International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 747-753
Published Online May 2020 in IJEAST (http://www.ijeast.com)

A STUDY OF CYBER SECURITY AND ITS CHALLENGES

Ayan Das, Dawn Saju
Student, Dept.IT
MRIIRS, Faridabad, Haryana India

Dr. Neha Gupta
Faculty of Computer Applications,
Manav Rachna International Institute of Research & Studies, Faridabad

Abstract: Cyber crimes and data breaches are the common problems these days & are occuring in thousands each year and some costing millions of money. Now a days more business projects are working online and computer system are used to store the informational data. This need is much increasingly clear as systems and applications are being circulated via insecure network for example internet. The internet alone has become a major problem for government organizations, companies, and thousands of other everyday user. A network of computer supports a large number of activities whose loss would paralyze these organizations. As a result, cybersecurity issues have become a world wide problem. Securing the internet is a difficult task.

I. INTRODUCTION

Today a person can send and get any type of information like e-mail, audio, or a video just by a click of a button, yet he never thinks about the safety of the information & keep on sending the data to the next person. TO keep data secure we need to understand about the cyber security. Nowadays internet is the fastest developing infrastructure and all the latest technologies of this era are based on the internet. But due to these rising technologies and advancements we are unable to safeguard and protect our private data in an effective manner and subsequently cyber crimes are increasing day by day. Today more than 60 percent of aggregate business exchanges are done online, so this field required a high caliber of security for a better transaction. Subsequently cyber security has become the most latest issue. The extent of the cyber security is not limited or restricted to securing the data in IT industry but also to various different fields like cyber space etc.

Cybersecurity is the protection of all the systems, software, hardware and data from the cybercrimes which is connected to the internet.

Cyber crime

Cyber criminals incorporates and sell malware/spyware online that generally take place in the hub of dark web, also services that acknowledges how robust a virus is. Nowadays Business intelligence dashboards to track malware associates deployment and tech support.

The professionalism of cyber crime adds up to enormous costs in damages every year, which influences individuals, businesses and government as well.

Experts estimated that cybercrime damages will reach about $6.2 trillion by year 2021.Making it more lucrative criminal enterprises.

As of now [IOT]-internet of things caused evolution of smart devices and made them more popular that has created more opportunities to penetrate security measures, gain unauthorized access, and commit crime.

Cyber security

The sole ideal practicing of protecting-systems, networks, programs and digital attacks.

These cyber attacks are particularly focused at accessing, changing or destroying sensitive information, extorting money from users, interrupting normal businesses. Incorporating effective cyber security measures is specifically challenging today. As (User's<DEVICES) and attackers become more innovative.

According to GDPR (General data protection regulation) and DPA (Data protection act) 2018 require organization to equipped with appropriate technical and organizational security measures to protect personal data or risk substantial fines.

3 important aspects of cyber security

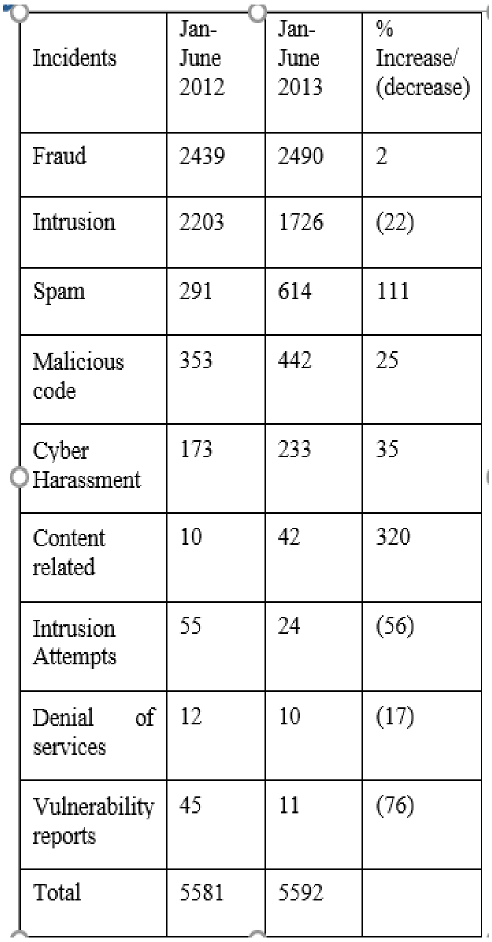
- PEOPLE: every employee needs to be aware about their role to prevent cyber threats.
- Processes: Documented processes should clearly defined procedures, roles, responsibility.
- Technology: from access control to installing antivirus, technology can be utilized to reduce cyber risks.

