EPiC Series in Computing

Volume 98, 2024, Pages 77–88

Proceedings of 39th International Conference on Computers and Their Applications

A Survey of Digital Security in Applications and Networking

Dylan Damiano, Isabella Mitchell Wynter, and Emdad Ahmed

Department of Mathematics and Computer Science
Central State University, Wilberforce, OH, USA
[ddamiano.csu, iwyntermichel.csu, eahmed]@centralstate.edu

Abstract

From the time the Internet was invented to now, security standards have changed drastically. Security risks are not only applicable to businesses but also has spilled over into the government and personal realm as well. Newly created threats are being created every day and mitigation techniques need to be capable of being changed in a moment's notice. Cybersecurity is an environment in which one must adapt to changes or else they will lose.
Keyphrases: SHA, RSA, public key, private key, asymmetric key, plaintext, digital signature, security.

1 Our Contribution

Throughout the course of this paper, our overall contribution is to better explain Cybersecurity concepts to those who are new to the field of study or are currently in it. Additionally, we seek to future explore and explain methods for securing data from maliciously-intentioned individuals. Review of both new and old information is always important and we are here to do just that. By exploring events such as the Florida's water treatment plant incident, we can recall the overall goal of Cybersecurity and prevent similar incidents in the future. Additionally, we explore different techniques to secure not only systems but also that of data. We hope to garner renewed interest in both new and older individuals to this field.

2 Rundown of Security Concerns

Security has become an important aspect in day-to-day life. Regardless of whether we are walking out in public or surfing the Internet, we wonder how much information about us or perhaps other people that may be floating around. In the sense of Cybersecurity, security can potentially fall under one of the five non-exhaustive umbrellas such as: Critical Infrastructure Security, Application Security, Network & Operating System Security, Cloud Security, and Internet of Things Security.

Each mode of security has its own concerns and approaches that security analysts need to consider. Some aspects of Cybersecurity are also more important than others as there are

different fallouts depending on where an attack occurs. For instance, an attack that halts the operation of an email service will certainly be damaging to both individuals and corporations alike. Furthermore, an attack on a personal computer will certainly almost always be the fault of negligent use of an operating system because of lack of due regard based on the usersś interactions.

2.1 Critical Infrastructure Case at Water Plant

Consider the case of a water treatment facility in Florida. On February 9, 2021, there was a reported break-in on an Information System. Security Magazine reported that after gaining access to the system, the attacker deliberately increased the concentration of sodium hydroxide from 100 parts-per-million (PPM) to 11,100 PPM [8]. According to CNN, the software that was at fault for the attack was TeamViewer [12], which has not been used for nearly six months. Building upon what was provided by CNN, considering that TeamViewer hasn't been used nearly six months. Some interfences as to how this was caused could be that the software had a security flaw or that credentials were cracked.

Fortunately for the treatment facility, they relied upon fault tolerance to reassure the public that their water was safe to drink. It would have taken 24-36 hours for the potential victims to have ingested dangerous water [8]. As we see, they successfully thwarted the threat contingency planning. As technology continues to grow, threats towards critical infrastructure just like the cyberattack on the water plant in Pinellas County will only continue to get more complex, which in turn requires more advanced measures to protect such infrastructure [8].

2.2 Application Security

Application security is defined by VMWare as "the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification" [15]. By ensuring the security of our applications, we can ensure that customer or employee data is secure and that it will not fall into the hands of bad actors. There are many applications on the Web that have a total disregard for security but instead just focus on getting the job done. The implementation of application security solely relies on the development team, government legislation and consumer feedback.

Application security can be maintained by not trusting user input, essentially a "zero-trust" framework. Therefore, everything that we ask the user for must be sanitized for only the relevant information that we absolutely need to perform a database query, file operation, or memory operation. Most attacks directed towards user input are preventable. Some examples of these attacks include SQL Injection, cross-site scripting (XXS), or improperly configured settings [11].

2.2.1 Application Configuration

Application configuration itself is a straight forward issue. Like that of SQL but much more preventable.

