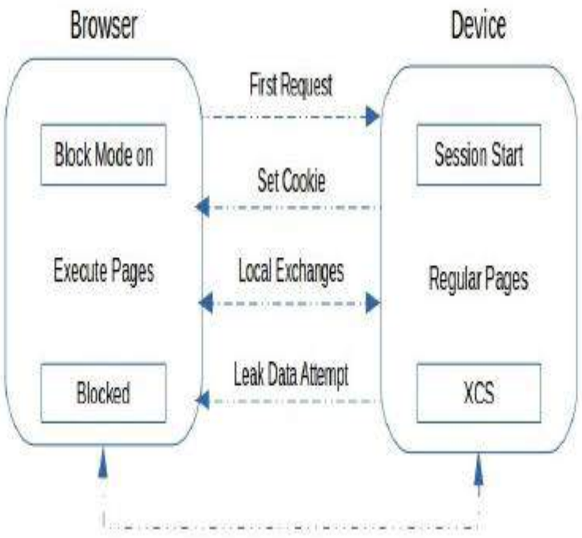
2) **Browsing malevolent content:** The next stage in cross channel scripting attack prevention is waiting for an user to visit a malicious site or infected sites. Then, browsing the infected site or malicious content by the user can be prevented in a number of ways: by preventing certain types of content from executing, by maintaining a list of malicious sites, as with No-Script extension for Firefox browser. Because, web based management interfaces are not public-facing, therefore the web interfaces cannot be inspected for malware content. As a result, websites or web servers containing malicious databases are inefficient for defending cross channel scripting vulnerabilities.

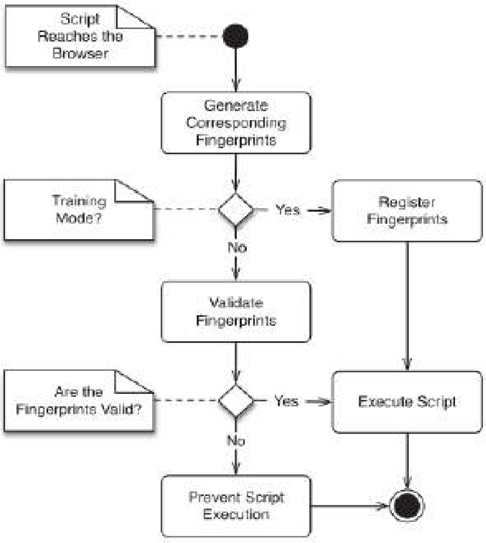
3) **Ghost injection:** Ghost allows injecting code into the top and bottom of the web template files without editing them. In cross channel scripting attack, a ghost script injection can take one of the forms: an invalid login, the submission form consits of an elements would accommodate HTML, a file rename or a stray network packet. The embedded device for server manufacturer can escape all input/output information that server will handle. As a result, this could be difficult to secure.

4) **Execution of the Payload:** An important and last phase of cross channel scripting vulnerability is an execution of the hacker’s content in circumstances of an administrators session. An admin views the infected page, unintentionally execute a malicious script embedded in it. Resulting, Reconfiguration of settings to creation of the new administrator’s account, deception to exhibit of fake information to the administrators browser, ex-filtration of the information from interfaces to adversary-controlled server and attacking other hosts on Internet.

8. CONCEPT OF FINGERPRINTS

Fingerprints are nothing but identifiers that presents the elements in the script and the context of execution at the browser. The authors in [31] introduced an whitelisting mechanism for scripts from protecting against XCS attacks with Javascript code. This approach consists of a interception layer for scripts in the browser engine, which detects the malicious script that reach client browser from every path. Fingerprints are developed on the server by the administrator using transparent layer called nSign [31]. After, the client browser receives all generated fingerprints from server in the secure manner. At last, script interception layer attains to match received fingerprints with the fingerprints that are generated while browsing. In addition, runtime checks are imposed to protect script from interacting with malicious domain. It is carried out by producing extra fingerprints for domains that are referenced by the script during production, which is illustrated in Fig. 5.





9. SITE-FIREWALL [4]

In this section, we describe Site-Firewall, which is used to prevent XCS attacks in the web applications. According to Bojinov et al. [4], the Site-Firewall is the client XCS prevention mechanism, which target ”payload execution phase” of an XCS attack. This approach imposes difficulty to exploit the client browser to ex-filtrate an information from the server. A Site-Firewall browser recieves the website specific policies from web content, the site could block malicious content served from it’s web server as well as blocks unauthorized access to the Internet or Intranet. By using a Site-Firewall layer in the user’s browser, an embedded device could explicitly specify the information served by an interface arrives from the device intrinsically and likely from vendor’s website. The user’s web browser would block connection to other websites, making it difficult to ex-filtrate an information as shown in Fig. 6.

10. CONCLUSION

In this article, we have presented a comprehensive survey on one of the most important web application vulnerability (i.e., cross channel scripting attack). It is examined to be a remarkable affliction for present web applications. XCS vulnerability permits an attacker to insert a malevolent data through embedded devices of a Web server, which de-facing web applications resulting in stealing of confidential information like cookies, passwords, information leakage, etc. In this article, we focused eight divergent types of consumer embedded devices across many vendors, all of the devices we reported contained significant XCS vulnerabilities. Network connected devices are commonly vulnerable to cross channel scripting attacks due to the variety of network protocols they implement. We have also described some state-of-art mechanisms based on XCS, identified their research gaps. We believe that this survey report provide a summary of all methodologies, techniques, and tools used for detecting, preventing XCS attacks, and their limitations and strengths as well. In order to mitigate the risks associated with XCS attacks in future, security framework should be developed, which encode all input fields and filters all special characters at user input. The source of XCS are embedded devices having smart capabilities and outdated libraries in the software code. As part of a XCS defence approach, ensures that security headers and cookie properties are set perfectly.

REFERENCES

[1] O. Z. de Paiva and W. V. Ruggiero, “A survey on information flow control mechanisms in web applications,” in High Performance Computing & Simulation (HPCS), 2015 International Conference on. IEEE, 2015, pp. 211–220.

[2] S. Gupta and B. Gupta, “Cross-site scripting (xss) attacks and defense mechanisms: classification and state-of-the-art,” International Journal of System Assurance Engineering and Management, pp. 1–19, 2015.

[3] B. Nagpal, N. Chauhan, and N. Singh, “Secsix: security engine for csrf, sql injection and xss attacks,” International Journal of System Assurance Engineering and Management, pp. 1–14. [4] H. Bojinov, E. Bursztein, and D. Boneh, “Xcs: cross channel scripting and its impact on web applications,” in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 420–431.

[5] H. Bojinov and Bursztein, “The emergence of cross channel scripting,” Communications of the ACM, vol. 53, no. 8, pp. 105– 113, 2010.

[6] B. B. L. B. T. Paulik, “Xcs based hidden firmware modification on embedded devices.”

[7] H. Bojinov, E. Bursztein, E. Lovett, and D. Boneh, “Embedded management interfaces: Emerging massive insecurity,” BlackHat USA, vol. 1, no. 8, p. 14, 2009.

[8] D. Stuttard and M. Pinto, The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws. John Wiley & Sons, 2011, vol. 20, no. 1.

[9] J. Grossman, XSS Attacks: Cross-site scripting exploits and defense. Syngress, 2007, vol. 58.

[10] I. Hydara, A. B. M. Sultan, H. Zulzalil, and N. Admodisastro, “Current state of research on cross-site scripting (xss)–a systematic literature review,” Information and Software Technology, vol. 58, pp. 170–186, 2015.

d policies,” in Proceedings of the

Quantum Cryptography and Use Cases: A Short Survey Paper

SANCHALI KSHIRSAGAR
DR. SANJYA PAWAR
SHRAVANI SHAHAPURE

Quantum Cryptography and Use Cases: A Short Survey Paper

Kshirsagar Sanchali
Assistant Professor
UMIT , SNDT Women's University
Mumbai, India
sanchali.kshirsagar@umit.sndt.ac.in

Dr. Sanjya Pawar
Principal
UMIT , SNDT Women's University
Mumbai, India
sanjay.pawar@umit.sndt.ac.in

Shravani Shahapure
Coordinator, Cyber security Research.
NCoE-DSCI
New Delhi
shravani.shahapure@dsci.in

[1] *ABSTRACT*—**The development in Quantum Computing threatens the existing public key cryptographic algorithms and builds fault tolerant systems for insecure communications channels. This paper is a short survey of different schemes of Quantum Computing with some possible use cases discussed for different application areas ,which can be explored by the research enthusiasts in the area of quantum computing.**

I. INTRODUCTION

Cryptography is the science of keeping the personal and important information confidential. It provides a secure shield to the important data from cybercriminals. In the rapidly digitally transforming world, data security is the topmost priority for most businesses and government agencies. Now the world is moving to the quantum era. Advancement in quantum computers and computation has enormous advantages, but it has also threatened the existing cryptographic algorithms. Shor's algorithm has the potential to break the 35 years old strong PKI schemes, RSA and Elliptic curve based cryptography.

II. QUANTUM CRYPTOGRAPHY

Quantum cryptography is the new revolution in modern cryptography. It provides an efficient and secure solution to the problem of key exchange on which the classical cryptography works. Due to these reasons, it is also imperative to upgrade current classical cryptography to work on algorithms which are considered quantum safe. This new cryptography is called post- quantum cryptography. There are two forms of quantum cryptography emerging nowadays

- Quantum Safe
- Quantum Enabled

III. QUANTUM SAFE

Quantum safe refers to the algorithms that are safe from attacks by quantum computations. The algorithm keeps the information secure even after the large quantum computers are built to attack the system. Even if the information is presently safe using strong cryptographic algorithms, it can be compromised by cybercriminal using quantum computation. The only solution to such a situation is to develop quantum-safe cryptographic algorithms.

The NIST has launched a competition to identify the best quantum-proof means of encrypting
data. The competition has recognized the following specific areas of quantum-proof solutions[1] shown in fig 1.

A. *Lattice-based cryptography*

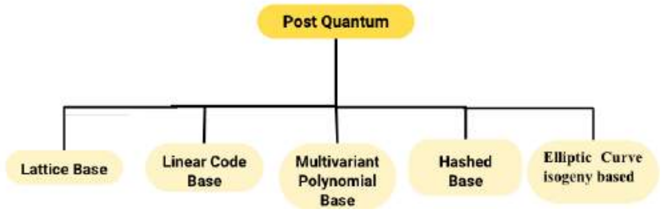


Fig 1 : Post Quantum schemes

Lattice-based cryptosystems are based on lattices, which are sets of points in *n*-dimensional spaces with a periodic structure. Lattice-based cryptosystems give strong security proofs and their implementation is usually simple, fast, and efficient. Lattice-based problems have the most attention. Lattice-based algorithms are very fast. LWE (Learning with Errors), NTRU and lattice based signature are candidates who deliver the best performance and security.

1. Learning with Errors (LWE) - Many hard mathematical problems constitute to develop lattice based designs. The most commonly used problem is the Learning with Errors (LWE) problem which finds a vector s when given a matrix M and a vector b = As + e where e is a small (unknown) error vector[2]. The schemes based on LWE is

- **Standards or random lattice based schemes -** this scheme is equivalent to worst case lattice problems which require large matrices and there matrix-vector multiplication[5]
- **Ideal or ring lattice based schemes** [6] - this scheme is that the matrix which is used has a single row ring lattice and needs to perform polynomial addition, polynomial multiplication, and modulo reduction.The details of the algorithm implementation can be check in [6]. But as mentioned in [5] the security of Ring-Learning With Error (R-LWE) or Ring Short Integer (R-SIS) depends on the ring variants
- **Module based schemes -** in this scheme the matrix has small dimensions and the coefficients of the matrix are no longer simple integers but entire polynomials. Therefore the number-theoretic transform (NTT) can be used for efficient polynomial multiplication. The security here is dependent upon variants of the original mathematical problems, e.g. Module-LWE or Module-SIS.[5]

2. NTRU - In 1998 NTRU first version was released by Hoffstein et al. [7] which followed the ring based

implementation . NTRU is a ring-based public key scheme based on the shortest vector problem in a lattice. It depends on four operations, i.e., setup, key generation, encryption, and decryption. explained in detail in [8]

3. There are two approaches for lattice based signature [1] one being the hash and sign approach . [9]In this scheme a message $\boldsymbol{\mu}$ is hashed to some point $h=H(\boldsymbol{\mu})$ which is in the range of trapdoor sampler/function f to form $\boldsymbol{\sigma} = f^1(h)$. The verification algorithm checks to confirm whether ($\boldsymbol{\sigma}$, $\boldsymbol{\mu}$) is a valid message signature pair

4. The second approach is the Fiat-Shamir[9] where identification scheme is initially built and then apply the Fiat-Shamir transformation . This scheme is based on the short integer solution problem. Lyubashevsky et al. proposed lattice-based signature schemes, BLISS (Bimodal Lattice Signature Scheme), currently the most efficient signature scheme.

