Michael Burns

CSC301-01

Professor Ola Ajaj

Final Cybersecurity Paper

Technology is involved more and more in our lives’ everyday. There have been so many breakthroughs and advances due to the innovation and development of technology. Our society would not be able to function without the current technology we have. However, with all these new advances to everyday life, there has also been many improvements to military equipment. Global powers have been replacing much of military weaponry with as much technology as possible. Cyber warfare is a new style of warfare that implements many uses of cybersecurity, and will continue to grow tremendously into the future.

Cyber warfare is a large domain with numerous aspects that are derived from it. One crucial aspect of cyber warfare is cybersecurity. Just the same way citizens, businesses, organizations protect their data from hackers, so do governments and military. Except there are even more substantial and strict practices they must follow. As citizens, we really are trying to diverge hackers from stealing our data by using strong passwords, changing them often and using two-factor authentication. While there are many more practices, these are the most practical and effective techniques to protect our data. Governments and militaries, on the other hand, have to be concerned with their data getting breached. This includes top-secret, classified information only meant to be in the hands of the government.

Cyber warfare changes an entire countries’ perspective on military resources. The idea of a sufficient and powerful military might have been thought as having the most advanced weaponry and armor for soldiers. It could also be thought of as having the most technologically advanced land vehicles, the most powerful tanks, the biggest ships and fastest planes. This would have been thought of as a powerful military before the age of computers. However, militaries now need to dominate the land, sea and air: as well as cyberspace. It is a new battle front that is fought not by pulling a trigger or dropping a bomb, but by using a keyboard. And that keyboard can hold more power than the most powerful piece of military equipment.

One recent example where cyberattacks have been prominent is the 2022 Russian Invasion on Ukraine. Russia is utilizing its military forces to overtake its opponent, and Ukraine is defending itself against all Russian attacks. From the media’s perspective, one can observe the destruction that has been caused in Ukraine. Russian fighter jets dropping bombs on the city, foot solider shoot-outs and some tension in the sea. One front that has not been thoroughly looked at since the start of the war has been cyberwarfare.

Until recently, there had not been much coverage on the events in cyberspace. That is until, The New York Times published an article around two weeks ago. The article describes how Microsoft had released a study about the cyberattacks that have been going on in Russia. What surprised experts in the study was how powerful Russia’s cyberarsenal is, and how they did not cripple Ukraine’s infrastructure within the first few weeks of the invasion. Russia is a world super world (Conger). Not only do they have a dominate military, but they’re cyberaresenal is incredibly advanced. Experts predicted that Russian hackers would have brought down Ukraine’s power grid and internet service providers and cut off President Zelensky from the rest of the world (Conger). These attacks would have crippled the entire infrastructure in Ukraine, including the military. Communication and electronic devices are so crucial in today's world that taking those two out will entirely cripple a nation.

The study conducted by Microsoft revealed that Russia used their superior hackers to conduct hacks across Ukraine (Conger). However, these attacks were more subtle, not really a “homerun” like causing a nationwide blackout (Conger). It turns out that Ukrainian hackers are the underdog and were much more skillful in defending off the superior Russian hackers. This surprised most experts in the study because of the shear strength of the Russian cyber sector.

The Russian cyber-attacks were done in order to propel the ground campaign on the Ukrainian front. However, Microsoft was unable to conclude whether or not the attacks were performed in synchronization with one another (Conger). For clarification, some examples of Russian hacks were pairing malware with missiles, including attacks on government agencies and TV stations (Conger). Microsoft had also concluded that Russia’s persistent use of cyberweapons suggested it had not played a significant role in the conflict.

Cyberwarfare is an important part of military defense that needs to be addressed and treated with much significant caution. One reason being that this issue needs to be discussed thoroughly with the public is because the DoD (Department of Defense) budget will most likely have to increase. There is currently controversy over the amount of national spending is dedicated to DoD already, considering the United States spends exponentially more than any other world superpower. To appeal to the public, who pay the taxes that fund government programs and spending, there must be emphasis on the fact that this new spending is absolutely necessary to protect infrastructure and to continue our standard of life.

