PRAMUN X, January 10–14, 2018
Gymnázium Jana Nerudy, Prague

CYBER SECURITY

Chaired by **Rey** Sweeney & **Jan** Bartůněk

Topic I:

Comprehensive plan for tackling worldwide ransomware attacks

Terms and Acronyms to Know

Bitcoin – a consensus network that enables a new payment system and a completely digital money

AIDS – (PC Cyborg Trojan), created by Dr. Joseph Popp, replaces the AUTOEXEC.BAT file, can count the number of times the computer has been booted.

CIGI – Centre for International Governance Innovation: think tank with an objective to bring clarity and innovative thinking to global policy making

ISOC – Internet Society: American non-profit organization to provide leadership in Internet-related standards, education, access, and policy.

UNCTAD – United Nations Conference on Trade and Development: main U.N. body dealing with trade, investment, and development issues.

ECOSOC – United Nations Economic and Social Council: brings people and issues together to promote collective action for a sustainable world.

NGOs – Non-Governmental Organizations: most often non-profit organizations, independent of governmental institutions, that promote humanitarian, educational, healthcare, public policy, human rights, environmental, and other areas for the benefit of all people.

I. Background

Ransomware attacks emerged shortly after the proliferation of the Internet, which constituted a new way for hackers to obtain money. Ransomware is a malicious software designed to block access to a computer system until a sum of money is paid. Ransomware is typically a virus that is downloaded onto a device. This usually occurs by clicking on a link or attachment in an email. Attackers persuade people to unknowingly download a virus by creating a sense of urgency to click on the link such as the offer only being available for a small amount of time.

The first known ransomware attack is known as AIDS in 1989. This virus had the ability to access the number of times the computer had been booted. Once the boot count reached 90, the attacker would deem the drive C: unusable and seize all the information on the drive until $189 was paid. This attack was ultimately unsuccessful because not many people owned personal computers at the time, and therefore not many people could have been affected.

In today's society, human beings across the world are completely interconnected through their personal devices. This network allows people to have a wealth of information at their fingertips, however it does not come without shortcomings. Vulnerabilities skyrocket because of our connections to different parts of the world. Attackers prey on people's reliance on digital storage to extort money. Sometimes, authorities have intervened in the problem and instructed victims not to pay the ransom amount, however there is not always a guarantee that information will be returned, so they are frightened into giving into the attackers for their precious information. Ransomware attacks can injure businesses, hospitals, schools, and any individual person with a computer. The average ransom amount is $300 per computer in Bitcoin, an online currency. Ransomware attacks steal over a trillion dollars a year.

More recently, the worldwide WannaCry attack occurred in May 2017. This ransomware attacked businesses, government entities, and Britain's National Health Service system. More than 300,000 computers were infected with this virus. Unlike other ransomware attacks, the virus was not downloaded by the user, instead the malicious software travelled from system to system on its own. This attack was possible because of a deficiency in Microsoft software.

WannaCry hackers used the EXTERNALBLUE exploit to find the flaw on Microsoft's system. Once this is complete, it will expand to any computer not updated to protect against the EXTERNALBLUE file. Attackers commanded that owners paid from a range of $300 to $600 via Bitcoin for their information. This attack revealed major faults in protecting valuable information that needed to be addressed.

II. UN Involvement

CIGI, ISOC, and UNCTAD joined forces to create the Global Survey on Internet Security and Trust. The survey took place from December 2016 to March 2017. Based on information from Australia, Brazil, Canada, China, Egypt, France, Germany, Hong Kong (China), India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, Republic of Korea, South Africa, Sweden, Tunisia, Turkey, United Kingdom and the United States, only 6% of internet users had already been affected by ransomware attacks, and 11% knew someone that had been affected.

ECOSOC held a special "Cybersecurity and Development" event on 9 December 2011. This event included nation states, the UN system, representatives from both the public and private sector, and other NGOs. The objectives were to build awareness at the international policy level by providing the current situation and concerns, identify a range of best practice policies and initiatives in place around the world to build a culture of cybersecurity, and explore options for a global response to rising cybercrime. Many at this conference concluded that preparing children for what is to come and how to approach security on the Internet would help the issue push the issue to decline. Attendees also agreed to the necessity of a global convention that would harmonize national laws concerning computer crimes such as copyright infringement, fraud, child pornography, hate crimes, and breaches of national security.