B. Code-based

The McEliece cryptosystem is the first public key ,for which a linear codes is used[11]. The two most important public schemes that use binary Goppa codes are McEliece's encryption function and Courtois–Finiasz–Sendrier (CFS) [2] signature algorithm. CFS signatures are very short in length and are very fast to verify. The detailed implementation using Goppa Code is described in [11].

C. Multivariate based

Multivariate based schemes [12][13 are public key cryptosystems using multivariate polynomials over finite fields, mostly quadratic polynomials. The security offered by these schemes rely on solutions of many quadratic equations in many variables over finite fields,which is an NP complete computational problem[12]. Hence these schemes have capacity to guard against quantum computer attacks**.** The most promising multivariate encryption scheme is currently the Simple Matrix (or ABC) encryption scheme. Multivariate cryptosystems are public-key based systems and can be used for digital signatures. The most promising signature schemes include UOV and Rainbow.

Other important examples of multivariate signature schemes include HFEv, Gui, and MQDSS (Multivariate Quadratic Digital Signature Scheme)[13]

D. Hash-based cryptosystem

Hash-based signature [13] schemes were first proposed in the late 1970s .The design principle of Hash Based Signature (HBS) to use cryptographic secure hash function that has any of the security property

- one-wayness
- pre-image resistances
- second-preimage resistance
- collusion resistance.

Based on key generation ,signature generation and other construction parameters the HBS schemes can be classified as stateless and stateful schemes which can be further categorized as One-Time Signature (OTS), F ew-Time Signature (FTS), Multi-Time Signature (MTS), and Hierarchical Signature. XMSS is a more current scheme and is in the process of becoming standardized. It builds on Merkle Trees. SPHINCS$^+$ is a stateless hash-based signature scheme It uses two different hash-based signature schemes: Winternitz One-Time Signature Plus (WOTS$^+$), a one-time signature scheme, and Forest of Random Subsets (FORS), a few-time signature scheme.[15]

E. Elliptic curve Isogeny based schemes

Here the scheme is based on signature schemes based on isogeny of Elliptic curves. These cryptosystems have their security based on the difficulty of finding a path in the isogeny graph of elliptic curves[14].

IV. Quantum Enabled

As quantum cryptography is a new emerging area. The roots of the Quantum lie in the smallest particle, PHOTON. These photons have more than one state simultaneously, and they are changing the state only when they are measured. This is what is used in quantum cryptography.·

The most talked research in quantum cryptography is Quantum key distribution (QKD).

It is a mechanism to agree on the encryption key between two parties. The hardness of these problems is not based on mathematics but laws of physics.

Quantum random number generators are widely used. Quantum RNGs exploit quantum optics processes to generate true randomness in the sequence.

The research is evolving in the various directions in quantum cryptography. The next section discusses the field of application and use cases for quantum cryptography

V. Use Cases

1) **Endpoint devices:** Endpoint devices such as personal computers, mobile devices, IoT devices are some examples which are any piece of hardware that is used by users to interact with the network. These devices are vulnerable to different attacks like unauthorized use, keyloggers, viruses, malware, and many more. It is very important to secure these devices and ensure that only authorized devices can access the system.

Quantum computing is a potential threat to endpoint devices, even if they are encrypted. Currently, we are using RSA, DSA protocols for authentication. These algorithms are susceptible to quantum attacks. Compromised endpoint devices not only are a threat to the security of the system, but they also result in the legal penalty by law for inadequate encryption.

2) **Cloud Security:** Cloud computing has enormous benefits like storage capability, accessing data from multiple locations with multiple devices, distributed computing power. IT sector has adopted cloud computing almost in every business. It is very important to provide strong encryption to the cloud server, endpoint devices, and security to network infrastructure. With recent development in quantum computing, we should adopt Quantum safe cryptography schemes for achieving security goals like confidentiality, authentication, and integrity.

3) **SCADA security:** SCADA systems are a crucial part of our industrial ecosystems. It is used in very critical sectors of the Industry like Oil, natural gas, mining, railways, traffic system, water treatment and distribution plant, energy sectors. A weak encryption scheme to these systems will give adversaries to attack them, and the destruction will be beyond quantification.

The application of post-quantum cryptography is essential for the SCADA system when quantum computers are on the doorstep. There are some critical applications where quantum-safe cryptography should be part of the system. [19]Discusses the frequent attacks on SCADA networks, and potential attack by a quantum computer. The paper also identified a big research gap in securing the SCADA networks from quantum attacks and post quantum cryptography.

4) **Health Care:** It is one of the very sensitive sectors of the Industry. Patients' personal information is shared with the healthcare industry. These data can be compromised if poor encryption algorithms are used to protect it. These can be unauthorized data access. Quantum Computing can be used to design a framework for the secure quantum encryption of healthcare images and data. With the current trends in quantum technologies, such as quantum teleportation, quantum cryptography, and quantum steganography can lead the path for usage of Quantum computing in this field[18].

5) **Banking and finance** are relying on the IT sector for most of the operations. They are using cryptography heavily in various roles like hiding the data, authentication of the user, and data integrity. Quantum cryptographic will play a major role in the banking and finance sector for storing the data and electronic transaction of important information.

6) **IoT:** IoT is a new revolution in the modern digital world. Sensors have been deployed for various applications around us, and they are collecting numerous data. These sensors are used for sensitive applications like health care, and data breaching can cost major damage. With the advancement in quantum computation, there is a threat to the IoT applications. Quantum cryptography can be a savior to such applications.

7) Machine Learning :Machine learning is a technology which exists in all the domains right from cars, to mobile phones, social media, to consumer appliances. Here we collect data and convert it into a model allowing it to be used in all applications. Quantum computing can be used to methods by enabling the training of machine learning models that are beyond the computational capabilities of our classical machines [17].

CONCLUSION

RSA and ECC are based on public-key schemes used in current security infrastructure to provide public-key encryption and key exchange. A large research is now being conducted into *quantum-resilient* or *post-quantum* cryptography. This paper provided a short survey on forms of quantum cryptography areas which emerge nowadays with the multiple schemes that exist in post-quantum. We have also listed some of the use cases which can be explored by Security researchers for opportunities to upgrade with quantum safe cryptography in these fields. It can act as useful for starters seeking to create quantum-resistant solutions .

REFERENCES

[2] Güneysu, Tim & Krausz, Markus & Oder, Tobias & Speith, Julian. (2018). Evaluation of Lattice-Based Signature Schemes in Embedded Systems. 385-388. 10.1109/ICECS.2018.8617969.

[3] Khalid, A., McCarthy, S., O'Neill, M., & Liu, W. (2019). Lattice-based Cryptography for IoT in A Quantum World: Are We Ready? In Proceedings - 2019 8th International Workshop on Advances in Sensors and Interfaces, IWASI 2019 (pp. 194-199). [8791343] IEEE.https://doi.org/10.1109/IWASI.2019.87913

[4] Hamid Nejatollahi, Nikil Dutt, Sandip Ray, Francesco Regazzoni, Indranil Banerjee, and Rosario Cammarota. 2018. Post-quantum Lattice-based Cryptography Implementations: A Survey. ACM Comput. Surv. 1, 1, Article 1 (January 2018), 38 pages. https://doi.org/10.1145/3292548

[5] A. Mariano, T. Laarhoven, F. Correia, M. Rodrigues and G. Falcão, "A Practical View of the State-of-the-Art of Lattice-Based Cryptanalysis," in *IEEE Access*, vol. 5, pp. 24184-24202, 2017, doi: 10.1109/ACCESS.2017.2748179.

[6] Roy S.S., Vercauteren F., Mentens N., Chen D.D., Verbauwhede I. (2014) Compact Ring-LWE Cryptoprocessor. In: Batina L., Robshaw M. (eds) Cryptographic Hardware and Embedded Systems – CHES 2014. CHES 2014. Lecture Notes in Computer Science, vol 8731. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-44709-3_21

[7] Tan, T. N. and Hanho Lee. "Efficient-Scheduling Parallel Multiplier-Based Ring-LWE Cryptoprocessors." *Electronics* 8 (2019): 413.

[8] Hoffstein J., Pipher J., Silverman J.H. (1998) NTRU: A ring-based public key cryptosystem. In: Buhler J.P. (eds) Algorithmic Number Theory. ANTS 1998. Lecture Notes in Computer Science, vol 1423. Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0054868

[9] R. Chaudhary, G. S. Aujla, N. Kumar and S. Zeadally, "Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions," in *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4897-4909, June 2019, doi: 10.1109/JIOT.2018.2878707.

[10] Howe, James & Pöppelmann, Thomas & Mcloone, Maire & O'Sullivan, Elizabeth & Güneysu, Tim. (2015). Practical Lattice-Based Digital Signature Schemes. ACM Transactions on Embedded Computing Systems. 14. 1-24. 10.1145/2724713.

[11] Fiat A., Shamir A. (1987) How To Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko A.M. (eds) Advances in Cryptology — CRYPTO' 86. CRYPTO 1986. Lecture Notes in Computer Science, vol 263. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-47721-7_12

[12] J. Faugère, V. Gauthier-Umaña, A. Otmani, L. Perret and J. Tillich, "A Distinguisher for High-Rate McEliece Cryptosystems," in *IEEE Transactions on Information Theory*, vol. 59, no. 10, pp. 6830-6844, Oct. 2013, doi: 10.1109/TIT.2013.2272036.

[13] M. Liu, L. Han and X. Wang, "On the equivalent keys in multivariate cryptosystems," in *Tsinghua Science and Technology*, vol. 16, no. 3, pp. 225-232, June 2011, doi: 10.1016/S1007-0214(11)70033-5.

[14] J. Ding and A. Petzoldt, "Current State of Multivariate Cryptography," in *IEEE Security & Privacy*, vol. 15, no. 4, pp. 28-36, 2017, doi: 10.1109/MSP.2017.3151328.

[15] S. Suhail, R. Hussain, A. Khan and C. S. Hong, "On the Role of Hash-based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions," in *IEEE Internet of Things Journal*, doi: 10.1109/JIOT.2020.3013019.

[16] "Post-quantum cryptography," Available at: https://csrc.nist.gov/ projects/post-quantum-cryptography (Accessed 29 Nov 2020).

[17] Galbraith S.D., Petit C., Silva J. (2017) Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems. In: Takagi T., Peyrin T. (eds) Advances in Cryptology – ASIACRYPT 2017. ASIACRYPT 2017. Lecture Notes in Computer Science, vol 10624. Springer, Cham. https://doi.org/10.1007/978-3-319-70694-8_1

[18] M. Roetteler and K. M. Svore, "Quantum Computing: Codebreaking and Beyond," in *IEEE Security & Privacy*, vol. 16, no. 5, pp. 32-36, September/October 2018, doi: 10.1109/MSP.2018.3761710.

[19] A. A. Abd El-Latif, B. Abd-El-Atty and M. Talha, "Robust Encryption of Quantum Medical Images," in *IEEE Access*, vol. 6, pp. 1073-1081, 2018, doi: 10.1109/ACCESS.2017.2777869.