Cyber security standards

- **<u>MCSS</u>**; minimum cyber security standard released by U.K. governance in 2018, proposed series of technical standards developed in a collaboration with NCSC (national cyber security center)

- **PAS555**; Released by BSI (British standards institution) in 2013.it was used to determine and confirm measures which are implemented are comprehensive.
- **ISO22301:2012;** It is international standard for a BCMS (business continuity management system) it aims not only on responding to recovering from disasters but also security, information and maintaining access to it.

Threats surrounding cyber security
Malware: it is an infective contraction due to a malicious software that corrupts devices And causes damage, in certain cases stealing of data\compromising with data integrity. Its often created by a group of anonymous people's i.e. hackers. They're just looking way to make money either spreading the malware by them only or auctionate a malware i.e. selling anonymously to the highest bidder that specifically takes place in dark web. But a malware can be accessed as a tool for protest, an alternate to test security and measures. Or can implement war between government.



Incidents	Jan-June 2012	Jan-June 2013	% Increase/ (decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious code	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion Attempts	55	24	(56)
Denial of services	12	10	(17)
Vulnerability reports	45	11	(76)
Total	5581	5592	

Types of malware:

- **Viruses:** It appears as their biological sakes, they connect/attach themselves to clean data files and corrupts its other clean data files, spreads uncontrollably, damaging a system's core functionality. they generally appear as executable file.(.EXE)
- **Trojans:** This type of malware disguises itself as fortunate software, or is hidden in important software or data file that has been tempered/manipulated. It acts discreetly and create backdoors in security to let other malware in.
- **Spyware:** Its designed to spy on data files on a device and observes user activity offline as well as online like getting an access to your passwords, credit cards numbers, etc.
- **Worm:** It can infect sources and entire network of devices, either via locally or via network interfaces. It uses an infected machine to infect others.
- **Ransomeware:** It typically lockdown devices files and threatens to erase everything until you pay a ransome.
- **Adware:** Though not always malicious in nature, aggressive advertising software can give your security an unhandled tick to serve you ads.

Identity theft and other fraud
Identity theft isn't certainly a cybercrime, these days it's more likely to happen via tech. It happens every second in todays world, for identity theft a hacker first need to access to their victim's personal data to ignite the crime.

Ways to access victim's data:

- **Phishing:** they use "bait" in form of fraud messages to lure victims to fake websites where user enters their personal details unwittingly and attacker gets access. Eg. user ID, password, bank details.
- **Pharming:** Its one step advance of phishing, it uses malware to reroute unsuspecting internet surfers to fake websites. their user unwittingly enter personal details.
- **Keylogging:** This is more of a spyware, as it secretly logs everything you type, hence
  Unknowingly giving personal data.
- **Sniffing:** If connected to unsecured/ un-encrypted network, hackers steal data via "sniffing".

Cyberbullying:
It refers to all terms of online harassment, including stalking, sexual harassment, doxing (exposing someone's personal information), frapping (Break into someone's social media accounts and accessing it)

Cryptojacking:
When attacker breaks into your device and mine cryptocurrency without your consent. miners do this using java script to damage your device after you visit an infected

website. causes performance issues and high electric bills for you.

Cyberextortion:
It is a digital version of extortion. most famous form is ransomeware.it also referred to blackmailing victims using their personal data or threatening business via botnet -Driven "DDOS" attack

Cyberespionage:
Worlds power uses a group of Anonymous people's termed as hackers, as weapons to consolidate complex matrix of global politics. Such as stealing classified intelligence and using malware to attack nuclear plants and sponsors them too so as to create havoc at world stage.

Email fraud:
E-mails are most popular these days using network interfaces still most prevalent method for cyber crime. Also its second most costliest cyber crime. It includes phishing attempts, malware in form of sketchy attachments and digital extortion might also possible through email fraud.

