Security Design Principles: Minimize Secrets Complete Mediation (and Defense in Depth)

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Review: The Eleven Design Principles

General/Fundamental Design Principles

1. Simplicity (related to Economy of Mechanism but not exactly the same)
2. Open Design
3. Design for Iteration
4. Least Astonishment

Security Design Principles

5. ***Minimize Secrets (not specifically identified by Saltzer and Schroeder)***
6. ***Complete Mediation***
7. Fail-safe Defaults
8. Least Privilege
9. Economy of Mechanism
10. Minimize Common Mechanism (related to Least Common Mechanism)
11. Isolation, Separation and Encapsulation

Review: Saltzer and Schroeder's Security Design Principles

Many security issues are a result of poor coding techniques which lead to flaws in the program which can result in a security hole that can be exploited

Saltzer and Schroeder came up with a list of 8 security design principles that, if followed, would help programmers reduce the number of errors and design more secure software

1. Economy of mechanism – A simple design is easier to test and validate
2. Fail-safe defaults –In computing systems, the safe default is generally "no access" so that the system must specifically grant access to resources
3. ***Complete mediation – Access rights are completely validated every time an access occurs***
4. Open design –secure systems, including cryptographic systems, should have unclassified designs
5. Separation of privilege – A protection mechanism is more flexible if it requires two separate keys to unlock it, allowing for two-person control and similar techniques to prevent unilateral action by a subverted individual
6. Least privilege – Every program and user should operate while invoking as few privileges as possible
7. Least common mechanism – Users should not share system mechanisms except when absolutely necessary
8. Psychological acceptability – users won't specify protections correctly if the specification style doesn't make sense to them

Minimize Secrets

There are two principles to Minimize Secrets

- Secrets should be few and changeable
- They should maximize ***entropy***, thus increasing the attacker's work

Entropy:

- This is a measure of randomness or uncertainty in a variable or other data
- Usually measured in “bits” of entropy
- For example, if I picked a random number between 1 and 10 it would have ~3.3 bits of entropy

Minimize secrets – a thoughtful addition to the list that could be prone to misunderstanding. Secrets should be few and changeable, but they should also maximize entropy, and thus increase the attacker's work factor. The simple principle is also true by itself, since each secret increases a system's administrative burden: a late 1990s fighter jet project required dozens of separately-managed crypto keys to comply with data separation requirements that had been added piecemeal.

- R.E. Smith, https://cryptosmith.com/2013/10/19/security-design-principles/

Another reason to minimize secrets:

- It is incredibly difficult to keep a secret
- The information probably won’t remain secret for long

Minimize Secrets

Keeping secrets

- The general rule: A secret shared by two people is no longer a secret
- If a second person knows your secret, they could share it with someone they trust
- Even if it isn’t malicious, trust isn’t transitive
  - Alice may trust Bob, and Bob may trust Carol
  - This does ***not*** imply Alice trusts Carol – and now Carol has the secret, and may pass it on to someone they trust…
- Allegiance also plays a role – you may share something BECAUSE you are working with someone
  - For example, in NATO there are a lot of different countries working together
  - They may all be allied with NATO, but they also have an allegiance to their own country

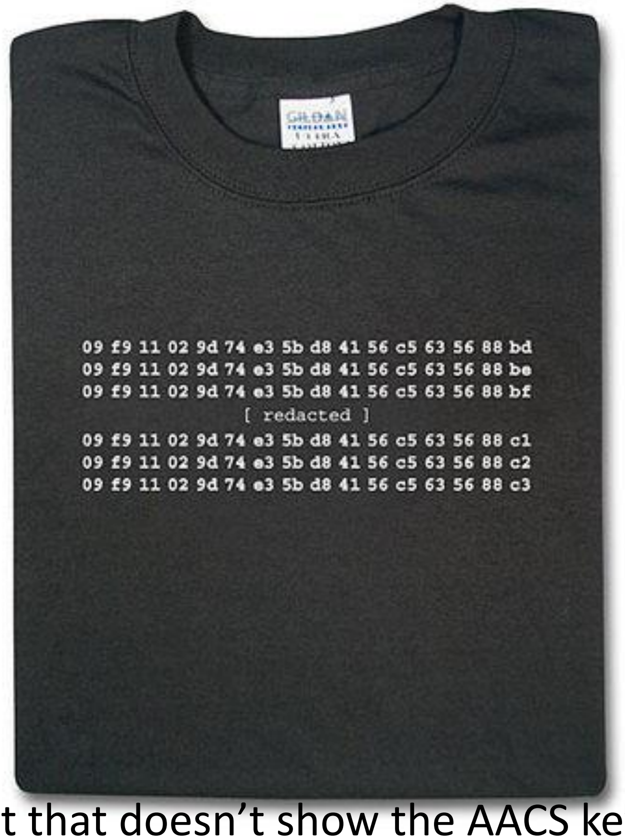
Replacing the secret

- If a secret is compromised, it must be replaced
- Fewer secrets – and fewer people who know them – makes replacing the secrets easier

Minimize Secrets

When designing a system with this principle in mind, there are several questions to ask:

- What is secret?
  - Everyone who is aware of the secret also has to know that it is secret
  - With classified information, it should be marked – CONFIDENTIAL, SECRET, TOP SECRET, etc. – which makes it easier
  - In business, it might be labeled Proprietary, Trade Secret, etc.
- What should be secret?
  - Other aspects of the system may also need to be secret
  - Not because, by themselves they are secret, but because they can give clues to the secret information
  - The t-shirt doesn't show the "secret encryption key" for AACS, but that doesn't really help
- How do we keep it secret?
  - Aggregation can allow secret information to be inferred
  - This may be done by combining data from different sources
    - A name, date of birth, and last-4 of a social security number (SSN) may not be secret
    - A name, and location of birth may not be secret
    - However, until fairly recently, that would be enough information to determine someone's full SSN – which is (supposed to be) secret
  - Freedom of Information Act (FOIA) requests can be an issue with data aggregation since they are considered independently, but may be combined to obtain secret information


09 f9 11 02 9d 74 e3 5b d8 41 56 c5 63 56 88 bd
09 f9 11 02 9d 74 e3 5b d8 41 56 c5 63 56 88 be
09 f9 11 02 9d 74 e3 5b d8 41 56 c5 63 56 88 bf
[redacted]
09 f9 11 02 9d 74 e3 5b d8 41 56 c5 63 56 88 c1
09 f9 11 02 9d 74 e3 5b d8 41 56 c5 63 56 88 c2
09 f9 11 02 9d 74 e3 5b d8 41 56 c5 63 56 88 c3

T-shirt that doesn't show the AACS key

Image source: https://www.wired.com/2007/05/not-an-aacs-tsh/

Minimize Secrets

Determine What Should Be Secret

- Identify critical information to determine if actions can be observed by adversaries (physical security) or accessed (computer security)
- Determine if information obtained by adversaries could be useful to them – and harmful to you
- Execute measures to mitigate this threat

Operational Security (OPSEC)

- What we mean by OPSEC is maintaining the security of daily operations that should remain secret or concealed from outsiders
  - Posting about being on a vacation could encourage someone to rob their house while they are gone!
- Recall the saying "Loose lips sink ships!" the Military Paradigm in the Open Design materials
  - Many of those posters addressed saying too much to others or being overheard
  - What is the modern equivalent?
  - Have you ever overheard people talking in a coffee shop – or on their cell phones?