[20] S. Ghosh and S. Sampalli, "A Survey of Security in SCADA Networks: Current Issues and Future Challenges," in *IEEE Access*, vol. 7, pp. 135812-135831, 2019, doi: 10.1109/ACCESS.2019.292644

Securing IoT using Permissioned Blockchain

SHALINI DHULL

Securing IoT using Permissioned Blockchain

Shalini
Cyber Division
Tata Advanced System Limited
Noida, India
Shalini.dhull@tataadvancedsystems.co
m

Abstract— **The security of cyberspace is paramount in today's world. The high dependency on technology allows hackers to steal IOT valuable information. The centralized IoT system uses one-time validity of credentials, makes the whole system remotely hackable and attackable. The Blockchain properties like immutability, transparency, decentralization immune to a single point of failure. This paper illustrates a Permissioned Blockchain (PBC) mechanism in a decentralized environment; establish security by authorizing a legitimate user in the system. The access control layer works on the permission management framework helps in sharing data between participating nodes of the IoT network. The blockchain stores the transactions as the hash. A digital token is required to access data by authenticating a legitimate user in a valid IoT zone.**

Keywords—component, formatting, style, styling, insert (*key words)***

I. Introduction

IOT- The attacks on the cyber-space by criminals is at a peak in today's world. The companies with big databases are the prime target for that. The internet of things made up of physical objects such as sensors, actuators; able to collect and transmit different kinds of data to its connected media ranging from simple temperature values to photographs taken by cameras without human interference. After connecting to the internet, the devices can connect and communicate with the other nodes in the network. (Porkodi, 2014). IoT architecture is made up of components like actuators and sensors for sensing; IoT gateway such as a router to provide route and server for the storage of the data. All these are linked to each other via the internet (Gartner, 2017). The IoT sensors and actuators at the starting level collect data from its surrounding environment and convert it into useful information. The Data acquisition systems transform the analog data generated by the sensor into digital form and transfer it to the gateway. The router as gateway route the data for storing it on the internet. For information exchange, IoT's are connected using the internet, become the reason for vulnerability, and make IoT devices remotely hackable. Here the need for blockchain can prove a good candidate for the safety and security of organization data.

The blockchain that is a decentralized ledger, has the capability to deal with the central point of failure. Transactions are grouped in form of blocks in the same order; they are completed, also the order of transactions is important. The minor changes in the transaction create completely a different hash. To store transactions in a block it should be approved by the maximum number of the network participating nodes. The data available on blocks cannot be altered it needs to change at all the participating nodes. The blocks saved on the blockchain creates the most secure network, makes it difficult to hack (Hounshell, 2018).

II. IoT Security Breaches

The security measures taken by the organizations for protecting the IoT are not enough. Due to this reason IoT hacks are increasing globally. The devices such as refrigerator, vehicle, or air conditioner, connected through the Internet open a new path for malicious nodes. The attacks like botnets, the Man in the middle attack, social engineering, data, and identity theft, Distributed Denial of Service threaten accessibility in IoT devices
(Khandelwal, 2018).

Some Real-World Examples of IoT Hacking and Vulnerabilities are as follows:

Stuxnet: Stuxnet *is* an extremely sophisticated malicious, undetectable computer worm, discovered in 2010 that has been designed to target SCADA (Supervisory Control and Data Acquisition) for nuclear power plants. Once entered into the network it affects centrifuges (IoT devices that isolate isotopes of uranium) and reprogram it.

Amazon FreeRTOSIoT: This vulnerability in the Operating System of Amazon FreeRTOSIoT allows the attackers to crash or inject and execute malicious code remotely on Iot device; leak information stored in its memory. The attacker can take complete control of the target device. (Khandelwal, 2018)

The Mirai Botnet (aka Dyn Attack): This is an IoT botnet attack by a malware called Mirai that occurred in October 2016. Once the computer gets infected by Mirai malware, it searches the network continually to gain access to vulnerable IoT devices (e.g. IP camera, monitors, loggers) using most common usernames and passwords like "admin" and "password" and convert the device behavior into a bot for serious attacks (Writer, 2017). To perform bulk massive attacks (DDoS) the collection of bots called botnet attacks on major networks.

The Hackable Cardiac Devices from St. Jude: St. Jude cardiac device had a vulnerable point that allows hackers to read or control sensitive information of the patient. These cardiac devices are used in healthcare for monitoring and controlling that heart-beat of patients and prevent heart attacks (Writer, 2017).

The Owlet WiFi Baby Heart Monitor Vulnerability: It monitors the heart rate of child; very easy to hack and can be life danger for the baby if compromised remotely.

The Jeep Hack: In July, 2015 A team of researchers was able to take control (turn on/off AC, Steering control, engine off) of a Jeep SUV without physical access

(Writer, 2017) due to the vulnerability of the jeep's dashboard. The dashboard could rewrite or update firmware on the chip. By rewriting the firmware to the chip, the researcher's team was able to control the car.

Black Hat: The Nest thermostat device turned into a smart spy. If the attacker gets physical access to that device, then only 10 seconds are needed to reset it by holding the power button. By inserting a USB flash drive, the custom firmware (not signed by nest) can be loaded to developer mode in just 5 seconds. In this way, it requires only 15 seconds for Nest to act as a smart spy. (Storm, 2018)

III. BLOCKCHAIN FOR CYBER DEFENCE

Blockchain records the transactions performed by network nodes in the form of blocks in the database. The blockchain protocol dictates the verification process of transactions when a new transaction is requested. If the maximum number of the participating nodes (Kim, 2018) agrees on the transaction validation process, the new transaction is added into the blockchain else the transaction will be cancelled (Dylan Yaga, 2018). The validation protocol when set up correctly, easily verify valid nodes, and reduce performing of false transactions.

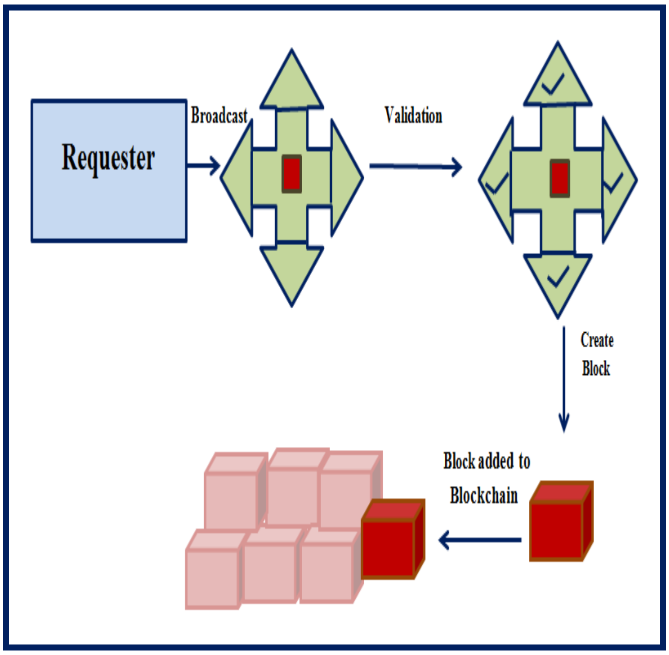


Fig 1: Functioning of Blockchain

IV. BLOCKCHAIN IN IOT AS PERMISSIONED BLOCKCHAIN

The Internet of Things (IoT) and Blockchain both are rapidly emerging technologies. When we merge blockchain with IoT to manage access to data; it provides additional security features for IoT devices. In blockchain the central authority is not there, so reduces the chances of a single point of failure. The blockchain property of transparency avoids the need for a trusted third party (Dylan Yaga, 2018) can be harmful here. As the nature of blockchain, the newly added block is replicated to all nodes connected to the blockchain. All nodes can view transactional data. There is no authentication and authorization mechanism for accessing data. For validating IOT transactions on the blockchain, the concept of proof of work required a large amount of computational power. This causes the problem when merging with IoT, as IoT devices which are mainly typical sensors having low computational and storage capacity. The transparency feature of the public blockchain, any node connecting to the network makes the IoT network vulnerable. Here, comes the concept of permission blockchain, only predefined nodes can participate in the network or connect to the blockchain and use the concept of smart contract automate the transactions. This makes the IoT network more secure and prevents it from malicious access. As, use of the Practical Byzantine Fault Tolerance (BFT) algorithm (Stefano De Angelis, 2018) reduces the energy consumption needed in the proof of work for performing computations.

The permissionless blockchain system has privacy challenges. Transaction privacy is mandatory in scenarios where sensitive data collected by the third party can be used for malicious purposes.

The permissioned blockchain offers access control using asymmetric (public-private) key cryptography and protects data from unauthorized access. Access control means the only authorized participants can access the sensitive data. Only enrolled devices can perform and validate transactions in the network.

V. IOT ACCESS MANAGEMENT FRAMEWORK FOR P-2-P NETWORK

The permissioned blockchain for IoT work at the Access control layer in the Trust management framework can be used in some areas such as finance, healthcare for data protection

(Antorweep Chakravorty, 2013). In medical the sensitive information shared by hospital staff can be fetched by cybercriminal to monitor the patient health (Nabil Rifi, 2018). To automate the transactions, a trustworthy 3 layers architecture framework for permissioned networks (Zheng Yan, 2014) is used. In the trust management framework, a trust layer is used between the physical layer and application layer which maintain privacy within a private network.

Low Level Layer: The physical layer devices the sensors and actuators work to provide reliable communication systems.

Middle Layer: The blockchain layer act as a middle layer helps to maintain the security in IoT applications built on the decentralized environment. The access control layer controls the entry in a permissioned blockchain network. The process of node enrollment, key exchange, Token issue, and Transaction completion are followed on the blockchain layer.

High Level Layer: The application layer exists at the highest level of the Access framework, responsible for the delivery of IoT services to the user and provides security by preventing unauthorized (Zheng Yan, 2014) access to the malicious user in the network by using permissioned blockchain.

VI. STEPS TO BE FOLLOWED IN PERMISSIONED BLOCKCHAIN

1) The Device wants to join the Private network requests to membership provider for Id.

2) Membership Provider (MP) generates a certificate with a private-public key pair to the requesting device and shares the public key to all the network nodes. The enrolled members become the trusted nodes of the network.

3) The enrolled requester wants to perform the transaction, request to a smart contract for a token.

4) The smart contract verifies the identity by the certificate and issue token to the requester.

5) The requester signs the token with its private key using the RSA Digital Signature algorithm attaches it with a transaction then transmits it to all participating nodes in the network.

6) The consensus policy specifies the number of devices required for this transaction validation. All certified devices verified the Digital Signature using the requester's public key. This ensures that the token is valid and coming from an authentic user. The certified members approve the transaction; send back the signed proposal responses to all devices.

7) The devices check for consensus policy is accurately followed and there are no conflicting transactions commit the transaction and save changes in the database.

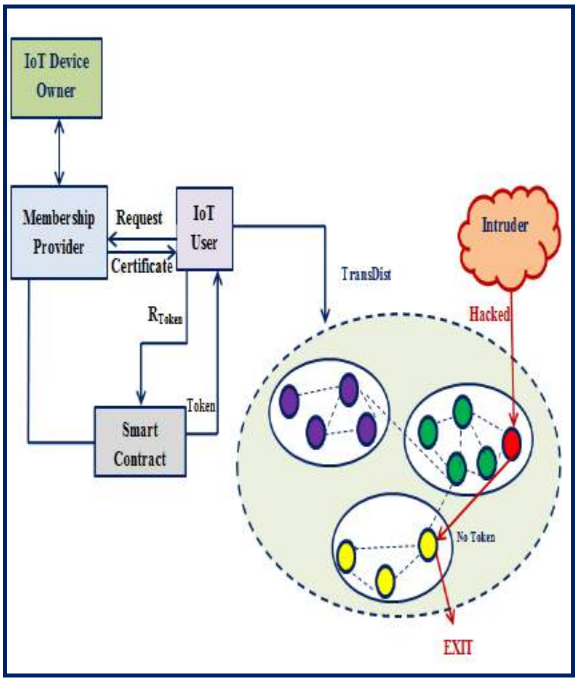


Figure 2: Architecture representation of permissioned blockchain

VII. Permissioned Blockchain as an Application in Smart Home Health Care

A home is called a Smart home (Ali Dorri, 2017) if it can monitor the health of the patient in the automation system. A network of sensors "smart devices" can capture data from the surrounding environment and make it available to authorized users for real-time management of patient health. A continuous data transfer among smart devices from the sensor worn by the patient. The risk of attacks on a smart lot device like a fitness band is very high and can be very dangerous for the patient sometimes. The attacker if obtains the sensitive information can harm the patient. For handling this kind of scenario, a safety mechanism should be taken. For accessing the data of IoT devices by any external identity it must be authenticated using permissioned blockchain technology. The smart contract controls the access, by deciding whose token can access or write data on the blockchain (Nabil Rifi, 2018).

