**Class Notes**

**August 26th, 2021**

**2FA**: Using two factors of authorization to authenticate something (Password & SMS)

**Social Engineering** – Using a human as the weakest link in a cybersecurity attack

**SIM-Swapping** – When someone uses a new SIM card to override another person SIM card in order to pretend to be them.

**Rubber Hose Attack** – When you physically beat someone with a rubber hose and get password data form them

**Vulnerability Disclosure** – Letting a company, or organization know of a vulnerability behind closed doors instead of in public to maintain security.

**Bug Bounties** – Where companies pay people to find bugs in software that they need to fix.

**Ethics and Legal Issues in Computer Security**

**Open Source Software:** Software which is free, with source code open to the public, and can be contributed to by the public

Example: Android, Linux, OpenSSL (APACHE web servers use this), Chromium

If there is a bug in open-source code, you need to have some sort of patching process.

Example: GitHub Issue

Patches can, but not always be used to also introduce vulnerabilities.

Dynamic testing can be used to verify the new source code

Static testing can also be used.

Eyeball testing is just looking over the code quickly to be sure theres no malicious code

Patching Process – Static , Dynamic, Eye-balling it

Top 3 Security Conferences

IEEE

USNEC

ASMCCS

**The University of Minnesota Case**

They submitted 3 Hyprocrit patches (less than 30 lines) that when merged into the source code could lead to greater vulnerabilities in the system.

They presented the paper at IEEE and were immediately ridiculed. They have been banned from contributing to Linux due to unethical means because it was performed on humans without the consent or prior knowledge from them.

They were forced to withdraw the paper.

**Ethics**

Was the Minnesota case unethical?

Yes: Developers are human, and had to manually check the code

No: The consent of humans would invalidate the research because it's no longer a blind study. Also you are not necessarily testing the individual humans, but the system in which the humans are part of.

These are both wrong lol.

**Institutional Review Board (IRB):** Responsible for reviewing research on human subjects.

What are the harms to the people in the study?

Does the purpose of the study outweigh the risk?

Human subject research must collect personal information about the people in the study, therefore the Minnesota case was not in violation according to the IRB.

**Improvements to the patching process that the Minnesota study found:**

* Verify the identity of the committer to have accountability.
* Add a line of text that says (“I agree to not intentionally introduce bugs to the source code”)
* Use more advanced tools to test patches.
* Allow the public to audit patches prior to acceptance.
* Preventative Patches (Allow patches for bugs that don’t exist yet, but might in the future)
* Raise Awareness of the Issue

**The Legal Side of Security**

**Laws applicable to: Criminals, researches, and law enforcement.**

The CFAA the Computer Fraud Abuse Act criminalizes 7 acts:

Section 1030 (a)(2) - Prohibits access to computer systems without authorization, or exceeding authorization.

EULA’s are used by companies to cover the authorization of use of their computer systems, and or software.

Precedent from different cases are common law and are used to determine which cases are in violation of the CFAA.

The right to privacy can be defined the **KATZ Test.**

Does the individual have an expectation of privacy?

The virtual theory of access says the login screen of a computer is like a locked door. You can’t just go up to a door and jiggle the lock to check if its closed.