Passwords

The most common authentication method for users is the "username/password" combination

In code, it might be an API token or other key

Far too often, these credentials are handled poorly

For example, North Carolina State University found over 100,000 GitHub repos that had leaked API tokens and keys

- https://www.zdnet.com/google-amp/article/over-100000-github-repos-have-leaked-api-or-cryptographic-keys/

Passwords are also compromised on a regular basis

- A website might be compromised and passwords harvested
- The passwords might be stored unencrypted – maybe in a file named "passwords"
- ***Note***: A standard red team technique is to immediately search for files named "password" (and variations) when they gain access to a system. Why? ***It works!***

MITRE maintains a list of "Common Weakness Enumerations" or CWE's

These list common software security weaknesses

- CWE-256: Plaintext storage of a password
- CWE-257: Storing passwords in a recoverable format.

CWE-257 would cover the case of Cisco's "Type 7 password" which uses the Vigenère cipher

- These can be instantly decrypted
- Generally found on older equipment that didn't support newer encryption methods
- However, password reuse on newer equipment can render stronger password encryption schemes irrelevant – the attacker can simply use the password from the older equipment

Passwords

While there is a problem with people sharing passwords – there is a worse problem of people selecting poor ones

Read:
https://en.wikipedia.org/wiki/Wikipedia:10,000_most_common_passwords

- Do you see patterns in the top 10?
- Do you see keyboard "walk" patterns?
  - 1qaz, asdf, etc.
  - Even if you used SHIFT to get a symbol instead of a digit, it isn't secure because it is a "known word"
  - Also, austin and dallas are far more popular the houston (at least for passwords) – antonio makes the list, but not sanantonio

Watch:

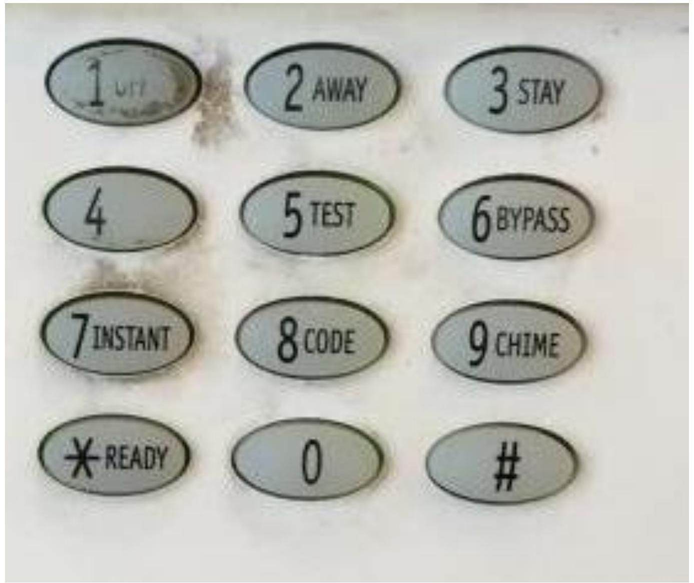
https://www.youtube.com/watch?v=5xKHx0X_LvM&t=26s

- This clip from *Ellen* is from 2012, but 4 of the top 5 from 2012 are still in the top 5!
- abc123 has fallen out of favor and is all the way down at #13

Passwords (and PINs)

PINs

- Without looking it up – what do you think the most common PIN is?
- ***Read***: https://www.pocket-lint.com/these-are-the-20-most-common-phone-pins-is-your-device-vulnerable/
  - Were you right about the most common PIN?
  - The top 20 passwords account for 26% of the total.
  - Also note that common PINs also used a “walk” pattern
  - People might also use an address
- They can also be compromised by dirt, wear patterns, or ***thermal artifacts***!
  - LockPickingLawyer:
  - https://www.youtube.com/watch?v=okgPbtz4ZkE



Dirt and wear on a keypad

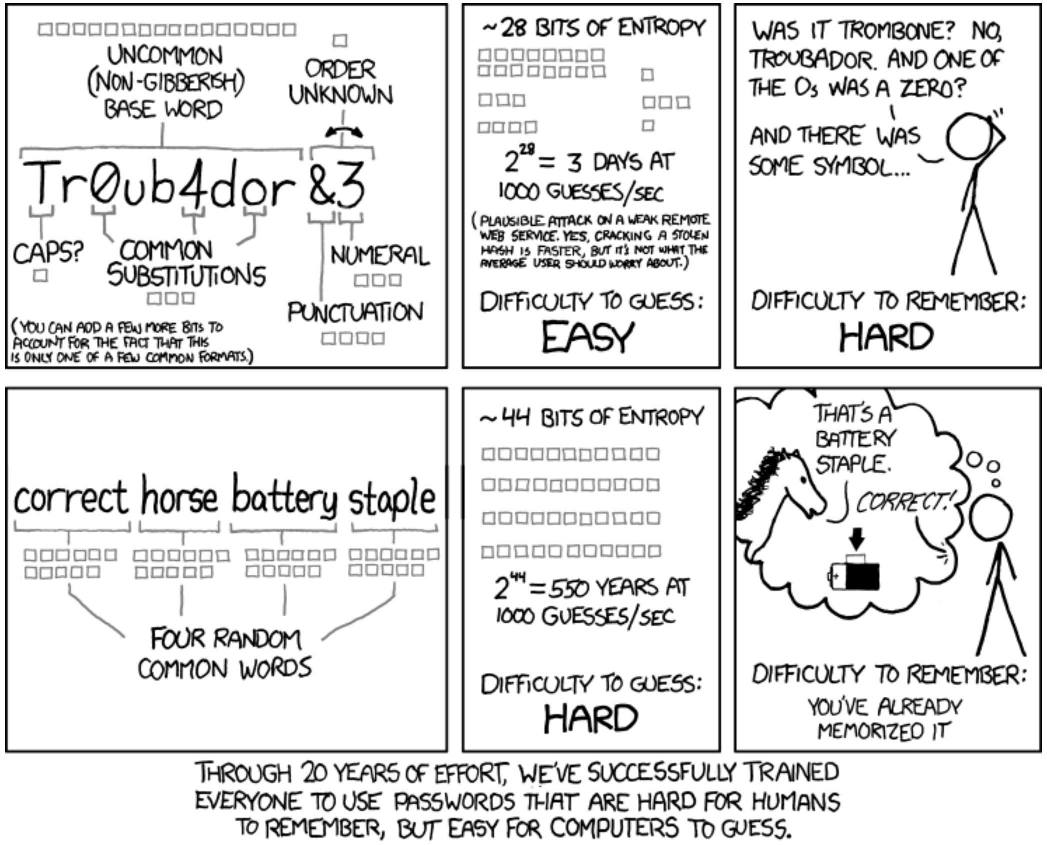
Passwords

Coming back to entropy

- We can calculate the entropy of passwords by raising the number of possible characters to the length of the password
- So, a 4-character, lower-case only password has:
  - 26^4 = 456,976 combinations or ~19 bits of entropy
- If we use upper- and lower-case letters we have:
  - 52^4 = ~7.3 million combinations or ~23 bits of entropy
- For 6-character passwords:
  - 26^6 = ~309 million combinations or ~28 bits of entropy
  - 52^6 = ~19.8 billion combinations or ~34 bits of entropy
- Notice we get far greater entropy from increasing the length of the password than adding to the character set
  - “Longer is better than more complex”

