ETHICS IN VULNERABILITY ASSESSMENT

CS-5156/CS-6056: SECURITY VULNERABILITY ASSESSMENT (SPRING 2025)
LECTURE 2

Outline

- **Background**
- Ethics
- Vulnerability Disclosure

Background and Definitions

- Vulnerability
  - Bug/weakness?/flaw in a software/system/network
  - A **defect** in *software*, *hardware*, *configuration*, *protocol*, *system structure*, and/or *personnel* mis-implementing or ignoring procedures and/or processes.
- Vulnerability Assessment
  - Identification and prioritization of vulnerabilities ***(more on this later)***
- Vulnerability Management
  - Assessment, **classification**, and mitigation of vulnerabilities
- CVE
  - **C**ommon **V**ulnerabilities and **E**xposures
  - A dictionary of **publicly known** vulnerabilities and exposures

Background and Definitions

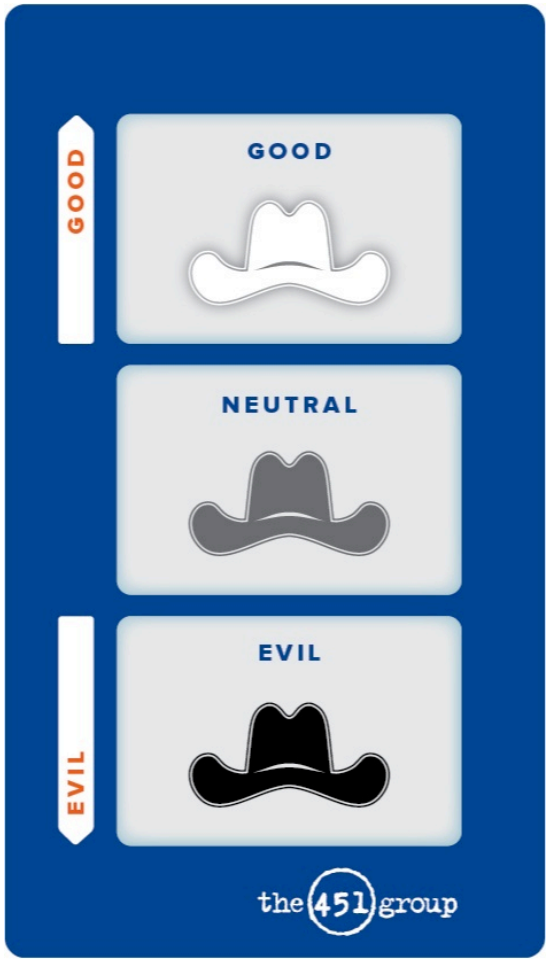
- Exploit
  - **Software** *or* **set of commands** used by a **threat actor** or an outside party to take advantage of a **vulnerability** in order to perform unauthorized actions within the system/network (e.g., control and/or damage some or all components of a system)
- Threat
  - Source and means of an attack
    - A potential cause of an unwanted impact to a system or organization (ISO 13335-1)
- Attack Surface
  - **Sum** of the different **vulnerabilities** that can be exploited
- Attack Vector
  - **Means** of an attack/exploit (e.g., the web browser, the Internet, etc.)

What is a Hacker?

- Someone who...
  - Thinks outside the box
  - Is technologically inclined
    - Normally with computers, but not always
  - Finds unconventional solutions to problems
    - Focuses on what is important

Hackers' Intentions

- Improve system's security
- Fun
- Money
- Destruction



Blackhat/Whitehat model is not sufficiently MECE (mutually exclusive, comprehensively exhaustive)
http://www.csoonline.com/article/2128587/social-networking-security/the-rise-of-the-chaotic-actor--understanding-anonymous-and-ourselves.html

MICE

- **Motivation of individuals** who commit espionage/spying
  - **M**oney
  - **I**deology (patriotic/religious)
  - **C**ompromise (Coercion)
    - Threatening someone to provide secret information
  - **E**go (Excitement)

