A brief overview of Cybersecurity

By: Chan Z. S., Loh Y. Y., Peh, A. T. W., Loh Z. X., & Lo, J. M. C | 11 November 2022

Written for the partial completion of NTU's CC0002 Navigating the Digital World

---

Our world has split into two. While we exist in the physical realm, we are increasingly reliant on the digital realm. We are more efficient and productive because we use it as a tool to enhance our way of life. An example of a sector going digital is the government's infrastructure, such as Singpass and national healthcare records (Teo, 2021). Doctors nation-wide are able to access up-to-date patient records and thus are enabled to give epistemologically-based standardised treatment. These systems must be protected because we, the users, are harmed by cybersecurity attacks. It disrupts our way of life and violates our privacy by making confidential information public. This is why corporations, governments and users must work together to maintain and strengthen the cybersecurity of our systems.

This paper will examine a case study on cybersecurity and recommend cybersecurity practices that general users can follow to keep themselves safe. First, this paper will discuss "HACKING GOOGLE", a mini-series by Google about Operation Aurora (a cybersecurity attack by China on Google's systems). Second, this paper discusses hardware and software vulnerabilities and cybersecurity techniques. Third, end-user best practices in maintaining cybersecurity will be discussed. Finally, the limitations of this paper will be noted in the conclusion.

Definitions

To discuss cybersecurity, this paper uses the following definitions —

The National Institute of Standards and Technology [NIST] (*IT System*, n.d.) defines an "Information Technology system" (IT system) as "a collection of computing and/or communications components and other resources that support one or more functional

objectives of an organisation".

The Cybersecurity and Infrastructure Security Agency [CISA] (2019) defines cybersecurity in two core aspects: the act of "protecting networks, devices, and data from unauthorised access or criminal use" and the "practice of ensuring confidentiality, integrity, and availability of information".

IST (*Cyber Threat*, n.d.) defines cyberthreats as "Any circumstance or event with the potential to adversely impact organisational operations [...] through an information system via unauthorised access, destruction, disclosure, modification of information, and/or denial of service."

NIST (SAMATE, n.d.) established a Bugs Framework (BF) to define and organise the various classifications of "bugs", which are "coding error[s] that needs to be fixed". The same framework also defines vulnerabilities as "an instance of a weakness type that leads to a security failure". Thus, a bug can lead to malicious acts, or be inherently harmless by causing a software to operate in unintentional ways. Compared to bugs, vulnerabilities are gaps in a system that will lead to cyber attacks.

From the definitions of cybersecurity and IT systems, the distinction between the two means it is not sufficient to only protect a system from attacks. It is also necessary for a system to be confidential and only available to those who are authorised. For example, if no one is attacking the Nanyang Technological University (NTU) database, but non-authorised members are able to access confidential information, the system is deemed unsafe.

Case study: HACKING GOOGLE

On 7 October 2022, Google launched a 5 part mini-series on YouTube called "HACKING GOOGLE" (Google, 2022). They discussed "Operation Aurora", a cyber attack launched by the government of the People's Republic of China on Google's systems (Google, 2022; ScienceDirect, n.d.; Ali, 2022). The incident occurred over several months in 2009.

Google went public on 12 January 2010, being not only the first major company to do so in the cybersecurity scene, as announcing cybersecurity incidents was not the industry standard back then, but also revealing that a government attacked a private corporation, the first of its kind.

In the report, Google stated that China's motivations remain unclear (Google, 2022; ScienceDirect, n.d.; Ali, 2022). The attack utilised a zero-day vulnerability within JavaScript on Google's machines, where employees clicked on phishing links, which led to the unintentional download of Hydraq, a trojan malware. Hydraq opened a backdoor within the machine, allowing China to spy on the information within Google's systems. During the attack, Intellectual Property (IP) theft occurred, along with Cyber Espionage on the Gmail accounts of Chinese dissidents and human rights activists. Ultimately, Hydraq was discovered and eradicated after Google did a hard reset — unplugging all machines, cutting everyone (both internally and externally) from the system, and resetting all passwords. While the purge was extreme, it was necessary.

From this case study, two insights can be made: (1) any sufficiently complex systems will have an unavoidable multitude of bugs. (2) cyberthreats come in all shapes and forms. Pre-Operation Aurora, companies had a different approach with cybersecurity. It was unthinkable that such a powerful force would violate a company's system. Now, companies and governments recognise cybersecurity for what it truly is. This will be explored in a later section.