It should be noted that using GPU’s for password cracking can result in far, far more than 1000 guesses/second

- ***Read***: https://securityledger.com/2012/12/new-25-gpu-monster-devours-passwords-in-seconds/



UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Image source: XKCD, https://xkcd.com/936/

Passwords

It should be stressed that a completely random, machine-generated password are generally ***not*** going to be a good password

If a user needs to write it down to remember it is probably ***not*** a good password

- However, writing it down on paper ***may*** be more secure than having it in a file on your computer
- Someone would need physical access to obtain it
- It ***may*** be better than having it in a file on your computer

If passwords need to be written down (disaster recovery or other emergencies) there are things to consider:

- It should be stored in a secure location
- If possible, it can be split among multiple locations/people and require several of them to recreate
  - Split password in 3 parts
  - Person_1 (PW1, PW2); Person_2(PW2, PW3); Person_3(PW1, PW3)
  - Now it takes 2 of the 3 to recover the password
- Or, it can be obfuscated by “stuffing” unused characters: password becomes pa1ss3wogrdx – with every 3rd character being “fake”

Passphrases is also a good way to create strong, easily-remembered passwords

Just don’t pick a common phrase, famous quote, popular song, or anything easily guessed

Password Mangers

Password managers can help in managing all the unique, complex passwords you have

- (Do you use a unique password for every account and website?)

LastPass is an example of a password manager

- You have a master password to unlock your password vault
- All of your other passwords are stored in the vault
- Browser plugins and apps allow you to use those passwords easily
- LastPass Introduction: https://www.lastpass.com/how-lastpass-works

The iCloud Keychain is another example of securing passwords and other information

The drawback:

- If the master password is compromised, then all your passwords are compromised
  - See this ArsTechnica story from February 2023: https://arstechnica.com/information-technology/2023/02/lastpass-hackers-infected-employees-home-computer-and-stole-corporate-vault/
  - From that story: "*…the same attacker hacked an employee's home computer and obtained a decrypted vault available to only a handful of company developers.*"
- Facial recognition can help secure things on your mobile device, but still isn't perfect

Two-factor Authentication

More recently, two-factor authentication is an option when using a username/password combination

This can be:

- Text message with a code
- Mobile app like Duo Mobile
- Token like a CryptoCard or SecurID
- Security key like YubiKey
- Badge or smart card like a government HSPD-12

Overall, authentication is generally said to come down to three things:

- Something you know (password, PIN)
- Something you have (phone, token, badge)
- Something you are (biometrics, facial recognition)

Combinations of these is generally better than using just one of them

Image source: Alexander Klink, Wikiedia, https://en.wikipedia.org/wiki/RSA_SecurID

Operational Security

Three components:

1. Identify critical information to determine if actions can be observed by adversaries
2. Determine if information obtained by adversaries could be useful to them
3. Execute measures to mitigate this threat

Look at the provided image and you can see the Wi-Fi SSID and password posted

- ***Note***: BWAA probably refers to the Baseball Writers' Association of America

This may be an issue – or not – depending how they architected the network

- However, they probably didn't expect it to be compromised on national TV

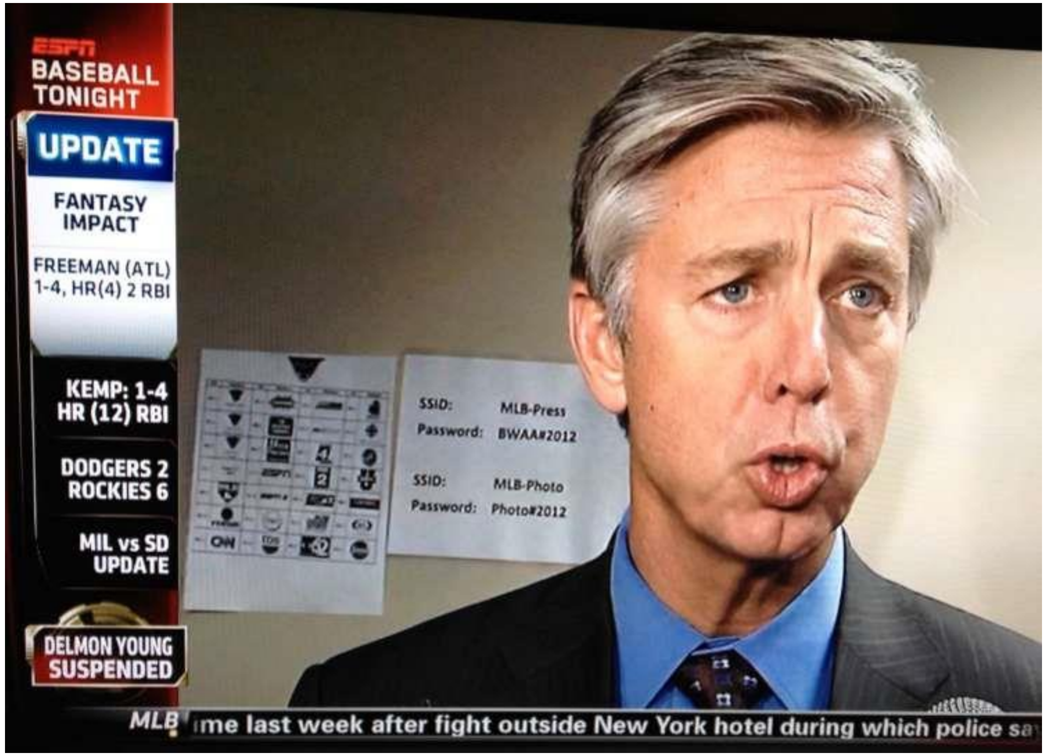


Image Source: ESPN

Operational Security

A more serious example:

- Locations of soldiers and military bases were leaked by fitness trackers
- ***Read***: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/
- To address this problem (Component #3) the Department of Defense banned fitness trackers for deployed troops
  - https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/

Of course, social media is still a problem:

- https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/

Military planning has also been detected by the amount of pizza delivered to the Pentagon

- https://www.army.mil/article/2758/2
- From the article:
  - *He described how the Pentagon parking lot had more parked cars than usual on the evening of Jan. 16, 1991, and how pizza parlors noticed a significant increase of pizza to the Pentagon and other government agencies. These observations are indicators, unclassified information available to all, Maj. Ceralde said. That was the same night that Operation Desert Storm began.*

