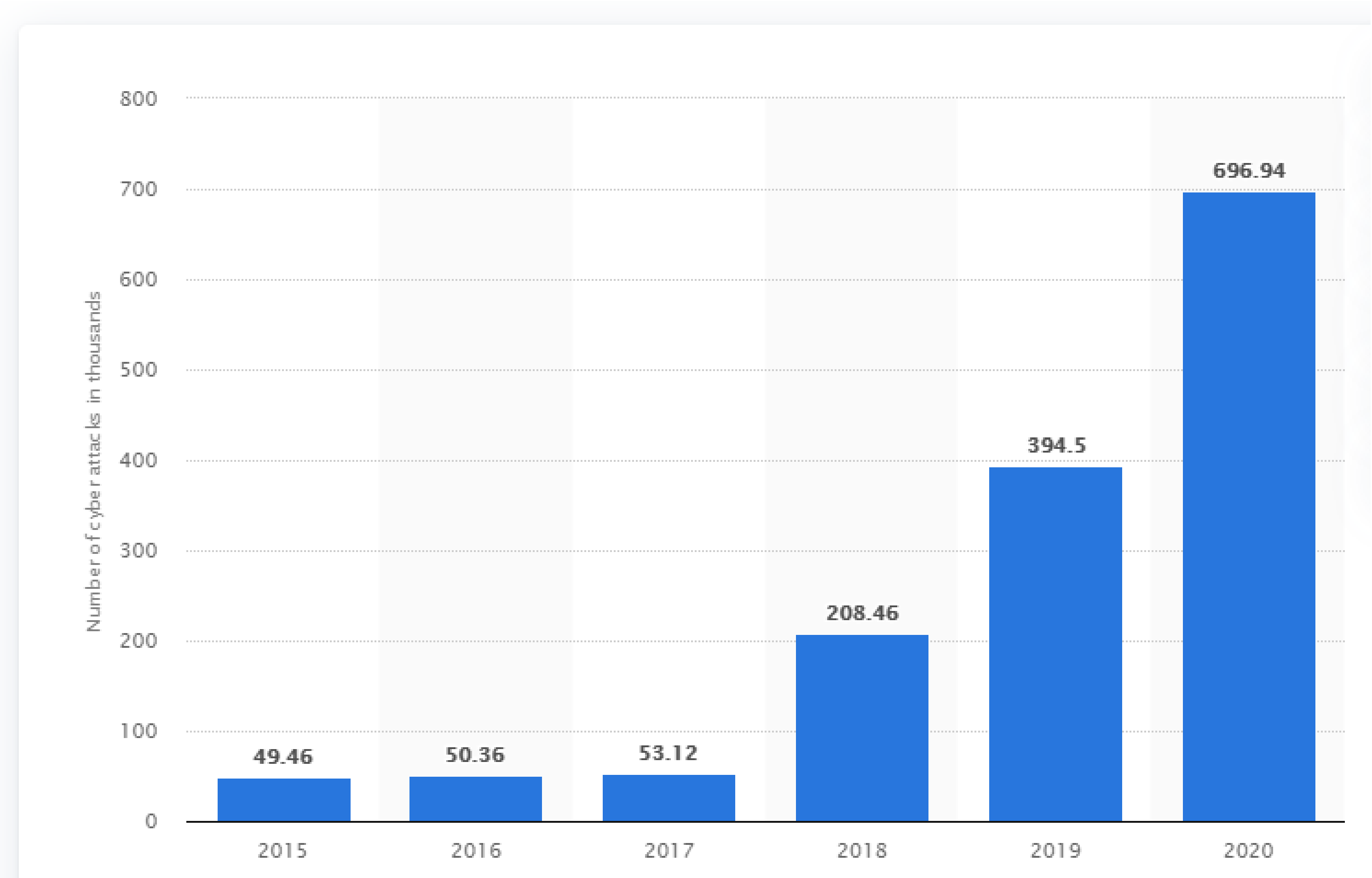
Introduction to Cyber Security

Dr. Amit Praseed


Number of cyber attacks in thousands
800
700
600
500
400
300
200
100
0
49.46
50.36
53.12
208.46
394.5
696.94
2015
2016
2017
2018
2019
2020

