Undergraduate Thesis Prospectus

Broadcasting System: Integrating mass messaging with an internal notification system

(technical research project in Computer Science)

Cybercrime vs Cybersecurity

(sociotechnical research project)

by

Michael Acolatse

October 27, 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Michael Acolatse

Technical advisor: Briana Morrison, Department of Computer Science

STS advisor: Peter Norton, Department of Engineering and Society

General Research Problem

How can cybercrime be prevented?

Cybercrime is a rising technical problem. While technology allows for increased interconnectedness, it also brings the risk of theft, fraud, and abuse (CISA, 2018). CISA is a government agency that works with the Department of Homeland Security (DHS) to solve these issues by conducting investigations, recruiting and training experts, and setting up standardized methods. Cybercrime endangers society so it is important to prevent it. As the use of IOT devices becomes more widespread, cyber threats become increasingly prevalent to the general public. Recently, CISA put out an insight "Public and private entities in Ukraine have suffered malicious cyber incidents, including website defacement and private sector reports of potentially destructive malware on their systems that could result in severe harm to critical functions" (CISA, 2022). This shows that cybercrime is an issue that needs attention.

Broadcasting System: Integrating mass messaging with an internal notification system

How may an internal chrome extension alert all Google engineers to a technical emergency?

This technical project was for an internship not associated with a class. An internal workflow team needed to mass notify engineers of a technical emergency via a chrome and dashboard notification. My task was to design and develop this system with support from my team. On December 1st, 2021, a security vulnerability was found in an open-source library called

Log4j. This called for engineers to ensure nothing was at risk from the technical threat. The internal workflow team was asked to send a warning message through their system. This internal tool has a user base of approximately 4,000 engineers so the message would have a significant reach. However, the team did not have a way to send out mass notifications since it was designed for individual notifications. This situation led to the idea of a broadcasting feature. The tool was recently launched in all the engineer's machines, increasing the user base from 4,000 to 100,000 engineers increasing the impact of the project.

Cybercrime vs Cybersecurity

How do users, financial cybercriminals, and cybersecurity engineers compete online to advance their respective agendas?

Digital transactions are subject to malicious activity. Through accessible technology, cybercriminals can commit financial crimes inconspicuously. In February 2018, the director of national intelligence and heads of the NSA, CIA, and the FBI warned that cyber attacks are one of the greatest national security threats (Borghard, 2018). Cybercriminals still attack the financial sector despite innovative security measures. Since private entities own and operate most of the financial sector's technical systems that would be targeted, U.S. government organizations (NSA, CIA, and FBI) and Section 9 firms must collaborate and work together in order to defend the homeland in cyberspace. (Borghard, 2018).

Participants include CISA, a government agency that studies and reports cyber and infrastructure security in the US (CISA, 2018). Their agenda involves strengthening cybersecurity and infrastructure protection across all levels of government. Participants also

include financial cybercriminals: these criminals operate on the basis of means, motives and opportunities (Ghosh, 2003). Participants also include cybersecurity engineers: Engineers are developing new ways to detect and test against cyber crime. Advanced security testing methods using a cyber-attack forecasting model are recently being utilized in the case of financial institutions. (Qasaimeh et al., 2022). With AI and deep learning, decision-making programs reveal patterns that engineers can use to prevent financial cyberattacks. Participants also include financial institutions: banks and companies that hold user finance. Lastly, participants include users of financial services: the internet society sheds light on the internet and advocates for a resilient internet including in hopes of bridging the digital gap between technology and the people(Internet Society, 2022).

Policymakers have developed programs to prevent financial cybercrime (Borghard, 2018). Focusing on the financial sector alone is not sufficient. Cyber criminals also manipulate trust to advance their agenda. CISA explains “Cyber threat actors are known to target managed service providers (MSPs) to reach their customers”(CISA 2022). Exploiting trust relationships in MSP networks allows cyber criminals access to victim MSP customers. As a result, service providers are urged to invest in cybersecurity services. These security services explain why the services are important to their customers, showing what can happen without their services, and emphasize building trust with their customers (Batavia 2022). Cyber criminals also pose as good firms to seem to be trusted by methods like phishing. The goal is to infect as many victims as efficiently as possible. (Computer Security Update 2012). Cyber criminals also use data collection to gain access to vulnerable users. Toolkits can be bought and downloaded by criminals which are run on commercial websites to find targets to exploit (Ghosh, 2003). User trust threats can be difficult for security entities to protect against. Education can help protect

against these threats. The Internet Society pushes for education on the internet as one of its goals (Internet Society 2022). CyberAngels is a program that focuses on teaching internet safety to families (CyberAngels 2022). This organization focuses on giving resources focusing on protecting against cyber threats. This method protects against the cybercriminals agenda of attacking the users trust.

