2017 CERT High School Cybersecurity Event

July 12, 2017

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

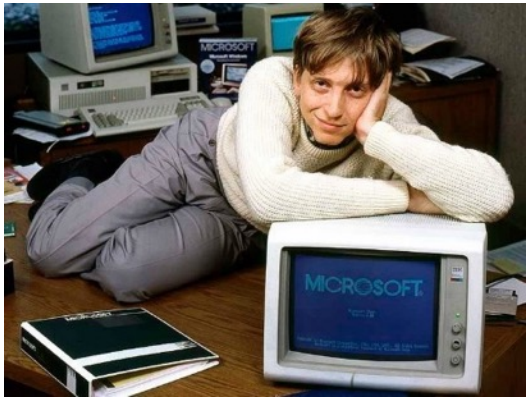
DM17-0419

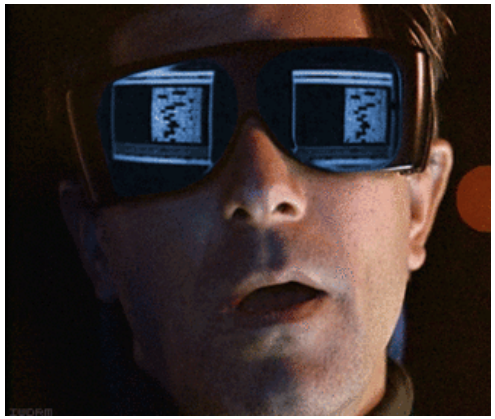
Agenda

- Importance of Cybersecurity
- Cyber Ethics
- Questions

Why is Cybersecurity Important?

What We Think Cyber Is





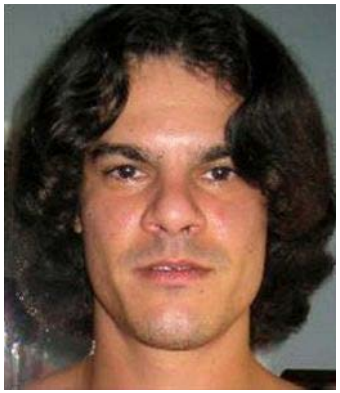
What Cyber Is In Reality

What Is This?

Picture (optional)

Notable Breaches and Attacks

- Petya
- OPM Breach (2105): 21.5 million SF-86 records
- DNC Hack (2016): ~19K e-mails and ~8K files
- Stuxnet (2010): targeted PLCs used in Iranian nuclear facilities
- TJX (2007): 45.6 credit and debit card numbers



Economic Impact of Cybercrime

429 Million Identities Exposed in 2016*

Global Cost

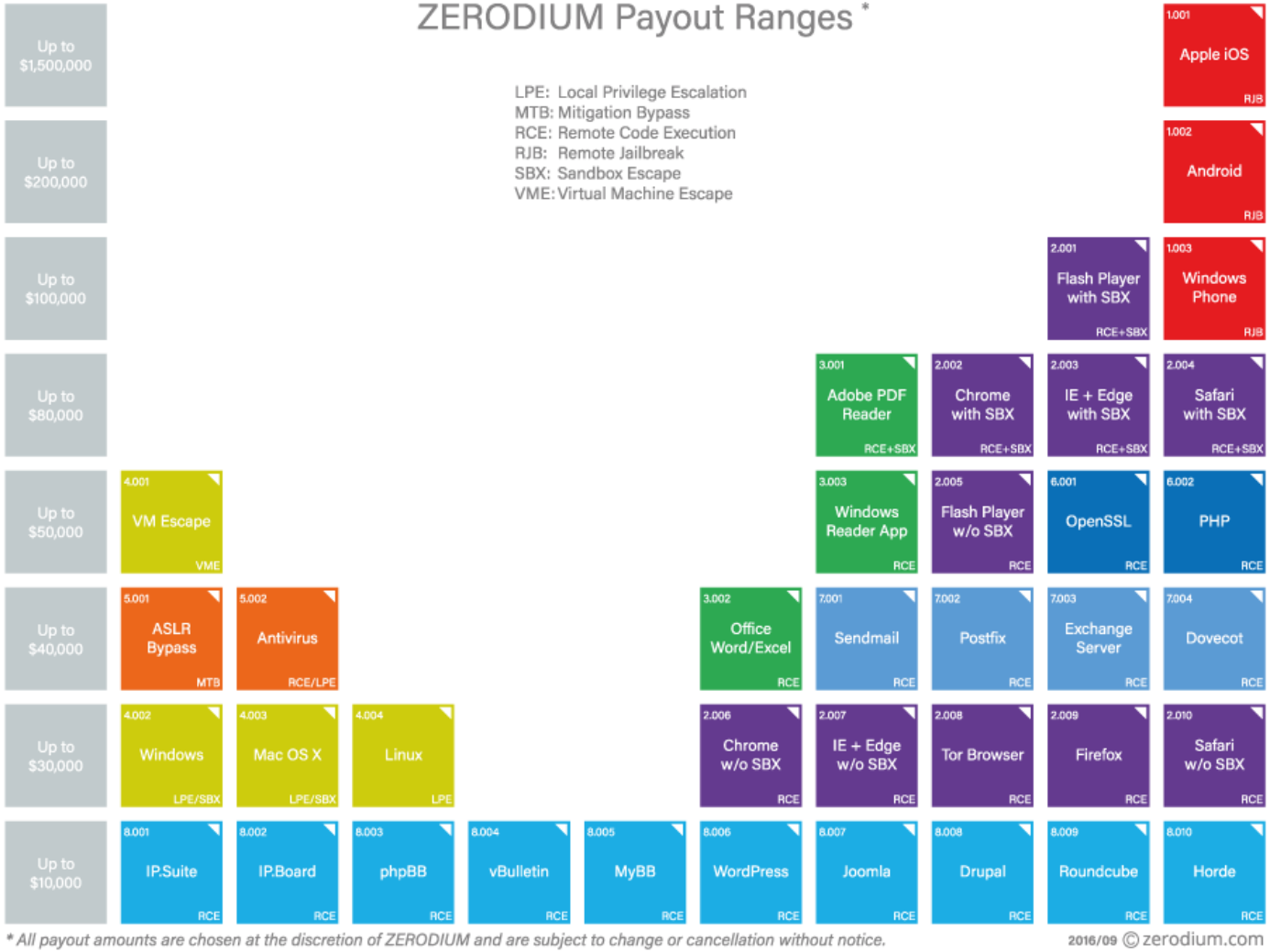
- 2014: $400 billion
- 2019 (projected): $2.1 trillion

