International Journal on Communications Antenna and Propagation (I.Re.C.A.P.), Vol. 7, N. 6
ISSN 2039 – 5086
November 2017
Special Issue on “ICMESCoE-2017”

A Survey on Evolution in Information Security

A. G. Vitekar, P. N. Kota

Abstract – *Information Security is relentlessly progressing and staging steadfast growth in many fields. This survey bolsters the belief that security will remain zestful and tumultuous. The Daily News asserts that cyber-attacks are not just a seasonal threat or dependent on specific industry environmental traits, but are constant and should remain forefront in every enterprise executive board work. Information Security is becoming popular by providing services like Cloud Security, Systems Security, Network Security, IOT Security, Automobile Security, Web-Application Security, Wireless Security, GSM Security etc. This survey paper focuses on the briefing of Information Security, on the fields in which Information Security is exponentially emerging and on new research trends in this area.* ***Copyright © 2017 Praise Worthy Prize S.r.l. - All rights reserved.***

***Keywords**: Information Security, Anonymity, Banking Security, Cyber-Terrorism, AI Security*

I. Introduction

Information Security is booming and it is the most advanced field in computer science that has evolved so vastly. Information security, also coined as InfoSec, is the focused on preventing unapproved access, disclosure, disruption, alteration, inspection, recording or ruination of Information [1]-[22].

It stands on the principles of three important pillars i.e., the CIA triad, which symbolizes Confidentiality, Integrity and Availability.

As new technologies burgeon into everyday life, new technologies are giving birth to different forms of information security. With the evolvement of innovation, there lies a question about the certainty of those technologies.

With the recent development and popularity of technologies like Internet of Things (IOT), Electric cars, Online banking, Cryptocurrencies, Healthcare/Medical, Telecommunication, Programmable Logic Controller (PLC) and Supervisory Control and Data Acquisition (SCADA), Transportation Systems, Artificial Intelligence (AI), Big Data, Machine Learning it has become necessary not to just develop these technologies and take them to the next level, but also to work on their security layer in digital as well as physical form to ensure individuals privacy and safety.

With new protocols being developed like Internet Protocol version 6 (IPv6), IPv6 Low Power Personal Area Network (6LoWPAN), Hyper Text Transfer Protocol Secure (HTTPS) / Hyper Text Transfer Protocol (HTTP) 2.0, it has become necessary to inspect the security policies that are being implemented with these protocols and also whether these protocols work up to the mark with the applications they’re being embedded with.

As per, Whitman, et al. [1] organizations are exposed to cybersecurity threats from within the organization and from the outside world.

The total financial losses due to computer breaches accounted approximately about $455,848,000 in 2001.

Still, Information Security remains ignored by top managers, middle managers and employees alike. The underground cyber economy is significantly growing due to a variety of factors like social media, economic slowdown and an increase in the number of internet users. [2]. According to the survey’s conveyed by Gordon, et al. [3], it was found that 91% of the security breaches were detected within 2001. This year was seen as the beginning of security breaches. The study also concluded that the total financial losses occurred by each organization approximated over $2 million. But it all doesn’t end here, the information security system management has been playing a vital role in top organizations and it is a necessity for each and every organization to have an Information Security Officer for risk assessment and management [4].

Economically, each and every nation in today’s modern world needs a good and effective cybersecurity plan to fight against cyber-attacks and prevent the same in the future [5]. Information security management has also some adverse effects if proper measures are not taken. As per Solmsa, et al. [6], few of the deadly sins in information security management are:

(i) not realizing that information security is a corporate governance issue.
(ii) not realizing that information security is a business issue and not a technical issue
(iii) not realizing that information security plans must be based on identified risks etc.

On a technical note, sophisticated attacks like side channel attacks on elliptic curve cryptography algorithms (the algorithms used in building cryptocurrencies) [7], various mis-configurations vulnerabilities like outdated versions of Secured Socket Layer (SSL)the encryption protocol present in web –applications [8] also in wireless

https://doi.org/10.15866/irecap.v7i6.13347

networks malicious nodes, can frame innocent nodes as clone nodes and clone nodes as innocent nodes which leads to framing attack.

This all leads to privacy evasion and data loss. This also tells that taking small measures and securing devices from these attacks will secure an individual's life.

In this paper, the different technologies used in everyday life have been surveyed and analyzed, as well as their impact on vulnerable systems, which leads to data loss, identity theft and other privacy issues.

After the survey, the final conclusion is that avoiding updating systems and applications from time to time and being casual about privacy could lead to disasters like ransomware attacks, cyber terrorism threats or even banking fraud. The different fields in which information security has rapidly evolved are contemplated and proved to be an important aspect in providing privacy and security at different layers.