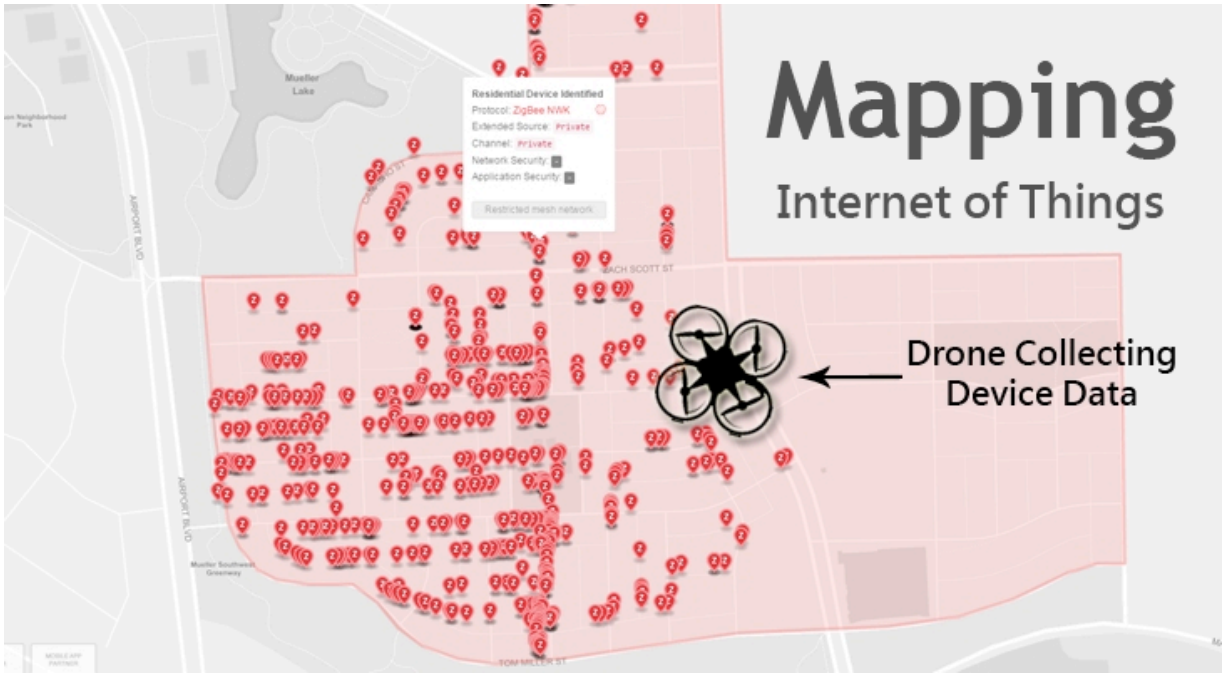
MEECES

- Extension of **MICE**
- Motivational profile for hacker community
  - **M**oney
    - Trading stolen credit cards
  - **E**go
    - drive to solve a problem, look inside the code, see how something works, and then get it to do something it wasn't created to do.
  - **E**ntertainment
    - Enjoying misery of Sys admins
  - **C**ause (ideology)
    - Hactivism. Most DDoS attacks on websites
  - **E**ntrance
    - Share successful break-ins to gain entrance into community
  - **S**tatus
    - The higher profile the target, the higher their status
- http://www.networkworld.com/article/2330885/lan-wan/meeces-to-pieces.html

Type of Loss Exploit can cause

- Loss of corporate assets
  - Bank: money
  - Defense contractor: US defense secrets
  - Aircraft engine manufacturer: intellectual property
- Loss of control
  - Aircraft designed to cooperate via RF communications can be disabled

Another Example: IoT Hacking Drone



- How does drone discover devices?
  - Sniffs for Zigbee beacons/traffic
- Hackers may also control entire network of devices (e.g., door locks, alarms)
  - Flaw in Zigbee protocol **authentication mechanism** that allows hackers to **sniff out exchange authentication keys**
- http://thehackernews.com/2015/08/hacking-internet-of-things-drone.html

Vulnerability Classification

- Excess privilege
- Privilege escalation
- Bug
- Configuration
- etc.

Outline

- Background
- **Ethics**
- Vulnerability Disclosure

What is Ethics?

- **Ethics** is the study of the **principles of conduct** that apply to an **individual or** a **group**

Ethics vs. Morals

- Both relate to "**right**" and "**wrong**" conduct
- **Ethics**
  - Series of **rules** provided to an individual by an **external source**. (e.g. their profession)
- **Morals**
  - An **individual's own principles** regarding right and wrong

Why Not Just Decide: What's Right?