Case Study: Angler Exploit Kit

* 2016 Symantec Internet Security Report

Payout for Zero-Day Exploits

Picture (optional)



Careers in Cybersecurity

U.S. is short 250,000 Cyber professionals

- Shortage: expected to double within 5 years
- Job Growth Rate: Greater than 3x the average
- Industry Growth: $75 billion (2015) to $170 billion (2020)

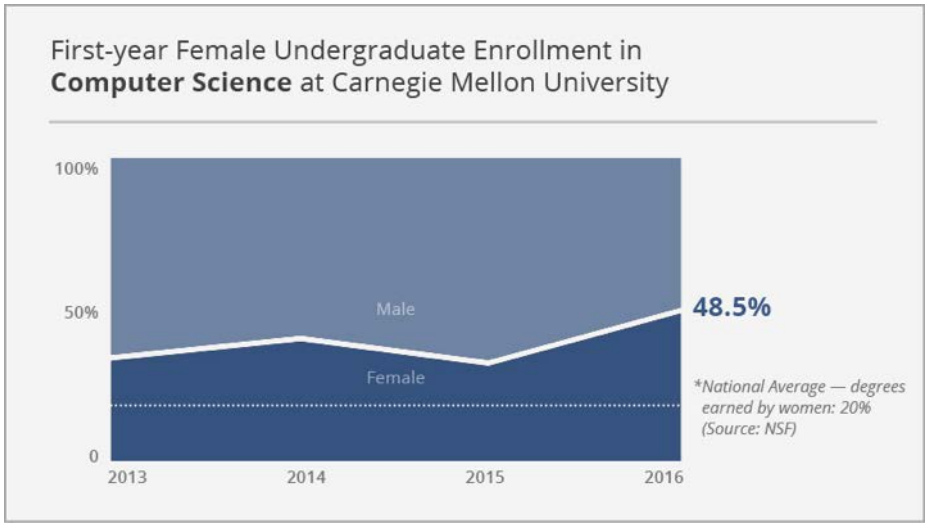
Bridging The Gender Gap

Gender Imbalance in Cyber

- Ratio of men to women is 5 to 1

Bridging the Gap

- Women in Cybersecurity (WiCyS)
- Grace Hopper conferences



Types of Hackers

White Hats: “Ethical hackers” that are hired by a companies to find security vulnerabilities and strengthen the security of a system.

Black Hats: Find and exploit vulnerabilities for personal or monetary gain, or other malicious reasons.

Gray Hats: Mix between the good guys (White Hats) and the bad guys (Black Hats). They will look for vulnerabilities WITHOUT permission. If they find something, they tend to report it.

- Still illegal since they don’t have permission.

Ethics

What are Ethics?

Why are they Important?

Where do they come from?

Cyber Ethics

Examples

Cyber Ethics Pledge

Cyber Crime

What are Ethics?

