

Chapter 27 – Security

- Three security events since 2010.
 - Stuxnet of 2010: <https://www.youtube.com/watch?v=6WmaZYJwJng>
 - Edward Snowden, 2013.
 - Ransomware, since 2013.
 - US Office of Personnel Mgmt was breached, 2015.
 - Election interference? 2016.
 - Huge ransomware attack of 2017.
- Who is responsible for ensuring system security? Sysadmin + everyone else.
- System is only as strong as the weakest link.
- What is an attack surface?
- Many companies spend more money on coffee machines than on security!

Elements of Security

- CIA triad.
- Confidentiality
 - Security of data: authentication, access control, encryption.
 - Integrity – authenticity of information, certificates, encryption.
 - Accessibility – accessible to authorized users, but with minimum access.
- Security-usability balance.

Compromising security

- Social Engineering - humans is the weakest link.
 - Phone calls.
 - Physical appearance.
 - Phishing and spear-fishing.
- Software vulnerabilities.
 - Programming bugs, exploring context dependencies.
 - Input validation vulnerabilities - buffer overflows.
 - Patch, patch, and patch!
- DDos
 - Aims at service disruption.
 - Financially motivated, political, retaliatory.
 - Botnets can be IoT.
- Insider Abuse
 - Employees, consultants and contractors.
 - Many reasons.
 - Most difficult to detect.
- Network, system, or app configuration errors.
 - Hackers exploit useful features of software.

- Enable password option in GRUB.

Basic Security measures

- No security out of the box.
- Apply Principle of least privilege in FW rules, user permissions, file permissions, etc.
- Layer security measures to achieve defense in depth.
- Minimize attack surface – less interfaces, services, systems, etc.
- Automation saves time and is consistent!
- Use Software updates:
 - Patches from vendors or local repositories.
 - Schedule patches reasonable, 1x a month, critical – anytime.
 - Often target old holes, but introduce new ones.
- Turn off unnecessary services:
 - Disable unneeded services and daemons when installing systems.
 - Limit system footprint – less sw packages, less security holes.
- Remote Logging
 - One centralized log aggregator to capture logs from many devices and analyze them.
 - Customize syslog, which is default.
- Backups
 - Store backups off site.
 - “Do not put all eggs in one basket”.
 - Protect backups by encryption and monitoring.
- Worms and viruses
 - Linux/Unix mostly immune. Why???
 - Access controlled environment limits the damage:
 - Write access to system executables is restricted at filesystem level.
 - What if malicious code is run by root?
 - Scan on Unix to protect Windows system.
- Root kits
 - Remain undetected on someone’s system.
 - Sony protects it’s CD copyrights.
 - Can be a hacked version of ps, ls, or kernel modules.
 - Can use host-based IDS OSSEC, monitor file integrity with AIDE, run scripts.
 - Better to reinstall from backups that clean.
- Packet Filtering
 - Use packet-filtering router or a firewall between system and Internet
 - Limit public exposure.
- Passwords and multifactor authentication

- Password on each account!
- Password rules!
- MFA systems (what you know, and what you have(phone))
- Duo is great for this.
- Biometrics
- Vigilance.
 - Regularly monitor the system, nw connections, process table..
- Penetration testing.
 - Have all applications tested.
 - Remember the weakest link!
 - Use third party and OWASP methodology.

Passwords and User Accounts

- In addition to securing all Internet-facing administrative access with MFA
- Manage passwords correctly.
- Implications of **sudo**.
- Random 12 or more character passwords withstand brute force attacks , but...
- It is hard to remember them.
- Never reuse same password elsewhere.
- Change passwds:
 - Every 6 months, or sooner.
 - When person who knows them leaves.
 - Any time you are wondering if security is compromised.
- Password vaults and escrows.
- Periodically check that all logins have passwords.
- Age passwords.

sudo chage -m 2 -M 90 -E 2017-07-31 -W 14 ben

Group Logins and Shared Logins

- Do not use group logins
- Often prohibited by HIPAA

User Shells

- Use standard login shell!

Rootly entries

- Back doors can be installed by changing UID to 0 in /etc/shadow file for other users.
- Disable remote root login.

CAPTCHA

- “Completely Automated Public Turing test to tell Computers and Humans Apart”.
 - Based on Turing test (which is based on imitation)
 - What is Turing test?
- Determines whether the user is real or a spambot.
- Invented to block spam software from posting comments on pages or purchasing things.
- Manipulate letters and numbers, and rely on human ability to determine what they are.
 - common form of CAPTCHA is an image with several distorted letters.
 - choose from a variety of images where you need to select a common theme (cars, traffic lights).
 - Some forms ask user to read text and then take a short quiz.
- Visual component makes it difficult for computers, but natural for humans.
 - It is difficult for computers to scan an image with distorted or moving text.
- Can be in audible format for visually impaired users.
- Uses of Catcha:
 - used on a variety of websites to verify that the user is not a robot.
 - used for online polls: best graduate school, best car, etc.
 - registration forms on websites such as Yahoo! Mail or Gmail where people can create free accounts to prevent creating spam accounts.
 - used by ticket selling websites to prevent ticket scalpers from over-purchasing tickets for large events.
 - used by web pages or blogs that contain message boards or contact forms to prevent spam messages or comments.

Does CAPTCHA work?

- Mostly.
- Hackers and spammers learnt to get around them, and even incorporate them into their sites to make them more believable.

