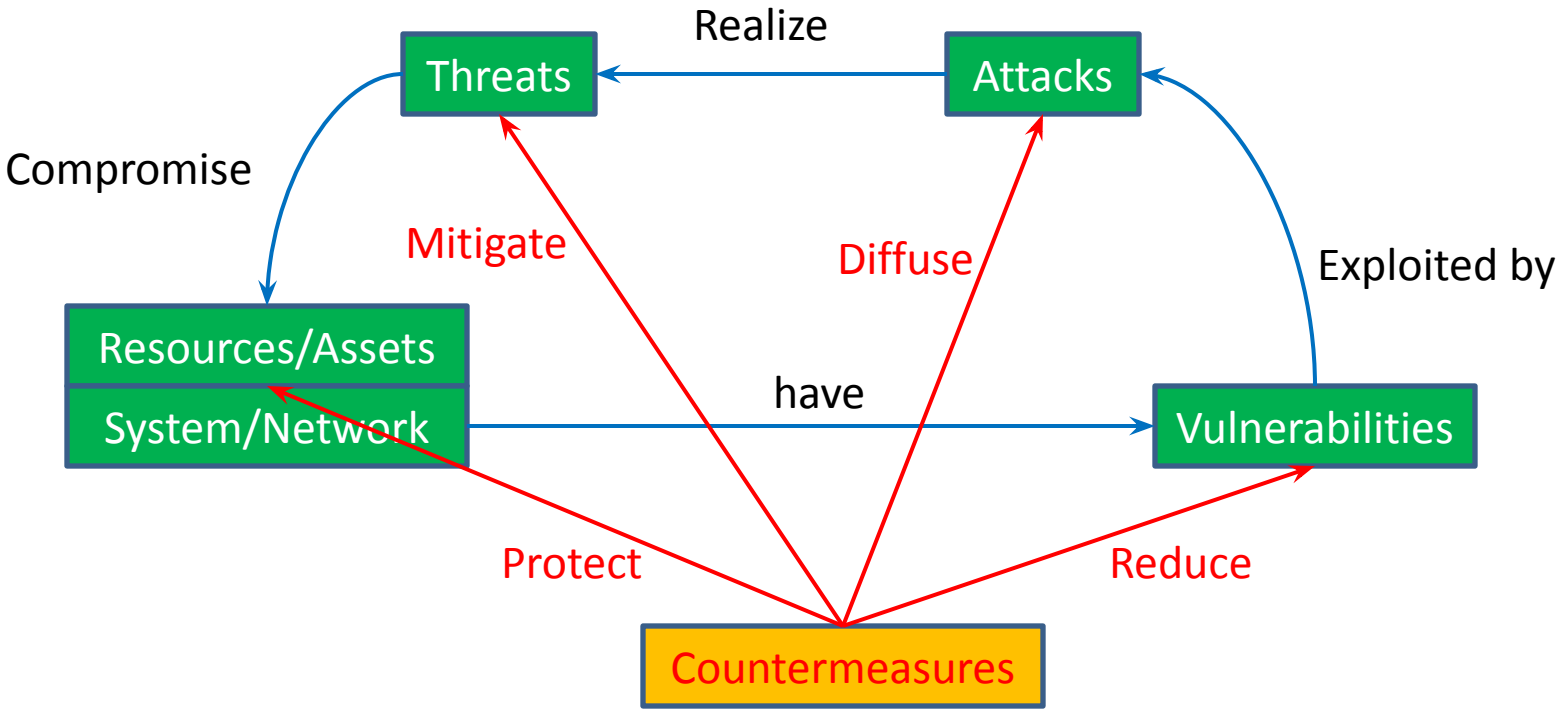
Computer and Network Security: Security Arena

Kameswari Chebrolu

Behold the Security Arena!



Example

- Asset: Student marks-sheet
- System: Residing on Instructor’s computer
- Threat: Student changing marks in the sheet
- Attack: Crack password
- Vulnerability: Weak password
- Countermeasures: Strong authentication; Strict punishment

Another Example

- Asset: Webpage
- System: Hosted on a web server
- Threat: Deface the webpage
- Attack: SQL injection
- Vulnerability: Application software
- Countermeasures: Validate input, Least privilege,

Vulnerabilities/Attacks

- Weakness in the system; Attackers exploit vulnerabilities

Sources of Vulnerabilities:

- **Clueless Humans**

"The user's going to pick *dancing pigs* over security every time" --*Bruce Schneier*

- **Clueless Humans**
  - Submit password details at fake look-alike site in response to email (**Phising**)
  - Open dangerous email attachments (Anna Kournikova computer **worm, trojans**)
  - Download malware app that boasts new features (whatsapp gold **malware; trojans**)
  - Trust pop-up ads that warn of computer infection and buy fake and potentially dangerous anti-virus protection (**scareware**)
  - The list goes on……

- **Software Vulnerabilities**
  - Sloppily written code (unintentional)
    - Attacks: **buffer overflow, cross-site scripting, SQL injection**
    - Permit data theft, data tampering, launching worms etc
  - Code tampering (intentional) by disgruntled employee
  - Mis-configuration
    - Attack: **Privilege escalation**
    - Permit data theft, install dangerous programs etc

- **Protocol Vulnerabilities**
  - Not developed with security in mind
  - Attacks: **ARP spoofing, DNS poisoning, TCP session hijacking, SYN flood DOS, IP smurf DOS** etc
  - Permit denial of service, impersonation, sniffing etc