Issuing certificates: The Membership Provider is working the same as a certificate authority, issues the certificates to the network participating devices, and the process is called enrollment. The membership provider can enroll or deny the request according to the defined policy. A new node can join the network dynamically at any time and can request a certificate from to membership provider. In the enrollment phase, the participant gets a private-public key and enrollment certificate. These certificates will be required by participants who want to perform data read or write transaction within the network. The MP also maintains Certificate Revocation List (CRL) contain a list for the invalid or no longer nodes.

Token-based Security: Each user has a unique private-public key pair assigned by the membership provider. The trusted node wants to perform any transaction, it requests a token to the smart contract via the application interface. Smart Contracts have unique tokens for each transaction. The smart contract checks the requester identity, permission level, organization to which it belongs, the validity of certificate with membership provider to verify requester permission level. It verifies the requester certificate then generates the token using various prediction models (Rahul Agrawal, 2018) on basis of permission held by that device. Tokens and private keys required to sign a token are stored in a digital repository. The generated token based on past trails record contains the timestamp values, requester device identity, user zone, and token validity period (Piotr, 2018). The requester signs the token using the RSA Digital Signature algorithm (Filip, 2017) with its private key. All certified trusted devices verify the Digital Signature first on the blockchain network using the sender's public key for proving the authenticity of the transaction. This ensures that the token is not used before by any other malicious actor in the network (if token theft). The token is added with the transaction and distributes in the network for validation using PBFT consensus (Stefano De Angelis, 2018). When transaction execution is successful, then-current tokens get disabled (can't use for any other transaction) and the block state gets updated with the new state. With the help of an authentic token, the requester gets access to blockchain to perform transactions by devices. The certified trusted devices approve the transaction and send their decision to accept or deny response to all network participating devices. The other devices check that consensus policy rules are followed, and they add that transaction to their own blockchain database.

CONCLUSION

The solution provided by this paper enhances security by the process of tokenization and access control in-valid IOT zone. The membership provider issues certificates to the participating devices in the network. The access control layer in a trusted framework ensures that only valid trusted participants can join, transmit, or gain access to sensitive data in the network. The certified nodes validate the transaction according to consensus policy, then a new block is added to the blockchain. The system becomes more tamper-resistant, immutable, and secure by the integration of permission blockchain with the decentralized environment in the IoT environment.

FUTURE RESEARCH DIRECTIONS

In this paper, the permissioned blockchain properties like decentralization, tamper-resistant, access control are used to secure IoT data by authorizing the user according to its permissions. Access control management can be improved by defining permissions of different users on multiple levels a permissioned blockchain. In the future, our aim to work on this limitation and to extend our work by the given solution defines permissions on multiple levels on a large scale of IoT zones.

REFERENCES

[1] L. Coetzee & J. Eksteen, “The Internet of Things-promise for the future? An Introduction”, IST-Africa Conference Proceedings, 2011.

[2] Zheng Yan, PengZhang & AthanasiosV.Vasilakos, “A Survey on Trust Management for Internet of Things”, Journal of Network and Computer Applications, June, 2014.

[3] Ville Sulkamo, “IoT from cyber security perspective. School of Technology”, Communication and Transport ,Information Technology, 2018.

[4] Leon Hounshell, “Cybersecurity, BlockchainAnd The Industrial Internet Of Things.” Serial Technology Entrepreneur, Nov 2018.

[5] R. Roman, J. Zhou & J. Lopez, “On the features and challenges of security and privacy in distributed internet of things”, Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2018.

[6] Global sign, “Common Cyber Attacks in the IoT - Threat Alert on a Grand Scale”, Apr 2016.

[7] Swati Khandelwal, “Critical Flaws Found in Amazon FreeRTOSIoT Operating System”, Retrieved from hrtps://Thehackernews.com, Oct 2018.

[8] Guest Writer, “The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History”, Retrieved from http:// https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/, May 2017.

[9] Darlene Storm, “Black Hat: Nest thermostat turned into a smart spy in 15 seconds”. Computerworld | AUG 11, 2014 12:25 PM PT.

[10] Krebs on Security, “IoT Devices as Proxies for Cybercrime”, Retrieved from https:// https://krebsonsecurity.com/2016/10/iot-devices-as-proxies-for-cybercrime/, Oct 2016.

[11] Timothy Jones, “Hackers obtain nuclear power plant plans in France”. Retrieved from https:// www.dw.com/en/hackers-obtain-nuclear-power-plant-plans-in-france/a-46126878, Nov 2018.

[12] Francisco Maroto, “Is Blockchain the silver bullet needed by the IoT industry”. February 13, 2017.

[13] Gartner & MONAX, “Permissioned Blockchains. Leading the IoT” 2017.

[14] Jon Wood, “Blockchain of Things—cool things happen when IoT& Distributed Ledger Tech collide”, Retrieved from https://medium.com/trivial-co/blockchain-of-things-cool-things-happen-when-iot-distributed-ledger-tech-collide-3784dc62cc7b, Apr, 2018.

[15] Dr. V. Bhuvaneswari & Dr. R Porkodi, “The Internet of Things (IoT)”, 2014.

[16] “Applications and Communication Enabling Technology Standards: An Overview”. Conference on Intelligent Computing Applications.

[17] Muhammad Bilal, “A Review of Internet of Things Architecture”. Retrieved from //https://arxiv.org/ftp/arxiv/papers/1708/1708 .04560.pdf, 2017.

[18] Dylan Yaga, Peter Mell, Nik Roby & Karen Scarfone, “Blockchain Technology Overview”, Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf, 2018.

[19] Stefano De Angelis,Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri & Vladimiro Sassone, “PBFT vs Proof-of-Authority” Retrieved from https://eprints.soton.ac.uk/415083/2/itasec18_main.pdf, 2018.

[20] Giang-Truong Nguyen & Kyungbaek Kim, “A Survey about Consensus Algorithms Used in Blockchain”, Journel of information processing system, Feb 2018.

[21] Antorweep Chakravorty, Tomasz Wlodarczyk & Chunming Rong,. ”Privacy Preserving Data Analytics for Smart Homes”, IEEE Security and Privacy Workshops 2018

[22] Nitesh Emmadi, Vigneswaran R, Srujana Kanchanapalli, Lakshmipadmaja Maddali & Harika Narumanch, “Practical Deployability of Permissioned Blockchains”, Conference Paper. Retrievedfrom https://www.researchgate.net/profile/Harika_Narumanchi/publication/325966342_Practical_Deployability_of_Permissioned_Blockchains/links/5b3f1d804585150d2309d5e8/Practical-Deployability-of-Permissioned Blockchains.pdf?origin=publication_detail, 2018.

[23] Rahul Agrawal, Pratik Verma, Rahul Sonanis, Umang Goel, Dr. Aloknath De, Sai Anirudh Kondaveeti & Suman Shekhar. “CONTINUOUS SECURITY IN IOT USING BLOCKCHAIN” ICASSP conference, 2018

[24] Filip Forsby, “The Digital Certificates for Internet of Things” Retrieved from https://kth.diva-portal.org/smash/get/diva2:1153958/FULLTEXT01.pdf, 2017.

[25] Nabil Rifi, Nazim Agoulmine, Nada Chendeb Taher & Elie Rachkidi, “Blockchain Technology: Is it a Good Candidate for Securing IoT Sensitive Medical Data? Wireless Communications and Mobile Computing” Retrieved from https://doi.org/10.1155/2018/9763937, 2018.

[26] Ali Dorri, Salil S. Kanhere, Raja Jurdak & Praveen Gauravaram, “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home”, Conference paper, 2017

[27] Polak Piotr, “Security Architecture for the Internet of Things (IoT) Commercial Buildings”, (Philips Lighting). Retrieved from https://www.fairhair,alliance.org/data/downloadables/1/9/fairhair_security_wp_march-2018.pdf, 2018.

[28] Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo & Antonio Puliafito, “Blockchain and IoT Integration: A Systematic Survey”, 2018

[29] Jollen Chen, “Hybrid Blockchain and Pseudonymous Authentication for Secure and Trusted IoT Networks” Flowchain Open Source Project Devify, 2018.

[30] Alexander Yakubov, Wazen M. Shbair, Anders Wallbom & David Sanda, “A Blockchain-Based PKI Management Framework”. IEEE/IFIP, 2018.

[31] Stefano De Angelis, “Assessing Security and Performances of Consensus algorithms for Permissioned Blockchains”, 2018.

An Analysis of Internet of Things(IoT) Architecture

YASSIR FAROOQUI
DR. KIRIT MODI

An Analysis of Internet of Things(IoT) Architecture: Novel Architecture, Modern Application, Security Aspects and Future Scope

Yassir Farooqui
Computer Science Department
Parul University
Vadodara,India
yassir.farooqui270062@paruluniversity.ac.in

Dr. Kirit Modi
Computer Science Department
Sankalchand Patel University
Visnagar,India
kiritmodi@gmail.com

Abstract: **The Internet of Things is a network where machines are becoming smarter every second, processing every second becomes noticeable and communication becomes resourceful every second. The Internet of Things is building its own brand and expanding its own dimension, and its utility can be seen as a global solution for linking different devices. The most significant parameter that applies to the same area is architecture. The lack of expertise in general architecture is still the issue that the researcher resists in paving the way for the Internet of Things overall reach. The IoT-related architecture is sufficiently appropriate for the improvement of instruments, methologies, and technology to satisfy researchers' requirements. Several architectures are introduced in this paper to enhance day-to-day issues by carving and integrating rich Internet of things marks. In order to get the exact power of the IoT, problems are also being implemented in the overall study of various architectures together with the domain and challenges.**

***Keywords*: *IoT,Architecture,Security,Reliabilty*.**

I. Introduction

The evolving area of IoT in different organisations and its presence all around us raises the need to ensure high-level security and to ensure that their data remains protected and capable of making the best use of IoT facilities. By growing the number of devices linked through the Internet over a network, IoT users predict that billions of users would be crossed by users. However, this increases security problems to a high point by 2020 and is thus one of the big IoT security and wireless system concerns [1]. The IoT architecture can be treated as a physical, virtual or hybrid system consisting of a number of active physical objects, sensors, actuators, cloud services, basic IoT protocols, communication layers, users, developers, and business layers. Unique architectures act as a pivotal aspect of the particular IoT infrastructure, thereby promoting a systematic approach to different components, resulting in solutions to related problems. For the sake of information, a well-defined type of IoT architecture is currently available.

In just years to come 25 billion devices will be connected to the internet and these connections will allow the data used to autonomously evaluate, pre-plan, manage, and make intelligent decisions [4]. IoT has been introduced by the US National Intelligence Council (NIC) as one of the six' 'Disruptive Civil Technologies" (National Intelligence Council, 2008..

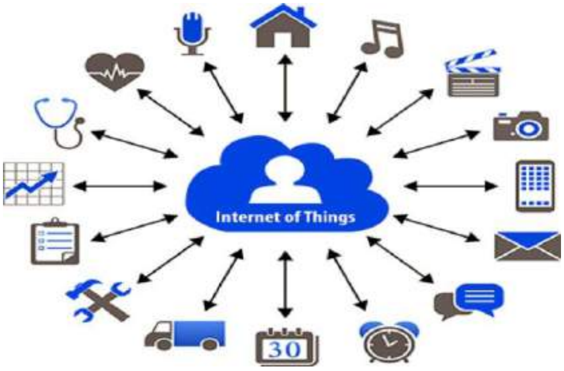


Fig1: Internet of Things in various Application.

. In this context, we can see that many sectors of operation are already benefiting from various architectural types of IoT, such as: transportation, smart city, smart domotics, smart health, e-governance, assisted living, e-education, retail, logistics, agri-culture, automation, industrial development, and business/process management etc

When the companies or organizations launch their products in market majorly wireless, they tend to say that they are secure and do send the patches regularly on day to day basis but a point comes when the focus from the previous devices shifts to a new launch just after a few days and then irregularity come into play, which for the network, device and IoT builds up the security threats [5]. Various practices are introduced in the world outside to ensure the device.