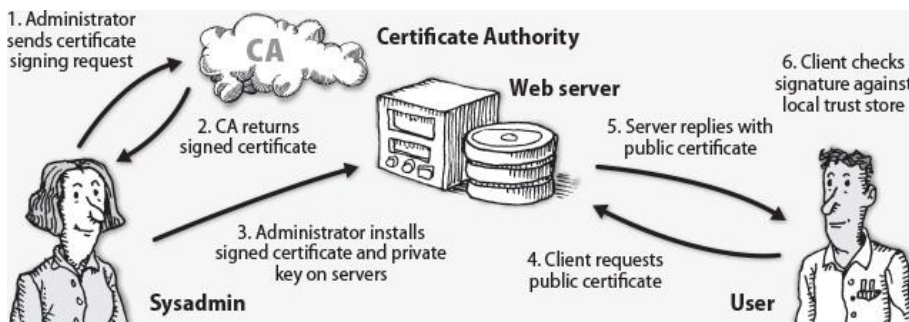
Cryptography Primer

- Allows to communicate secretly via unsecure channels.
- In the heart of all software design and network communication.
- Applied mathematics to problem of secure communication.
- Cypher – cryptographic algorithm – set of steps to secure the message.
- New algorithm is a very long process.
- Symmetric key cryptography
 - Classic or conventional.
 - Sender and receiver share a common key to encrypt and decrypt.
 - Efficient in terms of CPU used and size of encrypted payloads.
 - Often used in systems that need simple efficient process.

- How do you distribute the key?
- Used by AES, Twofish, Blowfish... and in SSH, TLS, IPSec, VPN, PGP, etc
- Public Key cryptography (Asymmetric cypher)
 - Addressed the problem of key exchange.
 - 1970s.
 - Diffie, Hellman, and Merkle key exchange.
 - Shared public key and secret private key.
 - Based on one-way function, or trapdoor function.
 - Youtube it: <https://www.youtube.com/watch?v=3QnD2c4Xovk>
- Public Key Infrastructure
 - How do you record and distribute public keys in a reliable and organized manner?
 - How do you validate the authenticity of public keys?
 - PGP adopted a “web of trust”.
 - Follow the indirect chain of trust (entities that trust each other)
 - PKI that implements web TLS (Transport layer Security) uses CA to vouch for public keys.

Certificate Authority

- Both A and B trust CA and have its public key.
- CA signs certificates for B's and A's public keys with its own private key.
- A and B check the CA's endorsements to make sure keys are legitimate.
- Certificates of major CAs (GoTrust and VeriSign) are bundled with OS distros.
- CA is listed in client's local trust store.
- Client checks if peer's certificate was signed by this CA.



- CA charge fees for signing services.
- “Extended validation certificates” for the entire subdomains are more expensive.
- CAs are targets for hackers!!!!
- Choose well and think twice before implementing on your own system!!!

TLS

- Successor to SSL
- TSL + HTTP = HTTPS
- Layer that wraps around TCP connections, between layers 4 and 7.
- Secures HHTP and SMTP protocols.

- In established connections contents are encrypted, except the host and port.
- One way – client validates server (typical),
- Two ways – server also validates client (mutual authentication).
 - Client presents its certificate to server
 - Netflix
- What to do:
 - Disable SSL in your system
 - Disable TLS 1.0
 - Use TLS 1.2
 - TLS 1.3 coming soon

Cryptographic hash functions

- Verify the integrity of things.
 - File's integrity
 - Message integrity
- Given input of variable length, generates small fixed-length value.
 - Finite number of output values exist
 - 8 bit hash = $2^8 = 256$ possible outputs
 - Different inputs generate same value – collision.
 - Cannot illuminate collisions entirely even with longer values.
- Output is hash value, hash, summary digest, checksum, fingerprint.
- Deterministic – same input generates the same hash.
- Cryptographic hash functions have the best security.
 - Entanglement.
 - Pseudo-randomness.
 - Nonreversibility.
- Families:
 - SHA-2 (Secure Hash Algorithm): SHA-256 (without version number)
 - SHA-3: SHA3-512
 - MD5 (vulnerable to collisions), ok for low security apps.
 - Open-source SW often release hashes to public for verification.
\$ sha256sum /etc/passwd
- To generate random numbers: use pseudo-device drivers:
/dev/random and **/dev/urandom**

PGP: Pretty Good Privacy

- Phil Zimmerman's tool chest
- Focused on e-mail security: encrypt data, generate signatures, verify origin.
- Many flaws, but still good.
- Being standardized under OpenPGP, many implementations exist.
- GNU project GnuPG at gnupg.org.

Kerberos

- Designed at MIT
- Authentication system that guarantees the identities of users and services.

- Uses symmetric and asymmetric cryptography to construct “tickets”.
- Kerberos daemon runs on authentication server issuing tickets to users that have correct credentials.
- Does not use unencrypted passwords on network
- Relieves users from typing passwords repeatedly.
- Does not supersede, but adds to other security measures on the system.
- Does not play well with Linux (use sssd daemon on Linux to interact with AD).

SSH

- Remote login protocol.
- Secures network services on insecure network.
- Can do:
 - Remote command execution
 - Shell access
 - Port forwarding
 - Network Proxy services,
 - VPN tunneling
- Great tool!!
- Uses cryptography for communication CIA
- Linux default has Open SSH.

OpenSSH

- OpenBSD project in 1999
- Connects on port 22
- More in textbook.

Firewalls

- Security on network level.
- Hardware or software that prevents unwanted packets from accessing nw and systems.
- Packet filtering FW
 - Limits what can pass thru gateway depending on the header info
 - **iptables** on Linux
 - Use dedicated appliances like Cisco and CheckPoint
- Can filter certain services
 - Two-stage filtering scheme
 - 1. Gateway to Internet
 - 2. Between GW and the rest of network
 - Start with no inbound services.
 - Allow useful services into the DMZ.
- Stateful inspection
 - Compare what is going on on NW with what “should be” going on.

- Firewalls should be part of multilayer security.

VPNs.