- How?
  - Instead of just decide if it is ethical, try asking the Magic Ball ☺

- Potential Problem:
  - **Depth of thinking varies** among individuals
    - (I) Superficial thinking
      - Lack of knowledge
      - Do what you are told
    - (II) Deep/Profound thoughts

Outline

- Background
- Ethics
- **Vulnerability Disclosure**

Should a 3rd party disclose a vulnerability it discovers?

- Type of 3rd Party
  - White Hat Researchers
  - Black Hat Coders
  - Vendors
    - Act to maximize profits – may not fix a vulnerability
  - Etc.

- Note: Non-disclosure doesn't stop others from finding vulnerabilities

Types of Disclosure

- Full disclosure
  - All details are made public immediately including PoC (Proof of Concept)
- Limited disclosure
  - All details given to the vendor but no details are made public
- **Responsible Full Disclosure**
  - All details given to the vendor
  - Just enough detail given publicly to mitigate the risk
  - Time is given to fix the vulnerability (**typically 90 days**)
  - After patching, all details are released to the public
  - Partial public release of details if vendor does nothing
  - Issues
    - Not all patches are applied on-time
    - Patches can be easily reverse-engineered
- Non-disclosure
  - No details are revealed to anyone
  - Black hat coders choice

The Economics of Software Development

- Why don't vendors make higher quality software?
  - In a free market, all other things being equal, higher quality should win out
- At the moment it is **expensive** and **time consuming** to make and sell high quality software
  - So, software with vulnerabilities exist, even though massive repair efforts may be required as vulnerabilities are discovered – developers are not accountable – law?
- But doesn't that mean lifetime cost is higher?
  - Nope – it is more efficient to let the market find the bugs for the vendor! Let the consumers become an ad-hoc quality-control department for the vendor! Anyway, most vulnerabilities will likely not be found and many others will likely be minor.
- But now the **consumer is burdened with the task of updating immediately** when a patch is published

Can disclosure cause legal problems?

- (Nearly) true story:
  - Student in security class finds vulnerability in Physics website
  - Student tells security professor
  - Professor tells Physics people and provides a fix
  - Everyone is happy, student gets an A
- Two months later:
  - Physics website is hacked badly – grades are changed!
  - FBI is called in
  - Physics people tell FBI that a vulnerability had existed but was found by a student of security professor and fixed
  - FBI asks security professor for name of student
  - Security professor refuses to give the name
  - FBI threatens security professor with court orders and several felony counts!
- Conclusion:
  - Student came forward voluntarily and was cleared
  - Professor changed class policy to don't-ask-don't-tell

Ref: https://www.csoonline.com/article/2121727/application-security/software-vulnerability-disclosure--the-chilling-effect.html

This does not benefit good guys

- No Binding Disclosure Policy and Low-Quality Software may result in nefarious behavior that does not benefit the Good-Guys
  - Mercenaries look for flaws then extort money from vendors to keep the flaws quiet
  - White hat researchers may report very minor bugs that really do not affect security adversely but sound scary enough to affect the vendor's reputation (and profits) https://www.reputationdefender.com/blog/smb/reputation-risk-management-a-false-sense-of-security
  - Good-guys are threatened with legal action or lawsuits for doing something that has great benefit for good guys

The case of Michael Lynn vs. Cisco

- Cisco routers had a bug known to Cisco and some security companies, particularly Intelligent Software Solutions (ISS)
- Michael Lynn worked for ISS and discovered that this (buffer overflow) bug could be exploited to seize Cisco routers and take over corporate and government networks
- Lynn wrote a paper which was accepted at Black Hat.
- ISS told Lynn to remove sections of the paper
- Lynn refused, left ISS, gave the talk
- Cisco demanded the paper be removed from the proceedings
- Cisco demanded that 2000 CDs containing it be destroyed
- Cisco sued Lynn
- Lynn agreed never to say anything about this publicly
- Lynn gave up all material related to his findings
- Black Hat & Lynn gave up recordings of his talk