Basic Features of IoT Architecture.

Connectivity, observing, incorporating, constructive interaction, and many more are the most critical features of the IoT that it operates on. Below, some of them are listed:

1. Connectivity

Connectivity refers to establishing a proper link between all things that may be server or cloud from the IoT to the IoT platform [8]. After the IoT devices are connected, high-speed messaging between the devices and the cloud is required to enable reliable, secure and bi-directional communication...

2. Sensing

The sensor devices that are used in IoT technologies detect and quantify any environmental changes and report on their status[6]. Passive networks are brought to active networks through IoT technology. There couldn't be a productive or true IoT world without sensors.

3. *Analysing*

After all the relevant things are connected, the collected data is analysed in real time and used to create efficient business intelligence.. If we have a good insight into data gathered from all these things, then we call our system has a smart system [6].

4. *Integrating*

To enhance the user experience as well, IoT incorporates the different models.

5. *Endpoint Management*

Otherwise it is necessary to be the endpoint management of all the IoT framework, causing the system to fail fully. For example, when a coffee machine itself orders the coffee beans when it finishes, but what happens when the beans are ordered by a retailer and we are not present at home for a few days, leads to the failure of the IoT device. So there has to be a need for endpoint control. [7] .

2 .Literature review.

The work done so far by scientists around the world is prescribed in this chapter. This section describes various domain-specific architectures based on broad fields, such as: RFID, service-oriented architecture, wireless sensor network, supply chain management, industry, healthcare, smart cities, logistics, connected living, big data, cloud computing, social computing, and security. The selection of these domains depends on the existing IoT applicability scenario [3]. As many directions have been tried to be integrated into this article, but present limitations have been produced due to the size con- strains. The core method-ology behind the survey depends on a few important factors where, based on their respective sub-domains, previously described domains are thoroughly investigated. This study is carried out to evaluate a number of segregated sub-domains in order to gain and provide important information on the following: architectural structure, applicability, applicability, At the end of this report, a precise, specific and succinct conclusion is drawn based on the interpretation of the survey. The overall approach behind the survey explains how IoT is implemented using specific architectures to the sub domains.The Various IoT Architectures are as follows:

1. *Service oriented Architecture:*

Service-oriented (SOA) architecture is an approach used to build architecture based on the use of system services. In the IoT domain, the inbuilt SoA approach is currently invoked, using the middleware concept i.e., a software layer superimposed between the application and technology layer that hides the unnecessary relevant details from the development, thus reducing the time of product development,helping

In a short period of time, the design workflow is simpler to ease the market process in terms of commercial results. RFID envolement, Middleware enablement, SOA management are methods used. The challenges and problems facing SOA are that SoA faces efficiency and cost-related problems. A large number of devices connected to the machine with scalability problems[5] must be addressed by SoA. The transfer, processing and management of data is a matter of burden over-headed by service.

2. *Wireless Sensor Network(WSN):*

A Wireless Sensor Network comprises a large number of circulating, self-directed, minute, low-powered devices called sensor nodes called motes, which are one type of wireless network. Certainly, these networks cover a large number of spatially distributed, small battery-operated, embedded devices that are networked to carefully collect, process, and transfer data to operators and have controlled computing and processing capabilities. Nodes are small computers which work together to form a network.. The issues in the wireless sensor network are energy efficiency, scalability, reliability, and robustness etc. parameters when designing a WSN powered system..

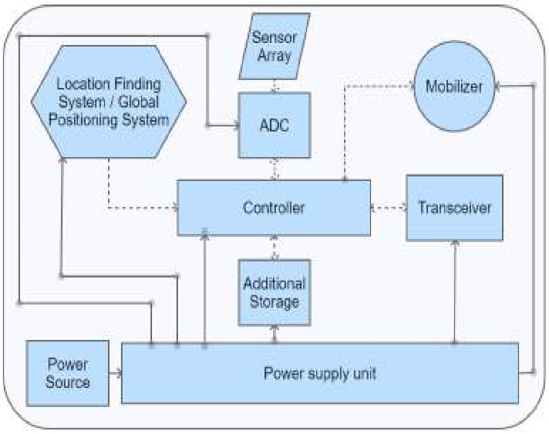


Fig2: Wireless Sensor Network

Wireless Sensor Network (WSN) [6] is one of the key parts of IoT system. It consists of a finite number of sensor nodes (mote) mastered by a special purpose node (sink) by employing multi layered protocols organization[7]. Primarily energy effi- ciency, scalability, reliability, and robustness etc. parameters are sought when designing a WSN powered system. Energy effi-ciency, scalability, reliability, and robustness etc. parameters are sought when designing a WSN powered system.

3. *Health care:*

Recently, smart healthcare system development and dissemi-nation has become possible by the convergence of various IoT architectures.). Bio-Patch takes decision when to call remote physician, emergency center, hospital, test clinic, and supply chain medicine retailers[1]. Authors have proposed iHome Health-IoT platform for in-home health care services based on the IoT; illustrating a 3 lay- ered open-platform based intelligent medicine box.

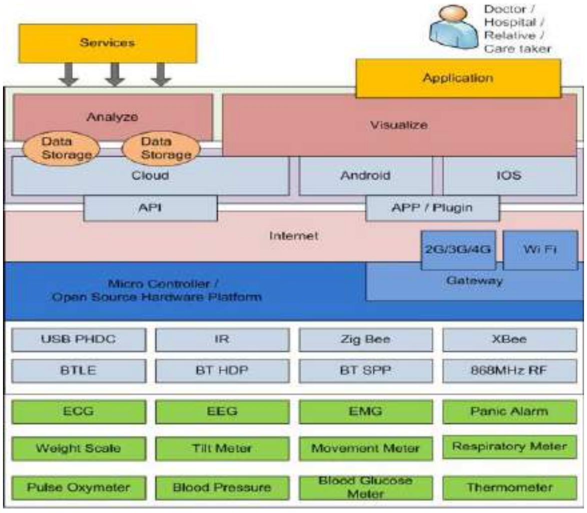


Fig3: Health Care

(iMedBox) to pursue various medical facilities integrated with sensors, devices, and communicate by means of WAN, GPRS, and/or 3G Services like intelligent pharmaceutical packaging (iMedPack) is enabled by RFID and actuation capability which are enabled by functional materials, flexible, and wearable bio-medical sensor device (Bio-Patch.Different types of health care are home health care,e-health,m-health,hospital management etc. As the time of data transfer over the network, if patient’s data is stolen or misplaced serious risk may arise which can cause even death to the user. In such sit-uation, it is noticed that most of the architectures do not include privacy, and security aspects into the respective concept which is drawback that needs to be clarified.

4. *Smart Society:*

In a Smart City, wireless sensor networks are the major sources of heterogeneous information generation. The information generated by different sensors often overlaps and is partial in nature. he main elements of the Smart City architecture to be smart health, smart environment, smart energy, smart security, smart office and residential buildings, smart administration, smart transport and smart industries[10]. For heterogeneous information generation, the sensor nodes deployed in each Smart City domain provide the primary data source. Using the existing communication services, information produced through the sensor nodes is collected. For example, the use of the satellite network for GPS devices, wireless networks such as GSM/3G/4G for mobile phones, and the use of the internet for raw data collection on PCs and other navigation devices. The information collected is then processed and analysed through the semantic web. Combination law, and Dempster-Shafer. The emphasis is on implementing the architecture as a software service on a cloud platform (SaaS).

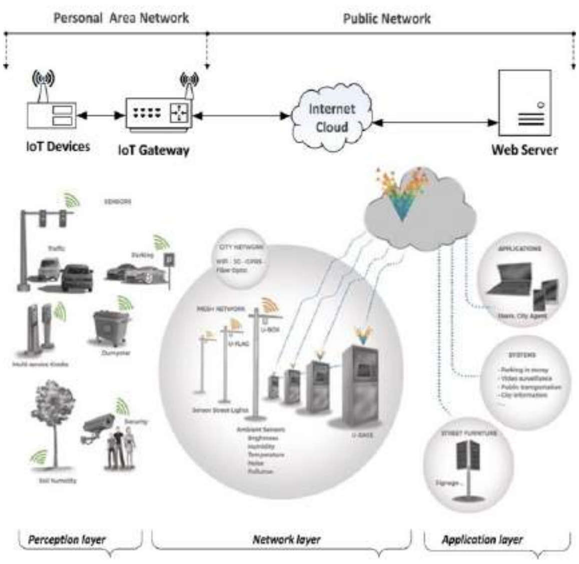


Fig 4. Smart Society

The different methods that can be used are Road conditioning monitoring, Traffic management, Smart city, Urban management, Smart environment etc .Issues that are related to smart society are Technology challenges with coverage and capacity, Digital security, Legislation and policies, Lack of confidence or reluctance shown by citizens (lack of clarity around benefits),Funding and business models, Interoperability, Existing infrastructure for energy, water and transportation systems[11].

5. *Cloud Service and Management:*

Cloud computing typically offers portal, infrastructure, and software as a service to customer systems in the form of pay-as-you go or free, for management, access, and processing purposes. IoT spans a wide variety of applications, covering businesses, governments and customers, and illustrates the convergence of systems from historically distinct communities:: Information Systems and Technology in Operations[12]. As a result, providing architectures, system concepts, and operations that can accommodate the interesting requirements of size, protection, reliability, and privacy is critical for IoT systems.

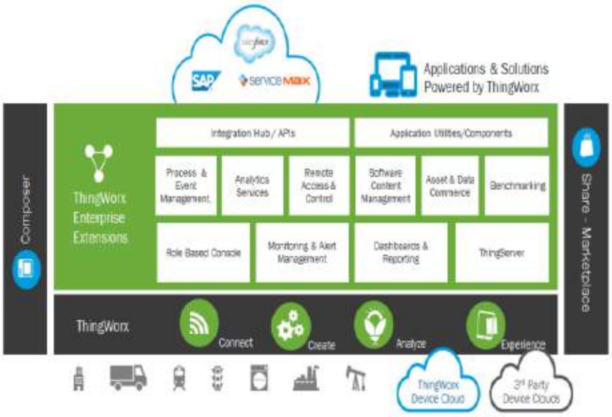


Fig 5. Cloud Service and Management

The different metholodigies that are used in Information exchange cloud, Vehicular cloud, Fog computing, Big data, Social Computing. Cloud infrastructure, IoT as services. Sensor discovery services etc[12The main concerns delaying the adoption of IoT Cloud Platforms are safety and privacy. Current IoT cloud systems can not always comply with requirements, thereby creating problems with interoperability. Heterogeneous modules or communication technologies may also not be supported by them.

6. *Social Computing:*

Different aspects of social computing currently being sought by IoT. Social IoT is a novel area of research that seeks to identify and harness the qualitative and behavioral values from robotic things while implementa-tion social rules upon them. Social Internet of Things-SIoT is proposed to seek various functionalities, such as: registration for a new social object to the platform, managing the system creation of new relationships, and creation of devices groups. This is innovative approach to integrated IoT with societal elements. [1]

Similar comprehension is seen through an open service framework for the Internet of Things which facilitates the IoT-related mass market by establishing a global IoT ecosystem with use of IoT devices and software has designed an architecture of social network of intelligent objects-Social Internet of Things (SIoT), where objects establish social rela- tionships among each other by enabling the capability of dis- covery, selection, and particular services. An open community-oriented platform has been investigated to support *Sensor Data-as-a-Service* (*SDaaS*) featuring inter- operability and reusability of heterogeneous sensor data and data services[1]. The concept behind virtual sensors and virtual devices are also identified to stream data continuously or discretely by scalable and context aware reconfigurable sensor data and services. The issues that can be raised are Lack of social media literacy, impact of social computing in diverse domain and complexity of features span diverse disciplines poses new challenges. different research issues such as trust and reputation, market structure, business.