When administering changes to an application, it is highly advisable that the user or system administrator is knowledgeable in making changes for the said application. Although application security varies from application to application it is advisable to consult with documentation from reputable sources when in doubt. Even though security varies from application to application, there are universally acknowledged features as to what makes an application secure,

such as [15]: Authentication, Authorization, Encryption, Logging, and Application Security Testing.

Authentication If an organization does not have authentication, then they are certainly inviting trouble. There are various modes of authentication, many of which pertain to file permissions and access controls (discussed later). There are four advanced forms of authentication and one basic form, which is the use of password protection. IBM lists the many forms of authentication such as [9, 5]:

- Multi-factor Authentication
- Biometrics
- Token Authentication
- OAuth Authentication

Additionally, if some platforms allow us to stack two or more forms of these advanced authentication measures on top of each other, those will further safeguards our account.

Authorization Authorization asks the "do you have permissions?" question. Furthermore, it answers the question by checking a storage configuration file in an operating system or application to ensure that a user cannot access what they do not have permission to access. Authorization plays an important role in security as it can also prevent users from reading files that are not intended for them but also to prevent overwriting, appending, or deleting files as well. Without the authorization step, we are certainly running a risk of potentially losing valuable data.

Encryption Encryption builds upon the Authentication and Authorization aspect of Application Configuration Security.

There are many encryption standards available to developers and system administrators such as (but not entirely limited to) Caesar Cipher (highly unadvisable), AES, RSA, Salting, etcetera. The strength of the encryption depends on how sensitive the data is and how quickly one need to access it. The stronger the encryption scheme, the longer it takes to decrypt and encrypt with the key. The same concept of decryption with a key also applies to that of doing so without a key; if we attempt to decrypt without a key, we are in for an exorbitantly long wait to get what we are chasing after. Encryption is commonly used in securing passwords, sensitive user data such as files or personally identifiable information.

Logging System administrators should take logging (SysLog) into consideration for their security routines because it allows us to keep a paper trail of the activity that occurs on a system. Many operating systems offer this feature, including those of Linux Distributions. Furthermore, applications may also have logging built into them to allow us to view the events that were performed throughout the duration of its runtime.

Logging allows the administrator to travel back in time to see network related events, user account control activity, startup, and shutdown events, etc. Basically, if it is operating on a computer, there is a way to monitor its activity from Power On Self Test (POST), BIOS/UEFI, Booting (stage I, II Bootloader) to shut down; however, there is nothing to monitor when a computer is powered off.

There are many factors to take into consider, many of which are overlooked. It is often best to get an opinion from an outside party or from someone who is actually going to be using the said application to assess where to place more emphasis on security. Although, if we place emphasis on one aspect of security, that may lead to us to also having to place emphasis on a field that is just as similar to make the integrity or confidentiality of the data more robust.

2.3 Network Security

Network Security is "...the protection of underlying networking infrastructure from unauthorized access, misuse, or theft," as defined by Cisco [6]. Network Security is also an integral part of Cybersecurity as there are many devices that we have to protect from outside threats. Additionally, networks don't have one type of device on them but rather a variety of different devices such as: Laptops, Desktops, Phones and Intermediary Services Layer (2, 3, 4 devices).

To maintain a properly security network, firewalls (*which can be of two types: hardware and software*) should be properly configured and authentication mechanisms need to be installed on all hosts and intermediary devices. Without such preventative measures, attacks may be able to reconfigure our switch by Telnetting (TELNET) (*listens to port 23*) or Secure Shelling (SSH) (*listens to port 22*) in it's virtual terminals from anywhere in the world. Furthermore, if an attacker gains access to a intermediary device they can view all network communication (say, by using open source tools such as WireShark) that occurs on such a device that it could cause a company or individual to leak valuable information about themselves or others.

Network Security can also be achieved by encrypting communications. That way, predetermined authorized devices can view information that is strictly intended for them. Few ways to do this are to implement: parity bits, checksums, Cyclic Redundancy Check (CRC) or use a secure-socket-layer channel on HTTP (*listens to port 80*) communications or using HTTPS (*listens to port 443*).

