Introduction to Cyber Security

Disclaimer

These slides are not based on the 2021 version of SAN's SEC301 course material in any way, shape or form because that would be a violation of copyright and distribution law.

Before we begin

Welcome!

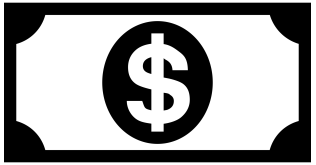
This is a very brief, high level overview of common topics in cyber security, not an exhaustive list.

It is meant as a starting point for further research (and also to bait you into attending more meetings).

If you would like to learn more about any topic in particular please let us know.

Foundations

Framework I: CIA Triad



Confidentiality - grant access only to those who need it

Integrity - only authorized data modification

Availability - able to use when needed

Ideally all 3 are equal,but in real life this isn’t possible.

Framework II: AAA (not for cars)

Authentication - Is the person who they say they are?

Authorization - What things are they allowed to do?

Accountability - What things did they actually do?

Principle of Least Privilege

Everyone can do everything they need and nothing more!

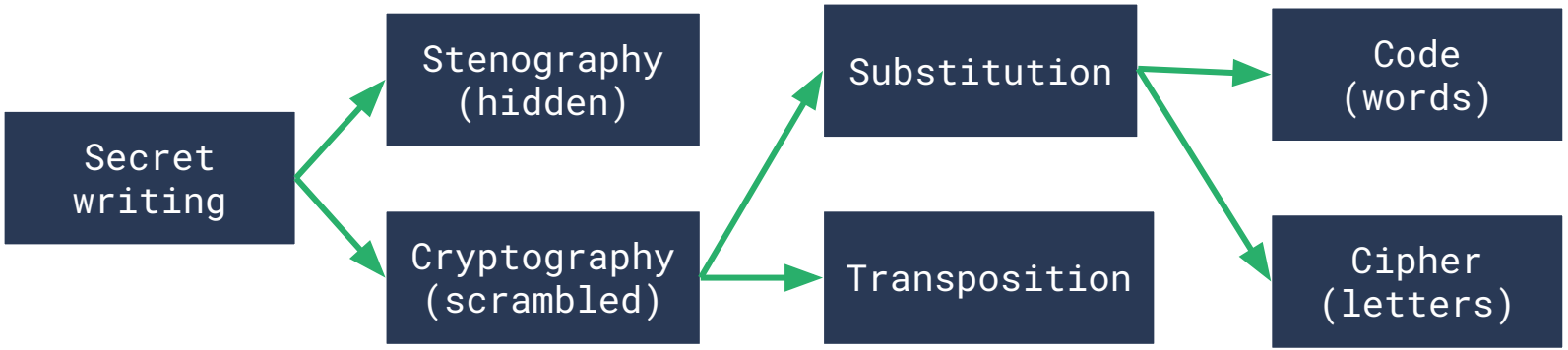
User privileges shouldn’t get in the way of security or vice versa.

Pop quiz: What command do you use to manage user/group permissions in Linux?

Cryptography

Cryptography

- Algorithms like DES and AES use a “random” key to encrypt/decrypt data
- Symmetric (same key) vs asymmetric (different keys, 1 public and 1 private/secret)
- Hashes ensure file integrity



Puzzle time

Can you figure out the message?

tan r olrisaeco

Answer: [redacted]

Next figure out what program this is.

62545b8eb17ddf27d5954ac5f8904814e12c5790d73daf545ef60bd97f4f2e12

Answer: [redacted]

Authentication

Passwords (+ how to pick a good 1)

Longer = better! Don't reuse, get a password manager.