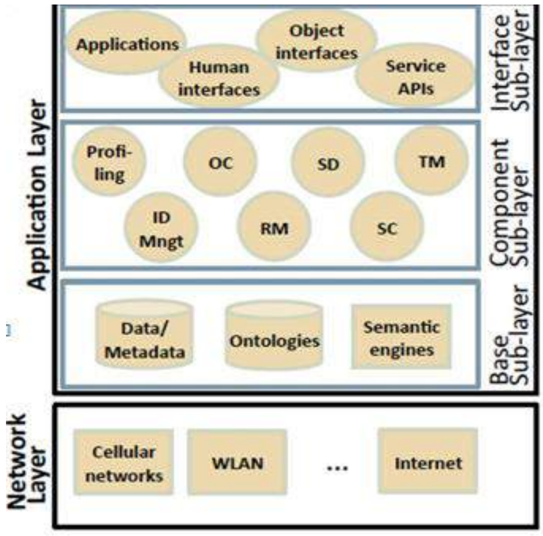


Fig 6. Social Computing

7. Security:

Security issue has always been an area where network related researchers are continuously striving to get through. IoT is not out of its scope. In this section a few relevant works are presented to cope up with architectural issues in IoT based security [1].

IoT can be used in various application in terms of security such that An End-to-End two way authentication security architecture for the IoT,

using the Datagram Transport Layer Security (DTLS) protocol has been evaluated. A cyber-physical-social based security architecture (IPM) is proposed to deal with Information, Physical, and Management security perspectives [1]. The IPM architec- ture is empowered by the Unit IoT and Ubiquitous IoT (U2IoT) architecture. U2IoT acts as the core of IPM provisioning three key supports, such as: establishing information security model to describe the mapping relations among U2IoT, security layer, and security.

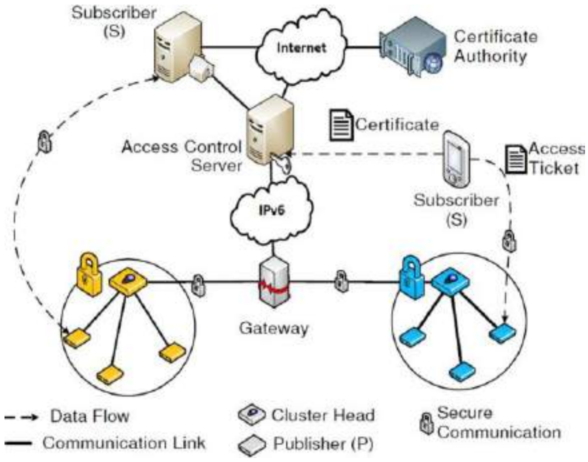


Fig 7. Security Architecture

requirement in which social layer and addi- tional intelligence and compatibility properties are infused into IPM; referring physical security to the external context and inherent infrastructure are inspired by artificial immune algo- rithms; and suggesting recommended security strategies for social management control.

A novel architectural approach-IoT NetWar has been proposed of inculcating advanced network based tech- nologies into the defense [11]. This is a 4-layered (i.e. Physical Sensing Layer, Gateway Communication Layer, C4ISR Management Layer, and Application Layer) invasion designed to assimilate IoT based integrated military commu-nication, intellectual intelligence, and C4ISR command under one roof. C4ISR Layer is the most crucial of all that specifically monitors the interactions between defense head quarter with its data center through voice collaborative support.

.

II. Analysis of Different Architecture: -

Domain	Architecture reference	Challenges and Issues
RFID	-EPC -uID -NFC and other Technologies -Beyond RFID	RFID readers and tags consist of a modern holistic framework where a specific identity will define each tag.
Service Oriented Architecture	-RFID Involvement -Middleware Enablement	SoA faces problems related to performance and cost issues. SoA has to deal with a large number of devices connected to the system that address problems with scalability. The transfer, processing and management of data becomes a matter of burden over-headed by the provision of services.
Wireless Sensor Network	-Systems -Environment Monitoring -Infrastructure -Agriculture -Aquaculture -Distributed Network	When designing a WSN driven device, energy consumption, scalability, reliability, and robustness etc. parameters are pursued.
Health Care	-Home Health Care -e-Health -m-Health -Ubiquitous Health -Hospital Management -WSN Integration	As the moment of data transfer over the network, if the data of the patient is stolen or misplaced, serious risk may arise that can even cause the user to die. It is noted in such situations that most architectures do not include privacy and security elements in the respective concept, which is an inconvenience that needs to be clarified.
Smart Society	-Road Condition Monitoring -Traffic management -Municipal Involvement -Link data for Society -Smart City -Accidental Measures -Smart Cycling -Home Entertainment -Smart Logistics	Coverage and capacity technology challenges, digital security, legislation and policies, lack of confidence or reluctance shown by citizens (lack of clarity on benefits), financing and business models, interoperability, existing energy, water and transportation infrastructure.
Cloud Service and Management	-Information Exchange Cloud -Vehicular Cloud -Cloud Infrastructure -Context Aware Services -Location Aware Service -IoT as a Service -Sensor Discovery Service -Fog Computing.	The key issues slowing the adoption of IoT Cloud Services are security and privacy. Current IoT cloud systems can not always comply with requirements, thereby creating problems with interoperability. Heterogeneous modules or communication technologies may also not be supported,.
Social Computing	-SIOT -Societal Data Service	New challenges arise from the lack of social media literacy, the impact of social computing in various fields, and the complexity of features across various disciplines. Various research issues, such as confidence and reputation, market structure, business models and interaction with customers.
Security	-Object Security -End-to-End Security -Cyber-Physical--Social Security -Hierarchical Security -Multimedia Traffic Security -Light Wight Security -Defense	Issues such as data security and privacy issues, secure restricted devices, high-accessibility malware and ransomed IoT cryptocurrency-oriented botnets.

Table 1. Analysis of different architecture

III. Proposed Novel Architecture:

As IoT is mostly used in all the application in day to day life. So Architecture are gaining importance and it will be an important foundation in IoT . So a novel architecture need to be proposed as fundamental model in which the layered components and how they will be connected to each other. Research regarding the new framework based on the architecture that covers the following areas such as governance, tourism, social, defense and security aspects need to be elaborated.

IV. Modern application, Security aspect and Future Scope.

Modern Application

other uses of IoT technology or the Internet of Things, are concerned with offering an innovative approach to quality of life, urban challenges, food production, agriculture, manufacturing, medicine, energy supply, water distribution and how to offer a wide variety of products and services [4]. The next generation IoT applications and their services, such as smart factory and smart city, require special attributes, as follows: Support of Variety of data types, Support a high number of customers and demands, Agility, Flexibility, Robustness of connection, Low Latency Reliable Communication.

Security Aspect

The Internet of Things needs to be designed in such a manner as to ensure that Clear and safe user controls. Consumers need trust in order toIn order to gain the future advantages, use the Internet of Things

- Data Confidentiality

Data security is a central concern in the IOT Scenarios, showing the assurance that only approved Data can be accessed and updated by organisations. Data protection could not be extended explicitly to Owing to two major restricting variables, IOT contexts. The first one The huge amount of data produced by such systems is worrying. It is also connected to scalability problems. Security is a big issue with IoT devices. With billions of devices being connected together over Internet, how can people be sure that their information is secure? These security issues can be of the following kinds. The widespread applicability of IoT and associated technologies shall largely depend on the network cum information security and data privacy protection [5]. The other issue is linked to It focuses on the need for online and flexible control of access to data, with access rights shifting during runtime and being extended to dynamic data sources.

- .Privacy

By ensuring that people can regulate which one of their own is The collection of personal data, who is collecting those data, Privacy should be secured if and when this occurs. In addition, the personal data collected should be used only for the purpose of with a view to promoting authorised services by authorised services, Providers of Utilities. Creation of new strategies for compliance, capable of Help the IOTT-characterized scale and heterogeneity scenarios. People be sure that their information is secure? These security issues can be of the following kinds. The widespread applicability of IoT and associated technologies shall largely depend on the network cumin formation security and data privacy protection. The other issue is linked to It focuses on the need for online and flexible control of access to data, with access rights shifting during runtime and being extended to dynamic data sources.

- Trust

The key issue in several approaches to confidence. The definition is that the establishment doesn't lend itself with metrics and methodologies for measurement [5]. Introduction of the vocabulary of simple confidence negotiation, Description of a Framework for Trust Negotiation, Creation an adequate identity management scheme of artefacts, Design of a general and scalable system of trust management

Future Scope

The future research should consider the fallowing objective to make designing and development of IoT will be of great help to various application of IoT, These includes: The design of IoT architecture and its management. Characteristics of different IoT applications and service requirements. Security and privacy of architectures. The different user interaction with architecture. Realistic energy consumption of architecture.

V. Conclusion:

Thus we have studied different architectures of internet of Things that are being used in various different domains. Each architecture has a specific challenges and issues that need to be satisfied and the way in which IoT is expanding. Security is the area that need to be look out. As a new industry, the IOT will encounter various security challenges in further development and application. In this paper we have discussed all the parameters of different IoT architecture.

VI. REFERENCES

[1] P.P Ray A survey on Internet of Things architectures [J]. Journal of King Saud University – Computer and Information Sciences (2018) 30, 291–319

2] Li Xianmin, Han Xiao. On the Security Architecture of Internet of Things[J]. Enterprise Technology Development,2015,34(18):80-81.

[3] Li Zhongnan. Research on Security Architecture for Application Layer of Internet of Things[D]. Dalian Maritime University, 2013.

[4] Li Panlong. Research on Security Architecture for Application Layer of Internet of Things[J]. Computer Disc Software and Applications,2014,17(16):41-42.

[5] Wu Chuankun. A preliminary discussion on the security architecture of Internet of Things[J]. Proceedings of the Chinese Academy of Sciences, 2010, 25(04):411-419.

[6] Wang Boshi.Discussion on Security Architecture of Internet of Things[J]. Information Network Security,2016(S1):137-140.

[7] Wang Huan.Research on Security Architecture and Key Technologies of Internet of Things[J]. Automation and Instrumentation,2016(08):80-81.

[8] Ma Yalei. Research on Security Architecture and Key Technologies of Internet of Things[J]. Electronics Production,2017(11):84-85.

[9] Li Zhiqing. Security Architecture and Key Technologies of Internet of Things[J].Microcomputers & Applications,2011,30(09):54-56.

[10] Gao Chong. Security Architecture and Technology Route of Internet of Things[J]. Information and Computer(Theory),2017(15):149-151.

[11] Ren Wei.Research on Security Architecture and Technology Route of Internet of Things[J]. Information Network Security,2012(05):70-73

[12] T. Gruber, Toward Principles for the Design of Ontologies Used for Knowledge Sharing. International Journal Human-Computer Studies, 43(5-6), pp. 907-928, 1995.

[13] I. Niles and A.Pease, Towards a standard upper ontology, Proceeding of FOIS ’01, pp. 2-9, 2001.

[14] N. Guarino, Formal ontology and information systems, Proceedings of FOIS. Vol. 98., 1998 [4] M. V. Assem, et al., RDF/OWL, Proceedings of The Semantic WebISWC 2004: Vol. 3. pp. 17-23, 2004.

[15] Satyanarayanan, Mahadev. "The Emergence of Edge Computing." Computer 50.1 (2017): 30-39.

[16] Songqing Chen, Tao Zhang, Weisong Shi, “Fog Computing”, IEEE Internet Computing, 2017, pp. 4-6.

Cyber Security-Modern Era Challenge to Human Race and it's impact on COVID-19

DR. SUMANTA BHATTACHARYA
BHAVNEET KAUR SACHDEV

Cyber Security-Modern Era Challenge to Human Race and it's impact on COVID-19

Dr. Sumanta Bhattacharya

Cyber Crime Intervention Officer under NSD ,Associate Member of National Cyber Safety and Security Standards, C.E, Ch.E, Zonal advisory at Consumer Rights Organization

Bhavneet kaur Sachdev

Political Science (Hons) Calcutta University , Post Graduation Diploma in Human Rights, Indian Institute of Human Rights.

Abstract

Cyber crime bloomed from the early 2000s when social media came into picture and people started uploading their personal information on different social media site which resulted in the rise of ID theft , which further resulted in different types of crimes like cyber bullying , child pornography, sexting , online sextortion and the gaming world which has also become a place of cyber crime, where everything happens on a digital platform and there exist no direct involvement , with the advance in technology and the use of Internet of all kind of official and unofficial purposes , simultaneously there has been a rise in cyber crime cases, cyber crime is an unlawful act and it is done using an electronic device. With the rising of COVID-19 situation , a global pandemic we see a rise in the number of cyber crime specially against women and children , in every 10 minutes a cyber crime case is reported ,debit/credit card fraud are at a rise with everything going digital . Today India has 650 million Internet users .