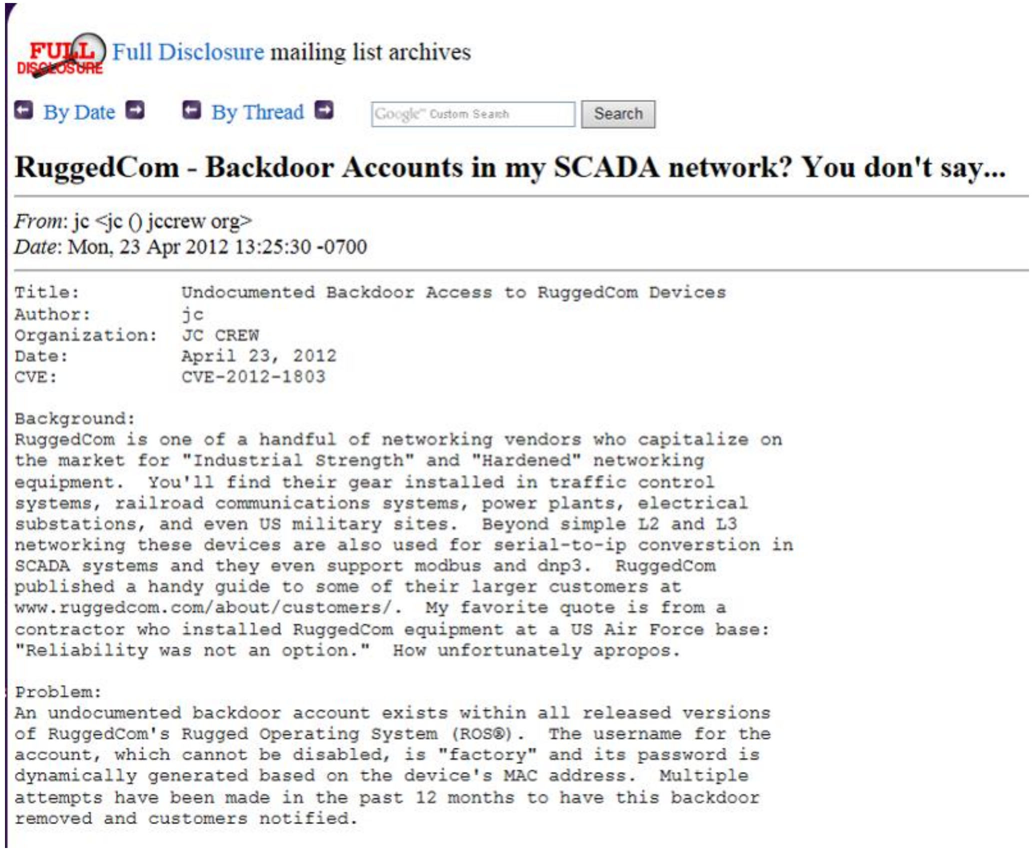
Responsible Disclosure

Responsible disclosure is a difficult line to draw

- One one side, you want to make sure that an organization fixes a problem that could be affecting thousands or millions of customers
- On the other side, you don't want to be the one to tell the Bad Guys about it (which does assume they don't already know about it)

The email image to the right is probably not reasonable since the author could have mentioned the problem without the details

More information on responsible disclosure can be found here: https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html



RuggedCom - Backdoor Accounts in my SCADA network? You don't say...

From: jc <jc () jccrew org>
Date: Mon, 23 Apr 2012 13:25:30 -0700

```
Title:          Undocumented Backdoor Access to RuggedCom Devices
Author:         jc
Organization:   JC CREW
Date:           April 23, 2012
CVE:            CVE-2012-1803

Background:
RuggedCom is one of a handful of networking vendors who capitalize on
the market for "Industrial Strength" and "Hardened" networking
equipment.  You'll find their gear installed in traffic control
systems, railroad communications systems, power plants, electrical
substations, and even US military sites.  Beyond simple L2 and L3
networking these devices are also used for serial-to-ip converstion in
SCADA systems and they even support modbus and dnp3.  RuggedCom
published a handy guide to some of their larger customers at
www.ruggedcom.com/about/customers/.  My favorite quote is from a
contractor who installed RuggedCom equipment at a US Air Force base:
"Reliability was not an option."  How unfortunately apropos.

Problem:
An undocumented backdoor account exists within all released versions
of RuggedCom's Rugged Operating System (ROS®).  The username for the
account, which cannot be disabled, is "factory" and its password is
dynamically generated based on the device's MAC address.  Multiple
attempts have been made in the past 12 months to have this backdoor
removed and customers notified.
```

Image source post: https://seclists.org/fulldisclosure/2012/Apr/277

Social Media

Organizations need to have a social media presence – but they also need a strategy to avoid embarrassing information and leaks being posted

This means:

- Partner with Marketing, Public Relations, and/or HR
- Define what is acceptable for employees to post
- Defining the boundaries between private and professional lives – especially with many people working from home
- This is also something to address with family members - especially children
- You don’t want a child to post, “My mom is sad today – she has to figure out who needs to be fired at her work.”

There are also a lot of other aspects to protecting children on social media – like cyberbullying – and it is important that parents work with their children to understand:

- They can’t monitor everything
- Children understand what is being monitored
- That rules are consistent
- There are a lot more aspects to protecting children on social media, but those are beyond the scope of this class

UTSA has a site on using social media:

- https://www.utsa.edu/marcomstudio/social-media/

Complete Mediation

By Saltzer and Schroeder:

Complete mediation: Every access to every object must be checked for authority. This principle, when systematically applied, is the primary underpinning of the protection system. It forces a system-wide view of access control, which in addition to normal operation includes initialization, recovery, shutdown, and maintenance. It implies that a foolproof method of identifying the source of every request must be devised. It also requires that proposals to gain performance by remembering the result of an authority check be examined skeptically. If a change in authority occurs, such remembered results must be systematically updated.

From Matt Bishop's book *Computer Security: Art and Science*:

Definition 13-4.The principle of complete mediation requires that all accesses to objects be checked to ensure they are allowed.

Whenever a subject attempts to read an object, the operating system should mediate the action. First, it determines if the subject can read the object. If so, it provides the resources for the read to occur. If the subject tries to read the object again, the system should again check that the subject can still read the object. Most systems would not make the second check. They would cache the results of the first check, and base the second access upon the cached results.

Quotes from:
https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/complete-mediation

Complete Mediation

US-CERT Description

A software system that requires access checks to an object each time a subject requests access, especially for security-critical objects, decreases the chances of mistakenly giving elevated permissions to that subject. A system that checks the subject's permissions to an object only once can invite attackers to exploit that system. If the access control rights of a subject are decreased after the first time the rights are granted and the system does not check the next access to that object, then a permissions violation can occur. Caching permissions can increase the performance of a system, but at the cost of allowing secured objects to be accessed.