CISA has partnered with nonprofits, middle and high schools, universities, and state school boards across the country to help incorporate cybersecurity concepts into classrooms (CISA 2022). This helps to advance their agenda by showing opportunities to young people. Furthermore, to encourage students to enter cybersecurity degree programs, CISA co-sponsors the CyberCorps: Scholarship for Service program, which offers scholarships for cybersecurity degree programs in exchange for service after graduation. They also have a website where they offer resources on cyber awareness, training and career opportunities. These efforts strengthen the cybersecurity workforce which contributes to their agenda of preventing cybercrime.

Cybercriminals are motivated by access to sensitive information or personal data, and generating profit. Three technical attacks used by cybercriminals include hacking, malware, and DDOS attacks (Moiseienko 2018). Ransomware is a major method that cybercriminals use to advance their agenda. By gaining access to sensitive information or interrupting services, they are able to use the interests of their victims against them. A study shows the prevalence of cybercrime in different countries (fig. 1). The data shows that cybercriminals are impacting the financial sector. Identity theft (IDT) is shown to be a major tool cyber criminals use to operate. CISA has resources directed towards prevention of identity theft. “Unfortunately, there is no way to guarantee that you will not be a victim of online identity theft. However, there are ways to

minimize your risk…"(CISA, 2022). It continues to list ways to minimize risk of identity theft and also explains how to know when their identity is stolen and what to do.

Cybercrime *i*	**Germany**	**United Kingdom**	**Netherlands**	**Poland**	**Estonia**	**Italy**
IDT wrt. online banking (%)	1.4	3.3	1.4	1.2	1.0	1.1
IDT wrt. bank cards (%)	3.5	4.8	2.0	0.9	1.7	2.7
IDT wrt. PayPal (%)	2.0	2.3	0.7	0.8	0.4	0.9
Online shopping fraud (%)	8.4	9.0	10.3	9.7	9.1	5.0
IDT wrt. online shopping (%)	4.3	4.1	1.1	0.9	0.8	1.9
Extortion (%)	5.1	2.8	1.1	1.4	0.6	1.5
Scams (%)	5.0	4.4	2.3	3.4	1.7	2.4
Total (%)	**22.2**	**21.6**	**15.7**	**13.9**	**13.2**	**12.1**
For comparison: Malware (%)	51.5	50.5	48.8	68.1	55.7	60.1

Figure 1. Cybercrime prevalence over the last 5 years by type of cybercrime i and country j (Markus, 2018)

Cybercrime is developing. A report for an international cyber policy center states, "Cybercrime can no longer be regarded as an emerging threat, but the reality of modern criminality"(Jeffray, 2015). Participants that align with cybersecurity pushes to use high tech solutions by buying security services but also use high sosh techniques of education which prevent cyber attacks and also strengthen the cybersecurity workforce. Cybercriminals work

towards innovating their technology but also use high sosh methods of manipulating the trust of users and services.

References

Borghard, E. D. (2018). Protecting Financial Institutions Against Cyber Threats: A National Security Issue. Carnegie Endowment for International Peace. JSTOR

CyberAngels. (n.d.). https://www.cyberangels.org/about/

CISA (n.d.). Cybersecurity and Infrastructure Security Agency.

Ghosh, A. (2003). Sizing the Opportunity for Opportunistic Cybercriminals. *Journal of Information Warfare, 2*(1) , 80–89. JSTOR

High Wire Networks (2022, May 20). How to Sell Cybersecurity Services.

Internet Society. (2022, July 12). https://www.internetsociety.org/

Jeffray, C., & Feakin, T. (2015). Underground web: The cybercrime challenge. Australian Strategic Policy Institute. JSTOR

Moiseienko, A., & Kraft, O. (2018). The Financial Dimension of Cybercrime. In From Money Mules to Chain-Hopping: Targeting the Finances of Cybercrime (pp. 7–22). Royal United Services Institute (RUSI). JSTOR

Qasaimeh, M., Hammour, R. A., Yassein, M. B., Al Qassas, R. S., Torralbo, J. A., & Lizcano, D. (2022). Advanced security testing using a cyberattack forecasting model: A case study of financial institutions. *Journal of Software: Evolution and Process*. https://doi.org/10.1002/smr.2489 [Original source: https://studycrumb.com/alphabetizer]

Riek M., and Böhme, R. (2018). The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates. *Journal of Cybersecurity 4* (1).

Worldwide Videotex (2012, Aug.). Cybercriminals Spam Victims Posing as Good Firms. *Computer Security Update 13*(8), 5-7. JSTOR.