Quite frankly, an effective war strategy is by disabling a countries’ communications. This is going back to the Civil War, when messengers on the battlefield were targets by the opposing military. The reason this is so effective is the value behind communication and coordinating in attacks. If a military cannot communicate to coordinate attacks, it doesn’t matter how powerful the military is, they are destined fail.

There are many extreme outcomes that can come from a successful cyber-attack. The worst-case scenario, in my opinion, would be nationwide blackout. A cyber-attack that would cripple the power grid, as well as taking down ISPs, would leave the country vulnerable to any attack. Citizens would not have the power to function as a society. Just take Internet out of the picture. Hardly any businesses, if any, would be able to go about their daily functions. Even though the United States has the world’s strongest military force, it would not matter when our equipment won’t be able to function.

Cyberwarfare can be avoided. The most effective techniques are to secure all forms of high-value assets that can be hacked. For example, government infrastructure needs to be secured to the highest it can possibly be. The most efficient tactic to make sure the systems are being secured is by providing adequate funding to the sectors that need it most. Without it, a cyber attack could cripple our countries’ entire infrastructure, leaving us vulnerable. It is quite scary to think about what the opposing country would want to do next.

Biometrics

Biometrics have become largely incorporated in society that we interact with them every day. It has become the new standard for automated security and authentication. Biometrics are body measurements and calculations to prove the authenticity of a person (Kaspersky**)**. There are many different types of biometrics, all with their specific purpose and use. However, every type of biometric has its pros and cons.

There are three types of biometric groups: biological, morphological, and behavioral (Kaspersky**)**. Biological biometrics uses traits that are fond at the molecular and genetic level. This may include DNA, blood, or bodily fluids. One type of biological biometric scan would be a blood test or hair sample (Kaspersky**)**. Morphological biometrics are based on the structure of your body, or physical traits. The scan observes features such as the shape or structure of the eye, face, or fingerprint (Kaspersky**)**. This form of biometrics is more popular and more acceptable as opposed to biological. Lastly, behavioral are based on a pattern related to a person’s specific behavior. This can include the way a person walks, speaks or writes (Kaspersky**)**.

We use biometrics every day, and the most popular type of biometrics is facial recognition. Majority of smartphones now use facial recognition on the lock screen to keep out unwanted users. Considering everyone uses their phone every day, facial recognition would probably be the most popular type of biometrics. Fingerprint scanners are probably the second most used. If a phone doesn’t have facial recognition, chances are it uses a fingerprint scanner to unlock it. Most laptops now come with fingerprint scanners to log in and/or make purchases as a more secure and quick method as opposed to typing in your password every time.

From a different perspective, when I used to work as a server in a restaurant, we would use the computer terminals to keep track of everything a table orders, split checks and send orders to the kitchen and bar. To be able to clock in using the computer, as well as access a table, you would need to put your fingerprint in every time. If another server wanted to look at your table, they would either need to put your fingerprint or a manager’s. This would help prevent any server’s accidentally going into a table that isn’t theirs and sending an order on the wrong table. This would cause a lot of confusion, and would make the actual server of that table look naïve doing their job.

The advances in technology have significantly improved the measures of keeping devices secured and locked out from intruders. On top of just securing your smartphone, facial recognition is utilized in a multitude of public services in order to keep the public and businesses safe. One prominent use of facial recognition technology is by law enforcement agencies. It is used to identify criminals and missing persons (Gargaro). The facial structures are stored in a database, and software is used to decipher the face of the person whom law enforcement is searching for. When searching for a criminal or missing person, law enforcement can use the facial recognition software to investigate potential matches in real-time (Gargaro). This use of biometrics helps immensely regarding locating criminals to give them the justice they deserve.

Another benefit of facial recognition biometrics is being used by medical professionals. In some cases, it is able to detect and notice genetic disorders (Gargaro). While this is still new and, in the works, the software is able to identify subtle facial features. It then takes that data and identify the genetic mutation that caused the disorder (Gargaro). This new form of facial recognition is not developed far enough to replace to strategies of identifying genetic disorders that already being used by medical professionals. However, with the further development of artificial intelligence, this technology may improve and be faster, more efficient, and less expensive that generic testing.