The Sarah Palin E-Mail Hack

- Sarah Palin was the US Vice Presidential candidate in 2008
- During her campaign, some of her emails were leaked online leading to speculation that her email was hacked
- The hacker was apprehended and revealed he had used Yahoo's security questions to gain unauthorised access to the account
- The security questions like birthdate, ZIP code etc were easily obtained from Wikipedia and Google searches

The Mat Honan Account Hack

- Mat Honan was a writer and editor for Wired and later moved to Buzzfeed
- In 2012, in a matter of hours, Mat's Google, Apple and Twitter accounts were compromised in quick succession
- Step 1 - Get the gmail address (mhonan@gmail.com) - easy, it is listed on his personal website
- Step 2 - Gmail account recovery. Mat had given a recovery email for Gmail account which was m****n@me.com. Any guesses what the email ID was?
  - It was mhonan@me.com (Apple ID)

The Mat Honan Account Hack

- Step 3: Get access to Apple account. Apple tech support would allow access to the account if a user provides the email address, billing address and last 4 digits of their credit card.
  - Email address --- already obtained
  - Billing address --- simple whois search or google search will give you this information
  - Credit card part is a bit tricky!!!
- Step 4: Contact Amazon customer service. You can add a new credit card number by simply providing name on the account, an associated e-mail address, and the billing address.
- Step 5: Amazon Customer Service part II: By providing a name, billing address, and the new credit card number you gave the company on the prior call, Amazon will allow you to add a new e-mail address to the account.

The Mat Honan Account Hack

- Step 6: Login to Amazon using the new email address. You can see the credit card details entered - the last 4 digits!!!
- Step 7: Use this credit card information to gain access to Apple account
- Step 8: Use the Apple account to gain access to Gmail account
- Once you do this, you can basically access any account linked to Gmail, such as Twitter, Facebook etc.

Point to note: The information (last 4 digits of the credit card) that Amazon considers unimportant is the information Apple considers crucial to give account access

What is Security?

- Simple Definition: Achieving some **objective(s)** in the presence of an **adversary**
- Computers are designed to work co-operatively
  - Browsers communicate with web (or cloud) servers
  - Devices communicate with each other (P2P)
  - Even isolated devices are rarely “isolated”
    - You plug in your flash drive in multiple systems!
- You are potentially communicating with unknown entities
  - People or systems you don’t know and don’t trust
  - You have no idea how your information is being routed
  - Any of these people or systems could be an adversary

Objectives of Cyber Security

- Confidentiality
  - Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals
  - Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- Integrity
  - Data integrity: Assures that information and programs are changed only in a specified and authorized manner
  - System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- Availability
  - Assures that systems work promptly and service is not denied to authorized users.

CONFIDENTIALITY

- Confidentiality is the concealment of information or resources
- Example: Enciphering an income tax return will prevent anyone from reading it. If the owner needs to see the return, it must be deciphered by entering a particular key
- Confidentiality also applies to the existence of data, which is sometimes more revealing than the data itself
- Resource hiding is another important aspect of confidentiality
  - Sites often wish to conceal their configuration as well as what systems they are using; organizations may not wish others to know about specific equipment

Confidentiality

- Situation 1: Student grades within an Institute
  - Only accessed by the student and the employees who need that information to work (faculty handling the course, office staff etc.)
  - HIGH CONFIDENTIALITY
- Situation 2: Student Enrollment Information
  - When the student joined, which courses he/she is taking etc.
  - Still confidential, but available to more people (all faculty, all office staff etc.)
  - MODERATE CONFIDENTIALITY
- Situation 3: Student / Faculty List at an Institute
  - Commonly available in public domain
  - Less likely to be of any issue if disclosed
  - LOW CONFIDENTIALITY

INTEGRITY

- Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change
  - data integrity: the content of the information
  - origin integrity: the source of the data (often called authentication)
- Example: A newspaper may print information obtained from a leak at the White House but attribute it to the wrong source. The information is printed as received (preserving data integrity), but its source is incorrect (corrupting origin integrity).

