Proceedings of International Web Conference "Cyber Security"
30th November 2022, Organized by Sbyte Technologies
Sponsored by INFISUM, USA.

Review Study on Some Topics Related to Cyber Security

Dr MAHALAKSHMI SHETTY
Associate Professor, AIML, Nagarjuna College of Engineering and Technology, Bangalore
Email : drmahalakshmi@ncetmail.com

Abstract : **Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of smart devices, including smartphones, televisions, and the various devices constitute the Internet of things (IoT). Cybersecurity is also one of the significant challenges in the contemporary world, due to the complexity of information systems, both in terms of political usage and technology. Its primary goal is to ensure the system's dependability, integrity, and data privacy**

Key words : **Network; Cyber Attacks; Multi Tenancy; Sensitive Information; Threat Factors;**

INTRODUCTION

After reviewing more than 200 scientific papers citing the term "fintech", a study on the definition of fintech concluded that "fintech is a new financial industry that applies technology to improve financial activities." Fintech is the new applications, processes, products, or business models in the financial services industry, composed of one or more complementary financial services and provided as an end-to-end process via the Internet.

Computer fraud

Computer fraud is the act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system. If computer fraud involves the use of the Internet, it can be considered Internet fraud. The legal definition of computer fraud varies by jurisdiction, but typically involves accessing a computer without permission or authorisation. Forms of computer fraud include hacking into computers to alter information, distributing malicious code such as computer worms or viruses, installing malware or spyware to steal data, phishing, and advance-fee scams. Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. These types of crimes often result in the loss of private or monetary information.

Cyberterrorism

Cyberterrorism, in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources. Acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by means such as computer viruses, computer worms, phishing, malicious software, hardware methods, or programming scripts can all be forms of cyberterrorism. Government officials and information technology security specialists have documented a significant increase in Internet problems and server scams since early 2001. Within the United States, there is a growing concern among government agencies such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) that such intrusions are part of an organized effort by cyberterrorist foreign intelligence services or other groups to map potential security holes in critical systems.

Cyberextortion

Cyberextortion is a type of extortion that occurs when a website, e-mail server, or computer system is subjected to or threatened with attacks by malicious hackers, such as denial-of-service attacks. Cyberextortionists demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cybercrime extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate, and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack. However, other cyberextortion techniques exist, such as doxing, extortion, and bug poaching. An example of cyberextortion was the attack on Sony Pictures of 2014.

Ransomware

Ransomware is a type of malware used in cyberextortion to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid. The Kaspersky Lab 2016 Security Bulletin report estimated that a business falls victim to ransomware every 40 minutes, and predicted that number would decrease to 11 minutes by 2021. With ransomware remaining one of the fastest-growing cybercrimes in the world, global ransomware damage is predicted to cost up to $20 billion in 2021.

Cybersex trafficking

Cybersex trafficking is the transportation of victims and then the live streaming of coerced sexual acts or rape on webcam. Victims are abducted, threatened, or deceived and transferred to "cybersex dens". The dens can be in any location where the cybersex traffickers have a computer, tablet, or phone with an internet connection. Perpetrators use social media networks, videoconferences, dating pages, online chat rooms, apps, dark web sites, and other platforms. They use online payment systems and cryptocurrencies to hide their identities. Millions of reports of its occurrence are sent to authorities annually. New legislation and police procedures are needed to combat this type of cybercrime. An example of cybersex trafficking is the 2018–2020 Nth room case in South Korea.

Cyberwarfare

The U.S. Department of Defense notes that cyberspace has emerged as a national-level concern through several recent events of geostrategic significance, including the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. In August 2008, Russia again allegedly conducted cyberattacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the military commanders will adapt the concept of cyberspace operations impact in the future.

Computer as a target

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world, in general, are towards combating these crimes. There are numerous crimes of this nature committed daily on the internet. They are seldom committed by loners, instead usually involving large syndicate groups.