II. E-Banking Security

II.1. E-Banking System

The basic structure of online banking is shown in Fig. 1. In any E-Transaction, the user first turns on the personal computer (PC) and launches a web browser to access the online banking website and enters the User ID or Personal Identifying Number (PIN) and the password by using the keyboard or a virtual keyboard.

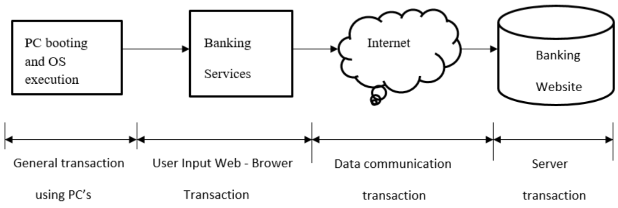


Fig. 1. Basic model of an E-Banking system

The SSL (Secure Socket Layer) encrypts the data transferred between client's PC and bank's server.

The server on the bank's end decrypts the transferred information and processes the user's authentication, account inquiry, account transfer [10].

During this whole process of transaction there lies a very great chance of the user leaking its sensitive data like the user account and password having a virus or keylogger installed on his computer without his knowledge or even if the user saves his login information in the browser the browser may leak data to a third-party software or even the browser can be compromised. The Vulnerabilities in the E-banking system can be from user's side as well as from bank's side (Sehgal, et al. [10]).

From Fig. 2. it is clear that most vulnerabilities are found in protection mechanism i.e. the encryption algorithm used or the application on which the transaction is taking pace or what standards are maintained while the transaction takes place i.e. the length of the password etc. [10]. Fig. 3 states that the most common vulnerabilities found are associated with software information disclosure and predictable user ID formats (57%). More than half of the systems (54%) were vulnerable to Cross-Site Scripting (XSS) attacks.

The exploitation of this vulnerability could grant the attacker to obtain access in the context of the targeted user if the victim navigated to a specially crafted website.

The vulnerabilities that caused attacks on user sessions also accounted for 54% session security attacks which include improper session termination, incorrect cookie settings, multiple sessions under one account, or a lack of association between user sessions and client IP addresses.

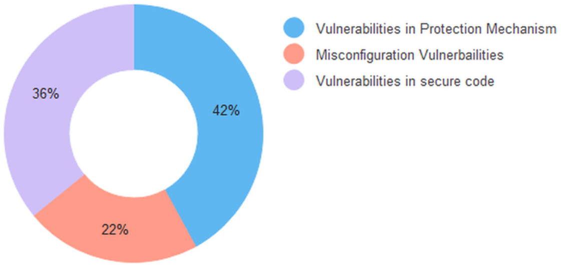


Fig. 2. Classification of Vulnerabilities

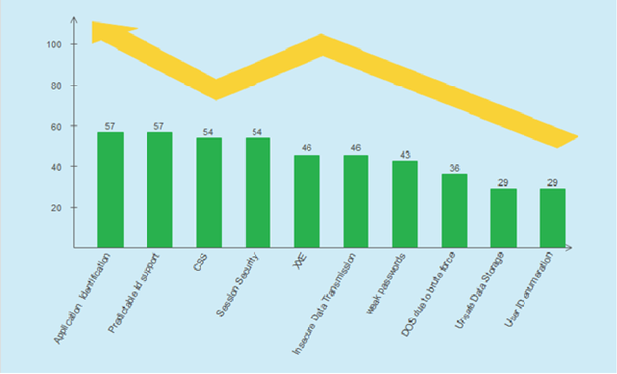


Fig. 3. Different types of Vulnerabilities

II.2. Remote Attacks on the System

1. *Phishing*: A highly sophisticated and dangerous attack in which the attacker tricks the victim to visit the malicious link and grab his credentials like username and password. Phishing and other similar attacks like desktop phishing and email spoofing, which compromise the credentials, fall into social engineering and web application attacks. The attacker clones a copy of the website and hosts on another server with a somewhat similar domain name. This copy includes all the codes from the original site (Sharma, et al. [11]). This makes it arduous to trace the attacker in the server logs as no suspicious access is made.
2. *Vishing*: An outdated yet very effective attack in which the attacker tricks the victim using social engineering techniques and convinces the victim to

reveal confidential information such as debit/credit card number.