For every requested action, check ***authenticity***, ***integrity***, and ***authorization***

- To be secure, the system must verify these three things before performing the requested action

Authenticity: Verify the claimed identity is genuine

Integrity: Verify the request received is the one made

Authorization: Verify the agent (user, identity, etc.) has permission to perform this action

Quotes from:
https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/complete-mediation

Authentication

Authentication is used to bind a subject to an identity

- For example, you authenticate to UTSA when you (subject) log in with your abc123 (identity)
- It is ensuring that an individual (subject) is who they claim to be (identity)

Access control is only allowing subjects to access authorized objects

- A student can only see their grades in Blackboard, but an instructor can see them all

Refer back to Lesson 0 regarding AAA Services, the components, and their definitions

Three Basic Authentication Techniques

Mentioned earlier they are:

- Something you know (password, PIN)
- Something you have (phone, token, badge)
- Something you are (biometrics, facial recognition)

There are problems inherent in these approaches

Smartphones have addressed many of these issues on a personal level, but it is still an issue at the organizational level

- Buying 25 iPhones for staff members to authenticate is expensive
- Often an organization has staff use their own phones, but that can cause other issues for data stored on those personal devices

Something you know

- The secret might be written down, poorly chosen or forgotten

Something you have

- Requires additional hardware (which can be expensive)
- Can be lost

Something you are

- Requires additional hardware
- Things about you can change
  - Sometimes facial recognition fails (ex. If your eyes are swollen from allergies) and you have to use a PIN to unlock your phone
- Certain users may dislike or distrust the systems
  - Retinal scans require beams of infrared light to be sent into the eyes

Access Controls

The first line of defense is physical security which starts at the facility perimeter

- You want to control access to your facility
- Secure facilities may have a single point of entry – but often this is impractical
- If an attacker can gain physical access then security is lost
- See this video for what an attacker could do:
  - https://www.youtube.com/watch?v=0_ZfuMINJk8

Physical locks can be picked or defeated in other ways

- Picking can use picks, bump keys, shims, or weaknesses in locks

Theft also becomes a real issue if an attacker gains physical access

- They can steal laptops, external storage devices, workstations – or just their hard drives
- This is why drives should always be encrypted
- This is why the data on the systems should be backed up
  - This also protects against the “Cup of Coffee” attack
  - Also, restoring from backups needs to be practiced

Dumpster Diving

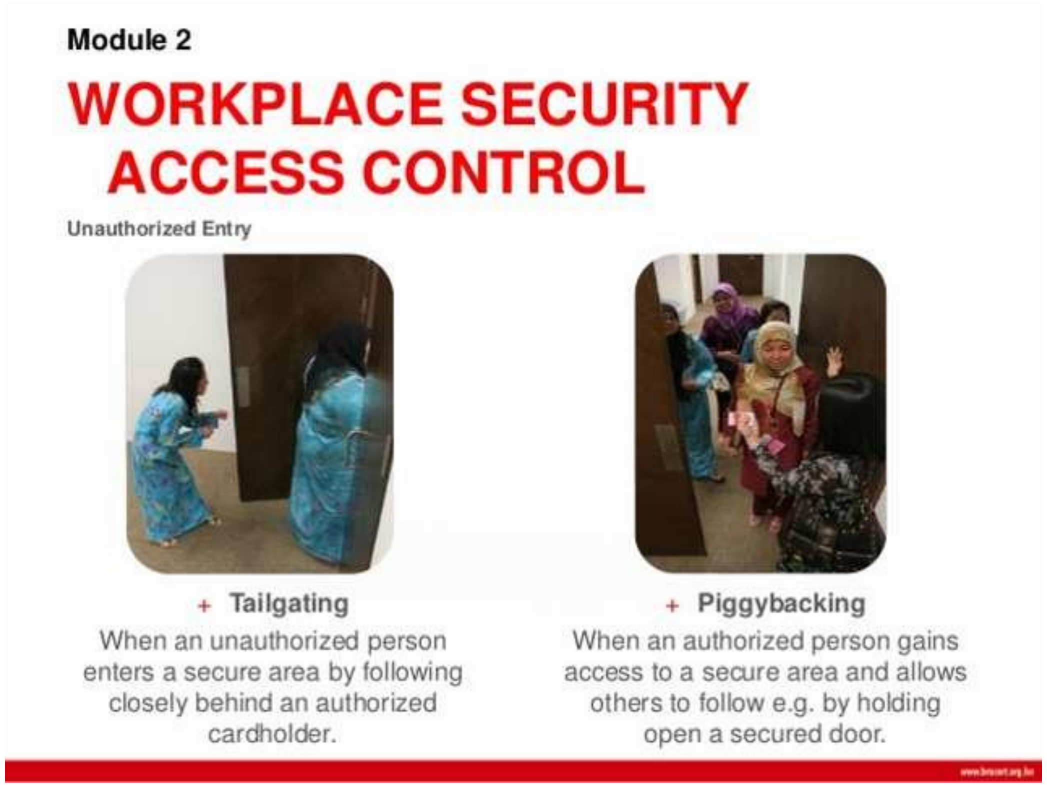
- In dumpster diving an attacker digs through trash to find valuable information/documents

Piggybacking and Tailgating

They are similar – but with slight differences

Another term often associated with Piggybacking is ***vouching***

- The authorized person is vouching for another person and giving them access
- For example, in a secure facility, an intern or someone interviewing may not have access
  - The hiring manager has to vouch for them to let them in
- Vouching can also happen if someone forgets their badge at their desk and they are let in to get it
  - This is allowed at some facilities, and not allowed at others



Module 2

WORKPLACE SECURITY
ACCESS CONTROL

Unauthorized Entry

+ **Tailgating**
When an unauthorized person enters a secure area by following closely behind an authorized cardholder.

+ **Piggybacking**
When an authorized person gains access to a secure area and allows others to follow e.g. by holding open a secured door.

www.brucert.org.bn

Image from: https://www.slideshare.net/salleh1n/itsa-end-user-2013

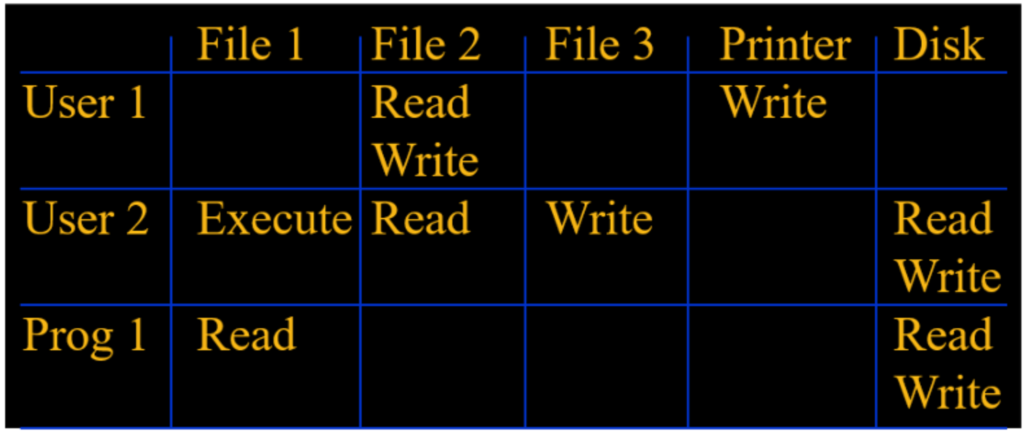
Access Controls

Access Control Matrix

- This lists every subject and every object available – and lists all the permitted actions
- We can see that User 1 has Read and Write access to File 2, but no permissions for File 1

This is a simple solution to the access control problem, but is extremely large

- Consider how big an access control matrix would be for Facebook
- Over a billion users and with every image, check-in, message, and post being an object
- Often, the matrix is sparsely populated, so most of it is blank



	File 1	File 2	File 3	Printer	Disk
User 1		Read Write		Write	
User 2	Execute	Read	Write		Read Write
Prog 1	Read				Read Write

Types of Access Controls

There are many models to conduct access control – with some designed for specific environments such as cloud computing

There are two variants of the Access Control Matrix that greatly reduce the storage requirements and usability:

- ***Capabilities List***: Each user (subject) has a list of the objects they may access, along with their specific permissions
- ***Access Control List***: Each file (object) maintains a list of what user can access it and what permissions they have
- ***Permission (protection) bits***: A simplified form of an ACL used in UNIX-based systems with a single bit representing whether access is allowed or not

Access Control Models:

Discretionary Access Control (DAC):

- Every object has an owner, and access can grant or deny access to any other subject

Mandatory Access Control (MAC):

- Labels are applied to objects and subjects. The subject must have a label that allows access to an object
- For example, to access a TOP SECRET file a user (subject) must also have the TOP SECRET label

Role-based Access Control (RBAC):

- Access is granted on a defined set of roles (and groups) for specific jobs (roles) that are commonly performed by individuals with the same role

Task-based Access Control (TBAC):

- Access is granted based on the files that a specific task requires.
- Access is only given to individuals who are authorized to conduct that activity (task)

Complete Mediation Examples

Matt Bishop:

When a UNIX process tries to read a file, the operating system determines if the process is allowed to read the file. If so, the process receives a file descriptor encoding the allowed access. Whenever the process wants to read the file, it presents the file descriptor to the kernel. The kernel then allows the access. If the owner of the file disallows the process permission to read the file after the file descriptor is issued, the kernel still allows access. This scheme violates the principle of complete mediation, because the second access is not checked. The cached value is used, resulting in the denial of access being ineffective.

Matt Bishop (again):

The Directory Name Service (DNS) caches information mapping hostnames into IP addresses. If an attacker is able to "poison" the cache by implanting records associating a bogus IP address with a name, the host will route connections to that host incorrectly

Quotes from:
https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/complete-mediation

Complete Mediation

Viruses cause havoc because, any program or script that is downloaded or received as an email attachment, runs with the privileges of the user or application that runs them

From ***CWE-638: Not Using Complete Mediation***

Invalidate cached privileges, file handles or descriptors, or other access credentials whenever identities, processes, policies, roles, capabilities or permissions change. Perform complete authentication checks before accepting, caching and reusing data, dynamic content and code (scripts). Avoid caching access control decisions as much as possible.

The Open Web Application Security Project links Complete Mediation with ***Defense in Depth***

- Their definition: *The principle of defense-in-depth is that layered security mechanisms increase security of the system as a whole. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system.*
- https://wiki.owasp.org/index.php/Defense_in_depth

Defense in Depth

According to Microsoft, the layers of defensive positions in defense in depth are as follows:

- ***Data***. An attacker's ultimate target, including your databases, Active Directory service information, documents, and so on
- ***Application***. The software that manipulates the data that is the ultimate target of attack
- ***Host***. The computers that are running the applications
- ***Internal Network***. The network in the corporate IT infrastructure
- ***Perimeter***. The network that connects the corporate IT infrastructure to another network, such as to external users, partners, or the Internet
- ***Physical***. The tangible aspects in computing: the server computers, hard disks, network switches, power, and so on
- ***Policies, Procedures, Awareness***. The overall governing principles of the security strategy of any organization. Without this layer, the entire strategy fails.
- https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc512681(v=technet.10)

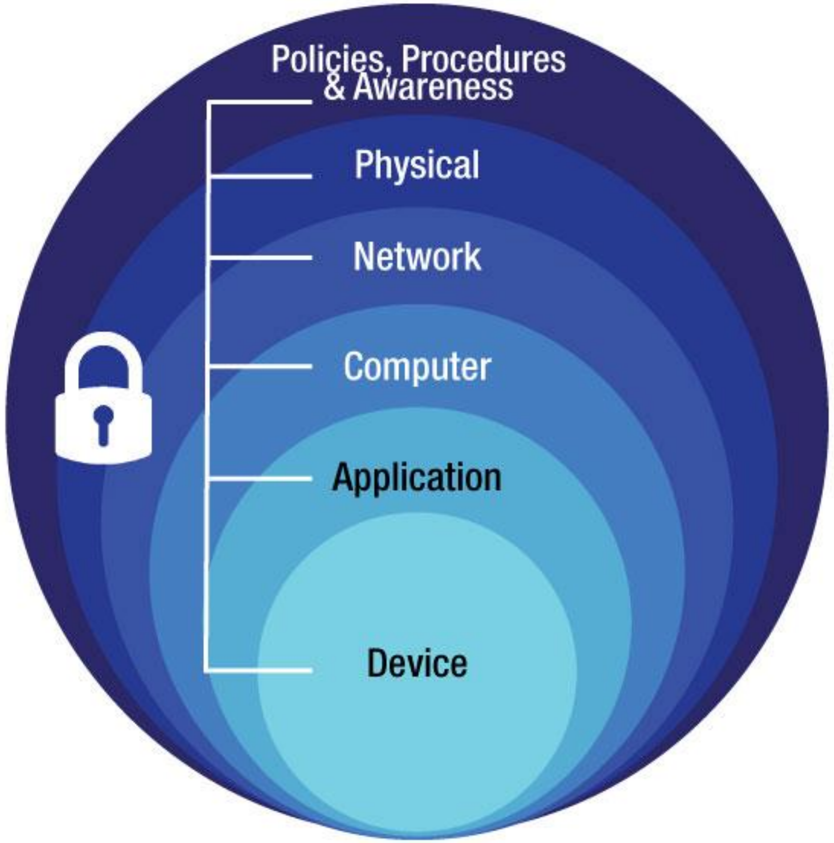


Image from Buffalo Tech: https://www.buffalotech.com/blog-helpful-tips/defense-in-depth-a-comprehensive-strategy-for-evolving-cyberthreats

Defense in Depth Commonly Used Methods

From Wikipedia:

System/ Application Security:

- Antivirus software
- Authentication and password security
- Encryption
- Hashing passwords
- Logging and auditing
- Multi-factor authentication
- Vulnerability scanners
- Timed access control
- Internet Security Awareness Training
- Sandboxing
- Intrusion detection systems (IDS)

Network Security:

- Firewalls (hardware or software)
- Demilitarized zones (DMZ)
- Virtual private network (VPN)

Physical Security:

- Biometrics
- Data-centric security
- Physical security (e.g. deadbolt locks)

Reference:

- https://en.wikipedia.org/wiki/Defense_in_depth_(computing)

Defense in Depth Strategies

Joel Snyder defines six strategies for defense-in-depth

- Quote from: http://www.opus1.com/www/whitepapers/defense-in-depth.pdf

  Defense-in-depth is not a product, like a perimeter firewall. Instead, it is a security architecture that calls for the network to be aware and self-protective. In studying the problem of adding defense-in-depth, we've identified six key strategies that security architects can use to change significantly the security posture of enterprise wired and wireless LANs (WLANs):

  Strategy 1: Authenticate and authorize all network users

  Strategy 2: Deploy VLANs for traffic separation and coarse grained security

  Strategy 3: Use stateful firewall technology at the port level for fine-grained security

  Strategy 4: Place encryption throughout the network to ensure privacy

  Strategy 5: Detect threats to the integrity of the network and remediate them

  Strategy 6: Include end-point security in policy-based enforcement

Remember the key thing on defense in depth:

- The protections have to in ***series*** not in parallel
- This way, if one mechanism fails, there are more mechanisms to detect or defeat an attack