Question

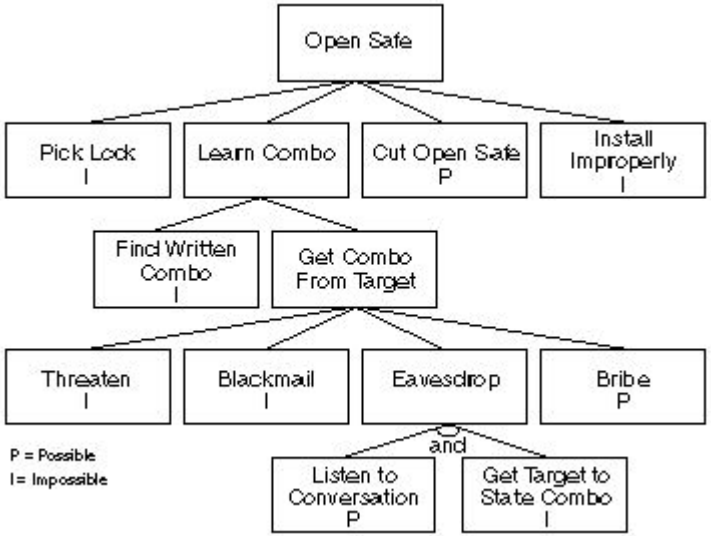
- How does one provide security systematically?

How Attacks Happen?

- Understanding helps design defenses that can disrupt, delay, deflect and defeat attacks
- Each step in attack is an opportunity for defense

Attack Trees/Graphs

- 1999: proposed by Schneier
- Formal methodology for analyzing security
  - Can apply defenses to each step in the tree
- Generalized to Attack Graphs
  - Can get very complex