3. *Voice-over-IP*: In VOIP attack, the attacker spoofs the caller ID of a well-known trusted service and calls the victim gaining his/her trust posing as an employee of the bank and extracts all the sensitive information [11].
4. *DNS cache poisoning*: In this attack, the attacker alters the Domain Name Service (DNS) entry into the hosts file of the victim’s machine using a keylogger. Whenever the victim tries to visit a website whose DNS record and IP address has been altered by the attacker in the host file the victim is redirected to a fake website which looks alike the original website he was intended to go to. Thus, the attacker immediately logs all his login information. [11].
5. *Keylogger/Remote Administration Tools*: These are tools mainly designed to steal or log the information on every change a victim makes to its system or while he works on some sensitive data, also the attacker has full access to victim’s computer once he manages to install a RAT/Keylogger on the victim’s computer.

II.3. Preventions

There are several measures an individual can take to ensure his online security and privacy. They include One-Time Password (OTP), tokens both online and offline OTPs, browser protection use of secure add-ons like Hyper Text Transfer Protocol (HTTPS) everywhere, two-factor authentication (2FA), strong passphrase i.e. a passphrase of good length, updating banking apps to their latest version to enable the use of new security protocols. Never enter any sensitive information on any third-party web page and pop-up window and prefer to use virtual keyboard for entering login information, avoid the use of E- banking accounts from cyber cafes, shared PCs, Unknown systems.

III. Internet of Things Security

The Internet of Things can be described as the network of devices connected with sensors where connection through a network will enable these devices to collect and exchange data with each other where these devices will be uniquely identifiable [23].

The devices embedded in this network can be a variety of devices namely automobiles with built-in sensors, electric dams in coastal waters, thermostats, dishwashers that can be remotely monitored and home appliances like smart TVs, smart microwave ovens etc. [12].

From Fig. 4 it is observed that IOT devices aren’t secure enough and there is a stronger chance that these devices may leak user sensitive personal information.

Then why would a user ever trust these devices? In order to curb these security and privacy issues, industries have to develop different standards while designing IOT devices and making sure they comply and work as directed to the user without any loss of personal data.

The security measures can be applied to numerous layers, as discussed in the next section.

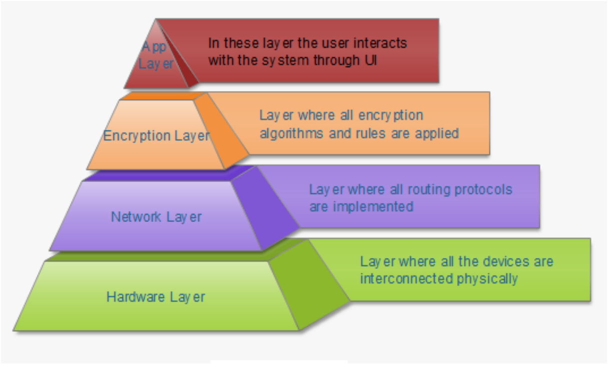

App Layer
In these layer the user interacts with the system through UI
Encryption Layer
Layer where all encryption algorithms and rules are applied
Network Layer
Layer where all routing protocols are implemented
Hardware Layer
Layer where all the devices are interconnected physically

Fig. 4. IOT Model

III.1. Hardware Layer

The devices which are interconnected to each other and form the IOT network need to be secured. They should be updated and upgraded from time to time to the latest products to ensure more efficiency and usability.

Often, to ensure the correct functionality, most devices should be air gapped and unauthorized radio signals should be intercepted by a jammer.

III.2. Network Layer

There are different measures that can be taken to ensure security on a network layer. It is advised to use WPA2 (Wireless Protected Access 2) rather than relying on WPA (Wireless Protected Access) and WEP (Wired Equivalent Privacy) [13]; to use different types of firewalls which can filter data on the basis of data packets that are being routed in the whole network, and also to use the IDP (Intrusion Detection System) and the IPS (Intrusion Prevention System).

III.3. Encryption Layer

Having a stronger encryption protocol is another measure which can be used to protect a network from attacks. As per Alabam et al. [13], the commonly used encryption algorithms are Ron Rivest, Adi Shamir & Leonard Adelman (RSA), Advanced Encryption System (AES), Data Encryption Standard (DES), 3 Data Encryption Standard (3DES), Message Digest 5 (MD5), Secure Hash Algorithm (SHA) [13].

By digging deeper in these encryption algorithms, three out of six of them are weak and they are prone to a collision attack [13].

Therefore, in order to curb the encryption weakness, it is advised to use algorithms which require high computational power to break them and also consume too much time for a collision attack to take place i.e. it is needed to implement stronger encryption algorithms.