Active Cyber Defense

From ActiveCyber:

- *Active cyber defense (ACD), also known as adaptive security, is a rapidly emerging branch of cyber security that integrates and enhances several cyber intelligence, cyber protection, and cyber analytics technologies to proactively and predictively combat cyber attacks and protect data assets. Within the evolutionary line of cybersecurity species, ACD's dynamic and proactive approach charges ahead of its closest ancestor, defense-in-depth, (which was limited by its static and reactive nature) and steps out of the jungle, upright and spear in hand. ACD enables a fuller situational context, which allows for greater precision and speed in cyber responses. ACD makes extensive use of automated courses of action, leveraging the resiliency of intelligent networks and the agility that virtualization offers to disrupt the attacker's kill chain.*
- https://www.activecyber.net/what-is-active-cyber-defense/

This introduces us to the idea of the (cyber) kill chain

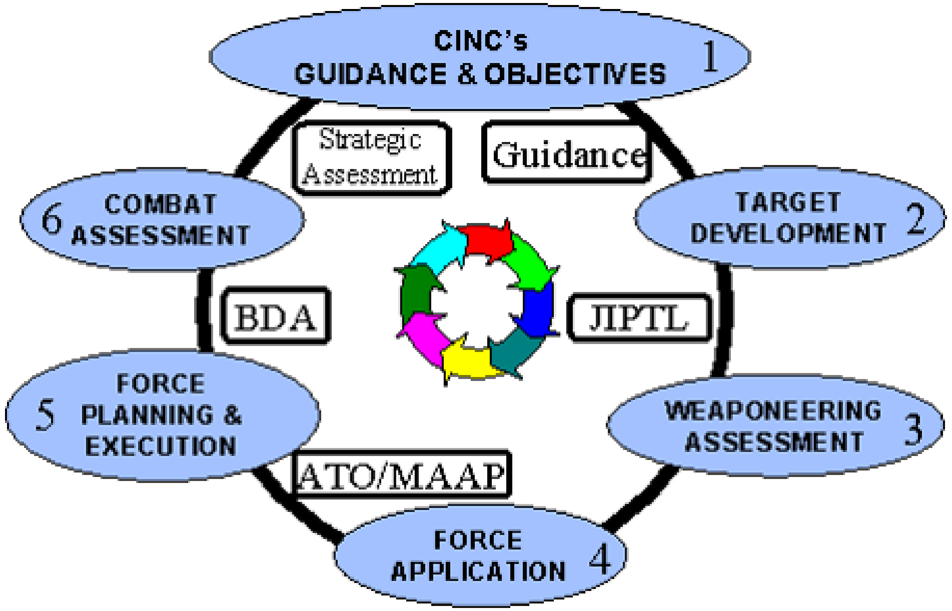
Kill Chain

Original concept was a military attack structure

“Breaking” an opponent’s kill chain meant having an effective defense or taking preemptive action

It was originally known as F2T2EA:

- ***Find***: *Identify a target. Find a target within surveillance or reconnaissance data or via intelligence means.*
- ***Fix***: *Fix the target's location. Obtain specific coordinates for the target either from existing data or by collecting additional data.*
- ***Track***: *Monitor the target's movement. Keep track of the target until either a decision is made not to engage the target or the target is successfully engaged.*
- ***Target***: *Select an appropriate weapon or asset to use on the target to create desired effects. Apply command and control capabilities to assess the value of the target and the availability of appropriate weapons to engage it.*
- ***Engage***: *Apply the weapon to the target.*
- ***Assess***: *Evaluate effects of the attack, including any intelligence gathered at the location.*



JOINT FIRES TARGETING CYCLE

Information and image from Wikipedia: https://en.wikipedia.org/wiki/Kill_chain

Cyber Kill Chain

Lockheed Martin developed the concept of the Cyber Kill Chain® in 2011

This describes the steps an enemy takes to attack information systems and networks

Wikipedia describes the phases as:

- ***Reconnaissance***: Intruder selects target, researches it, and attempts to identify vulnerabilities in the target network.
- ***Weaponization:*** Intruder creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.
- ***Delivery***: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives)
- ***Exploitation***: Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.
- ***Installation***: Malware weapon installs access point (e.g., "backdoor") usable by intruder.
- ***Command and Control***: Malware enables intruder to have "hands on the keyboard" persistent access to target network.
- ***Actions on Objective***: Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.
- https://en.wikipedia.org/wiki/Kill_chain#Cyber

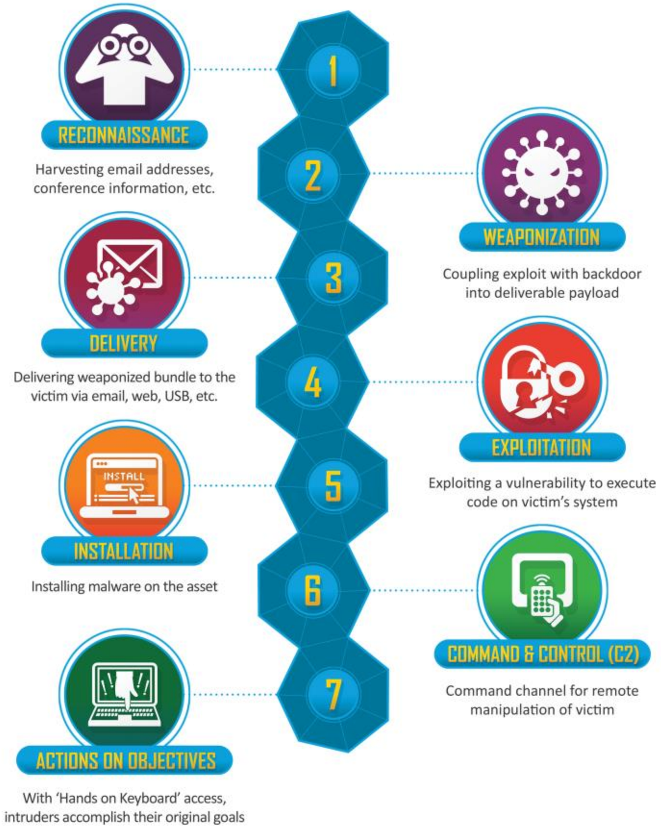

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Image from Lockheed Martin: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