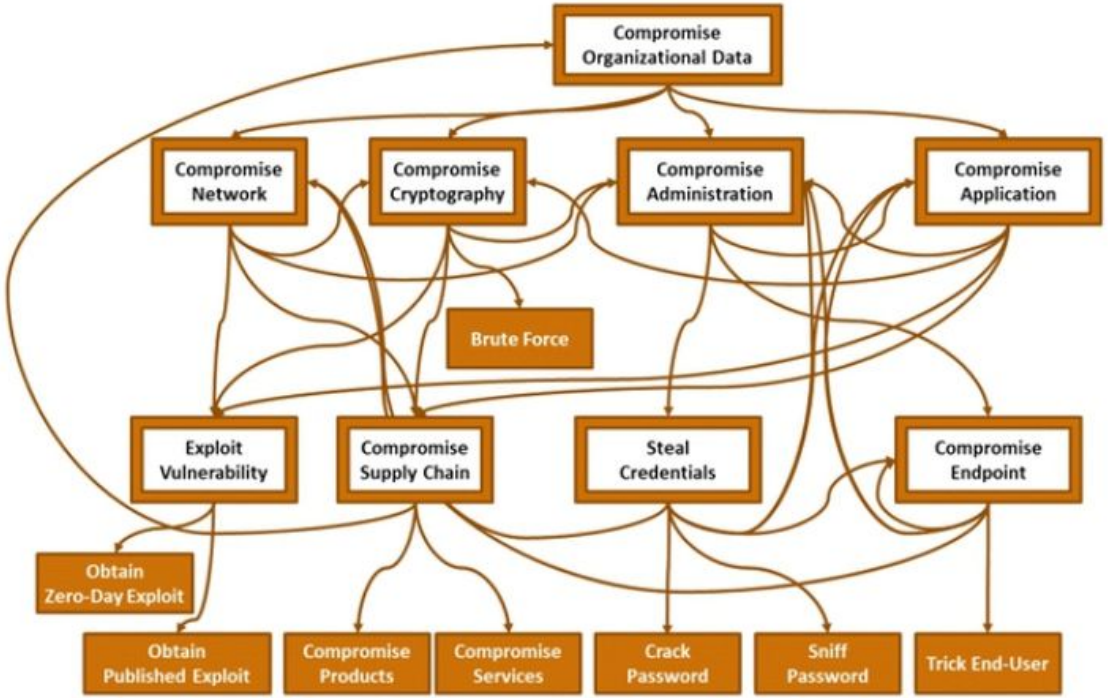


Attack Graph to Compromise Data

Components are interconnected and depend on, each other

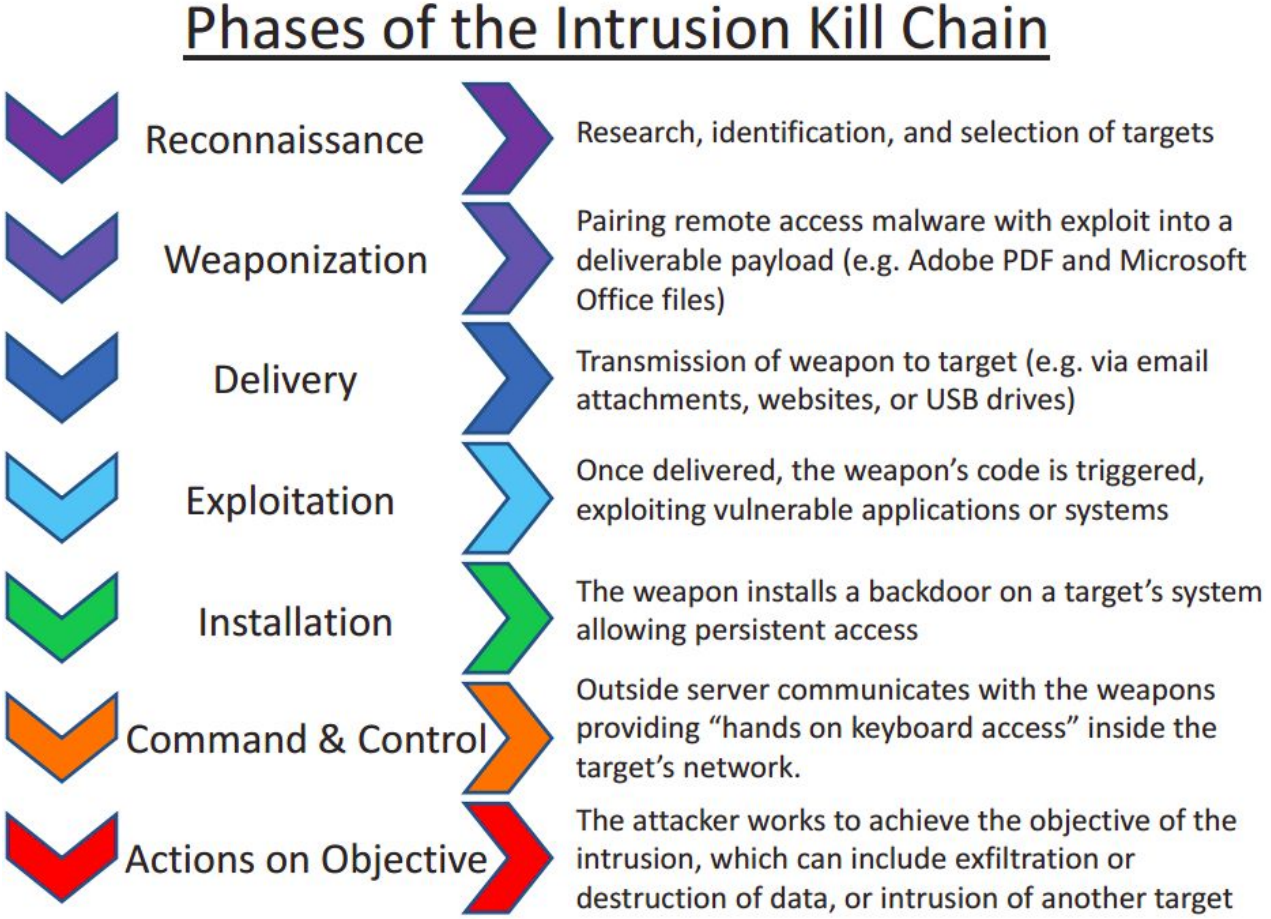
A breach anywhere can eventually be exploited to compromise the entire enterprise

A very complex scenario



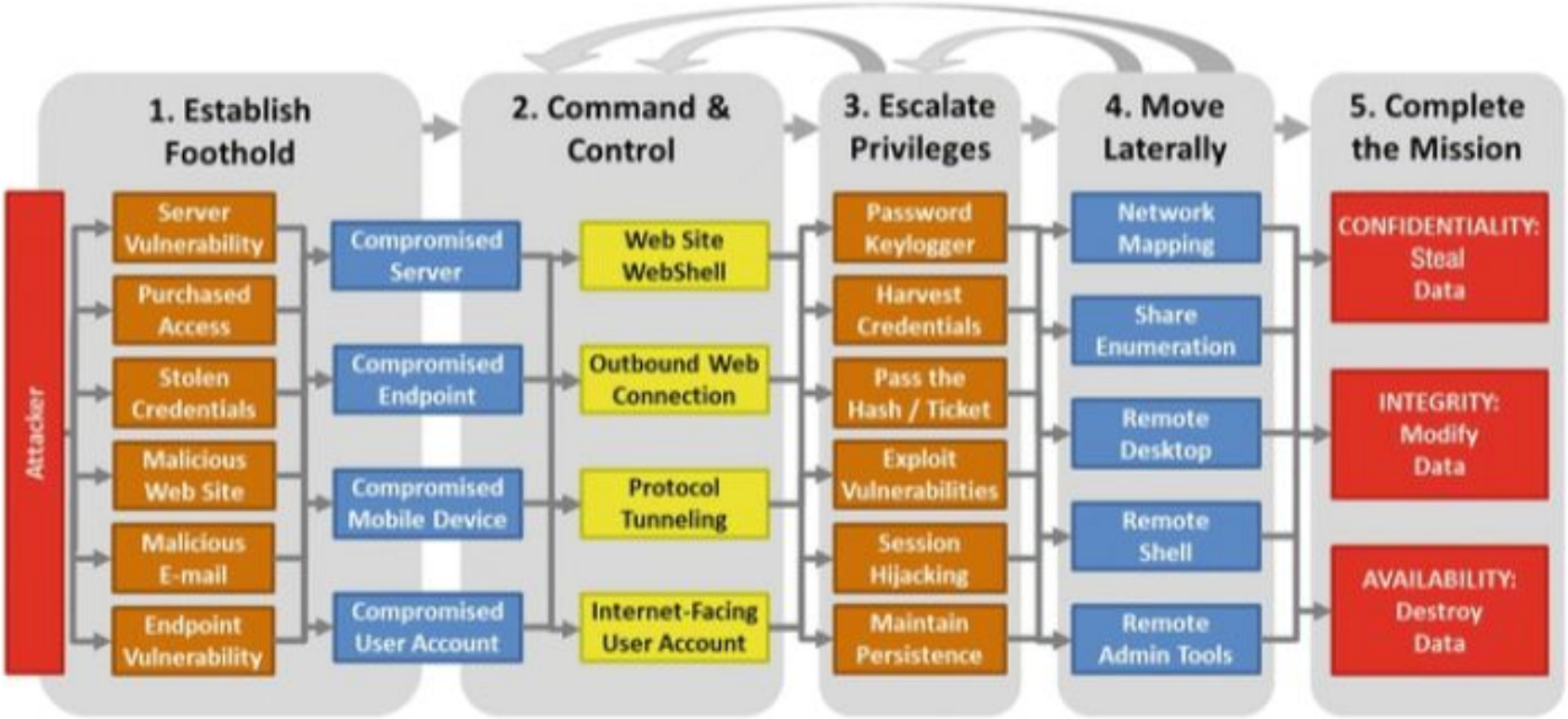
Kill Chains

- A simplified model of generalized attack trees/graphs
  - But powerful in terms of actionable results
- Few popular kill chains
  - Lockheed martin, Mandiant, Unified etc



Lockheed Martin Kill Chain

Simplified Kill Chain



Establish Foothold

- First step: gives attacker ability to access resources of an enterprise
  - Can be end-points, mobile devices, servers, or cloud-based systems

How achieved?