III.4. Application Layer

This is the layer through which the user interacts with the devices on a daily basis and some of the highly severe vulnerabilities lie in this layer. To minimize the chances of letting a vulnerability being exploited and gain the full remote or local system control, vendors should provide security guidance for the application (Alaba, et al. [13]). Various attacks like Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) are mostly seen in action on the application layer. CSRF is a technique in which the attacker conceals himself as a legitimate client and alters the user's firewall settings.

Also, it is advised to check the vendor's website for important security updates and upgrades which will help in hardening the applications against different attacks.

Fig. 5 summarizes the ever growing IOT devices and networks which are huge and complex to handle. Their security should not be neglected because, without enough security, these devices will not be useful, but will prove harmful to human beings. Most IOT security breaches are caused by End-User carelessness which accounts for 56%, 42% breaches account for Malwares, 32% for Spywares, 29% account for external data breaches, 25% for Mobile devices etc.

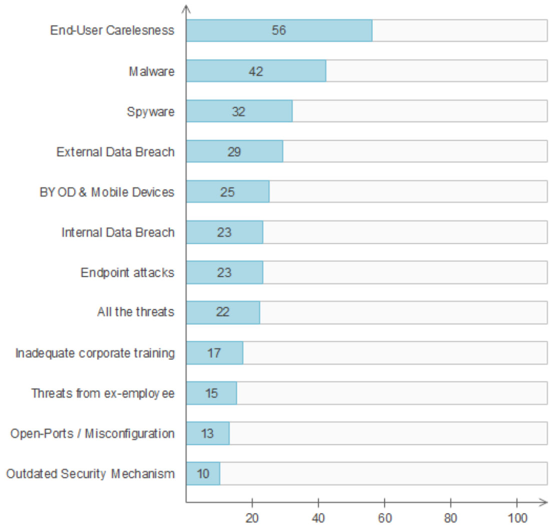


Fig. 5. Different attacks on IOT systems

IV. Artificial Intelligence (AI) Security

Artificial Intelligence is the field which would profit the most from InfoSec/Cybersecurity. According to Dilek, et al. [14], if machines get more intelligent they would implement algorithms that would immediately identify cyber threats and also warn humans about the same. While most Cybersecurity firms are busy in developing automated systems for threat analysis and incident response, we are still far behind in developing artificial intelligent systems for cybersecurity. A new breed of algorithms that help systems to identify what was previously missed by manual mechanisms are being developed by security researchers as they provide more accuracy in securing the system.

With the ever-increasing devices connected to the internet, how can the devices and networks be secured?

The answer is simple with the help of artificial intelligence. We would soon be able to design and implement new intelligent machines which will implement self-learning algorithms and help us combat cyber threats.

In the previous section, securing IOT devices was discussed, now it is assumed that there are billions of devices connected with each other and that some attacker finds a vulnerability in all these devices and exploits it.

These devices would start attacking each other and the only way to mitigate this type of attacks is by having automated intelligent machines that are able to detect such threats before the attack takes place and run necessary counter-measures [14]. The major problems in this type of attacks are the speed of the attacks and the data required to respond in real time. In today's world, the use of AI with the mix of cyber security would be in defense or so-called "Cyber-Defense". It is pretty obvious that, in order to fight cyber weapons, more intelligent software is needed. Considering worms and viruses, for example, the Mirai worm (a worm which turns Linux systems into a part of the bot) which in turn can be remotely controlled and be used for unethical purposes (Bertino, et al. [15]).

The worm was first found in late August 2016 by a white hat security firm named MalwareMustDie and was mostly used to carry out Distributed Denial of Service (DDOS) attacks on celebrities and journalists websites [15]. One of the worst characteristics of the Mirai worm was that it could continuously scan for IP addresses of devices connected together in the IOT network. It was also instructed not to infect the networks having private IP addresses, but to only target US Postal Services (UPS) and the Department of Defense (DOD). On 20th September, 2016, the Mirai worm was used alongside BASHLITE (a malware which infects Linux systems for carrying out a DDOS attack) on the website of "kerbs on security" which is run by a cybercriminal journalist, and the attack reached 620 Gbps (Bertino, et al. [15]). Mirai was also used to carry out a DDOS attack on Liberia's internet infrastructure in November 2016. Meanwhile, on 21st October 2016, Mirai was used to carry out a DDOS attack on a DNS service named Dyn which caused the Mirai worm to spread on the IOT devices which resulted in inaccessibility of websites such as GitHub, Twitter, Reddit and Netflix [15]. Later in end of November 2016, a new variant of Mirai bot A software application that runs automated tasks over the internet was discovered to have infected 0.9 million routers from Deutsche Telekom (Bertino, et al. [15]) which crashed due to failed exploitation. From the above examples, it is clear how a cyber weapon caused destruction to so many organizations and people.