2.4 Cloud Security

Cloud Computing and it's Cloud Security have become a hot topic in computing today. With emerging services such as Azure, AWS, Google Cloud. International Business Machines (IBM) list some of the major challenges approaching cloud security such as [10]: Lack of Visibility, Multitenancy, Access Management and Shadow IT, Compliance, and Misconfigurations. According to IBM, there are three components to cloud computing [10]. These are: Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), and Software-as-a-Service (SaaS). Recently, few more terms are coming into play, such as: Function-as-a-Service (FaaS), Containers-as-a-Service (CaaS).

The cloud provides great reliability to resources that an individual may need access to. Furthermore, for example, if an employee needs to work from home, they can utilize the cloud to access company resources in order to properly get their tasks done for the day. First, a brief explanation or review of cloud services will be conducted then we will dive into the concerns that clouds over them as a whole.

2.4.1 Cloud Security Concerns

Cloud Security is huge because it is a continuously growing field. Cloud Computing allows individuals to store information from a distance or across the world. Furthermore, cloud computing makes hosting applications from our local network much easier as we do not have to open ports to ensure that traffic can get inside our network – making it more secure. Instead, an external

organization such as Amazon, Microsoft, or Google will typically handle this for an individual or business client at certain levels.

Lack of Visibility Exactly as it sounds, lack of visibility is the idea of not knowing what is going on within a cloud environment. IBM further describes the "Lack of Visibility" as "... [losing] track of how your data is being accessed and by whom" [10].

In a corporate environment, corporations may want their employees to work from home, furthermore, these employees will need to have access to corporate and clientele information that is stored on the cloud. However, the security of the computer that is owned and maintained by the employee is outside of the company's reach. A corporation may set policies that an employee must follow, however, these employees may disregard the policies as there is no supervisor present.

Multitenancy Multitenancy is the capability of containing many clients in a digital space under a service hat a organization may provide [10]. Multitenancy is an issue in the cloud because if one user gets infected on a machine that is not properly secured, then other machines on the cloud (including the host) can get infected as well [10].

For instance, if we deviate from the cloud environment for a second, imagine that someone has a machine with multiple users. On one machine, there can be any amount of users. Now if one user gets infected with Malware (*Malicious Software*) on one machine, then the Malware will spread to other user profiles as well, the same concept goes for the cloud. A cloud will consist of multiple machines that have to connect to it. So if a user can send or pull data from a cloud, then if a file is infected and not isolated from the cloud, then it would spread to the other 'sectors'. This is where cloud instances need to be totally isolated from one another by ensuring that data on one's cloud client cannot spread to another client on the cloud.

Access Management and Shadow IT IBM describes Access Management and Shadow IT as "... [restricting] access points across on-premise systems..." furthermore adding on "... dangerous for organizations that don't deploy bring-your-own device (BYOD) policies" [10]. Basically, when a user is unsupervised, they are capable of performing any action that they wish, if there are no access controls in place. On-site devices are more secure than allowing employees to access the corporate network remotely in a cloud because the network administrators can set more rigid security policies.

If an employee's device becomes compromised, an attacker will be able to use the said employee's credentials to access the corporate network assuming that the employee's device is also whitelisted and that they have access to their credentials as well.

Compliance IBM states that "regulatory compliance management if oftentimes a source of confusion for enterprises using public or hybrid cloud deployments" [10].

In the United States and the European Union (EU), there are laws that govern the collection of data and facilitating the privacy of such data. Not only are there laws of nations that one have to follow, but one also have to follow local laws. There are a few questions such as:

- What if an individual wants to view some one else's data from a nation that prohibits such data?
- Are there certain protections that apply to children?
- What are repercussions for not complying with local, national, or international law?

As we see, this becomes a headache and where having a legal team comes in great for making sure that some one's business or some one as an individual are storing the data correctly and accurately.

Misconfigurations Misconfigurations is huge in a digital landscape. This section ties very well into application security and is just as dangerous, if not more dangerous than application security as cloud services can be accessed by anyone anywhere at anytime without setting the right policies in place.