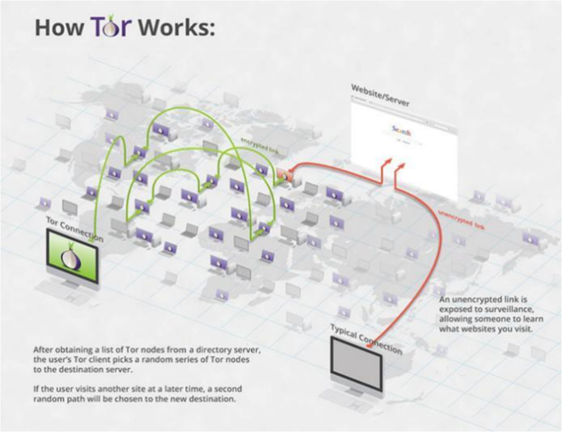
Dark Web – origin of cyber crime
Deep web refers to all remaining parts of internet that can't be accessed by any regular search engines like Google, yahoo etc. a subset of deep web is dark web/ darknet. That requires special browser to access it, Such as "Tor" browser. Although Darknet isn't illegal but the anonymity it affords makes it a hotbed for criminal activity.

Some most dangerous and odious commodity exchange happens such as drugs, weapons, child pornography even contract killing. Also stolen Credit/debit card are sold and bought here.

Cyber safety tips - protect yourself against cyberattacks

- Update S/W and operating system: This means you benefit from the latest security patches.
- Use anti-virus software: Security solution like mc Afee_SECURITY will detect and removes threats. Keep your software updated for the best of protection.
- Use anti-virus S/W: Security solutions: Kaspersky Total Security will detect & removes threats. Keep your software updated for best level of protection.
- Do not open email attachments from unknown resources: These could be infected malware.
- Do not click on links in emails from unknown resources/ unfamiliar websites: its a common way that malware is spread.

Avoid unsecure WiFi networks in public places:



An unencrypted link is exposed to surveillance, allowing someone to learn what websites you visit.

After obtaining a list of Tor nodes from a directory server, the user's Tor client picks a random series of Tor nodes to the destination server.

If the user visits another site at a later time, a second random path will be chosen to the new destination.

Cloud computing:
Nowadays all small, medium, large organisation are adopting for cloud computing. The security outlook of cloud computing is entirely different. In other words we can say that the world is moving towards the clouds. This new trend will be a big challenge for the cyber security. In addition, number of software and application available in cloud increases, which is a big concern, as cloud services need to expand or evolve in order to prevent the loss of valuable data and information. The cloud computing is also developing in there own way to meet the latest security issue. The cloud may provide many new opportunities but it is also to be noted that as cloud expands new security issue also expands.

Benefits of cloud computing:
Cost: cloud computing eliminates expensive purchasing of hardware and software setting up and running on site data centre's.
Global Scale: the benefits include ability to scale elastically, means delivering right of IT resources i.e. providing more computing power, storage bandwidth etc at right geographic location
Security: providers offers sets of policies, techs, and control security posture overall,
Enabling protect your data infrastructure from potential threat.
Speed: Most computing services provide on demand services and vast amount of computing resources rather in just few clicks.
Reliability: cloud computing ensures data backup, disaster recovery and business continuity easier and way less expensive.

Types of cloud computing: not all sets of cloud computing soothes every user that's why there are several's of models. As follows.
Public cloud: owned by a third party providers, delivers computing resources like servers and storage over internet

Private cloud: It provides services and resources used specifically single business organisation that can be located physically on company's data centre.
Hybrid cloud: it is combination of public and private clouds bound together allowing data and application to be shared by them. That gives business more flexibility.

Types of cloud services:

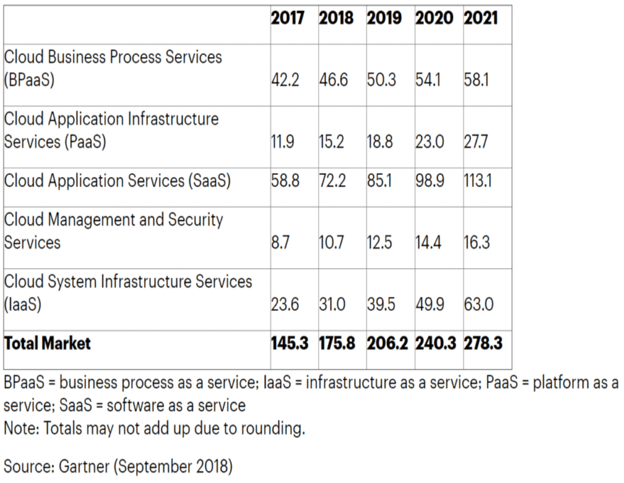
- **IaaS : infrastructure as a service**
- **SaaS: software as a service**
- **PaaS: platform as a service**
- **Server less computing**

Cryptography:

- cryptography is a process or a technique for a secure communication between two devices. It helps in analysing and developing protocols which helps to prevent the attack from third parties from retrieving the data. In todays world, in which 50% of crime are done online, cryptography plays a very important role in securing the data, which helps cybersecurity.