In future, the integration of artificial intelligence and cybersecurity will prove to be very beneficial to the information security industry.

The need is thus to develop more intelligent systems which can combat such deadly weapons. AI systems with huge processing power and intelligent algorithms will be useful for combating security challenges.

V. Cyber-Terrorism

The evolution of Information Security doesn't always have a positive impact on the world; there are individuals and organizations that have been using the cyberspace to spread hatred and create chaos in the world in the name of religion and racial bias. As per Fig. 6, after surveying around 115 individuals on "What causes most cyber-attacks?", 87% individuals thought there is a political reason, while 77% thought it is just a digital means or target, 70% stated its fear of outcome, 47% responded it is a violence against people, 42% thought it is just criminality etc.

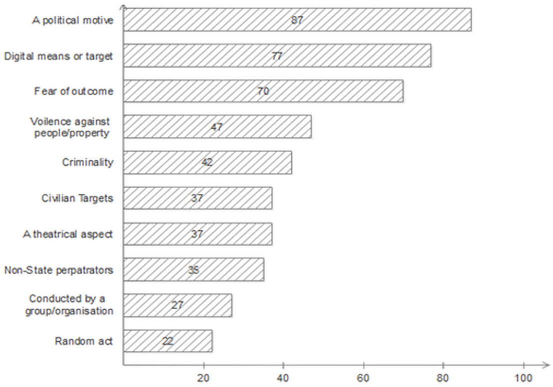


Fig. 6. A survey on What causes the most cyber- terrorism attacks? Answered by 115 individuals

Terrorist organizations are using social media like twitter and facebook as a mode to convey their message and spread terror in the rest of the world.

To drive deeper, consider the case of the attacks in San Bernardino, California, USA (Froomkin, et al. [16]).

In 2015, after the terroristic shoot-out carried out in San Bernardino, the Federal Bureau of Investigation (FBI) seized an iPhone 5C from the shooter which contained sensitive information about the attacks that were carried out by the shooter and his organization. The FBI was unable to recover any data from the device due to its high-end encryption algorithm which took a lot of expertise and high computational power to be decrypted.

The goals of the FBI were clear, they needed a backdoor which would let them extract data like contacts, photos and calls from the locked iPhone [16]. On the other hand, they were also breaching the United Sates District Court's law under the All rights Act of 1789. In order to gain access to the phone, the FBI approached Apple Inc, but it refused to decrypt the phone stating that it would breach their privacy policy of an end-user. Despite FBI's continuous attempts of unlocking the iPhone the United Sates District Court's and Apple Inc denied their request to unlock the iPhone. Later, the FBI somehow managed to decrypt the iPhone with the help of a third party white hat cyber security firm without the court order and without the help of Apple Inc. [16]. This implied that it was successful in breaking the Apple's encryption algorithm and also that FBI was successful in carrying out a collision attack on the iPhone's encryption protocol.

The other possible reason that Apple was unable to decrypt the iPhone is that it does not keep a copy of the encryption keys and the only way to dodge this encryption problem was to brute-force the encryption keys which would take a lot of time (Froomkin, et al. [16]). The other way to decrypt the iPhone would be to use acids and lasers to access the data stored in the seized iPhone, in layman's terms, performing microscopic surgery on the wiring of silicon chips. The reason behind this was that Apple uses the famous Advanced Encryption Standard (AES) cryptographic algorithm to protect user data [16]. Each iPhone has a unique number called the "encryption key" which is needed to encrypt and decrypt data on the iPhone. The key string is 256-bits long which directly implies that it would make trillions encryption keys, which are impossible to crack in a lifetime. On the other hand, the main reason for Apple to have such a high-end encryption algorithm is not just for encrypting data, but also to secure the user's passcode which is used every time by the user to unlock the screen of an iPhone. To unlock the encryption, the chip has about 10,000 or 1 million values. According to [16], in most iPhones and if the person is too privacy conscious, the passcode could be an alphanumeric passcode which would add more values to the passcode.

The third way to unlock such a high encryption scheme would be to perform a "replay attack" in which the attacker could maliciously and fraudulently limit or delay the passcode by cloning the device's memory bank by making a few guesses, then reverting the token by rolling back the device's state before any guess is made.