Google's vested interest in cybersecurity is unique in two ways: (1) because of Operation Aurora and (2) because the company controls large quantities of sensitive information. Google's search engine is designed to analyse and disseminate information. Governments and private corporations rely on Google being secure as they submit sensitive data to Google's databases. If Google sorts information incorrectly, i.e. listing sensitive

information under public-accessible databases, security breaches will occur. This will be Google's fault, undermining the reputation of their service.

Motivations behind cyber attacks

The motivations behind cyberthreats are vast. In general, there are three types of hackers: white-hat, black-hat, and grey-hat hackers (Zetter, 2016). White-hat hackers are ethical hackers; They are security experts who hack to identify vulnerabilities within systems to discover and fix them. Black-hat hackers are unethical hackers; some steal from financial institutions, others steal sensitive information and hold it ransom. Grey-hat hackers are neither ethical nor unethical; they are independent hackers who sell their discoveries to governments and companies for personal profits.

In the case of Operation Aurora, China could have been politically motivated to attack Google, as they (China) wanted private information about their citizens and to undermine the credibility of a company (Google) of their rival global superpower (The U.S.).

Google's response to Operation Aurora

Google responded to Operation Aurora by restructuring their cybersecurity protocols to contend emerging threats. They created director-level positions and formed specialised teams. One such director is Stephan Micklits of Engineering, who's job is to manage Google's global privacy and security (Friedli, 2022). He works with Google's "Red Team", who constantly attack the system without notifying anyone about the specific details until vulnerabilities are fully exploited. After every successful attack, the Red Team builds and publishes security features throughout Google and to a centralised, public database where companies can modify and utilise such security patches.

Another such team is "Project Zero" (Greenberg, 2014), experts who hunt for "zero-day vulnerabilities", bugs that have been discovered but not patched. They exploit both Google and non-Google systems and produce case reports describing the nature of the

vulnerabilities and how to patch them. The team then sends the report to the companies they hacked. If said companies fail to ratify the vulnerabilities within 90 days, the team publicises the vulnerabilities, forcing said companies to fix the bug. The team found 58 zero-day cases in 2021, compared to 25 in 2020, highlighting the vastness of such vulnerabilities.

By doing so, Google systematised and standardised internal cybersecurity standards. They also made the internet safer as the same frameworks are implementable elsewhere.However, Google recognises its limitations. This is why they employ the help of members of the public through the Bug Hunter's programme (*Bug Hunters*, n.d.) where members of the public can report their discoveries for financial rewards under the Vulnerability Reward Program [VRP\ (HT Tech, 2022). Since its inception eleven years ago, Google has paid US$35,628,309 in rewards.

Hardware security

As a system consists of both hardware and software, each must be equally protected. Google advocates for Multi-Factor Authentication [MFA], where users must input several types of data, such as (1) knowledge, i.e. passwords, (2) possession, i.e. using a trusted device, and (3) inherent, i.e. biometric data (Google, 2022). Google mandates its employees to use a "Titan Security Key" (*Titan*, n.d.; Google, 2022), a physical biometric key which encompasses possession and inherentness in a MFA. Google claims this reduces successful phishing attacks to zero (Google, 2022). With only one factor of authentication, one's security is weak. Passwords are easily stolen as it is digital. If a user employs MFA, hackers will need all factors of authentication to gain access. As some factors of authentication are digital, while others are physical, it would become infeasible to gain unauthorised access to one's account.

Google launched the Titan Security Key to the public, allowing users to link the key to their accounts. The key interfaces with most devices either through a USB port or a

[Near-Field Communication] NFC input, the same technology that enables contactless payment (Apple's Paywave, Singapore's public transport gantries; Apple, 2022; Smart Nation Singapore, 2019).

Google also launched "Cloud HSM", an online course about hardware cybersecurity (Ramesh, 2018; *Cloud HSM*, n.d.). This advanced course is for users who wish to encrypt data through hash functions on Google cloud. The course is "FIPS 140-2 Level 3 certified HSMs", i.e. it meets the standards for usage within the healthcare and financial sector. However, a system's hardware can be exploited. Vulnerabilities such as "side channel attacks" and "rowhammer attacks" exploit the fundamental protocols that allows machines' hardwares to interface with its softwares (Fournaris et. al., 2017). To patch such vulnerabilities, companies require updating the hardware itself. Thus, outdated hardware do pose as cybersecurity risks.

Software security

One way unethical hackers can steal sensitive information is through phishing, the coercion and theft of sensitive information by pretending to be an authoritative figure or the likes (DBS, 2021). A common phishing tactic is to pretend to be a financial institution, such as a customer representative of DBS. Hackers then send an official looking email and convince unsuspecting users to click a harmful link. Users who click such links unintentionally share passwords to hackers, resulting in identity theft and more. Phishing scams are so commonplace that in two months, 900 police reports were made by victims (SPF, 2022).