Keywords-Cyber Crime, Covid-19,Cyber Space, Going Digital.

Introduction

Cybercrime is unlawful acts. This affects the computer data or systems. These are illegal acts where a digital device or information system is a tool or a target or it can be the combination of both.

Whenever an act is done with any Ill intention or with Mens Rea, and it is also done accordingly, then we call it an Offence.

To the law, the wrongful act is an offence and to the Society, it's a Crime. So Cyber Crimes are no doubt it is an Illegal Act to the Society and also the state, thus in the eye of law it's offences are punishable.

It's Blessing of the technology that in this pandemic situation all the communications and transactions can be done through the internet without getting direct touch with the Human Society, It also raises the Questions of Law and Justice when a person is being affected or becomes a victim of the Cyber Crimes.

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW made a global framework for the formation Electronic Commerce and being the signatory to it, India with their mutual legal provisions and model of Law, India Adopted the Information Technology Act.

Now is the Digital Sphere due to increase of the Digital Equipments it is inevitable to amend the existing laws on this regard. It not only influences the E-Commerce laws but also made an Impact on Indian Penal Code, Code of Criminal Procedure, Indian Evidence Act and other statutory acts related to it. So there were certain Changes done safeguard laws in the Dynamic Digital Sphere which has taken place in the last decade. So this way Information Technology Bill was introduced in the parliament and soon the IT Act of 2000 came into force. Slowly due to the rise of the Internet users the Cyber Crime cases started to increase and it has taken a high rate of growth in the last decade.

Similarly the Indian laws were gradually amended according to the necessary changes and it also made various structural changes in the procedural laws also to secure cyber safety and do justice.

Cyber Crime

The cybercrime can also be called as electronic crime, e-crime, information age crime, high technology crime. In simple words, we can say that cybercrime is the type of crime in which there is the use of a computer or digital system to do unlawful or illegal acts. As there is no specific definition of cybercrime given in the IT ACT 2000, its definition may be accepted in a wider aspect. Cybercrime can be committed in two ways – one in which a computer is a target of the cyber attack, and the other is which a computer is used to commit a crime against a person. The alien mark of cybercrime is that the sitting target and the felon will never have a face to face junction

Cyber Crimes are not needed to be committed through online, the Crime can be a combination of both online and offline as well.

Types of Cyber Crime

1. Child pornography

Child pornography also known Child sexual abuse material, is a kind of pornography where children are stunt for the purpose of sexual excite. It is assembled either by direct participation or through sexual violence/assault of a child or called child sexual abuse images.

2. Cyber Bullying

Cyber bullying also known as online bullying where a person is harassed through the medium of an electronic device such as laptop , computer or mobile phones . It can also happen through Text online apps, social media forum and many gaming apps in which people share and get involved .It incorporates , projecting or sharing detrimental content about someone else on an electronic platform.

3. Cyber Stalking

Cyber Stalking involves the use of electronic devices to plague someone , track a person or try to communicate with a person who is showing complete disinterest , Cyber stalking is done by sending e-mails , messages etc . It can target an individual , organization or a group .

4. Cyber Grooming

Cyber Grooming is a process by which an adult tries to build an emotional relation / connection with a young person with the intention of using that person for sexual activities and trafficking .

5. Online Job Fraud

Online job fraud are at a rise with everything going digital , its a fake job scam which aims are stealing personal information about the users .This is very common in cases of work from home job market. It uses false application , false money transaction , false advertisement to get access to an individual data and information. With the global pandemic and lockdown situation , many people have lost their jobs in private sector , and work from home is the order of the hour and everything going online , there has been a rise in online fraud cases with people looking for jobs online , many people have become a victim of online job fraud.

6. Sextortion

Sextortion is a crime which happens on an online platform where a person is forced or threat to send or share sexual pictures of his or her online or present sexual favours on a webcam .Sextortion can happen on any site , dating apps or even while playing online games.

7. Vishing

Vishing is an electronic fraud in which individuals are mislead by unauthorised entities to provide personal information and finance related information like Banking password ,OTP, ATM PIN etc using mobile phones .Vishing can be done without using Internet also .

8. Sexting

Sexting is the practice of taking sexually picture of yourself typically from a cell phone and sending it to someone , it also includes steamy text messages.

9. Smshing

Smshing is an artifice that uses the tool mobile phone to send text messages, pretending to be from well respected companies so that individuals are convinced to disclose their personal information such as credit card or debit card details , ATM PIN etc.

10. SIM SWAP SCAM

SIM Swap Scam is a type of subterfuge where the attacker intention is to get hold of your personal information , so that they can get access to your bank account. It is a kind of buyout account fraud generally aims a fragility in two-component validation and two-pace confirmation .

11. Debit/credit card Fraud

Debit or credit card fraud refers to the unlicensed utilize of credit and debit card or alike payment tools to illegally obtain money or property. Credit or debit card number can be acquired through unsecured websites or through the identity theft scheme.

12. Impersonation and identity theft

Impersonation and identify theft refers to an artifice where a person uses other person’s personal information such as password , electronic mark for economic purpose.

13. Phishing

Phishing is a kind of cyber attack that uses email as an instrument to gather personal/ sensitive information of a user like bank account details , password. The aim is to mislead the beneficiary through mail saying that this message will provide them maximum benefit bu downloading a link or attachment .

14. Spamming

Spamming happens when a person accept an unsought trade messages by email, SMS, or any other alike electronic means . They may try to coax the beneficiary to purchase or avail a service, or visit a website by which can try to ruse him/ her into imparting bank account or credit card details.

15. Ransomware

Ransomware is a kind of malware that encodes a users files, designed to block or limit the users access to his or her system until you pay an amount as ransom .

16. Virus, worms and Torjan

Computer virus is an application to enter into your computer or laptop to damage files and data and then replicate themselves.

Worms are destructive programs which spread copies of themselves from one computer to another and can replicate themselves without human involvement and does not require to connect themselves to any software to cause damage .

Torjan horse or Torjan is a kind of software which is planned to destroy,disarrange or steal or impose some harmful exertion into your data or network.

17. Denial of Service Attack

Denial –of-service attack is a cyber attack by which computer and other devices becomes unavailable to the intended users by interrupting the device's functioning . DoS attacks functions by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed .A DoS attack is characterised by a single computer to launch the attack.

18. Data Breach

A data breach is a security occurrence in which data can be obtained without sanction.

19. Website defacement

Website displacement is an ambush on a website which changes the perceptible image of a website or a web page. The attacker might try to upload sensitive images , videos etc on the web page.

20. Online drug trafficking

Online drug trafficking means selling and purchasing of drugs on an electronic platform ,Drugs are traded on the dark web , using cryptocurrency

21. Espionage

Espionage or spying is the process in which you get access to the user's data and information without their knowledge .

Being a vast sphere, this cyber crimes and its procedure to lodge a Fir is quite complex and this results a confusion to the victims to understand how to lodge a complaint or Cyber Crime FIR. Unlike general FIR Procedures that is lodged at police station, the Cyber Crime FIR procedure is lodged at Cyber Cells in various cities all around India. The first city to register a Cyber Cell was Delhi, there after Visakhapatnam, Chennai, Hyderabad, Bangalore and lastly Kolkata. The Cyber Law has a Global Jurisdiction, that means if a Person has suffered a Cyber Crime at his Place at Bangalore but presently he is at Kolkata, he can complain at Kolkata and it shall be sent to Cyber Cell of Bangalore and FIR will be lodged there.

India's progress towards a vision of Digital India is also a Very Important factor that has taken a 'J' Curve in the growth of the Internet users in India. This began with the demonization in 2016 and a huge number of people started to use the Online Transactions in a one night wonder. Gradually Online Applications and Transactions started to increase and people started to connect their online businesses with the online platforms. The growth rate continued with the availability of affordable handsets that started to sale along with the affordable data packs. Today almost 650 Million Internet Users are in India.

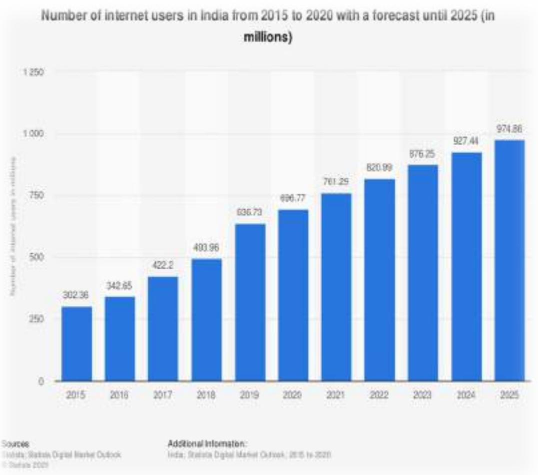


Figure 1 : Number of Internet users from 2015 to 2020.

Thus there is vast number of User of the Internet who uses the Internet for the Business that saves the Rent of any Store and the other Charges for a Shop that needs any Physical Existence. This also created a possibility of Cyber Crimes that takes place with the users, not only in Economical aspect but also in Social Aspects also.

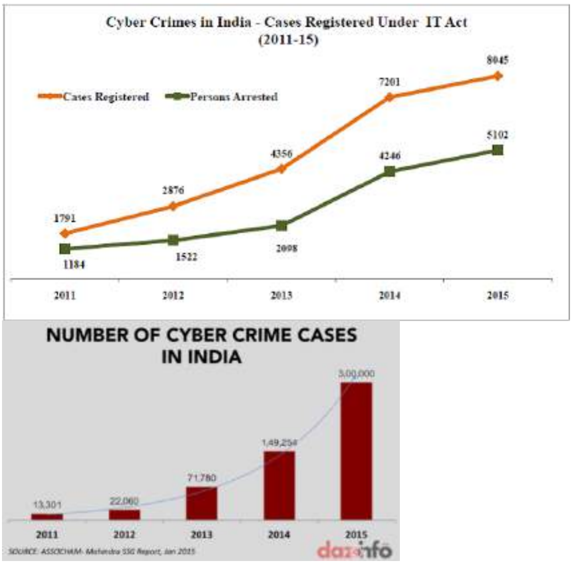


Figure 2 and 3 : Show the rise in cyber crime cases from 2011- 15

In a Study it has been found that in India after 2016 one Cyber Crime is reported in Every 10 minutes. The Cyber Crimes against women and Children is also rising. Thus Cyber Cells are developing their sphere and under Section 150 of the CrPC , the Global Jurisdiction of Cyber Crime features to lodge a complaint in any nearest Cyber Cell of the Victim, no matter from where the offender's I.P. Address belongs, the police officer shall transfer the matter to appropriate Cyber Cell.

The COVID Situation necessitated the growth the Internet Users and Online Transaction. For the first time ever, the whole world is doing Online Meetings irrespective of Government and Private Organisations. The Online Classes and exams are also being taken officially. All these things made increase on the Rate of Cyber Crimes in the whole world including India. These Cyber Crimes are not only limited to Civil matter but also Criminal and International matters as well

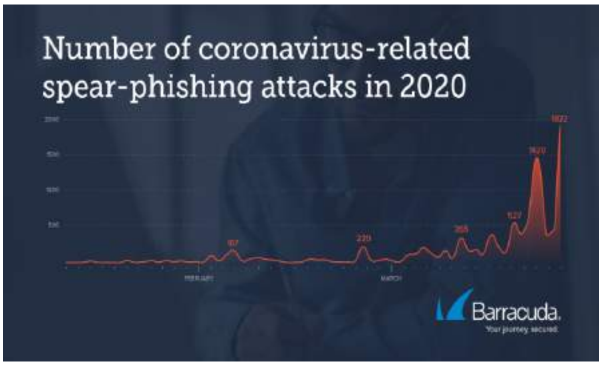


Figure 4 :Diagram shows rise in cyber crime cases during COVID-19

Covid and rise of cyber crime

After the rising of the COVID situation the Cyber Crimes tent to rise in India as the Internet users are using more and more Internet facilities for the purpose of " Work from home" and to keep themselves connected with Social media in order to socialize and keeping alive their creativeness and social interaction that maintains the motto " Stay home, stay safe" This has led to the magnification of Online businesses, meetings and online classes which has resulted in the mandatory use of Internet by Childrens.