In short, the extensive use of encryption protocols on personal devices like smartphones, Personal Digital Assistants (PDA), Laptops can be useful when it comes to privacy and anonymity. But in the described above cases when it is about the lives of people while criminals and terrorists use these encryption standards to safeguard their crimes, can't lawmakers and IT giants make an exception to such cases by providing access to the attackers' personal devices and help the law enforcement to combat cyber-terrorism? On the other hand, while government organizations are running mass surveillance programs and evading the citizen's privacy, they are still unable to combat cyber-terrorism. Are these programs still worth it?

It can be concluded that, as the internet is growing faster and more and more data is being generated every day in exabytes and petabytes, it's also the responsibility of these IT giants and vendors to safeguard user's privacy and not let it slip into the hands of terrorist organizations and individuals who would cause harm to people in the cyberspace.

VI. Ransomware

With the ever-increasing use of the internet to download data like music, videos, apps and documents there lies a very good chance of the files being infected with a malware. Malware functioning is shown in Fig. 7.

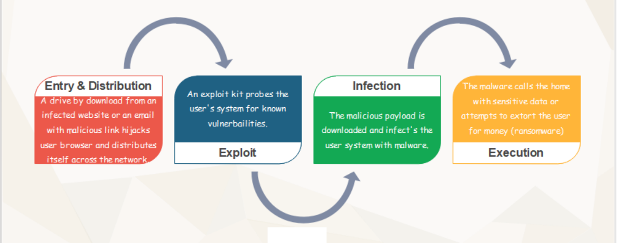

Entry & Distribution
A drive by download from an infected website or an email with malicious link hijacks user browser and distributes itself across the network.
An exploit kit probes the user's system for known vulnerbailities.
Exploit
Infection
The malicious payload is downloaded and infect's the user system with malware.
The malware calls the home with sensitive data or attempts to extort the user for money (ransomware)
Execution

Fig. 7. Basic Model of a Ransomware

In history, there is evidence of various highly sophisticated cyber-attacks and, recently, on 12th May 2017, a Ransomware (a malware that encrypts files and unlocks them only after the ransom is paid) called WannaCry hit the web and started infecting all the computers running on Microsoft's Operating Systems (Patil, et al. [17]). With further investigation and after examining the binary samples of the malware, it was found that the Ransomware attacked the vulnerability present in the Server Message Block (SMB, which operates as an application-layer network protocol mainly used for providing shared access to files, printers and serial ports); this vulnerability is mostly found in the following versions of Microsoft's Operating Systems: Windows XP, Windows Server 2003, Windows Server 2008, Windows 7, Windows 8, Windows 8.1. It is exploited using the "EternalBlue" exploit denoted by the entry CVE-2017-0144 along with the "DoublePulsar" payload [18]. The malware starts looking for the vulnerability present in the system on the same Local Area Network (LAN) and starts spreading alongside once it finds the vulnerable version of SMB. The EternalBlue exploit triggers the vulnerability along with DoublePulsar which acts as a payload; the ransomware give access to the attacker and starts encrypting the files.

The encryption algorithm used by the ransomware is quite sophisticated as it uses Advanced Encryption Standard (AES) and Ron Rivest, Adi Shamir and Leonard Adleman (RSA) [18]. It is quite impossible to brute-force or to try any other offline attack to break the encryption.

Steps of encryption used by WannaCry Ransomware:

1. Each file is encrypted using a AES-128-bit key.
2. This key is further encrypted using RSA-2048 public key and stored in 0000000.py file.
3. The private RSA key of the above Public RSA key is encrypted using the RSA Master key.
4. The private RSA key of the RSA Master public key is known only by "Ransomware Authors" [18].

As per Fig. 8, the actual file is first encrypted using an AES 128-bit random key. Then using a RSA master private key encapsulated with a RSA master public key, along with RSA-2048 public and private key, it is encrypted again and finally the encrypted file is generated which is a combination of all the encryption algorithms mentioned in Fig. 8. All the encrypted files extensions are shown in Fig. 9.

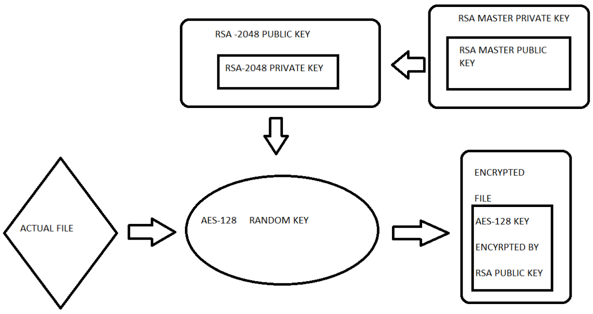
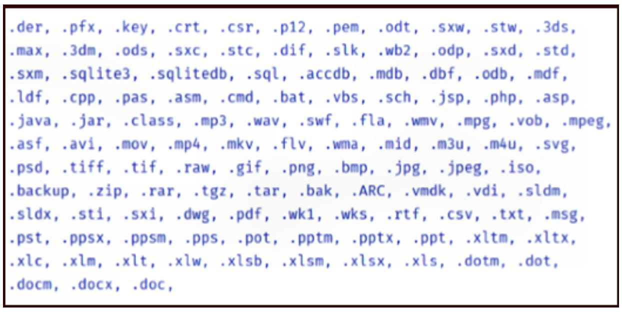