Crimes that primarily target computer networks include: Computer viruses, Denial-of-service attacks, Malware (malicious code)

Computer as a tool

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the like existed before the development of computers and the internet. The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend. Crimes that use computer networks or devices to advance other ends include: Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime) The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions. Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware. Or, they may contain links to fake online banking or other websites used to steal private account information.

Obscene or offensive content

The content of websites and other electronic communications may be distasteful, obscene, or offensive for a variety of reasons. In some instances, these communications may be illegal. The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs. One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world.

Ad-fraud

Ad-frauds are particularly popular among cybercriminals, as such frauds are less likely to be prosecuted and are particularly lucrative cybercrimes. Jean-Loup Richet, Professor at the Sorbonne Business School, classified the large variety of ad-fraud observed in cybercriminal communities into three categories: (1) identity fraud; (2) attribution fraud; and (3) ad-fraud services. Identity fraud aims to impersonate real users and inflate audience numbers. Several ad-fraud techniques relate to this category and include traffic from bots (coming from a hosting company or a data center, or from compromised devices); cookie stuffing; falsifying user characteristics, such as location and browser type; fake social traffic (misleading users on social networks into visiting the advertised website); and the creation of fake social signals to make a bot look more legitimate, for instance by opening a Twitter or Facebook account. Attribution fraud aims to impersonate real users' behaviors (clicks, activities, conversations, etc.). Multiple ad-fraud techniques belong to this category: hijacked devices and the use of infected users (through malware) as part of a botnet to participate in ad fraud campaigns; click farms (companies where low-wage employees are paid to click or engage in conversations and affiliates' offers); incentivized browsing; video placement abuse (delivered in display banner slots); hidden ads (that will never be viewed by real users); domain spoofing (ads served on a website other than the advertised real-time bidding website); and clickjacking (user is forced to click on the ad). Ad fraud services are related to all online infrastructure and hosting services that might be needed to undertake identity or attribution fraud. Services can involve the creation of spam websites (fake networks of websites created to provide artificial backlinks); link building services; hosting services; creation of fake and scam pages impersonating a famous brand and used as part of an ad fraud campaign. A successful ad-fraud campaign involves a sophisticated combination of these three types of ad-fraud—sending fake traffic through bots using fake social accounts and falsified cookies; bots will click on the ads available on a scam page that is faking a famous brand.

Academics

Artificial Intelligence (AI), Blockchain, Cloud Computing, and Big Data are considered the four key areas of FinTech. Artificial intelligence refers to the intelligence demonstrated by machines, in contrast with "natural intelligence" displayed by humans and animals. AI is assuming an increasingly important role in traditional banking as it provides technologies such as voice recognition, natural language processing, and computer vision for user-account management and fraud detection, machine learning methods and deep learning networks for anti-moneylaundering and credit modeling. Mobile and internet payment systems are closely connected to cloud computing. The past ten years have witnessed increasing adoption of cloud computing by financial institutions around the globe.

FinTech Industry

Financial technology has been used to automate investments, insurance, trading, banking services and risk management. The services may originate from various independent service providers including at least one licensed bank or insurer. The interconnection is enabled through open APIs and open banking and supported by regulations such as the European Payment Services Directive. Robo-advisers are a class of automated financial adviser that provide financial advice or investment management online with moderate to minimal human intervention. They provide digital financial advice based on mathematical rules or algorithms, and thus can provide a low-cost alternative to a human advisers.

Technologies

Fintech companies use a variety of technologies, including artificial intelligence (AI), big data, robotic process automation (RPA), and blockchain. AI algorithms can provide insight on customer spending habits, allowing financial institutions to better understand their clients. Chatbots are another AI-driven tool that banks are starting to use to help with customer service. Big data can predict client investments and market changes in order to create new strategies and portfolios, analyze customer spending habits, improve fraud detection, and create marketing strategies. Robotic Process Automation is an artificial intelligence technology that focuses on automating specific repetitive tasks. RPA helps to process financial information such as accounts payable and receivable more efficiently than the manual process and often more accurately. Blockchain is an emerging technology in finance which has driven significant investment from many companies. The decentralized nature of blockchain can eliminate the need for a third party to execute transactions.