All these factors creating a situation that giving internet access to minors and other digitally incompetent persons who have less awareness and knowledge on the Technical and Internet material.

This is no doubt a high time for Hackers, Cyber Terrorists, and Cyber offenders to commit various kinds of Cyber Crimes in huge numbers.

The rate of Cyber Crimes was eventually rising up to 86% during March April of 2020 after the Lockdown Effect of the COVID Issue. The Cyber offences are quite becoming creative in nature also like Fake Fundraising links that appears behalf of the Government, Fake News that Offers or gives access to Corona Virus safety tips, Fake Job offers, Fake Flash Sale offers, Fake Recharge offers of Data Packs and Free Internet with unlimited calling offer, Fake Apps etc. Beside these Civil misconducts, there are Criminal Acts as well like Sexual Offences through internet against Women and Children. The more untrained users are having compulsory access to the internet, the more they are being affected. All these factors have resulted a huge rise to Cyber Crimes during the COVID situation and the rate is still increasing.

Here are some types of Offences faced by Internet users in India During COVID19 :

Increase in phishing attacks:

During this COVID Situation, the Phishing attacks rate increased. These Emergency situations, Lockdowns and other serious matters became created Confusion to the public that they are scrammed by fake apps and Fundraising Links. The more people are being engaged with Charity or Religious institutions and NGOs, it is also creating more confusion and trusts with such links to the common people. Since

January 2020, one of INTERPOL's private partners, Trend Micro, detected 907,000 messages linked to COVID-19 . Taking advantage of the economic downturn and people's anxiety during the pandemic, cybercriminals have enhanced their social engineering tactics by using COVID-19 as a basis in their attacks

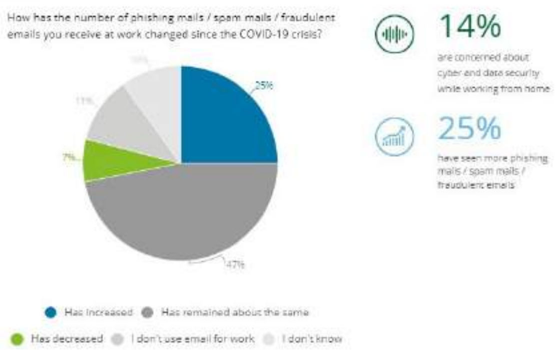


Figure 5 : Increase in Cyber Crime cases over the years especially during Covid-19

Fake Job Offers and Frauds:

During this COVID Situations a huge mass of people lost their jobs especially in the Private sector, they anxiously were searching for new jobs and facilities like earning money from home. Beside the jobless, there were many unemployed people including women and students who were looking for new jobs especially OnlineJobs and earning opportunities they faced so many Fake Job Offers and Frauds that resulted to a huge loss of money.

Fake News or Rumours:

With fake job offers and phishing, there have been large numbers of fake news as well. For example, the fake news of "Chicken carrying Corona virus", Hot water treatment of Corona at home etc.However, some of the measures were taken by the government specifically in a few regions. The Whatsapp Messages that used to contain any word relating to Covid-19 used to be tracked and the Group Admins were held liable for spreading fake news in some cases. The fake news relating to Corona Virus was taken very seriously and specifically in Hooghly the Internet Connection was banded for a few days to stop the spread of fake news and other fake data relating to COVID and lock situations. It was also taken into action just to stop the Rumours relating to community clashes. But however, in spite of these efforts to the spread of fake news, it failed

Fake treatments and Fake Anti-Corona Medicines:

One of the most irritating contents that were ever shared and spread in Social Media and Online selling website that is fake treatments and anti-COVID medicines that would have been able to cure any person of the corona by boosting up the immune system. Various Popular brands were also engaged in such things against which legal action was taken later on. This resulted in fraud in the medicine business and those who were engaged with it were legally charged.

Sexual Crimes against Women and Children:

The most burning social problem during COVID is the Cyber Crimes that are faced by Women and Children. The COVID Situation necessitated the Online Classes that are taken by Female teachers to the minors and Students who are not well trained in the Online Platform.

It has been seen in many recent cases due to the Excitement of adolescence psychology of the teenagers they have engaged themselves in sexting and sharing their private photos. Although it is a consensual act, those contents were misused in pornographic show business. There are examples of many cases where the children have been brainwashed to share the Debit Card Pin code or OTP that is received by the device they are using during class. Several Children's games are there on the phone which uses the children to expose them and share the OTP or passwords. The Phones are also being used as a device for tracking, kidnapping, and Black mailing.

Infodemic breakout in Social Media :

The Term Infodemic means a massive spread of any information irrespective of true or false that takes place in a short period of time relating to a particular interest or subject.

During the COVID Situation, there were more than 361,000,000 Videos were Uploaded on Youtube relating to COVID and 550 million tweets included the terms Corona virus,

COVID-19. etc. Besides these millions of rumours, Videos and written information were shared in Whatsapp relating to COVID and Lockdown. All these factors created a Confusion in Social Media Users who does not even know how to verify this information. This was one of the worst examples of infodemic ever seen.

Violation of the Right to Privacy :

To track the COVID Infodemic situations through the internet and Social Media, the Government launched various policies that shall track the Information shared through social media by the public. However, it raised a Paradoxical Situation that violated the Right to privacy as well. Right to privacy is a Constitutional Right of every Citizen of India, the exception of the right came in to force when the government started to trace the Personal Data of the devices and also launched various apps for public services that used to have access to Contacts of every smartphone. The Violation of the right to privacy was not limited to the government and public, there were so many hackers and specially programmed Apps that used to share information and personal data of smartphones through its hidden access features. So many women were harassed sexually as their images were used in pornographic purposes and the hacking of Phones and unauthorized money transactions had been very common.

Business-related frauds :

As the online transactions and Social media became very popular during the COVID situation, it gave rise to a huge number of Internet users as well as Consumers. There were a huge number of cases of fraud relating to business. Some of these examples are:
Online Education Applications Scams, Supply Scams, Counterfeit of Drugs, Covid19 Testing and Treatment Package Scams,Duplicate Products related Scams, Healthcare Service Scams, Charity, and Investment Scams.

All these types of Scams raised a huge number of Business related Scams most of which resulted to frauds.

Online Gaming and gambling-related frauds:

During this COVID situation, it was a golden opportunity to get rich by playing gambling online. This resulted in a huge number of frauds that were found fake and many games were related to this gambling which affected a huge number of internet users. These types of frauds are nonjusticiable and illegal itself, that's why the victims were helpless.

Other types of Crimes during Covid:

Besides the above-mentioned crimes, there were few more infodemic kind of crimes that affected so many internet and social media users some of the examples are:

A. Aadhar Card Update related frauds,
B. KYC Update related frauds,
C. Pan Card Linking related frauds,
D. Banking related online frauds,
E. ATM card related frauds,
F. SMS Spoofing,

All these types of social-economical or business-related factors resulted huge numbers of cybercrime cases during the COVID Situation.

Dark Web

The dark web is an untouched part of the internet in general that normal internet user does to have access to it. But the untouched area of the Internet world has a lot to do with cyber crimes as those areas of the internet deals with various illegal activities both in respect of the internet and society. This untouched area of the internet is known as Dark Web. There is no specific data that shows how much users are engaged with such activities but one thing is for sure that it exists and cannot be banded for its illegal activities.

The dark web is not discussed in Legal Researches and Legal Discussion as It is ambiguous matter to itself. There is no exact process to have access to this part of the internet and there is no specific website or procedure to work with it.

It is an Eco-System itself as it has its own Economical Currency and process of business. Mostly it deals with illegal and mysterious activities like selling Human Flesh, Child Pornography, hiring of serial killers, Hacking activities targeting the government websites, selling of arms and drugs, Human trafficking business, etc.

Dark Web runs on Tor Browser and the websites are encode .There are other encryption tools and corresponding browsers such as I2P (these are not universal, by design) and you have to know the exact URL in order to access the site like onion is a section particularly used on the dark web.

Another coating of invisibility is the method of payment. Silk Road, for example, only accepted payment via Bit coin, which is an unregulated crypto currency. As with the Dark Web generally, there's nothing illegal about using Bit coin. But the anonymity of Bit coin payments is attractive to those making illegal transactions.

This Dark Web helps to commit various offenses to international Criminals. The secret societies use this Dark web to communicate their tribe members. Various Dark Web Activities has been arrested by the laws in various parts of the world, for examples:

Any type of crime with covert transactions, whether it involves drugs, money, or even human beings, can be committed on the Dark Web, some of the crimes include Murder for Hire, Blackmail/Extortion, Illegal Drug Sale, Illegal Arms , Sex trafficking and Terrorism. There has been a rise in dark web crimes over the years and this COVID-19 has provided dark web with the opportunity to gain as much as possible on a global scale .

Conclusion

Cyber Crime is an amplified topic , with the advance in technology we see an increase in the number of cyber crime cases. After the rise of the COVID-19 situation , the rate at which cyber crime tent to increase as Working from home has become the need of the hour for economic gain . Every incident is taking place on a digital platform .The reliance on technology has amplified since lockdown all over the world and we see a rise in cyber crime cases globally . Online traffic has soared due to continuous video conferences, online classes , meetings etc. We have also seen an increase in the mode of payment which has gone online and the uses of apps like paytm , google pay and phonepe for money transaction which has increased the cases of bank frauds, SIM SWAP Scam to a great extent .Now that everything is being done only both official and unofficial work using laptops and computers. Hackers are creating virus and fake website which can directly attack the system and trap the users , there has been a rise in phishing , hacking at companies and offices , cyber bullying , debit and credit frauds and many other cyber crimes are taking place in India. There are many cyber laws existing in India , The Information Technology Act 2000 , which deals with cyber crime , cyber laws and provides remedies and punishment The Cyber Laws and Policies in India have various loopholes in respect to their implication in various sectors. The Vision of Digital India also Includes Cashless Economy that means all the banking and E-Commerce Transactions shall be done digitally through E-Banking, Net Banking, and Online Payment, etc. However, in this Present Situations, there are many loopholes in the Cyber Laws and Policies that are needed to be looked upon. In many cases, it has been found the Apps which used in the Online payment, net banking, and other Digital Platforms take access to SMS, Debit Card details of the customer by which the Bank Account details are passed on through the Apps without leaving any mark. For the first time ever in the world, Pornography has gained popularity in public without any Charge and that is easily available over the internet. Porn websites have the largest growth in the Digital Economy. However, Pornography is compromised of Legal and illegal provisions. The most obsessive nature of those Websitesare that in most cases cannot do the Age verification of the visitors. Although the publication of these pornographic contents Social media is illegal however it is not quite effective in practice. , Child pornography is strictly banned and illegal all over the world but due to lack of legal Sanctions, the high consumption of the internet, lack of taxation, lack of security provision the pornographic contents remained uncontrolled obscene publications all over the world. There are potential cyber security challenges like lack of cryptographic measures , poor encryption key management , non-existent secure devices on boarding services, weaponized machine learning technologies by cyber attackers , lack of knowledge of social engineering and insufficiency antimalware software , DDoS attack . We require a strong cyber security system in India and we need to make strong policies and laws to control the rate of cyber crime in India and the development of more cyber cells in every city and state.

References

1.Sarfaraz Shaikh , June 19, 2020 ,Cyber crimes go up in lockdown .

2.Inhof Robert, “Cyber crime and Telecommunication law “(2010). Thesis .Rochester Institute of Technology .

3.Melissa E. Hathway and John E.Savage , Stewardship of Cyberspace (2012), Cyber threats and cyber realities:Law , policy, Regulation in Business , the Professions and National Security.

4.Sushant Kulkari , May 20,2020 , In Maharashtra , 400 cyber crime cases filed on covid issues , mos on hate speech and communal accusations.

5.Press Trust of India , Kanishka Sarkar , June 28,2020 Business e-mail compromise most common online fraud : Delhi police.

6.Ministry of Communication and Information Technology, cyber crime,cyber security and Right to privacy.

7.A.R Raghavan and Latha Parthiban , The Growing case of cybercrime and types of cyber crime on a Global Scale.