- Server vulnerability: often Internet-facing (e.g. web server, email server)
  - Frequently exploited due to a system misconfiguration, or an application vulnerability due to a programming flaw or a missing patch.
- Purchased Access: Attackers can purchase access to systems from botnet operators in black market
  - Can purchase access to servers, endpoints, mobile devices and user accounts

- Stolen Credentials: Attackers can obtain stolen credentials for user accounts with remote access or to cloud services
- Malicious web sites: can infect endpoints (or servers) that visit them
- Malicious e-mail: infects end-points
  - executable malware attachments, malicious document attachments, and links to malicious web sites
- Endpoint vulnerabilities: one compromised endpoint infects other endpoints
  - via vulnerabilities or compromised network credentials

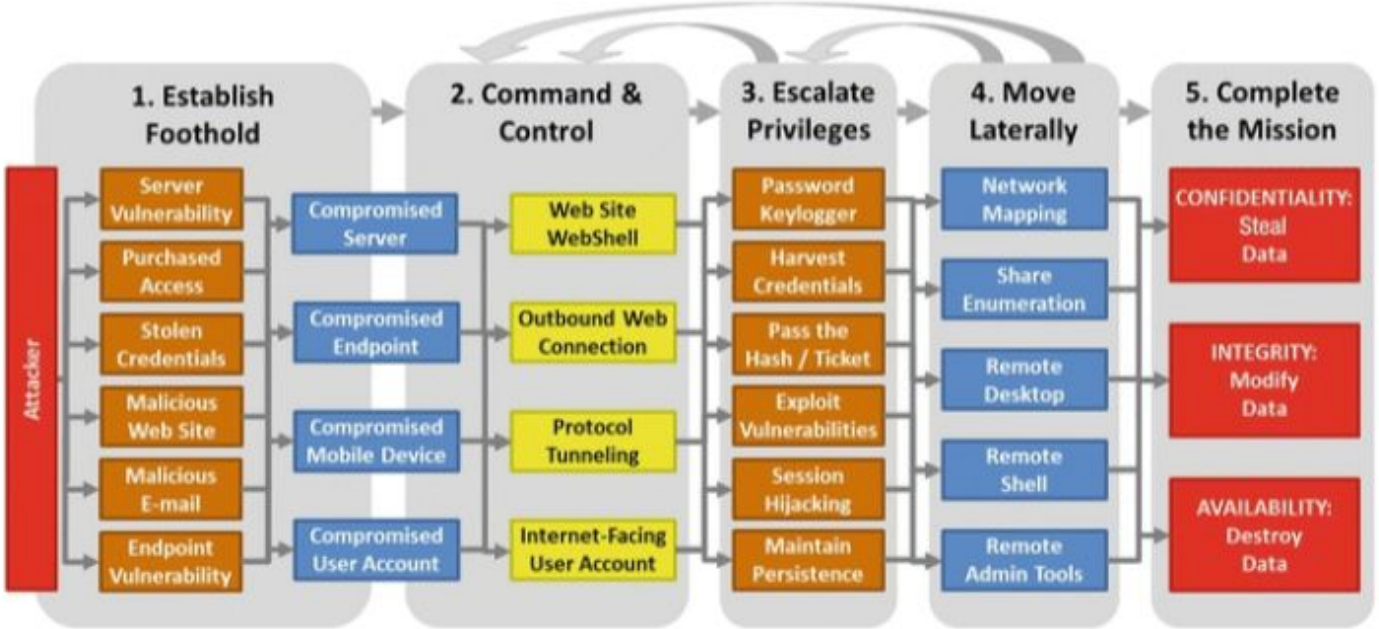
End Result:

- A compromised server : attacker has control of the server or its application software
- A compromised endpoint: attacker has control of an endpoint computer or device inside the victim network

- A compromised mobile device: can connect to the victim network or handles data from the victim enterprise.
- A compromised user account: permits accessing Internet-accessible resources, such as web mail, employee portals, or virtual private networking

From the foothold, attacker then moves on to the next attack sequence step—command and control

Simplified Kill Chain



2,3 and 4 may not happen in sequence

Command and Control (CC)

Second Step: Attacker uses CC to control the activities within the victim systems

How achieved?