Ethics: The study of right and wrong

Examples of ethical behavior:

- Not lying
- Not stealing
- Not taking credit for others
- Not cheating on tests
- Not abusing one's power, position, or skills

ARISTOTELIS DE
MORIBVS AD NICOMACHVM
LIBRI DECEM.

Græcis Latina eregionè respondent, interprete DIONYSIO LAMBINO: cum eiusdem Annotationibus, & THEOD. ZVINGGERI Scholijs.

LIBER PRIMVS.

CAPVT PRIMVM.

Tria ueluti prolegomena declarat: Subiectum scilicet philosophiæ Ethicæ: Modum siue rationem eius tractandæ & explicandæ: & Qualem auditorem esse oporteat.

OMNIS ars, omnisq; docendi uia, atq; institutio, itēq; actio, & consilium, bonū aliquod appetere uidet. Iccirco pulchrè ueteres id esse bonum pronunciarūt, quod omnia appetūt. Sed uidētur fines inter se discrepare. Alij enim sunt muneris functiōes: alij, præter eas, opera quædam. Quarū aūt rerū, præter actiones, aliqui sunt fines, in his operasunt actionib. meliora natura. Cūm uerò multę sint actiōes, artes & scientię: tū multi quoq; fines extiterūt. Nā medicinę finis est, bona ualetudo: artis ædificādarū nauiū, nauis: artis imperatoriæ, uictoria: rationis eius, quæ in re familiari tuēda uersat, diuitiæ. Quæcunq; aūt artes huius generis uni alicui facultati subiectę sunt, (ut equestri ea, quę in frenis cōficiēdis occupata est, cæteraq; oēs ad instrumēta equestria cōparatæ: atque hęc ipsa equestris, oēsq; actio militaris, atti imperatoriæ: itēq; aliæ alijs:) in his omnibus fines earū, quę principē locū obtinent, earū quę eis subiectæ sunt, finibus

a sunt

wikimedia.org

Why are Ethics Important?

- Promote a sense of "fairness"
  - We assume that other people will act ethically.
- They benefit the common good.
- Keep us out of trouble!
  - If you have to ask if something is ethical, then it is more than likely not ethical.

wikimedia.org

Cyber Ethics

Adds a new dimension to right and wrong

Issues:

- Stalking
- Hacking
- Bullying
- Plagiarism
- Digital rights management
- Digital trespassing
- Vandalism, defacing
- Denial of service
- Online personas
- Jurisdiction and location

wikimedia.org

Cyber Ethics Pledge (1 of 2)

- I will always consider the social consequences of the program I am writing or the system I am designing
- I will always use a computer in ways that ensure consideration and respect for my fellow humans
- I will always use a computer in a manner that will honor my family, my community, and my high school
- I will not use a computer to harm other people
- I will not break any laws with my computer
- I will not interfere with other people's computer work
- I will not snoop around in other people's computer files
- I will not use a computer to steal

Cyber Ethics Pledge (2 of 2)

- I will not use a computer to bear false witness
- I will not copy or use proprietary software or media for which I have not paid
- I will not use other people's computer resources without authorization or proper compensation
- I will not appropriate other people's intellectual output
- I will not use a computer to bully, humiliate, hurt, or take vengeance on another person
- I will not use a computer to access, post, or process pornography, foul language, violence, or other adult content

Cyber Crime Laws

18 Pa. Stat. § 7611

§ 7611. Unlawful use of computer and other computer crimes.

(a) Offense defined.--A person commits the offense of unlawful use of a computer if he:

(1) accesses or exceeds authorization to access, alters, damages or destroys any computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device or any part thereof with the intent to interrupt the normal functioning of a person or to devise or execute any scheme or artifice to defraud or deceive or control property or services by means of false or fraudulent pretenses, representations or promises;

(2) intentionally and without authorization accesses or exceeds authorization to access, alters, interferes with the operation of, damages or destroys any computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device or any part thereof; or

(3) intentionally or knowingly and without authorization gives or publishes a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network, computer database, World Wide Web site or telecommunication device.

Unlawful Use of Computers and E-mail, Possession of Online Child Pornography, Computer Trespass and Computer Theft are felonies of the third degree. These offenses are punishable by up to seven years imprisonment and/or fines not exceeding $15,000.

Cyber Crime Laws

Computer Fraud and Abuse Act

18 USC 1030 make it a crime to access or attempt to access a computer or computer network without authorization or in excess of authorization

- Covers virtually all computers involved in interstate commerce including foreign computers
- - Only need to intend to cause damage to be found guilty

Maximum of 10 years in prison (first offense); 20 years (second offence). State offense count as prior

Questions?

wikimedia.org