- Data integrity, data confidentiality, non-repudiation, authentication are principals of cryptography.

Table 1. Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)



	2017	2018	2019	2020	2021
Cloud Business Process Services (BPaaS)	42.2	46.6	50.3	54.1	58.1
Cloud Application Infrastructure Services (PaaS)	11.9	15.2	18.8	23.0	27.7
Cloud Application Services (SaaS)	58.8	72.2	85.1	98.9	113.1
Cloud Management and Security Services	8.7	10.7	12.5	14.4	16.3
Cloud System Infrastructure Services (IaaS)	23.6	31.0	39.5	49.9	63.0
Total Market	**145.3**	**175.8**	**206.2**	**240.3**	**278.3**

BPaaS = business process as a service; IaaS = infrastructure as a service; PaaS = platform as a service; SaaS = software as a service
Note: Totals may not add up due to rounding.

Source: Gartner (September 2018)

Plaintext :hello
Ciphertext :Jhhnn

Functions-of-Cryptography:
•**Privacy:** guaranteeing that nobody will access message except receiver.
• **Authentication:** the method of proving one's identity.
•**Integrity:** reassuring receiver's finish hasn't altered from original.
• **Non-repudiation:** A mechanism to proves sender very sent this message.
• **Key exchange:** the tactic by that crypto keys shared b/w sender and receiver.

(:- P =Plaintext, C =Ciphertext, E =Encryption-method, D =Decryption-method, and k = Key)
TYPESOF Cryptographical ALGORITHMS

• **Secret Key Cryptography (SKC):** Uses single key for each secret writing and secret writing. known as rhombohedral secret writing.

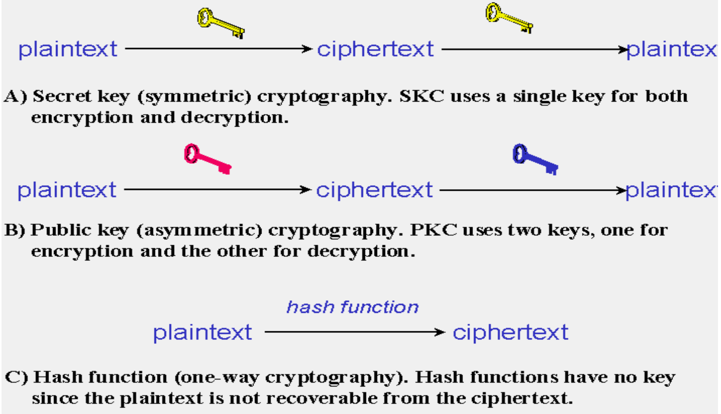
• **Public Key Cryptography**: Uses a key for secret writing and another for secret writing. called uneven secret writing. Primarily used for authentication, non-repudiation, and key exchange

.
• **Hash Functions:** Uses a mathematical alteration to once and for all "encrypt" data, providing a digital fingerprint. Primarily used for message integrity.

Secret Key Cryptography

- methods use one key for each cryptography and secret writing.
- the sender uses the key to inscribe the plaintext and sends the ciphertext to the receiver.
- The receiver applies same key to decode the message and recover the plaintext.
- As one secret's used for each functions.
- Secret key cryptography schemes area unit usually categorised as being either stream ciphers or block ciphers.
- Stream ciphers: Stream ciphers treat one bit (byte or laptop word) at a time and implement some sort of feedback mechanism so the secret's perpetually ever-changing
- Self-synchronizing stream ciphers: calculate every bit within the keystream as a operate of the previous n bits within the keystream.
- it's termed "self-synchronizing" as a result of the secret writing method will keep synchronous with the cryptography method simply by knowing however so much into the n-bit keystream
- Synchronous-stream ciphers: generate the keystream in a very fashion freelance of the message stream however by mistreatment a similar keystream generation operate at sender and receiver.
- whereas stream ciphers don't propagate transmission errors, they are, by their nature, periodic so the keystream can eventually repeat.