For instance, we want to use a database which happens hosted under the Infrastructure-as-a-Service umbrella [4]. If we set up our database to be accessible anywhere around the globe, we need to be sure that we are giving access to the correct individuals. In order to do this, we may need to filter access by IP Address, furthermore, implement an underlying password architecture. As an added security measure, we may need to encrypt the data in case unauthorized individuals were to bypass all of our two authentication and authorization security procedures. If we backtrack we see that without the IP whitelist, anyone can access; furthermore, they can now go straight to attempting to crack the password. Once they crack the password, they can attempt to obtain data. Configuring a cloud service to use more than one form of security is great for added redundancy.

Misconfigured cloud services led to approximately 86% of the data breaches for cloud services in 2019, according to data by acquired from IBM [10].

2.5 Internet-of-Things Security

The Department of Homeland Security (DHS) mentions that the capabilities that IoT provides is appealing to attackers as it has more interactions with highly valuable data because of it's close-up interactions consumers and manufacturers as a whole [13].

Basically, Internet of Things can consist of electronics such as Thermostats, Alarm Systems, Doorbell Cameras, Security Cameras etc. If it connects to the Internet and communicates with other devices by providing environmental or sensor-based information, then it classifies as IoT.

The security of IoT devices is critical because not only are they new but also they play a much more critical role in our personal lives. If an attacker wanted access to what is going on in one's front lawn or wanted to disturb one in their sleep with a false alarm, that certainly be an flagrant violation of privacy!

Not only can IoT Devices be used at home, but they can also be used in the workplace. In the workplace, we may find IoT devices keeping track of where products are at in a store, such as Amazon's cashierless "Go" store [7]. With digital devices, any type of attack is possible; therefore, if attackers wanted to, they could likely force a check-out process if the unsuspecting shopper was within the vicinity of the store. IoT is slowly becoming more mainstream, and the security of such devices will be important in the coming years.

3 Further Mitigation Techniques

Mitigation Techniques is not a one-size fits all. Each piece of technology in a network requires a different approach to safeguarding the operations that a system performs. We will further explore what common mitigation techniques exist and how to apply them into real world scenarios.

3.1 Basic Preventions

Although this seems to be harped on, we're going to keep harping on this until the point gets across. There are many forms of mitigation techniques that allow an organization or individual to better prepare for cyber-related events. Once again, this is not a one-size fits all and is not a comprehensive list so we must determine what fits our own needs.

Corporations may find hiring external contractors to come in and evaluate their systems is an excellent form of assessing the threats that exist and the vulnerability of their information systems. Furthermore, organizations will also find it useful to do activities such as train their employees to be more technologically literate, and question activities they do on the web prior to executing them.

As for individuals, they may not have the leisure to hire external consultants to come in an evaluate their personal devices, so they must resort to basic forms such as updating software, utilizing authentication techniques, installing anti-virus applications and so on.

3.1.1 Employee Training

The training of employees is generally a no-brainer. Employee training falls under the category of *Administrative Security*. With this in mind, administrators must account for the varying level of security background among their users.

Training employees will give them exposure to dangers that exist on the world wide web. Furthermore, it will not only make them more aware but also make them more technologically literate while also further developing their critical thinking and analytical skills.

Imagine if John wanted to click a link that led to "free-money.com" and download suspicious files for 'money!' That will almost certainly put his organization in jeopardy currently or at a later date. *All employees must be formally trained on how to handle scam on: phishing, vishing and smishing.*

3.1.2 Update Software

This falls under the category of *Logical Security*. Updating Software plays an important role in ensuring the proper operation of the application that we are wanting to use. For newer, maintained software, *software patches and service packs* are pushed as often as possible and as needed; however, for older, unmaintained software, patches are rarely pushed through and using this older software puts you at risk of inviting intruders into our system.

Not only should we update our Software for security considerations, but we should also update software as new updates bring better performance and new features. Why would we want to be left behind? Besides, staying ahead of the game is great as newer patches require hackers to change their approach. For instance, take a zero-day attack for instance. A zero-day attack occurs when a security flaw has yet to be discovered by the system administrators, software developers, or security professionals. The National Security Agency (NSA) future clarifies that "'N-day' exploits can be as damaging as a zero-day" [1]. In the context that the NSA has provided this, they are stating that zero-day exploits occur when they have not been discovered (only by the attacker), but when an "nth" amount of time has surpassed, in addition to not updating the software for that time frame, the damage can be just as bad if not worse.