With all the advances being made with technology and the improvement of facial recognition technology, there are downfalls. While society is reliant upon technology, and it improves and becomes more reliable everyday, technology is still imperfect and has flaws. One issue is that it is less effective at making matches with people of color and women (Gargaro). The root cause of this is technology itself being imperfect. The algorithm used in the software to identify faces are better at identifying white males because the databases contain the most information about them. While it’s a positive the algorithm can identify white men sufficiently, the algorithm will continue to unintentionally make itself more biased (Gargaro).

Referring back to the point stated about facial recognition technology being used by law enforcement to catch criminals, sometimes it catches the wrong criminal. The software can improperly identify the criminal as someone who has a very similar facial structure (Gargaro). Unfortunately, this downfall makes the purpose of the software contradictive. There are more issues with recognizing faces. This can include the angle of the picture, the amount of light when the picture was taken or poor picture quality. Disguises are also worn by criminal to throw off their appearance, and this can trick the software (Gargaro).

There are issues with facial recognition software that conflict with privacy and personal rights. For one, everyone’s face has to be stored in a database in order to know which face to identify. This inflicts on privacy to the extent that two cities: Cambridge, Massachusetts and San Francisco, California have banned law enforcement’s real-time face recognition surveillance equipment (Gargaro). In these two cities, police are allowed to use recordings from personally owned security cameras, but using facial recognition software is banned.

While facial recognition software seems that it has many benefits when it comes to catching criminals and securing smartphones, people feel the opposite way. Being recorded and scanned makes people feel like they’re judged for their behavior (Gargaro). Running real-time facial recognition software also makes people feel like they’re being treated as a criminal. Being surveyed without probable cause can seem like it is an infringement of personal rights. There is no cause that you did something wrong, so is it justifiable that the police can choose to scan your face whenever they feel like it?

Cloud Security

Cloud computing is the delivery of computing services that include, but are not limited to, servers, storage, databases, networking, software, virtual computing power, that are used over the Internet or “the cloud” (Ranger). One benefit of cloud computing is the quick, reliable, and cost-effective measures of expanding a business’s technology department. Cloud computing is being adopted by more and more companies everyday due to its practicality and cost efficiency. While there seems to be only benefits to cloud solutions, there are security risks to be concerned about.

Cloud computing is revolutionizing technology practices. Whereas most companies would maintain own their own on-site technology equipment, like servers and storage devices, they now can rent the equipment that is stored in an off-site data center (Ranger). Contrary to popular belief that owning something, in the long term, is usually cheaper than renting does not necessary apply to cloud services. Companies only pay for what services they use. For example, say a company purchases a server, but only uses twenty percent of the total computing power on that device. It is a financial burden to have to purchase the entire server, install it on-site that takes up space, and be maintained either by the companies’ IT department or a third-party IT company. Then only use one-fifth of its total power. Cloud computing solves this.

A company will only pay for the services it uses. If the company only operates from nine to five, Monday through Friday, they can rent the server through a cloud service and only pay for the power utilized during those hours of operation. This significantly reduces the cost in the IT department and reduces wasted computing power. It is estimated that in 2022, almost two-thirds of spending on application software will be through cloud services (Ranger).

The backbone of cloud computing is the Internet. To use cloud services, you must use the Internet to connect to the data center in order to retrieve the data you want to access. One significantly used part of cloud services are phone and picture backups. You can back up all your pictures to your computer, and store them on the hard drive for free, or pay a few dollars a month for a cloud back up. One main difference here is that if your hard drive fails on your computer, you not only lose your phone back up, but everything on the hard drive as well. Unless you are using RAID (redundant array of independent disks), everything is gone. Whereas in the cloud, if that were to happen, all the data is backed up by RAID and there is virtually no loss of data.

Cloud computing is an evolving technology that is only predicted to get larger and larger. However, that comes with the cost of more security concerns. The more that a system is being used, the more of a chance there is that someone does not know the proper security configurations. This can lead to major data breaches, malware attacks, denial-of-service, etc.