LMMs0aT~Tcj0tM2 - 1.49 million centuries

MeowMeowMrrpPurrr:3! - 11.52 trillion centuries

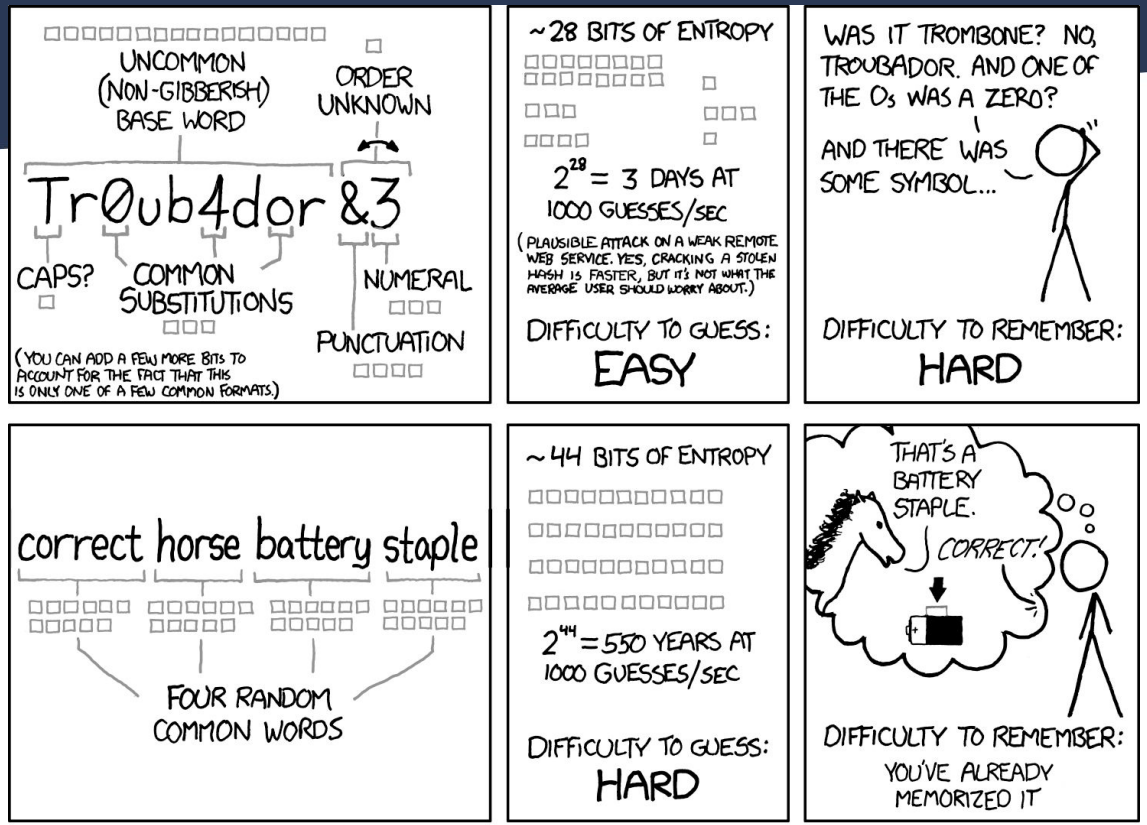
Eepy - nap time

Password crackers: John the Ripper, Hashcat, THC-Hydra

How long would your password take to crack?

https://www.grc.com/haystack.htm

Source: https://xkcd.com/936/



CYBER SECURITY CLUB AT UC DAVIS

Security Technologies

IOT Security

- NIST standards were released only last year!
- Many devices connected via Bluetooth SSP
- Wifi can reveal things like location history or anything transmitted over HTTP
  - Use HTTPS or a VPN!
- Android is the highest target for malware after Windows
  - The reason is because Android manufacturers make money off of the device itself, whereas IOS profits from app revenues.
- Don’t trust random USBs and external drives
  - *except for anything I give you :)

Social Engineering

The longest-standing and most underrated cyber security attack category (in my opinion)

Examples:

- Phishing/vishing (UCD phishbowl)
- Tailgating someone through a door
- Shoulder surfing
- Dumpster diving
- Pretending to be a service tech, delivery person, etc

Malware

- Virus: parasitic code that infects executables
  - Retrovirus: disables antivirus
- Worm: self-standing & self-executing but dumb
- Trojan: software with a nasty secret
- Logic bomb: executes at a certain time
- Rootkit: sneak in through the back door
- Spyware: records browsing, keystrokes, mouse clicks, etc
  - Keystroke logger: legal w/authorization
- Cryptojacking: use victim’s computer to mine crypto
- Ransomware: lock data until ransom is paid
- Factories: DIY malware kits

Anti-malware

- How does it detect malware?
  - Signature: every virus has unique string
  - Heuristics: strange syscalls or behavior
- Web analysis: Virustotal, HybridAnalysis

Try putting this into the sites above and see what you get:
http://malware.wicar.org/data/eicar.com

Note: Don't open the link unless you wanna download malware! Just copypaste the url.

Firewalls

- Exclusive lookup: give up after 1st match
  - Order of rules is important!
- Shallow (headers only) vs deep inspection
- Types of firewalls
  - Packet filter: shallow inspection, common on routers
  - Proxy: makes 2 separate connections/sessions
  - Stateful inspection: deep inspection of 1st packet, most common type
  - Web application: specialized proxy for web traffic
- Not enabled by default on Macs

Further Learning

Networking

Having network fundamentals down is integral to understanding how many cyber security concepts work.

Applications:

- Configuring firewalls
- Packet sniffing
- DDOS
- Port scanning/probing
- DNS spoofing/hijacking
- Man in the middle attacks

Other Topics Not Covered

- CS concepts - OSI model, base conversion
- Browser & web security - cookies, JS, DNS resolution
- System security - hardening, cloud, virtualization
- Network security - IDS/IPS, packet sniffer, port scanner, vulnerability scanner, wardriving
- Defensive measures - honeypots, penetration testing, threat hunting, geolocating attackers (jk…unless?)
  - Note: Do not hack people back! This is illegal + unethical.

Bonus Section

Careers

Blue Team (defensive):

- Information Security Analyst
- Digital Forensics
- IT Auditor
- CISO

Red Team (offensive):

- Penetration tester
- Researcher
- Security Application Engineer
- Operations Lead
- Head Eepy