3.2 Advanced Methods

There are many more advanced options to maintaining the integrity of our information system. Not only can we go out and purchase more complex hardware, but we can also write our own

software or go into our system and tweak less frequently used settings.

3.2.1 User Account Control

User account control is one of the many advanced methods that a system administrator can implement into their security policy. Not only is User Account Control (UAC) useful but it allows us as an administrator to predefine what users have access (e.g., Access Control List (ACL)) to in conjunction with what they are or are not authorized to do on an information system.

Applications of UAC Authorization If one have utilized a Windows device before, one may be very well familiar with User Account Control. User Account Control comes in handy when dealing with potentially malicious applications by prompting a user for administrator credentials. However, User Account Control is not only limited to Windows devices but can also be utilized in a Mac or Linux operating system as well. Many individuals may be familiar with trying to install an application, in which one were met with a faded screen with a security shield prompting for administrator approval. That is UAC at work.

3.2.2 Email Filters

Today, many individuals still get infected through a common form of Internet communication, which is email.

Often, we will see email being used in personal day-to-day interactions, business, or governmental communications. However, more often than not, both individuals and consumers are the common targets of malicious activity on the Internet.

Introducing email filters in a security policy is great because it allows you to filter out suspicious forms of communications or specifically warn that an email that was sent has suspicious signatures and clicking links should be exercised with caution. Email providers such as Yahoo and Gmail provide "SPAM" inboxes to filter out suspicious emails. However, even though email filters target suspicious emails, they also target emails with legitimate use. Back-tracking to training, if an email filter is implemented or not, individuals should always be trained on how to properly identify which emails look suspicious or not as clicking and downloading a dangerous file always traces back to the user. After all, we are our own best and worst email filter.

3.2.3 Firewalls

Firewalls are great for filtering network communications that are mission-critical or not mission-critical. In many cases, it is certainly advisable to close unused ports as unused applications for these ports can lead to your information system being unsuspectingly infiltrated later.

Let's for instance assume that we have an application that runs on a specific port. Furthermore, let's assume that an insider or another application has leaked the information for this 'specific port' out to a suspecting attacker. The application in question has the capability to execute any command or request that is provided to it. Certainly, we see the following risks:

- Open ports lead to backdoors.
- Applications with open ports and unpatched vulnerabilities are capable of being used for operations outside of their designated purpose.

Before opening a port on a system, one should ask themselves whether or not the port is going to be needed temporarily or long-term. Understanding the tasks that an application will perform on this type of port and it's potential users will allow professionals to further prepare for additional issues in the future.

Once again, this is not a complete list of questions, but rather rhetorical ones that lead to a bigger scope of ideas.

4 Encryption and Maintaining Privacy

So far, we have touched base on everything ranging from application security, system security, and real world scenarios. Furthermore, we also discussed different ways to mitigate threats. However, data encryption is worthy of it's own section. As noted back in the section "Network Security", what if devices are compromised from clients that do not reside in the same network? How do we protect this data? The simple answer is to give the attacker a harder time to essentially 'decode' the data which lies in a cryptographical concept called 'encryption.'

4.1 CIA Triad

Encryption is an implied-component of the CIA triad in security which refers to the Confidentiality, Integrity and Accessibility of data. Basically, this is a mnemonic to help security consultants and researchers remember what is at stake.

Confidentiality asks 'is this data private between a selected group of individuals?' Furthermore, Integrity allows us to develop methods such as checksums or simply ask whether or not a file has been modified by a 1st, 2nd, or 3rd party source; it further follows that accessibility ensures that data is able to be accessed at predefined moments by individuals who deem it's presence important. However, when it comes to the CIA triad, it is best to keep in mind to take a "zero-trust" approach as mentioned earlier in 2.2.