Google acknowledged this, which motivated them to strengthen Gmail's filters (Google, 2022). Google scans and analyses every email for potential scams, and blocks 100 malicious emails per second. These filters are dynamic, constantly learning from what has been blocked in real-time, allowing for it to keep up with the evolution of scams. Google

boasts a 99.9% success rate with its filter.

Google also launched the "Advanced Protection Program" (*Advanced*, n.d.), a programme that allows any user opt-into enhanced software protocols. Users under this programme will experience more rigorous checks, i.e. when downloading an app, Google will analyse it under a stricter protocol to weed out even more potentially malicious threats. Additionally, personal information associated with the user's Google account will be kept under stricter protocols, i.e. when third-party apps request for such information, users have to go through additional steps to release the data. Users are also required to utilise the Titan Security Key.

Best practices

Four cybersecurity practices will be discussed in this paper: (1) passwords, (2) VPNs, (3) keeping softwares up-to-date and (4) being alert of phishing tactics. Unfortunately, due to the scope of this paper, this list is not exhaustive.

Passwords are the first line of defence. All companies mandate passwords as log-in credentials. SingCERT (2022) outlines several good habits such as (1) having a unique password for every log-in credential, (2) creating strong passphrases, i.e. 12-characters long, mix of symbols, numbers, letters, (3) changing passwords every few months, (4) enabling Multi-Factor Authentication [MFA]. By adhering to this, passwords will take unreasonably long time and resources to gain access (WEF, 2021).

Virtual Private Networks [VPNs] are digital network tools that allow users to hide their internet usage information from Internet Service Providers [ISPs] and others (CISCO, n.d.). For example, if a user is not using a VPN and a hacker is listening to the user's internet usage, the hacker can see everything the user does, e.g. what passwords they use, their bank account details if they log-in to their iBanking services. Under the same scenario, if the user is using a VPN, the hacker will only see lines of gibberish as all data is encrypted and routed

through the VPN servers.

All applications that one uses should be kept up to date, as outdated software may have zero-day vulnerabilities which have been patched by latest updates (Hetler 2022). With each new update, additional functionalities may be added, or vulnerabilities may be patched. Users should be alert to potential phishing attacks so that one can avoid it. Gosafeonline (2021) outlines 6 common characteristics: (1) mismatched and misleading information, (2) the use of urgent or threatening language, (3) the promise of attractive rewards, (4) requests for confidential information, (5) suspicious attachments such as files and links and (6) unexpected emails from both known and unknown recipients.

There are other practices users should adhere to in order to ensure their safety online. Users should only connect to trusted WiFi networks and avoid accessing sensitive information in public spaces as hackers may control such networks.

In general, when sending an email to hundreds of recipients, one should utilise the blind carbon copy [BCC] feature in order to keep email addresses private. Additionally, users should not insert foreign, unknown objects such as USB drives found in public into personal devices. Such devices may be malicious and harmful. Users should also not download unknown applications such as pirated games from websites, as users may be downloading malwares. Users should also keep their anti-virus softwares up-to-date, usually done by updating their operating systems [OS] such as Windows or MacOS. Companies such as Microsoft and Apple ensure their customer's data's safety by including security updates. Users should also run manual virus scans periodically to ensure their safety.

Conclusion

This paper has explored what cybersecurity standards currently are. However, it has not discussed what cybersecurity standards ought to be.

Not everyone is able to follow the cybersecurity guidelines outlined in this paper. Those who

are technologically unfamiliar are both vulnerable to attacks and are the vulnerabilities. Thus, cybersecurity must be universally accessible.

Due to the scope of this paper, this statement is not proven to be true or false. It is a conclusion that is arrived at after analysing the current standards. Tangentially, several questions remain unanswered. How should companies adapt to evolving cyber threats? Should emerging technologies be adopted into cybersecurity infrastructure? How can users ensure they are not misinformed or disinformed about cybersecurity standards? What information should technological companies have in the first place? How can we mitigate the social severity of cyberthreats?

These questions must be addressed so that comprehensive cybersecurity standards can be created. Users, companies and governments must discuss and shape the digital world for the better.

References

Apple (n.d.). *Apple Pay security and privacy overview*. https://support.apple.com/en-sg/HT203027.

Cisco (n.d.). *What Is a VPN? - Virtual Private Network*. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html.