- Block cipher: It encrypts one fixed-size block of knowledge at a time.
- plaintext block can continuously inscribe same ciphertext once mistreatment a similar key (i.e., it's deterministic) whereas a similar plaintext can inscribe completely different ciphertext in a very stream cipher.
- Block ciphers will operate in one in all many modes:
- Electronic Codebook (ECB) mode is that the simplest, most blatant application: the key secret's wont to inscribe plaintext block to create ciphertext block
- whereas blood profile protects against several brute-force, deletion, and insertion attacks.
- Cipher Feedback (CFB) mode: it's a block cipher implementation as self-synchronizing stream cipher.
- CFB mode permits knowledge to be encrypted in units smaller than block size. input.
- Counter-(CTR)-mode: is comparatively fashionable addition to dam ciphers.
- DES: encoding normal most well-known and well-studied SKC schemes DES was designed by IBM within the Nineteen Seventies and adopted by the National Bureau of Standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 for industrial and unclassified government applications. DES could be a Feistel block-cipher using a 56-bit key that operates on 64-bit blocks. DES contains a advanced set of rules and transformations that were designed specifically to yield quick hardware implementations and slow software system implementations



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

MOBILE NETWORK & new internet protocol – IPV6

Today everyone is able to connect to anybody in any part of the world. But this mobile device security has become very important issue. nowadays different security measures are becoming unsecure as people are using different devices like PC, tablets, smart phones etc. all of which require more security apart of the present one.

The rollout of fifth-generation mobile networks — which provide the potential for downloads speeds of up to ten times quicker than today's — can amendment however we tend to communicate, work and stream video.

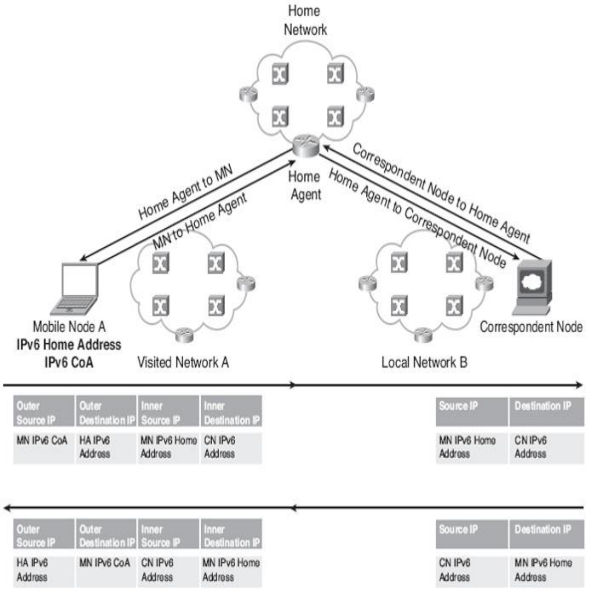


Figure 5-27 *Mobile IPv6 Bidirectional Tunneling Mode*

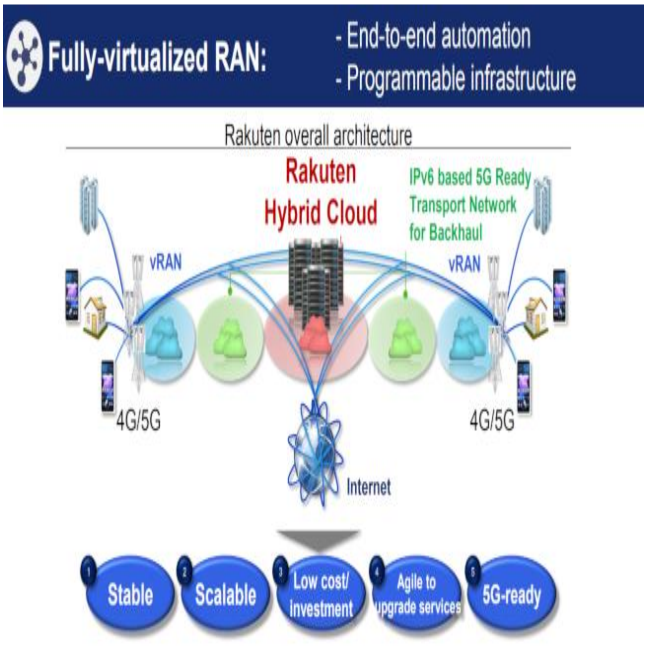
However, the quicker speeds also are possible to gift a chance for hackers to focus on additional devices and launch larger cyber attacks, consultants say.