One significant concern regarding cloud security is moving technology services from an on-premises location with trusted IT staff to a data center with unknown staff. This reduces the overall control that the company has with its data (Morrow). The company still has rights to its data stored on the rented equipment as well as the services rented, but it still is on a third parties’ equipment. There is less control now that the equipment is being overseen and secured by the cloud provider, which increases security risks (Morrow).

Another security issue that arises with cloud computing is having two separate technology entities: on-premise and staff employed by the cloud provider. Most companies need some type of IT department- whether that be a fully staffed full-time department or a contractor. When the hardware and software are no longer being fully serviced on site by the IT staff, and moves partially to the cloud, this is called a hybrid cloud solution (Morrow). While this sounds like a complex, efficient new form of computing, this can create new issues. Mainly, it can put significant pressure upon the on-site staff. They now need to know how to utilize the cloud with the backend of the on-premises technology, and it can get tricky (Morrow). There is crucial information and training that staff need to go through to ensure all new configurations are correct, secure, and efficient.

Furthermore, organizations that either have an over-worked IT department or no IT department at all runs into cloud migration issues or moving data from on site to the cloud. This process takes a long time, and an extreme amount of planning. A company with a tight budget might recognize the financial gain of a hybrid cloud solution, and want this change done immediately so the money saved can be spent in reinvesting in the business. Employees want to impress their boss. And bosses, for a lack of a better term, can be stringent with deadlines and want to advance quickly. Although computers are fast, small, and efficient, this is not a “copy and paste” scenario like backing files up to a USB drive. Migrating a substantial volume of sensitive data from one location to another and making sure the functionality of accessing the data stays intact does not just happen overnight. Thankfully, there are trained professionals who take every measure vulnerability into consideration, plan countless hours with the cloud provider to ensure their transition from one location to another is smooth.

When I used to work as a server, we had a contracted IT person who came in as needed. Usually about every month he was there doing some type of issue that was called in. The point-of-sale software we used was backed up to the cloud in case the computer terminal unexpectedly shut off or needed to be rebooted (which happened multiple times a night). Majority of the time when he had to come in to resolve an issue, he was waiting to hear back from a technical support representative because there were issues on their end.

While cloud computing is a great way to have access to your data at anytime and anywhere with an Internet connection, there is still data loss. Like I stated in the point before about facial recognition, technology is not perfect. It improves many aspects of our life, and society has relied upon it so much now that we can’t go away from it. One way data loss occurs is by human error. Humans still manage the daily operations of the data center, both physical equipment and the software running on the devices. There is the chance that a technician can accidentally delete data. With RAID, when a hard drive fails, another hard drive already has all the data written on it. However, if a technician removes the wrong hard drive when going to install a new one, this leads to permanent data loss.

In order to ensure that all the data is completely lost when discarding failed hard drives, cloud providers shred them. The reason they are shredded and not thrown in dumpster is due to the dumpster diving. Yes, the old school way of stealing personal information by someone not shredding important papers is the modern day of attempting to steal data.

Works Cited

Conger, Kate, and David Sanger. “Russia Uses Cyberattacks in Ukraine to Support Military Strikes, Report Finds.” *The New York Times*, 2 May 2022, www.nytimes.com/2022/04/27/us/politics/russia-cyberattacks-ukraine.html.

Gargaro, David. “The Pros and Cons of Facial Recognition Technology.” *IT PRO*, Future US LLC, 22 Apr. 2022, [www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology](http://www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology).

Kaspersky. “What Is Biometrics? How Is It Used in Security?” *Www.Kaspersky.Com*, 9 Feb. 2022, www.kaspersky.com/resource-center/definitions/biometrics.

Morrow, Timothy. “12 Risks, Threats, and Vulnerabilities in Moving to the Cloud.” *SEI Blog*, 4 Mar. 2018, insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.

Ranger, Steve. “What Is Cloud Computing? Everything You Need to Know about the Cloud Explained.” *ZDNet*, 25 Feb. 2022, www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud.