BRIEFING NOTES

#BN-18-Cyber and space as key enablers-Oct2020

EMERGING TECHNOLOGIES, CYBERSECURITY, PUBLIC POLICY, AND AI

Authors: Rezvan Nozaripour[1] and Kash Khorasani [2]

[1] Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- It is important to keep up with latest technologies as to not only stay updated but also safe. In this BN we will emphasize the emerging technologies that will improve security of information systems from being attacked by hackers.
- A few technologies that will improve cyber security are: Hardware Authentication, Cloud Technology, Blockchain, User-behavior analytics, and AI and Deep Learning.
- Cyber security professionals are obligated to follow certain ethical standards. Some of the most important ethical issues in cybersecurity are privacy, resource allocation, transparency and disclosure.
- Cyber-physical systems (CPS) are intended to be merged into socio-technical systems that interact with humans in the loop. Consequently, the study of their ethical behavior translates currently a major stake. Some of these ethical considerations and behaviors are integrity, safety, security, altruism, accountability and equitability.
- New emerging technologies that have been introduced to the market represent as boons to hackers, who capitalize on people's lack of understanding of how these technologies operate, as well as undiscovered vulnerabilities in new systems security.
- Quantum Computers, 5G Networks, Internet of Things, Artificial Intelligence (AI) and Cloud Storage represent as some of these emerging technologies that can be used by hackers for new threats.
- Considerations such as post-quantum cryptography in case of using quantum computers, protection of third-party cloud providers for protecting cloud storage need to be taken into account when using these new technologies.

CONTEXT

- The increasing digital connectivity and automation of virtually all processes in the world throughout the entire value chain have led to creation of agility. This has also contributed to presence of extremely high threats being developed with the potential for cybersecurity being significantly increased.
- In order to address these threats, it is important to incorporate cyber security into applications, as well as all the devices that are interconnected from the start and early stage. We should be leveraging new technologies with the existing fundamentals that are in place to improve cyber security.
- Hackers are becoming increasingly innovative with techniques that they use to access sensitive data. In many cases, new technologies that have only recently entered the market

are boons to hackers, who capitalize on people's lack of understanding of how these technologies work, as well as undiscovered vulnerabilities in new systems security.

- On the other hand, cybersecurity experts are highlighting certain technologies that have been repeatedly exploited by hackers, calling for greater understanding of their vulnerabilities to malicious actors.
- The following represent as emerging technologies that pose threats to modern cybersecurity.

CONSIDERATIONS

- **Hardware Authentication**:
  - The hardware authentication refers to any sort of security measure requiring a certain hardware device to be involved in the user screening process. A hardware for validating user identity can come in many forms such as an ID with unique QR codes that check the validity of an authorized person that wants to access the network.
  - The other type is using fingerprint to unlock the phone or optical recognition systems. USB security keys or security tokens, are other approaches that one needs to plug in these into the computer and enter a security code to process the authentication step.
  - Recently, companies such as Intel have developed advanced Hardware Authenticator devices such as the latest Core vPro processor that can simultaneously combine various hardware components with enhanced factors for validation of the user identity. This dedicated a part of computer processor for security reasons, removes the need for a separate USB device, and makes a device part of the entire process of the authentication.
- **Cloud Technology:**
  - Mechanisms such as virtualized intrusion detection and prevention systems, virtualized firewalls and virtualized systems security are now being used from the cloud technology. An infrastructure such as a service provider can accomplish these goals on a very large scale for all of its customers and relieve the need to perform them for an individual cloud customer.
  - As an example, private and public entities, such as Firehost or Amazon, have doubled their data-center security using IaaS (Infrastructure as a service) solutions. The GSA FedRAMP (The Federal Risk and Authorization Management Program) is another perfect example of cloud-based certified secure services that makes it easier for small to medium sized business enterprises to have a data security center.
- **Blockchain:**
  - Blockchain-based applications are helping organizations in dealing with the traditional problem of data storage and protect sensitive data of business customers. Blockchain technology can prevent a variety of data breaches, cyberattacks, identity thefts and treachery in transactions. Blockchain ensures that the data remains private and secure in all the blocks it creates to maintain transparency.