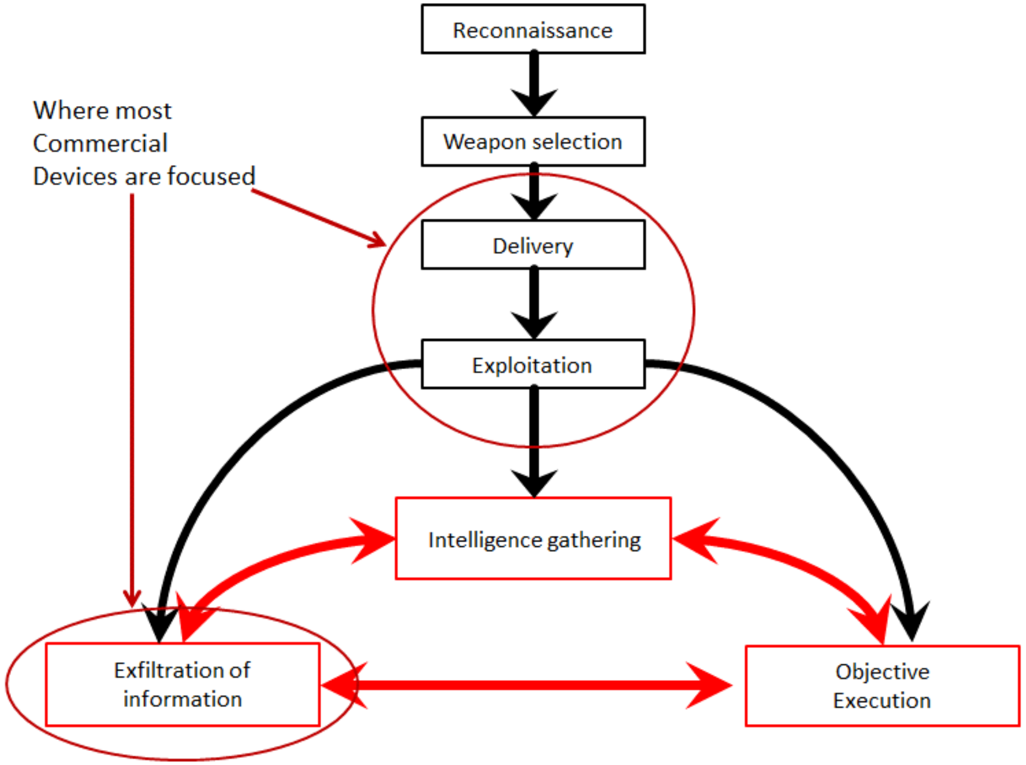
Cyber Kill Chain - Modified

Dr. Jim Rutherford, UTSA '17, as part of his dissertation analyzed the Lockheed-Martin Kill Chain and proposed some specific modifications to it

The major differences (as can be seen in the diagram) are that the chain can loop and proceed in a non-linear manner and that some of the steps can be "skipped" as well

The new model also points out where most commercial products are focused – and where they aren't

If you can disrupt or "get inside of the kill chain" a defender can effectively nullify that attack



The Need for Active Cyber Defense

Read: *What is Active Cyber Defense?* by CyberSecurityChief for ActiveCyber

- https://www.activecyber.net/what-is-active-cyber-defense/

You will be responsible for knowing the content of this article

- Pay close attention to the phases and advantages of the OODA loop
- Also make note of the Active Defense Capability Areas listed at the bottom

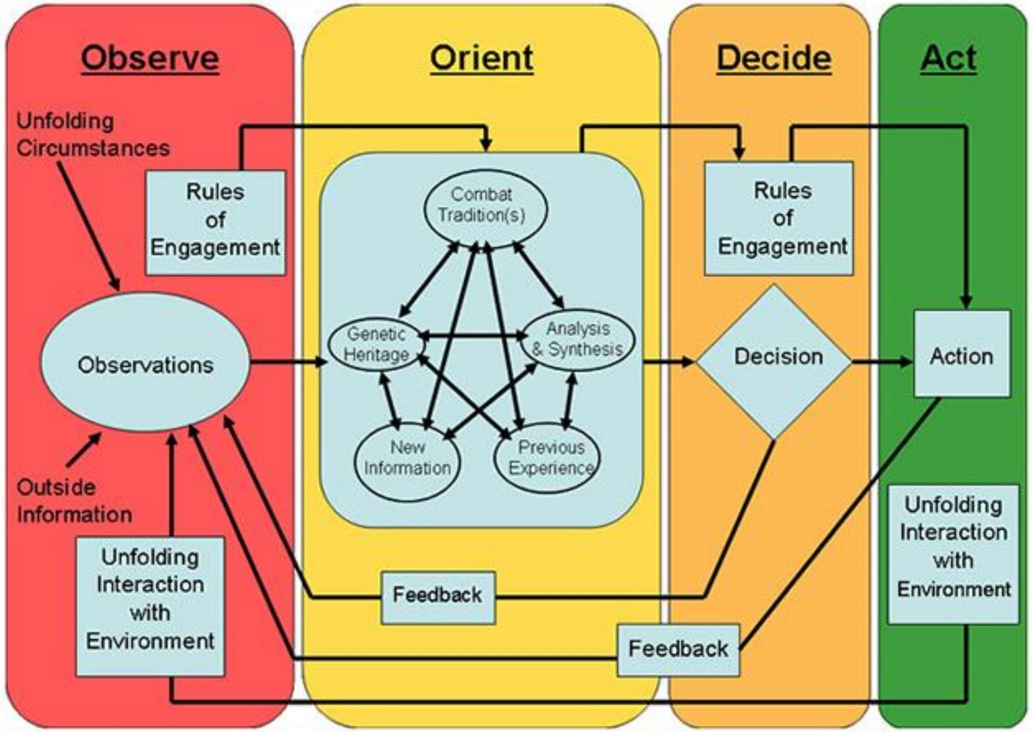


Image from ActiveCyber: https://www.activecyber.net/what-is-active-cyber-defense/

Active Defense Capability Areas

ActiveCyber lists the capability areas as:

- Intel-based Defenses
- The Three Ds (Detection, Deception & Delay)
- Intelligent Networks
- Automated Orchestration
- Agile Cloud Security
- Adaptive Endpoints

These are all areas of active research and development

Many of them have come together in the MITRE ATT&CK® Framework

MITRE ATT&CK Framework

From https://attack.mitre.org/

- *MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations*

ATT&CK is currently a critical tool in defending enterprises from attackers

It also hits on many of the active defense capability areas

- It is based around threat intelligence
- It provides tools to help detect an attack using ATT&CK-based Analytics
- It's analysis can be automated
- There is also an ATT&CK for Cloud
  - There is a presentation available from ATT&Ckcon in 2020 where Jen Burns presents on the latest developments
  - https://attack.mitre.org/resources/attackcon/
- This doesn't solve all the active defense capabilities necessary, but it definitely is a good start

New Paradigms

Bring your own device (BYOD) breaks the perimeter of traditional security approaches

Compared to providing a device, it is far less secure

- Company data may end up on a personal device
- May provide an attack vector for malicious code
- May expose employee PII to the organization

BYOD policies need to explicitly define:

- What types of devices can be used
- What the device can be used for
- How it connects to the corporate network
- What happens if there is a data breach involving the device
  - It may need to be confiscated to clean up the breach

The cloud brings many capabilities to an organization – and substantial opportunities for cost savings

However, by running virtualized systems on top of cloud infrastructure, this increases complexity

It also creates a trust relationship with the cloud provider

- Not only for uptime of the network and systems, but also storage, backup, and other enterprise-level required services

Security specifics also depend on the type of cloud service:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)
- Each one has a different security model – and different responsibilities for the cloud provider and the organization

Summary

Minimize Secrets: Secrets should be few and changeable

Secrets should maximize entropy, thus increasing the attacker's work

Operational security MUST be emphasized as it is frequently the weakest link in the system

Complete Mediation: Access rights are completely validated every time an access occurs

Authentication: making sure you are who you claim to be

Three general ways to do authentication

- Something you know, have, or are

Authorization and access control establishes what a user can do to a file or other resource

There are several different access control models

Defense-in-depth is the principle stating that layered security mechanisms increase security of the system as a whole