Fig. 8. Encryption Process of WannaCry Ransomware



.der, .pfx, .key, .crt, .csr, .p12, .pem, .odt, .sxw, .stw, .3ds,
.max, .3dm, .ods, .sxc, .stc, .dif, .slk, .wb2, .odp, .sxd, .std,
.sxm, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .mdf,
.ldf, .cpp, .pas, .asm, .cmd, .bat, .vbs, .sch, .jsp, .php, .asp,
.java, .jar, .class, .mp3, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg,
.asf, .avi, .mov, .mp4, .mkv, .flv, .wma, .mid, .m3u, .m4u, .svg,
.psd, .tiff, .tif, .raw, .gif, .png, .bmp, .jpg, .jpeg, .iso,
.backup, .zip, .rar, .tgz, .tar, .bak, .ARC, .vmdk, .vdi, .sldm,
.sldx, .sti, .sxi, .dwg, .pdf, .wk1, .wks, .rtf, .csv, .txt, .msg,
.pst, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx,
.xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotm, .dot,
.docm, .docx, .doc,

Fig. 9. Filetypes affected by the WannaCry Ransomware

The ransomware asks the victim to pay the ransom which varies from 300-600 in order to decrypt the files after a specific period of time. If the ransom is not paid, all the files are deleted and the victim loses control over his files permanently. In order to stop this ransomware from spreading and encrypting the files over the other systems, a British security analyst named Marcus Hutchins discovered the "kill-switch" which stopped the ransomware from spreading. However, after some time, the 2nd version of "WannaCry" started surfacing the web, which had patched the loophole discovered by Marcus Hutchins.

The kill-switch discovered by Marcus Hutchins was to lookup the previously unregistered domains. The malware was coded to register the unregistered domain names, so if the domain names are registered, the exploit won't work and it will stop spreading. Soon, Microsoft released a patch to all the operating system's running the vulnerable version of SMB and recommended all its users to patch their system with the security update named "KB4012598" [19]. This patch would update the SMB of their system to its latest version and thus stop the widespread of ransomwares like "WannaCry".

VII. Conclusion

In the modern world, as Information security is advancing in every field, it has become crucial for vendors to spread the awareness and the need for securing devices to ensure user safety and security. This paper presents the different scenarios and statistics of how information security is playing a vital role in reshaping industries. Moreover, different cases are studied which give a good insight on how attacks are being carried out at the different layers and which measures an individual can take to fortify the safety of his personal data from being public. The different presented statistics showcased how vulnerabilities are emerged and patched in new technologies in order to guard the safety of users online and offline data. At last, it can be concluded that, with the advancement of technologies, our data is more endangered by cyber-attacks and one can only take measures but cannot assure the security of data.

References

[1] M. E. Whitman, “Enemy at The Gate: Threats to Information Security”, *Communications of the ACM*, Vol. 46, n. 8, pp. 91-95, 2003.

[2] L. Corrons, “The Business of Rogueware”, *Communications in Computer and Information Science*, Springer, Vol. 72, pp. 7-7, 2010.

[3] L. Gordon, M. Loeb, “The Economics of Information Security Investment”, *ACM Transactions on Information and System Security*, Vol. 5, n. 4, pp. 438-457, 2002.

[4] G. Dhillon, J. Backhouse,” Information System Security Management in the New Millennium”, *Communications of The ACM*, Vol. 43, n. 7, pp. 125-128, 2000.

[5] R. Anderson, T. Moore, “The Economics of Information Security”, *Sciencemag*, Vol. 314, n. 5799, pp. 610-613. DOI: 10.1126/science.1130992, 2006

[6] B. V. Solmsa, R. V. Solms, “The 10 deadly sins of information security management”, *Computers & Security*, Elsevier, Vol. 23, n. 5, pp. 371-376, 2004.

[7] Alkhatib, M., Alsalem, A., Efficient Hardware Implementations for Tripling Oriented Elliptic Curve Crypto-System, (2014) *International Review on Computers and Software (IRECOS)*, 9 (4), pp. 609-617.