III. Possible Solutions

There have not been any global solutions made to solve this pressing issue. However, some individual countries have come up with ways to assist in the decrease of ransomware attacks. First, countries can encourage their people to follow the five pillars of computer security: Encryption, Data Integrity, Non-Repudiation, Authentication, and Availability. Encryption is encoding information to make it confidential to other computers. Data Integrity ensures that computers are protected by up-to-date virus

software, and that other computers do not have the ability to change or alter information. Non-repudiation safeguards that connectivity between two devices is completely confidential and all links are real and safe. Authentication assures that all links and contacts are valid and that links

do not contain a virus. Finally, availability is the guarantee that access to files is always accessible, and nothing can turn that off. Advocating for education of these principles would protect people from ransomware attacks.

Punishing ransomware attackers publicly would assist in decreasing the number of attacks because they would then understand the ramifications that come with hacking into others property. Nation states could encourage creating backups of information, especially in government structures and businesses, to prevent the complete loss of information if attacked. The government and companies would then be able to focus on catching and exposing the attackers rather than the possible destruction of their information.

IV. Questions to Consider

- What has your country done to prevent cyber-ware attacks?
- How involved has your country been in participating in global meetings regarding cybersecurity?
- To what extent can your country take action?
- How can we share cyber-attack and protection intelligence and law enforcement data to solve cyber-crime and prevent world-wide cyber virus infection?
- How can the world come together to create a global solution?

V. Websites to Look at

- http://money.cnn.com/2017/05/15/technology/ransomware-wannacry-explainer/index.html
- https://bitcoin.org/en/faq#what-is-bitcoin
- https://www.knowbe4.com/aids-trojan
- http://money.cnn.com/2017/06/27/technology/ransomware-why-keep-happening/index.html
- https://cio.economictimes.indiatimes.com/news/digital-security/most-people-are-ill-equipped-to-deal-with-ransomware-global-internet-user-survey/58714733
- https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

Topic II:

Establishing a universal right to privacy in the digital age

I. Background

Digital communications have become part of everyday life all around the world due to its easy and fast international communication. We live in online era of Internet, phones and other digital technologies. According to internetlivestats.com around 40% of the world population has access to the internet (at home) today. Although, only 22 years ago, in 1995, this percentage was less than 1.

Highly rising number of access to information and fast real-time communication and technology innovation has led to boosting freedom of expression. It has also provided a way for people to live and participate in democratic lifestyle by talking online about issues and problems of today´s world. Not only enjoyment is the only site of modern technologies. Governments, companies and individuals use this technology to collect data of others, which in some cases may violate basic human rights. Also, these technologies are easy to hack, although it may serve for tracking purposes of terrorists, people might use it to track and harass individuals and then they violate their right for privacy.

Definition of key terms

Right to privacy – "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks," by the Universal Declaration of Human Rights (UDHR) published by the United Nations.

Digital age – Period of time happening from 1970s till now. Digital technologies took over the world and we use them for direct communication.

Communications Surveillance – "Communication surveillance is the monitoring interception, collection, collection, preservation and retention of information that has been communicated relayed or generated over communications networks to a group of recipients by a third party."

Cookies – Collected and stored data about web users. The place where it is stored varies on web browser.

II. UN involvement

UN has passed General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014, as well as Human Rights Council resolutions 28/16 of 26 March 2015 on the right to privacy in the digital age and 32/13 of 1 July 2016 resolution on topic of right to privacy in the digital era. They passed all of these resolutions in order to increase security of internet and to ensure privacy of the people. On 27 February 2014, OHCHR addressed a questionnaire to member states, national human rights institutions, non-governmental organizations and businesses. UN is still searching and looking for new solutions. UN is mostly seeking cooperation of all member states to not to collect all data from their people at first. UN encourages all States to promote an open, secure, stable, accessible and peaceful information and communications technology environment based on respect for international law.

III. Questions to consider

- What has your country done to solve this issue, if anything?
- Have there been incidents that abuse the right to privacy in your country?
- What is your country´s policy on personal freedoms (speech, petition, etc.)?
- Are there certain companies or non-governmental organizations that have been abusing online privacy?
- Has your country banned some of the global social networks?

IV. Sources

- http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
- http://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx
- https://policyreview.info
- http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
- https://www.accessnow.org/cms/assets/uploads/2016/09/privacy-resolution-2016-UNGA.pdf
- https://www.cfr.org