    A few advantages of Blockchain that help enterprises in cybersecurity can be linked as follows:
    - Safeguarded Edge Computing with Authentication
    - Cutting-edge Privacy and Data Integrity
    - Protected Private Messaging
    - Improved Public Key Infrastructure (PKI)

- Reduced distributed denial-of-service (DDoS) attacks

- **User-behavior analytics:** Once a person's credentials have been compromised, a cybercriminal with access to this information can penetrate a network and engage in all kinds of malicious behavior. Such a behavior can trigger a red flag to the existing system defenders if they are using UBA (user behavior analytics). This technology uses big data analytics to detect any unusual behavior. This technology is important and it helps address blind spots in an enterprise security system. Visibility into an activity that does not fit the norm of a legitimate user can close a blind spot in the middle of the attack chain.
- **AI and Deep Learning:** There is a significant deal of interest for achieving systems security by utilizing machine learning and artificial intelligence techniques. Deep learning, as in the UBA focuses on anomalous behavior. Whenever AI and machine learning systems are fed with the right data, they can recognize where malicious behavior deviates from legitimate or acceptable behavior as far as security is concerned. Intelligent systems will monitor user information to analyze user behavior, device usage, network activities and location and application data. Using such information, the system will change any user's access rights automatically to ensure that the data is secure on remote networks.

Ethical Issues in Cybersecurity:

Overemphasizing cybersecurity technical aspects may violate fundamental values such as equality, fairness, freedom or privacy. However, neglecting cybersecurity technical aspects could undermine citizens' trust and confidence in the digital infrastructure, in policy makers and in state authorities. Understanding this and other value dilemmas have become imperative, yet cybersecurity is still an under-developed topic in technology ethics. Below are some of the ethical issues in this domain.

- **Harms to Privacy:** Poor cybersecurity practices can ravel our lives and belongings. One of the most common cyber threats to privacy is identity theft, in which personal identifying information are stolen and used in financial transactions to impersonate victims. Poor cyber security practices can therefore be more than ineffective, they can be unethical. To the extent that as they unnecessarily or negligently expose others to significant harm to privacy of people or organizations.
- **Cybersecurity Resource Allocation:** cybersecurity efforts can negatively impact data storage capacity, network and download speeds, power efficiency, and system usability/reliability. Therefore, the role of finding a fair balance between resourceful cybersecurity and other functionalities is ethical, since it requires that the harms, advantages, rights and principles inherent in such a decision be properly discussed, and the possible impact of the action on other people's ability to follow and lead good lives.
- **Transparency and Disclosure:** Cybersecurity is a form of risk management, and it is an ethical obligation to report such risks when identified, so that informed decisions can be made by those concerned. For example, it is generally agreed that when an organization discovers that its software has a critical vulnerability, it should alert its customers of this discovery in a timely fashion to warn them to install a patch (if available) or take additional security actions.

Ethical Behavior of Cyber-Physical Systems (CPS) and Autonomous Systems

The autonomous and autonomous unmanned systems as well as CPS can behave and evolve in space independently neither from the decision of a human operator nor from its designers. They can integrate

Artificial Intelligence-based learning mechanisms enabling them to improve their decisions with time and adapt to an evolving environment.

There is a need to foster researchers working on this kind of CPS to pay attention to the possible consequences of their design on the welfare of humans interacting with these CPS. Due to this fact the ethical behavior of CPS and autonomous systems should be concerned and some of the ethical behavior components are as follows:

- **Integrity**: Integrity is the first component of ethicality. That is the ability to perform in such a way that the information coming from the CPS is trustable and others are confident in the CPS's ability to take steps to accomplish explicitly defined and clear objectives.
- **Safety**: Safety of the people involved and in direct connection to the considered CPS is a second component of ethicality. To ensure a system is safe and to limit the risk of injury to persons depending on the CPS is the least it can be accepted to determine whether a CPS is ethically active.
- **Security**: Security refers to the CPS resistance to unforeseen offensive actions. It is a matter of the CPS's ability to limit its vulnerability and intrusion, cyberattacks and threats which come not only from outside the system and events, but also within the CPS, which is new to the ethics principle.
- **Altruism**: This is an additional safety view. Altruism is more concerned with the well-being of persons who do not interact with the CPS, while safety concentrates on people who interact with the CPS. It concerns the ability to act in accordance with others (other technical systems, other CPS or human beings) welfare.
- **Accountability**: The CPS's responsibility for an issue ensures accountability. If a CPS is accountable, its legal responsibility could be considered in the event of hazard and the funds could be allotted to the injured.
- **Equitability**: This implies that if the CPS becomes an artificial entity who is rational and accountable and who can spend money on insurance (accountability), then it must be able to make money as a counterbalance. This must be achieved in a fair way and the cash obtained by its use must be allocated in balance to ensure its ethical behavior.
- **Quantum Computing:**
  - The technology of quantum computers will continue to progress in years to come, threatening encrypted data sets that organizations such as banks have been defending for decades.
  - Security experts expect that quantum computers can break encryption that currently helps secure everything from e-commerce transactions to health records by harnessing exotic phenomena from quantum physics to generate exponential leaps in processing power.
  - Quantum researchers advise companies to consider implementing current and potential types of encryption algorithms that are capable of withstanding a quantum threat. In addition, government organizations need to collaborate on post-quantum cryptography principle and standards to make the process simpler.
- **5G networks:**
  - The recent arrival of 5G, as the next generation of wireless networks, will fundamentally transform current operating environments with dramatically higher speeds, increased capacity and lower latency. However, such advantages come at the cost of growth on the surface of the attack.
  - This is not only the faster internet, but also the design of 5G will mean that by 2025, the world will enter into an era where, 75 billion new devices will be connecting to the internet every year. It will give the infrastructure to link entirely new industries, geographies and communities but at the same time will dramatically alter the threat environment, as cybercrime is theoretically transformed from

an invisible, financially oriented problem into one in which real and significant physical harm happens at a pace of 5G.
- In addition, the network itself will become a greater target due to the fact of increased usage, which is the result of increased bandwidth.

- **The Internet of Things (IoT):**
  - The "internet of things", or networks specifically made for internet-connected devices and appliances to communicate with each other, is now used widely across industries.
  - Integration of IoT into everyday activities and procedures-from manufacturing equipment control to medical devices and military communication networks.
  - However, as this technology becomes more popular, hackers are increasingly finding vulnerabilities in IoT networks and use them to jeopardize the activities of companies and organizations.
  - The data collected by any organization using IoT is more extensive than ever before, and if the network is targeted, billions of data points will be affected.
  - Moreover, as one computer is connected to an entire eco-system, a minor vulnerability could lead to more severe cyber-attack harm to the wider network.
- **Artificial Intelligence (AI):**
  - As artificial intelligence makes leaps forward in sophistication and versatility, hackers are already using it to get around cybersecurity defenses. Hackers will easily scan networks using AI systems, identify weak points or predictive text functions to relay sensitive information to insider people and manipulate them into transmitting sensitive information.
  - Criminal use of AI will almost certainly generate new attack cycles, highly targeted and deployed for the greatest impact, and in ways that were not thought possible in industries never previously targeted: in areas such as biotech, for the theft and manipulation of stored DNA codes; mobility, for hijacking of unmanned vehicles; and healthcare, where ransomware will be timed and deployed for maximum impact.
- **Cloud Storage:**
  - Many companies migrated their data and information to the Cloud in 2019, assuming that this would help mitigate cybersecurity threats. However, simply moving data to the Cloud does not guarantee that data is safer in any manner.
  - In addition, "Cloud Jacking" will possibly become a more prevalent challenge to cybersecurity threat as cloud storage becomes more widely used.
  - The cloud defense architecture should become more complicated as attacks on Cloud services also grow more sophisticated. The protection of third-party cloud providers would probably be one of the most important considerations