Awards and recognition

Financial magazine Forbes created a list of the leading disruptors in financial technology for its Forbes 2021 global Fintech 50. In Europe there is a list called the FinTech 50, which aims to recognise the most innovative companies in fintech. A report published in February 2016 by EY commissioned by the UK Treasury compared seven leading fintech hubs: the United Kingdom, California, New York City, Singapore, Germany, Australia and Hong Kong. It ranked California first for 'talent' and 'capital', the United Kingdom first for 'government policy' and New York City first for 'demand'. For the past few years, PwC has posted a report called the "Global Fintech Report". The

2019 report covers many topics of the financial technology sector, describing the landscape of the "Fintech" industry, and some of the emerging technologies in the sector. And it provides strategies for financial institutions on how to incorporate more "fintech" technologies into their business.

Outlook

Finance is seen as one of the industries most vulnerable to disruption by software because financial services, much like publishing, are made of information rather than concrete goods. In particular blockchains have the potential to reduce the cost of transacting in a financial system. While finance has been shielded by regulation until now, and weathered the dot-com boom without major upheaval, a new wave of startups is increasingly "disaggregating" global banks. However, aggressive enforcement of the Bank Secrecy Act and money transmission regulations represents an ongoing threat to fintech companies. In response, the International Monetary Fund (IMF) and the World Bank jointly presented Bali Fintech Agenda on October 11, 2018 which consists of 12 policy elements acting as a guidelines for various governments and central banking institutions to adopt and deploy "rapid advances in financial technology". The New York Venture Capital Association (NYVCA) hosts annual summits to educate those interested in learning more about fintech. In 2018 alone, fintech was responsible for over 1,700 deals worth over 40 billion dollars. In 2021, one in every five dollars invested by venture capital has gone into fintech.

Challenges and solutions

In addition to established competitors, fintech companies often face doubts from financial regulators like issuing banks and the Federal Government. In July 2018, the Trump Administration issued a policy statement that allowed FinTech companies to apply for special purpose national bank charters from the federal Office of the Comptroller of the Currency. Federal preemption applies to state law regarding federally chartered banks. Data security is another issue regulators are concerned about because of the threat of hacking as well as the need to protect sensitive consumer and corporate financial data. Leading global fintech companies are proactively turning to cloud technology to meet increasingly stringent compliance regulations.

ACKNOWLEDGEMENTS

Author hereby thanks Dr.Sridhar Seshadri, Ex.Vice-Chancellor, for his continuous support, guidance and mentorship. His comments while reviewing this paper for publication are highly appreciable and well taken to modify this final version .

REFERENCES

[1]. Larabel, Michael (28 December 2017). "Syzbot: Google Continuously Fuzzing The Linux Kernel". www.phoronix.com/. Retrieved 25 March 2021.

[2]. Law, Laurie; Sabett, Susan; Solinas, Jerry (11 January 1997). "How to Make a Mint: The Cryptography of Anonymous Electronic Cash". American University Law Review. **46** (4). Archived from the original on 12 January 2018. Retrieved 11 January 2018

[3]. Lazarus, Ari (23 February 2018). "Phishers send fake invoices". Consumer Information. Retrieved 17 February 2020.

[4]. Lehman, Jeffrey; Phelps, Shirelle (2005). West's Encyclopedia of American Law, Vol. 3 (2 ed.). Detroit: Thomson/Gale. p. 137. ISBN 9780787663742.

[5]. Leigland, R (September 2004). "A Formalization of Digital Forensics" (PDF).

[6]. Lewis, James (February 2018). "Economic Impact of Cybercrime - No Slowing Down" (PDF).

[7]. Lieber, Ron (April 11, 2014). "Financial Advice for People Who Aren't Rich". The New York Times.(subscription required)

[8]. Liu, Jinan; Rahman, Sajjadur; Serletis, Apostolos (2020). "Cryptocurrency Shocks". SSRN Electronic Journal. doi:10.2139/ssrn.3744260. ISSN 1556-5068. S2CID 233751995.

[9]. Malvino, Albert P., & Brown, Jerald A. (1993). Digital Computer Electronics, 3rd Edition. New York, New York: Glencoe McGraw-Hill

[10]. Matteo D'Agnolo. "All you need to know about Bitcoin". timesofindia-economictimes. Archived from the original on 26 October 2015.

[11]. Michael G. Noblett; Mark M. Pollitt; Lawrence A. Presley (October 2000). "Recovering and examining computer forensic evidence". Retrieved 26 July 2010.

[12]. Millman, Renee (15 December 2017). "New polymorphic malware evades three-quarters of AV scanners". SC Magazine UK.

[13]. Milutinović, Monia (2018). "Cryptocurrency". Ekonomika. **64** (1): 105–122. doi:10.5937/ekonomika1801105M. ISSN 0350-137X.

[14]. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[15]. Nakashima, Ellen (26 January 2008). "Bush Order Expands Network Monitoring: Intelligence Agencies to Track Intrusions". The Washington Post. Retrieved 8 February 2021.

[16]. Null, Linda, & Lobur, Julia. (2019). The Essentials of Computer Organization and Architecture. 5th Edition. Burlington, Massachusetts: Jones and Bartlett Learning.

[17]. Pagliery, Jose (2014). Bitcoin: And the Future of Money. Triumph Books. ISBN 978-1629370361. Archived from the original on 21 January 2018. Retrieved 20 January 2018.

[18]. Parker D (1983) Fighting Computer Crime, U.S.: Charles Scribner's Sons.

[19]. Patt, Yale N., & Patel, Sanjay J. (2020). Introduction to Computing Systems: From Bits and Gates to C and Beyond, 3rd Edition. New York, New York: McGraw Hill Education.

[20]. Pernice, Ingolf G. A.; Scott, Brett (20 May 2021). "Cryptocurrency". Internet Policy Review. **10** (2). doi:10.14763/2021.2.1561. ISSN 2197-6775.

[21]. Perrin, Chad (30 June 2008). "The CIA Triad". techrepublic.com. Retrieved 31 May 2012.

[22]. Petzold, Charles. (2009). Code: The Hidden Language of Computer Hardware and Software. Redmond, Washington: Microsoft Press.

[23]. Pitta, Julie. "Requiem for a Bright Idea". Forbes. Archived from the original on 30 August 2017. Retrieved 11 January 2018.

[24]. Polansek, Tom (2 May 2016). "CME, ICE prepare pricing data that could boost bitcoin". Reuters. Retrieved 3 May 2016.

[25]. Ruddenklau, Ian Pollari,Anton (August 9, 2021). "Pulse of Fintech H1 2021 – Global - KPMG Global". KPMG. Retrieved January 3, 2022.

[26]. Sanicola, Lenny (February 13, 2017). "What is FinTech?". Huffington Post. Retrieved August 20, 2017.

[27]. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. **12** (2). ISSN 1558-7215.

[28]. Schueffel, Patrick (March 9, 2017). "Taming the Beast: A Scientific Definition of Fintech". Journal of Innovation Management. **4** (4): 32–54. doi:10.24840/2183-0606_004.004_0004.

[29]. Scott, John Clark. (2009). But How Do It Know? The Basic Principles of Computers for Everyone. Oldsmar, Florida: John C. Scott.

[30]. Stevens, Tim (11 June 2018). "Global Cybersecurity: New Directions in Theory and Methods" (PDF). Politics and Governance. **6** (2): 1–4. doi:10.17645/pag.v6i2.1569.

[31]. Stoneburner, G.; Hayden, C.; Feringa, A. (2004). "Engineering Principles for Information Technology Security" (PDF). csrc.nist.gov. doi:10.6028/NIST.SP.800-27rA.

[32]. Van Loo, Rory (February 1, 2018). "Making Innovation More Competitive: The Case of Fintech". UCLA Law Review. **65** (1): 232.

[33]. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 978-0-201-70719-9.

[34]. Warren G. Kruse; Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 978-0-201-70719-9. Retrieved 6 December 2010.

[35]. Webroot (24 July 2018).