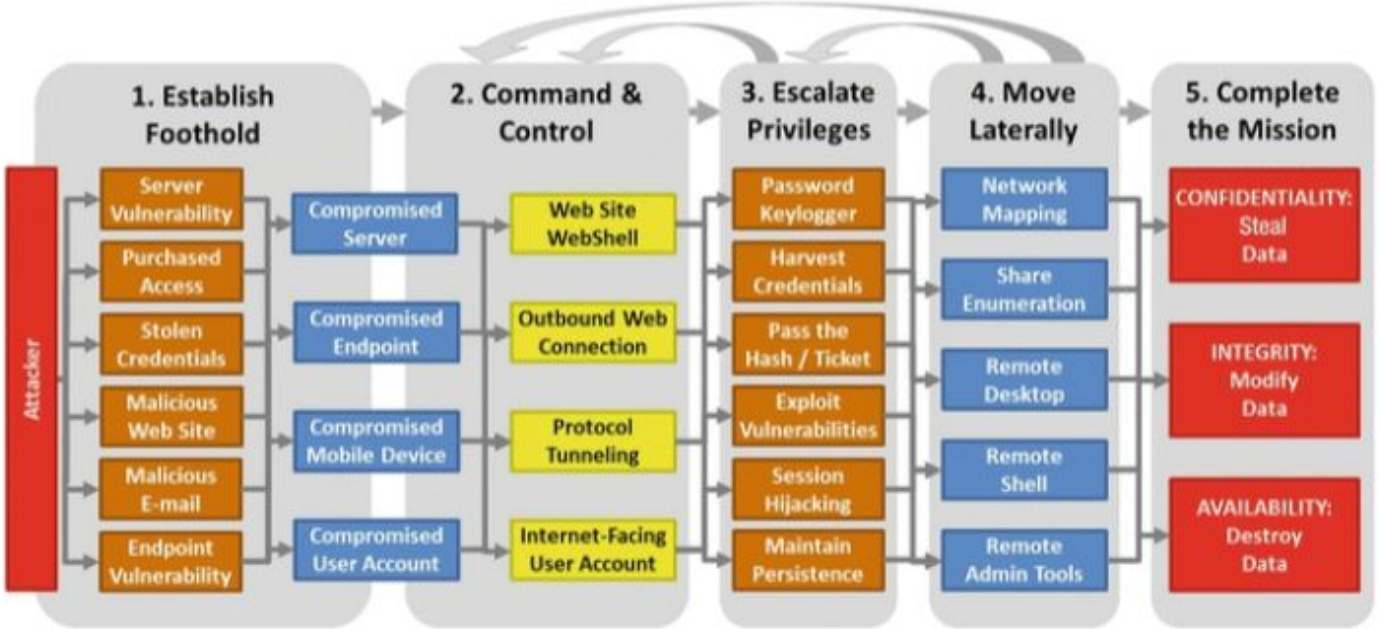
- Web site webshell: an attached web page allows attackers to execute commands
- Outbound web connections: enables malware on systems to contact CC servers
  - Request commands and report back results
  - Connections encrypted using SSL or TLS making it difficult to detect

- Protocol tunneling: encodes command and control traffic inside of other protocols
  - Protocols that are frequently allowed across firewalls
    - Domain Name Service (DNS), Internet Control Message Protocol (ICMP) and Simple Mail Transport Protocol (SMTP)
  - Uses extra fields or data payload space
- Internet-facing user accounts: accounts control web services that are Internet-facing
  - commonly used for command and control of cloud services

After CC,

- attacker can execute commands in the victim enterprise
- install and operate additional malware and tools

Simplified Kill Chain



2,3 and 4 may not happen in sequence

Escalate Privileges

- Need to take control of additional servers and endpoints closer to the attack goal
  - Involves gaining control of system administration accounts
    - These have permissions to log on to large numbers of machines

<u>How achieved?</u>

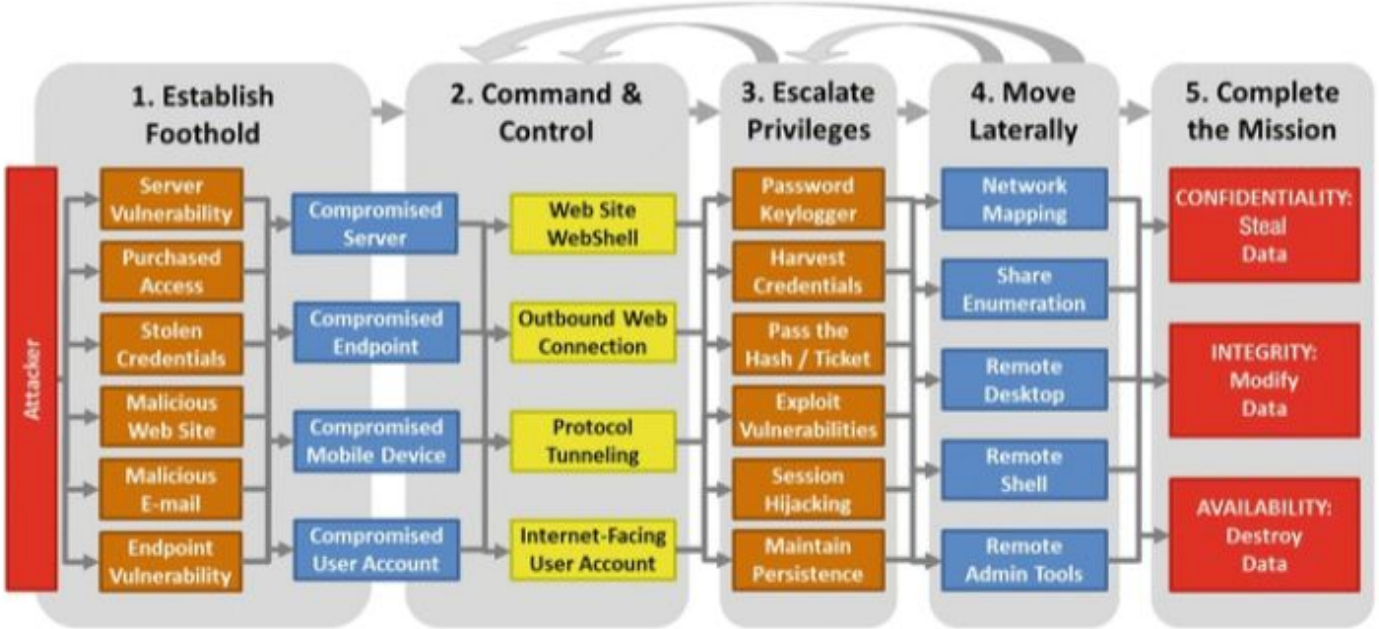
- Password keylogger: captures passwords of users and administrators when they log on from compromised machines (specifically servers)