The problem is unlikely to be the protection of 5G technology itself. Despite researchers uncovering apparent flaws in 5G's security — like the flexibility for attackers to use faux mobile base stations to steal data — 5G's stronger coding of information and higher verification of network users are wide thought of to be a big improvement on 4G.

Experts say that the weak link in 5G's security is probably going to be communication between devices connected to the net.

These devices, called the net of Things (IoT) — wherever everything from cars and works assembly lines to baby monitors and traffic lights have embedded internet-connected sensors-growing quick. the quantity of internet-connected things can grow from fourteen.2bn to 25bn by 2021,

- IPv6 offers a near-limitless variety of addresses. as a result of this, NAT (Network-Address-Translation) isn't formally supported in IPv6. In fact, NAT isn't alleged to be enforced on IPv6 networks in the slightest degree. NAT is employed to permit multiple devices to share a similar IP address. This was necessary in IPv4 as a result of there aren't enough addresses for everybody and everything. In fact, all IPv4 addresses have currently been assigned . There are not any new addresses left for anyone. The implications of each single device having a novel, globally accessible IPv6 address are large. A little-known reality of mobile IPv4 is that NAT will increase the latency by many milliseconds. this can be as a result of the network switch has got to translate the IP addresses for routing packets between the general public IP address employed by the switch, and also the internal IP address employed by the mobile network. this can be conjointly true with home web connections similarly.



II. CONCLUSION

As world is getting interconnected, computer security has become an extensive topic in present world. Day by day the cyber crimes are increasing that may lead to the biggest challenge of securing the information for the organisation. According to current scenario demand for cybersecurity professional will be high in future. Till date there is no perfect solution to control these cyber crimes, but we can try to control or minimize these crime for a better future.

III. REFERENCES

1. https://www.ft.com/content/ anikkei company, c papers, 2020,cryptography.

2. https://www.garykessler.net/library/crypto.html All material on this site © 1996-2020, Gary C. Kessler @digital certificates.

3. https://azure.microsoft.com/en-in/overview/what-is-cloud- computing/cloud-computing-models/ blogs

4. https://www.knowbe4.com/phishing May 7, 2020 10:36:01 AM By Stu Sjouwerman The latest example of a modern-day ransomware attack.

5. https://www.malwarebytes.com/ April 30, 2020 by Christopher Boyd Cybercrime and the economy have always been intertwined, blog

6. https://goosevpn.com/blog/origin-cybercrime Robert Herjavec Los Angeles, Calif. – Jun 19, 2019compiled a list of historical hacking incidents

7. https://www.itgovernance.co.uk/cybersecurity-standards Luke Irwin 9th April 2020./blogs

8. https://www.forcepoint.com/cyber-edu/cybersecurity TUESDAY, APR 28, 2020 BY ANKUR CHADDHA. /BLOG

9. https://www.dhs.gov/topic/cybersecurity CISA role in cyber security /(c)dbs blogs.

10. https://www.cshub.com/CSHub.com Editorial Staff 03/16/2020/blogs

Books:

11. The Art Deception: Controlling the Human Element Security in their security chain (Mitnick and Simon 2011;Patrick et al. 2003).

12. Hacking: The Art of Exploitation *"Book Review: Hacking". 25 July 2004. Archived from the original on 25 July 2004. Retrieved 26 July 2018.*

Schaefer, Ed. "Hacking: The Art of Exploitation, 2nd Edition : Linux Magazine". Linux Magazine. Retrieved 26 July 2018.

^"Archived copy" (PDF). Archived from the original (PDF) on 2017-12-24. Retrieved 2019-12-16.

13. Applied cryptography *"UK Data Encryption Disclosure Law Takes Effect". PC World. 1 October 2007. Retrieved 26 March 2015.*

^ Ranger, Steve (24 March 2015). "The undercover war on your internet secrets: How online surveillance cracked our trust in the web". TechRepublic. Archived from the original on 12 June 2016. Retrieved 12 June 2016.

14. Malware analysis International Journal of Advanced Research in Malware Analysis" (PDF). ijarcsse. Archived from the original (pdf) on 2016-04-18. Retrieved 2016-05-30.

15. Malware evasion techniques**.** Keragala, Dilshan (January 2016). "Detecting Malware and Sandbox Evasion Techniques". SANS Institute