Computer Security Resource Center [CSRC] (n.d.). *IT System*. National Institute of Standards and Technology [NIST]. https://csrc.nist.gov/glossary/term/it_system.

Computer Security Resource Center [CSRC] (n.d.). *Cyber Threat*. National Institute of Standards and Technology[NIST]. https://csrc.nist.gov/glossary/term/cyber_threat.

Cybersecurity and Infrastructure Security Agency [CISA] (2009, May 6). Security Tip (ST04-001) - What is Cybersecurity?. https://www.cisa.gov/uscert/ncas/tips/ST04-001.

Friedli, S. (2022, August 8). *Meet the team responsible for hacking Google*. Blog - Google. https://blog.google/technology/safety-security/meet-the-team-responsible-for-hacking-google/.

Fawad A. (2022, March 16). *Everything You Need to Know About Operation Aurora*. MakeUseOf. https://www.makeuseof.com/operation-aurora/.

Gosafeonline (2021, June 28). *Cyber Tip - Spot Signs Of Phishing*. DBS. https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/spot-signs-of-phishing.

Google (n.d.). *Advanced Protection Program*. https://landing.google.com/advancedprotection/.

Google (n.d.). *Cloud HSM*. https://cloud.google.com/kms/docs/hsm.

Google (n.d.). *Google Bug Hunters*. https://bughunters.google.com/.

Google (n.d.) *Titan Security Key*. https://cloud.google.com/titan-security-key.

Google (2022, October 3). *HACKING GOOGLE*. YouTube. https://youtube.com/playlist?list=PL590L5WQmH8dsxxz7ooJAgmijwOz0lh2H.

Greenberg, A. (2014, July 15). *Meet 'Project Zero,' Google's Secret Team of Bug-Hunting Hackers*. Wired. https://www.wired.com/2014/07/google-project-zero/.

Hetler, A. (2022. May 18) *5 reasons software updates are important*. TechTarget. https://www.techtarget.com/whatis/feature/5-reasons-software-updates-are-important.

HT Tech (2022, August 21). *Joy for bug bounty hunters! Google has paid over $29 million in bounties so far to 2022 researchers*. Hindustan Times. https://tech.hindustantimes.com/tech/news/joy-for-bug-bounty-hunters-google-has-paid-over-29-million-in-bounties-so-far-to-2022-researchers-71627528233628.html.

Ramesh, P. (2018, August 23). *Google introduces Cloud HSM beta hardware security module for crypto key security*. Packtpub. https://hub.packtpub.com/google-introduces-cloud-hsm-beta-hardware-security-module-for-crypto-key-security/.

Singapore Police Force [SPF] (2022, February 24). *Police Advisory – Re-Emergence Of Phishing Scam Involving Impersonation Of Spf Officers*. https://www.police.gov.sg/media-room/news/20220224_police_advisory_reemergence_of_phishing_scam_involving_impersonation_of_spf_officers.

SingCERT (2022, June 24). *Importance of Using Strong Passwords, and Ways to Safeguard Your Passwords and Accounts*. Cyber Security Agency. https://www.csa.gov.sg/singcert/Advisories/ad-2022-008.

Smart Nation Singapore (n.d.). *Contactless Fare Payment For Public Transport*. https://www.smartnation.gov.sg/initiatives/transport/contactless-fare-payment.

ScienceDirect (n.d.) *Operation Aurora*.

https://www.sciencedirect.com/topics/computer-science/operation-aurora.

Software Assurance Metrics And Tool Evaluation [SAMATE] (n.d.). The Bugs Framework (BF). National Institute of Standards and Technology [NIST]. https://samate.nist.gov/BF/.

Sgouras, K. I., Kyriakidis, A.N., Labridis, D.P. (2017, September 5). Short-term risk assessment of botnet attacks on advanced metering infrastructure. *IET Cyber-Physical Systems: Theory & Applications*, 2(3), 143-151. https://doi.org/10.1049/iet-cps.2017.0047.

Teo, J. (2021, October 12). *Boosting digitalisation will help in building a future-proof healthcare system: Forum*. The Straits Times. https://www.straitstimes.com/singapore/health/private-healthcare-players-vwos-need-to-step-up-data-sharing-says-healthtech-chief.

World Economic Forum (2021, December 7). *This chart shows how long it would take a computer to hack your exact password*. https://www.weforum.org/agenda/2021/12/passwords-safety-cybercrime/.

Zetter, K. (2016, April 13). *Hacker Lexicon: What Are White Hat, Gray Hat, and Black Hat Hackers?*. Wired. https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/.