- Harvest credentials: Can be harvested from applications, memory, and the hard drive
  - Modern operating systems provide for credential caching
    - Users do not have to type in their passwords every time
  - Username and an encoded hash of the password can be extracted by malware
  - e-mail servers can be modified to record the logon credentials of everyone who logs on to the server

- Pass the hash or ticket: can be used with some network protocols
  - even if the attacker does not have the original password
- Exploit vulnerabilities in the operating system or application software
  - Particularly dangerous because internal computers are seldom firewalled
  - Numbers of potentially vulnerable services that are exposed from one internal computer to another are significantly greater

- Session hijacking: take advantage of legitimate administrative sessions
  - Can defeat multi-step and multi-factor authentication (which are resistant to credential theft or password cracking)
- Maintain persistence: migrate malware from the running session and embed it into the OS, hard drive, or device firmware
  - malware will be re-launched every time the computer restarts

Simplified Kill Chain



2,3 and 4 may not happen in sequence

Move Laterally

- Fourth Step: attacker moves from computer to computer increasing footprint
  - Often via system administration tools
  - Few safeguards to protect against this abuse

How achieved?

- Network mapping: gain intelligence on the victim network
  - identifying subnets, computers, servers, exploitable vulnerabilities, and other aspects of the victim enterprise

- Share enumeration: identify major network shares containing data repositories
  - Helps understand use of file shares, file transfer protocol servers, and other collaboration tools
  - Can escalate privileges to get administrative control of the shares and all of the data contained in them

- Remote desktop: Helps obtain an administrator desktop interface on target systems
  - Using systems administration credentials
  - most robust method of lateral movement
  - a full graphical user interface to work and a robust and easy-to-use environment
- Remote shell: Helps obtain a text-based command prompt using administrator credentials
  - Generally runs using different ports and protocols from remote desktop
  - It may be permitted when remote desktop is not (or vice versa)
  - Command shells allow execution of arbitrary commands up to the permissions of the account used to connect.

- Remote administration: built into most modern operating systems; allow executing a reduced set of commands compared to remote shell
  - Can help reconfigure servers and endpoints and install malware and toolkits
  - Help inject software into the computer memory and run it
    - can install malware that may not be detectable by traditional anti-virus or other endpoint detection technologies

Summary so far

- Attacker generally goes through several cycles of privilege escalation and lateral movement
  - Starting from a regular user computer, the attacker may obtain endpoint administrator privileges
  - Then use those privileges to get to a file server
  - From the file server, the attacker obtains the privileges of an e-mail administrator and jumps to an e-mail server
  - From the e-mail server, the attacker might obtain domain administrator privileges and then jump into the enterprise's domain controller server
  - Can get complete control of the enterprise and all of its endpoints and servers

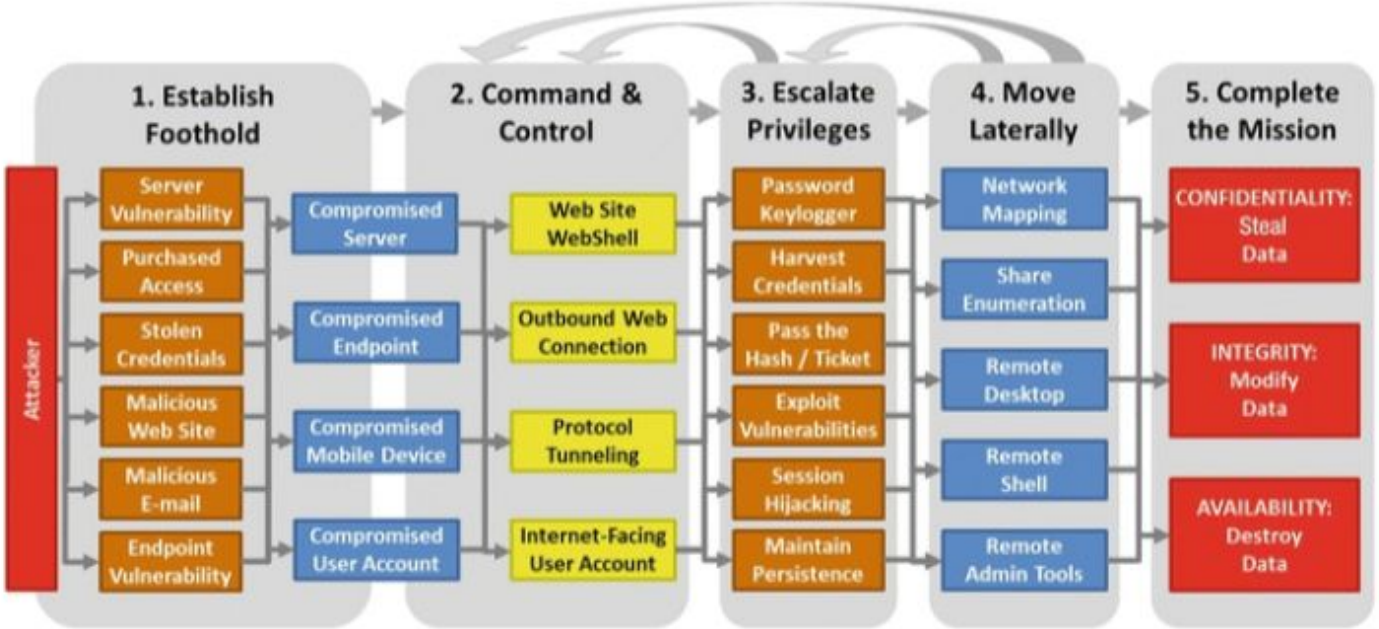
Complete the Mission

Mission generally falls into three categories:

- Confidentiality: steal data
  - steal login credentials, credit card numbers or financial accounts, or healthcare information for identity theft
- Integrity: modify data on the victim network
  - Less common than confidentiality
  - Steal money by either altering financial records or using compromised credentials to move money out of victim accounts

- Availability: destroy data or make systems unavailable
  - Disgruntled employees or other insider attackers frequently use this attack method
  - Can also be used for blackmail
    - Use ransomware that encrypts victim's data and then charges the victim for the decryption keys
  - Some distributed denial-of-service attacks do not require successfully penetrating an enterprise
  - An attacker may also use availability attacks as a distraction

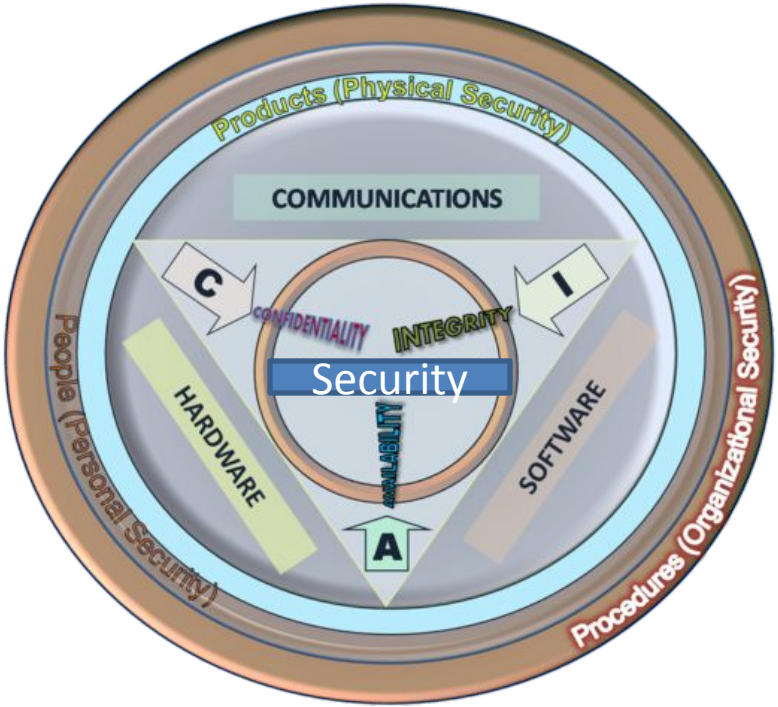
Simplified Kill Chain



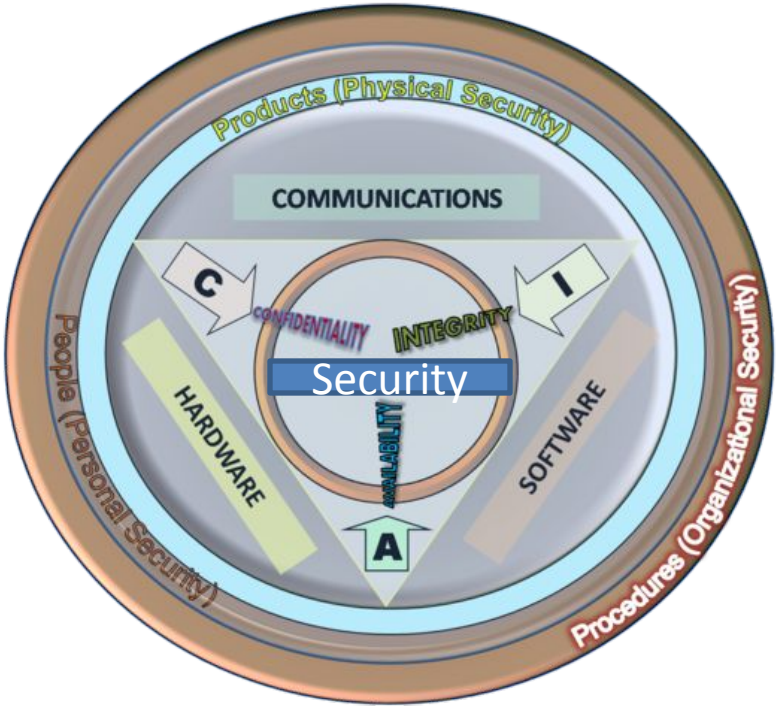
2,3 and 4 may not happen in sequence

Security Building Blocks: CIA Triad

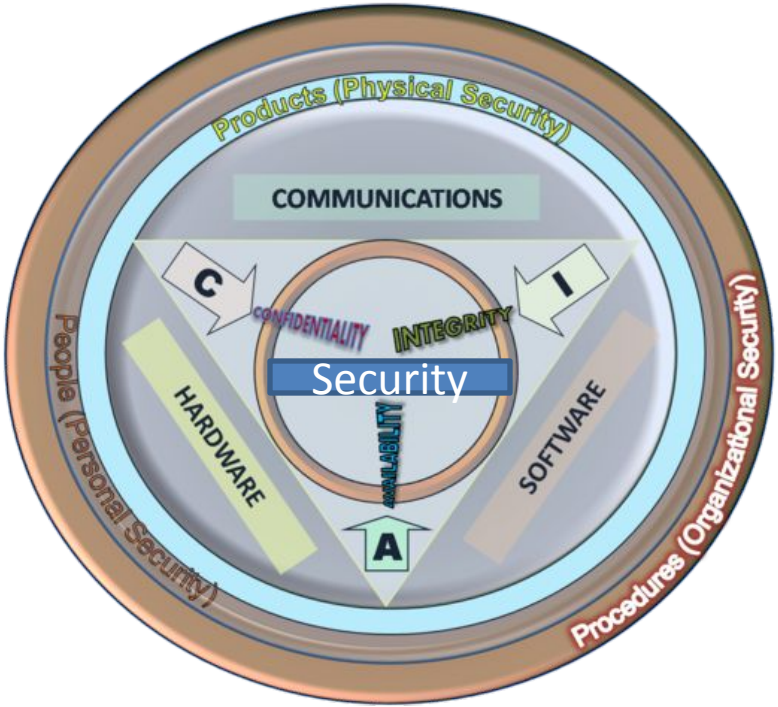
- **Confidentiality:** information/resource is not made available or disclosed to unauthorized individuals, entities, or processes
- Example: Online shopping
  - Credit card info not available to third parties