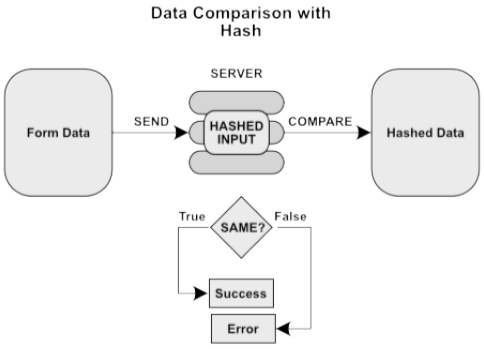

Figure 1: Hash and Comparison

4.2 One Hash, One Encryption

4.2.1 Why use encryption?

First, before beginning we must explain why one should use encryption. Everyone has had a situation at some point in their life where they reasonably want privacy between themselves and

another individual. Encryption facilitates privacy when two devices are communicating in the digital aspect. For obvious reasons, it would be bad if a third party or second party received information that they were not supposed to receive; in which politely asking one to 'delete' unintended communications can only go so far. So, to prevent so-called 'eavesdroppers', we introduce encryption because it can obfuscate. When performing encryption operations, there are secure and nonsecure ways; furthermore, security analysts and researchers should be aware of both, although that is outside of the scope of this paper!

4.2.2 Secure Hashing Algorithm

When we hear of SHA, we often think of a checksum or hashing a password. SHA is exactly that. Hashing is *one-way*, by practice a method that cannot be reversed; but instead, can be sidestepped using complex 'rainbow' tables of known hashes. As mentioned earlier, SHA can be used when computing a checksum or hashing a password. Essentially, we are encoding the text with the help of mathematical formula; after which, we could compare possible user-input with stored text and determine whether they are identical or different.

SHA comes in a variety of different flavors; the only noticeable difference is the length of the bits and the underlying algorithm [14]. The NIST states that there are three different types of SHA techniques currently out in the wild which are formally known as: *SHA1, SHA2, SHA3*. Each could be used for a variety of different reasons. The larger the bit-length of the underlying algorithm, the harder it is to not only collide but also to randomly guess and compute a list of all possible values by utilizing a rainbow table. For instance, one could easily convert a string to a hash in Python by utilizing the built-in "hashlib" module.

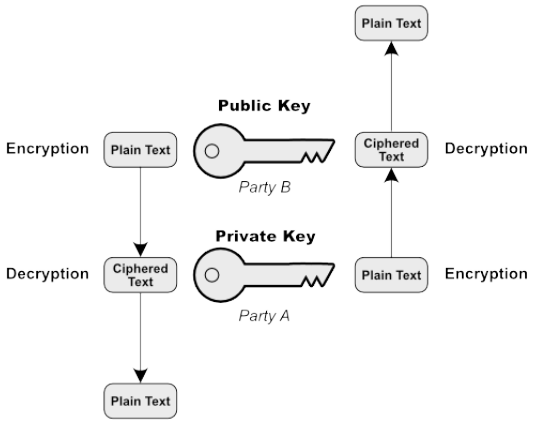

Figure 2: RSA Simplified

4.2.3 RSA

The Rivest-Shamir-Adleman encryption standard is a method to where we can not only encrypt data but also decrypt data [2]. This method is asymetric meaning that one need a private key and a public key. Usually, each party has one key. However, what does each key do?

The public key is known to encrypt data which will later be decrypted by a private key. Once the data is encrypted, one cannot decrypt it with the same key as that method is reserved for symmetric-key based algorithms. The public key works the same way, instead the process

between private and public key is reversed. The public key encrypts data for the private key. When conducting encryption operations, it is important to keep in mind that it is theoretically possible to break the RSA encryption scheme and it has been done. Although, to conduct a brute-force attack, it would require immense resources, which usually cannot be done in a timely manner when using complex algorithms [2].

As an added reminder this, we could encrypt plaintext with $pvt(c)$ and decrypt plaintext with $pub(m)$; conversely, one could encrypt with $pub(m)$ and also decrypt with $pvt(c)$. Instead of utilizing the method above, we could also use pre-created libraries or functions for the respective programming language that we are using, or perhaps a third-party application.