Ref: https://boingboing.net/2005/07/29/michael-lynns-contro.html

The case of Michael Lynn vs. Cisco

- Aftermath:
  - Lynn's presentation went online but was removed due to a cease-and-desist order https://www.eweek.com/security/cisco-tries-to-quash-vulnerability-talk-at-black-hat
  - Cisco's public relations department downplayed the flaw
    - “It is important to note that the information Lynn presented was not a disclosure of a new vulnerability or a flaw with Cisco IOS software. Lynn's research explores possible ways to expand exploitation of known security vulnerabilities impacting routers."
    - "Cisco believes that the information Lynn presented at the Blackhat conference today contained proprietary information and was illegally obtained."
  - Cisco also said Lynn 'unzipped' a Cisco image to do his work and this is a violation of Cisco's user agreement
  - Lynn got a job at Juniper

The case of Michael Lynn vs. Cisco

- Thoughts?
  - Cisco/ISS customers have the right to know about the vulnerability that Cisco has hid for sometime?

The case of MBTA vs. three MIT undergrads & MIT

- MBTA (Massachusetts Bay Transportation Authority)
- Students circumvented security features of the MBTA computerized CharlieTicket and CharlieCard fare media systems so that a subway rider could enter the system without paying a fare.

The case of MBTA vs. three MIT undergrads & MIT

- What is **claimed by the MBTA**:
  - Students circumvented security features of the MBTA computerized CharlieTicket and CharlieCard fare media systems
  - Students **publicly offered** "free subway rides for life" over the Internet
  - Students plan to allow others to duplicate their claimed "breaking" of the Fare Media's security systems by presenting a paper, releasing software tools, and giving **demonstrations at the next DEFCON hackers convention**
  - MIT is unwilling to set limits on the students' activities despite MBTA requests
  - Students have declined to inform MBTA of the details of their supposed hack
  - **Students did not allow MBTA to fix flaws before going public**

The case of MBTA vs. three MIT undergrads & MIT

- What happened:
  - MBTA got a temporary restraining order to prevent the students from presenting at DEFCON
  - MBTA argued that students were giving instructions to people to defraud the MBTA
  - Students argued that submitting research for review by a government agency before publication is unconstitutional pre-publication censorship (censorship of expression by the government before the expression takes place)

The case of MBTA vs. three MIT undergrads & MIT

- What happened:
  - MBTA got a temporary restraining order to prevent the students from presenting at DEFCON
  - MBTA argued that students were giving instructions to people to defraud the MBTA
  - Students argued that submitting research for review by a government agency before publication is unconstitutional pre-publication censorship (censorship of expression by the government before the expression takes place)
  - Students did not have to go to DEFCON – their results were posted in district court's public website as exhibits

The case of MBTA vs. three MIT undergrads & MIT

- **Result of this case**
  - *The students win*!
  - This is considered academic research
  - Future academic research could be suppressed otherwise
  - "transmission" in the **Computer Fraud and Abuse Act** cannot be construed/interpreted to mean any form of communication
- Thoughts?

The Web Complicates Disclosure

- Is a front door to a house considered a vulnerability?
  - Not really, unless it is unlocked or left open
- Is using a password considered a vulnerability?
  - Not really, unless it is something like 123123

The Web Complicates Disclosure

- Is apache webserver vulnerable if a user allows injecting malicious code into a user-owned website?
  - Not really, it's the user who is the vulnerable one
  - Check this javascript out – looks perfectly benign, right?:
    - print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print “</html>”
  - Attacker submits comment
    - <script>doSomethingEvil();</script>
  - User gets:
    - <html>
<h1>Most recent comment</h1>
<script>doSomethingEvil();</script>
</html>
  - XSS (Cross Site Scripting) Attack

The Web Complicates Disclosure

- Possible dark future for disclosing Internet vulnerabilities
- Consider:
  - Person X applied to USC but was denied
    Person X pulled sensitive data from USC website that was hidden
    (no link to such data was available anywhere in the site code)
    The data were sent to a third party who notified USC
    Person X was charged and pled guilty to unauthorized access
- What the Law says — Legal vs Ethical — :
  - Unauthorized access of computers is illegal
    But how can you say that access of a public website is unauthorized
    Isn't it implied that everyone has permission to access websites?
- Future Law?
  - Exploring all ways a website works is prohibited!!
  - Yikes – then vulnerability testing becomes illegal!!