- **Integrity:**
  - Information/programs not improperly modified
  - System performs intended function
- Example: Online Purchase
  - Change price of item from Rs 5000 to Rs 1

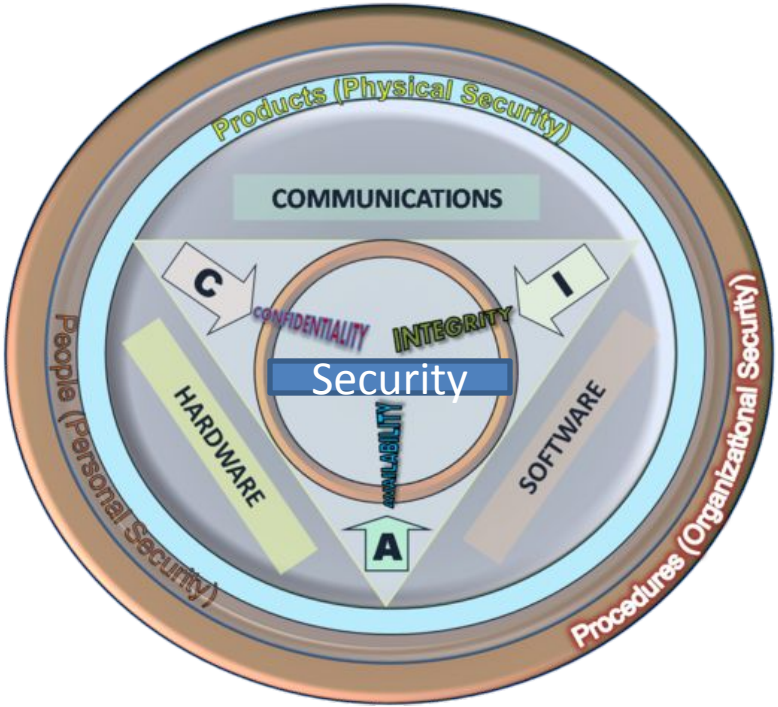


- **Availability**
  - Information/resource accessible to authorized users
- Example: Online Purchase
  - Bring the web server down; deny service to other shoppers



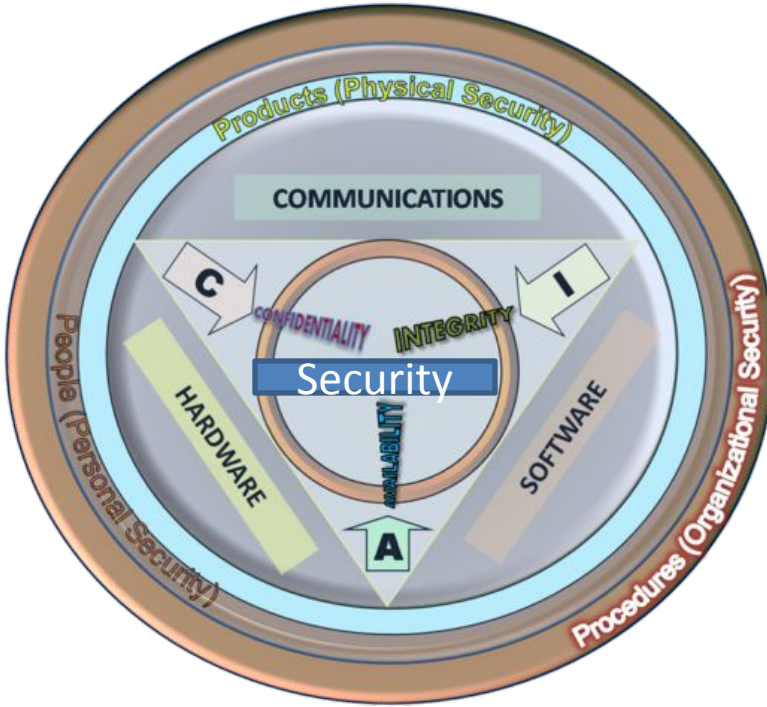
Entities

- CIA has to be realized over below entities
- Hardware (Computer, hard drive)
- Software (Operating System, Web browsers etc)
- Communications/network (LAN, WAN, Cellular)



Further Layers

- Procedures within Organization
  - E.g.: Compromise of root privilege in employee computer, report within 8 hrs
- People:
  - E.g. Background checks, user training
- Products
  - E.g. Biometric lock to a room, CC cameras



Effective Security Program in Enterprise

Risk Management

- Bullet proof protection impossible
- Conflicting goals
  - E.g: Disconnect machine from Internet: increases confidentiality but availability suffers
  - E.g: Extensive data check by different entities: Improves integrity but confidentiality suffers
  - E.g. Anonymity vs Accountability
- Focus: Lower risk
  - Cost of protection < value of resource

Risk Management

Steps

- Calculate value of asset to the organization
- Identify vulnerabilities/threats to the asset
- Decide on countermeasures: cost of protection vs value of asset (proportional response)
- Evaluate the effectiveness of the countermeasures (periodic review)

Summary

- Understood terminology: Assets, threats, attacks, vulnerabilities, controls etc
- Looked at how attacks happen (kill chains)
- Enterprise security more complex
  - Technology is just one part, others: processes, people, budget, compliance etc play a role too
- Security is all about risk management!