Introduction to Security Course Introduction

Ming Chow (mchow@cs.tufts.edu)

Twitter: @0xmchow

Tufts UNIVERSITY | SCHOOL OF ENGINEERING Computer Science

What This Course Is NOT

- Hack all things
- Be an 31337 h4x0r (“leet speek” for “elite hacker”)
- Introduction to Cryptography
- Save the world
- The answer is “black or white”

What This Course Will NOT Cover

- Social engineering
- x86, x64, ARM reverse engineering
- Privacy
- Cryptocurrency
- Security management

What This Course IS

- Controversial
- WARNING: A little about a lot
    - Why: Cyber Security is a very broad field as evident by list of topics that will not be covered in this course
- Provides exposure to tools that the attackers and defenders are using
- Understand tradeoffs
- Make you think like an attacker
- Be informed of the issues. Because most in Computer Science or in tech just do not know them.
    - Many developers don’t even consider security in software.
    - You can’t complete a Civil and Environmental Engineering degree without learning anything about health, safety, and security but you *can* complete a Computer Science degree without learning anything about critical infrastructure, health, safety, and security.

Software and Hardware Requirements

- **Absolute Requirements**
  - A modern web browser (e.g., Firefox, Google Chrome, Chromium, Safari, Microsoft Edge)
  - A command line interface to run Unix/Linux commands
- **Strongly Recommended Requirements**
  - A computer with at least 40 GB of hard disk space free and 4 GB of RAM
  - [Kali Linux and a Virtual Machine Hypervisor]
  - Why is this strongly recommended and not mandatory? Telling students to have beefy computers especially to run virtual machines in order to take this course is sending the wrong message. Cyber Security must be accessible as possible.

The Basic Skill Necessary: Exposure, Experience, and Comfort with Command Line Interface (CLI) / Terminal

- Versatility, productivity, accessibility, scripting
- Not everything can be accomplished by fancy graphics and GUIs (sometimes constrained to certain features too)
- Many systems do not use a windows manager or have a graphical desktop interface (e.g., servers)
- Graphical interface (especially on servers) => more software requirements, more overhead, more bloat, more vulnerabilities
- Many security tools are command line based
- Remote execution of commands –for good and bad.
- *This is the first lab*

Why is it Called Cyber Security?

- Should it be called “Information Security”? No. Because there’s a lot more than information we are concerned with. Case-in-point: hardware and the “Internet of Things”
- Should it be called “Computer Security”? No. Technology is not everything. Sometimes the best solution (or attack) is not technical. Examples: social engineering, lock picking, impersonation, phishing.

Why is This Course Now Named “Introduction to Security” and not “Introduction to Cyber Security”?

- Do we need to put “cyber” in front of every word now?
  - Cyber war
  - Cyber weapons
  - Cyber deterrence
  - Cyber espionage
  - Cyber ___________

Running List of Thoughts on What Cyber Security Is (from former students)

- Make sure your data is protected
- Want data to be private
- Want to preserve the integrity of the data
- Preservation of the status quo
- Access control
- Protection of hardware and networks => physical security
- User security (protecting themselves)
- Knowledge of what the attackers / adversaries are doing
- Maintaining good governance
- Punishment of the attackers, strike back?
- Containment, stop the bleeding
- Resilience, separation of concerns, redundancy
- …and the list goes on…

By Definition, What is Cyber Security?

- The “CIA Triad”
  - Confidentiality
  - Integrity
  - Availability

Convention Used in Notes

- **bold** – keyword or definition
- *italic* – to be discussed in more details later
- `code via Courier New font` – code or command

Basic Definitions

- Why is vocabulary important?
  - There is a problem with vocabulary in this field. Many words have different context and meaning to different groups (e.g., the policy folks in the field).
  - Many words are also misused by media.
- **Event** - Could be anything
- **Incident** - A malicious event
- **Bug** - An error that exists in the implementation-level (i.e. only exist in source code); very correctable
- **Flaw** - An error at a much deeper level, particularly in the design, and likely in the code level; can be very difficult and costly to correct
- **Hacker** - A creative programmer; a positive connotation
- **Cracker** - The bad guy, the attacker, what media coins "hacker" (the negative connotation). We'll use **attacker** in this class.

Tufts UNIVERSITY | SCHOOL OF ENGINEERING Computer Science

Basic Definitions (continued)

- **Black hat** - An attacker with malicious intents
- **White hat** - An attacker with good intents (i.e., the white knight)
- **Gray hat** - An attacker with good and bad intents
- **Script kiddie** or **skiddie** - Nuisance; not going away any time soon; 1337 (i.e., elite) wannabes; use scripts and exploits written by others and do not understand how they really work; always a lamer
- **Vulnerability** - A security bug (thanks Giovanni Vigna); a weakness in a system that can potentially be exploited by an attacker
- **Exploiting** or **exploitation** - The act of taking advantage of a vulnerability
- **Exploit** - Software program that performs the exploiting
- **Risk** - The likelihood that an attacker will take advantage of that vulnerability
- **Threat** - The likelihood that an incident will happen
- **pwn3ed** - Owned; successful exploitation; computer system completely compromised
- **Zero day** - an undisclosed vulnerability that attackers can take advantage of. A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability—hence "zero-day." https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

Violating the CIA Triad: If You Were An Attacker, What Are Your Goals?

- Preventing enemies from communicating over network
- Steal information for attacker's benefit and get away with it
- Disruption of business, daily life, day-to-day operations
- Inserting information that "shouldn't be there”
- Destroy information, resources
- Gain access to a system and maintain access to system for a long time
- Monitoring people what they are doing (e.g., webcams)
- Challenging adversaries, pinpointing weaknesses
- For fun and profit (e.g., the black market)
- Spread propaganda
- Building a blueprint of weaknesses…
- …and keep it for future reference

Why the Rash of Incidents: Behind the Breaches and Attacks (thoughts from former students)

- Trust relationships, lots of implicit trust
- Data is very valuable
- Convenient to put everything online; sharing
- Lack of education; people are not being informed
- No barriers to entry
- Lack of deterrence
- Software vulnerabilities
- Misconfigurations
- Human elements, social engineering
- Scapegoating

The Trinity of Trouble: Why the Problem is Growing (by Gary McGraw)

- Connectivity
- Extensibility
- Complexity
- Read: https://freedom-to-tinker.com/2006/02/15/software-security-trinity-trouble/