[8] Wainakh, A., Wabbi, A., Alkhatib, B., Design and Develop Misconfiguration Vulnerabilities Scanner for Web Applications, (2014) *International Review on Computers and Software (IRECOS)*, 9 (10), pp. 1682-1691. doi:https://doi.org/10.15866/irecos.v9i10.3840

[9] Geetha, R., Kannan, E., Secure Communication Against Framing Attack in Wireless Sensor Network, (2015) *International Review on Computers and Software (IRECOS)*, 10 (4), pp. 393-398. doi:https://doi.org/10.15866/irecos.v10i4.5520

[10] R. K. Jassal, R. K. Sehgal, “Online Banking Security Flaws: A Study”, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, n. 8, pp. 1016-1021, 2013.

[11] T. S. Brar, D. Sharma, S. S. Khurmi, “Vulnerabilities in e-banking: A study of various security aspects in e-banking”, *International Journal of Computing and Business Research*, pp 1-14, 2012.

[12] J. S. Kumar, D. R. Patel, “A Survey on Internet of Things: Security and Privacy Issues”, *International Journal of Computer Applications*, Vol. 90, n. 11, pp. 20-26, 2014.

[13] F. A. Alaba, M. Othman, I. A. Hashem, F. Alotaibi “Internet of Things security: A survey”, *Journal of Network and Computer Applications*, Vol. 88, pp. 10-28, 2017.

[14] S. Dilek, H. Çakır, M. Aydın “Applications Of Artificial Intelligence Techniques To Combating Cyber Crimes: A Review”, *International Journal of Artificial Intelligence & Applications (IJAIA)*, Vol. 6, n. 1, pp. 21-39, 2015.

[15] E. Bertino, N. Islam “Botnets and Internet of Things Security”, *Cybertrust IEEE Computer Society*, Vol. 50, n. 2, pp. 76-79, 2017.

[16] D. Froomkin, J. McLaughlin “*FBI vs. Apple Establishes a New Phase of the Crypto Wars*” The Intercept, 2016.

[17] S. Mohurle, M. Patil, “A brief study of WannaCry Threat: Ransomware Attack 2017”, *International Journal of Advanced Research in Computer Science*, Vol. 8, n. 5, pp. 1938-1940, 2017.

[18] S–Connect, “*WCRY or WannaCry Ransomware Technical Analysis*” Cybrary.it, 2017.

[19] Microsoft, “*Microsoft Update catalogue for “kb4012598”*, Microsoft Update Catalog, 2017.

[20] Enshaei, M., Mohd Hanapi, Z., Othman, M., A Review: Mobile Ad Hoc Networks Challenges, Attacks, Security, Vulnerability and Routing Protocols, (2014) *International Journal on Communications Antenna and Propagation (IRECAP)*, 4 (5), pp. 168-179.

[21] Adnan, A., Hanapi, Z., Geographic Routing Protocols for Wireless Sensor Networks: Design and Security Perspectives, (2015) *International Journal on Communications Antenna and Propagation (IRECAP)*, 5 (4), pp. 197-211.

[22] Bafandehkar, M., Yasin, S., Mahmod, R., A Literature Review on Scalar Recoding Algorithms in Elliptic Curve Cryptography, (2015) *International Journal on Communications Antenna and Propagation (IRECAP)*, 5 (4), pp. 183-189.

[23] Bani Yassein, M., Abuein, Q., Bani Amer, A., Energy Saving in Constrained Application Protocol of Internet of Things, (2016) *International Journal on Communications Antenna and Propagation (IRECAP)*, 6 (3), pp. 160-168.

Authors’ information

Department of Electronics and Telecommunication Engineering, Modern Education Society’s College of Engineering, Pune, India.

E-mails: amitvitekar@ymail.com
prabhakar.kota@mescoepune.org

Amit Vitekar was born in Pimpri-Pune in the state of Maharashtra, India. He is pursuing his Bachelor of Engineering in Electronics & Telecommunication at the M. E. S College of Engineering, Pune under Savitribai Phule Pune University. His areas of interest are Web-Application Security, Systems Security, Network Security, Wireless Security, Reverse Engineering, Exploit Development and GSM/LTE Security.

Prabhakar Kota received the B.E(E&TC) and M-Tech degrees in Microwave engineering from Pune University, Pune, India, in 2000 and 2008, respectively, and he is a Research student at Sinhagad Institute of technology, Pune. He is now an assistant Professor at MES college of engineering, Pune.