5 Related Work

5.1 Personalized Secure Communication

[2] briefly discussed the overall focus of cybersecurity and also discussed how the RSA algorithm works form a conceptual standpoint as well. Furthermore, they took a unique approach to RSA which involves obtaining a symmetric key for the encryption algorithm rather than a asymmetric. The method involves generating a key that can be added or subtracted meaning that the two parties communication with one another have the private and public key.

5.2 A Survey of Security in the Virtual Computing Cloud

[3] discuss the various types of cloud architectures and the security concerns revolving around them. The paper described doesn't dive into better techniques for securing such data but rather the techniques that the providers use to ensure the integrity and safety of information stored on their systems.

6 Conclusion and Future Works

Cybersecurity is overall about staying a step ahead of the threats and constantly being aware of the changing digital landscape. Cybersecurity has a lot of important parts and getting the basic security measures down makes a big difference. Furthermore, knowing what options are available to you assists you in making a better well-formulated decision. Cybersecurity is also a big deal on the on and off the web as it focuses on not only physically securing systems but also securing the software and hardware as well. Tampering with a system is much easier to do personally than it is to do over a stream of bits. Identifying our physical infrastructure that is critical and vulnerable is key to also ensuring our well-being as a civilized society. Without our vital infrastructure, there will be societal unrest. Preventing a cyberattack is also important from a business standpoint since there are potential ramifications such as legal penalties. Security concerns are only going to continue to grow as computers get more powerful. In future we will explore the use of machine learning in security and privacy.

7 Acknowledgement

This work is partially supported by the Department of Mathematics and Computer Science of Central State University as well as generous support from Google in the form of unrestricted gift.

References

[1] National Security Agency. Nsa's top ten cybersecurity mitigation strategies. *https://www.nsa.gov/portals/75/documents/whatwedo/cybersecurity/*, 2018.

[2] Emdad Ahmed, Scott Payne, and Craig Matherly. Personalized secure communication. In *The 33rd International Conference on Computer Applications in Industry and Engineering*, volume 75, pages 1–10, 2021.

[3] Jeremy Black, Bryan Freed, Jeremy St. Clair, and Emdad Ahmed. A survey of security in the virtual computing cloud. In *29th Annual Spring Pennsylvania Association of Computer and Information Science Educators (PACISE) Conference*, pages 62–68. California University of Pennsylvania, April 2014.

[4] BluePi. Different types of cloud computing service models. *https://www.bluepiit.com/blog/different-types-of-cloudcomputing-service-models/*, December 2015.

[5] National Cyber Security Centre. Authentication methods: choosing the right type. *https://www.ncsc.gov.uk/guidance/authentication-methods-choosing-the-right-type*, September 2022.

[6] Cisco. What is network security? *https://www.cisco.com/c/en/us/products/security/what-is-networksecurity.html*.

[7] D. Coldewey. Inside amazon's surveillance-powered, no-checkout convenience store. *https://techcrunch.com/2018/01/21/*, January 2018.

[8] M. Henriquez. Hacker breaks into florida water treatment facility changes chemical levels. *https://www.securitymagazine.com/articles/*, February 2021.

[9] IBM. Forms authentication. *https://www.ibm.com/docs/en/sva/9.0.4?topic=methods-forms-authentication*, March 2021.

[10] IBM. What is cloud security? *https://www.ibm.com/topics/cloudsecurity*, April 2023.

[11] Paul Ionescu. The 10 most commmon application attacks in action. *https://securityintelligence.com/the-10-most-common-application-attacks-in-action/*, December 2000.

[12] E. Marquardt, E. Levenson, and A. Tal. Florida water treatment facility hack used a dormant remote access software, sheriff says. *https://www.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html*, February 2021.

[13] Department of Homeland Security. Securing the internet of things. *https://www.dhs.gov/securingtheIoT*, June 2022.

[14] National Institute of Standards and Technologies. Nist policy on hash functions. *https://csrc.nist.gov/Projects/Hash-Functions/NIST-Policy-on-Hash-Functions*, June 2023.

[15] VMWare. Application security. *https://www.vmware.com/topics/glossary/content/*.