Integrity

- Situation 1: Patient Allergy Information
  - Doctors need to be sure the information is correct
  - If, knowingly or unknowingly, the information gets modified, it must be possible to identify the error and/or rectify it as soon as possible
  - Incorrect information could result in severe consequences
  - HIGH INTEGRITY
- Situation 2: Online forum discussing GoT fan theories
  - If the information is overwhelmingly incorrect, the website owner will lose traffic
  - MEDIUM INTEGRITY
- Situation 3: Anonymous Online polls
  - Everyone knows the polls are not trustworthy
  - LOW INTEGRITY

AVAILABILITY

- Availability refers to the ability to use the information or resource desired
- Someone may deliberately arrange to deny access to data or to a service by making it unavailable (Denial of Service Attacks)
- Very difficult to detect, because the analyst must determine if the unusual access patterns are attributable to deliberate manipulation of resources or of environment

AVAILABILITY

- Situation 1: Bank websites, authentication services
  - Financial transactions might be interrupted, heavy loss of revenue
  - HIGH AVAILABILITY
- Situation 2: University websites
  - a site is not a critical component of the university's information system, but its unavailability might cause loss of reputation
  - MEDIUM AVAILABILITY
- Situation 3: Online telephone directory
  - Offline options available
  - LOW AVAILABILITY

Threats and Attacks

- A threat is a potential violation of security. The violation need not actually occur for there to be a threat.
- The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for). Those actions are called attacks. Those who execute such actions, or cause them to be executed, are called attackers.

Classes of Threats

- Disclosure: unauthorized access to information
- Deception: acceptance of false data
- Disruption: interruption or prevention of correct operation
- Usurpation: unauthorized control of some part of a system

THREATS AND ATTACKS

Threat	Attack Scenarios
Disclosure	Exposure: Sensitive data released to an unauthorized entity. Interception: An unauthorized entity accesses sensitive data in transit Inference: An unauthorized entity indirectly accesses sensitive data by reasoning Intrusion: An unauthorized entity gains access to sensitive data by circumventing a system’s security protections.
Deception	Masquerade: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. Falsification: False data deceive an authorized entity. Repudiation: An entity deceives another by falsely denying responsibility for an act.

Threats and Attacks

Threat	**Attack Scenarios**
Disruption	Incapacitation: Prevents or interrupts system operation by disabling a system component. Corruption: Undesirably alters system operation by adversely modifying system functions or data. Obstruction: A threat action that interrupts delivery of system services by hindering system operation.
Usurpation	Misappropriation: An entity assumes unauthorized logical or physical control of a system resource Misuse: Causes a system component to perform a function or service that is detrimental to system security

Threats and Assets

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made	A working program is modified to cause it to fail during execution or do some unintended task
Data	Files are deleted, denying access to users	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Policy and Mechanism

- A security policy is a statement of what is, and what is not, allowed
- A security mechanism is a method, tool, or procedure for enforcing a security policy
- Policies may be presented mathematically, as a list of allowed (secure) and disallowed (nonsecure) states
- Eg: A website requires users to login to the system (policy). Users can login using a user name and password pair (mechanism). They can also login using their Gmail or Facebook accounts (another mechanism).

Goals of Security

- Prevention means that an attack will fail. For example, if one attempts to break into a host over the Internet and that host is not connected to the Internet, the attack has been prevented
- Prevention means that an attack will fail. For example, if one attempts to break into a host over the Internet and that host is not connected to the Internet, the attack has been prevented
- Recovery has two forms
  - Stop an attack and to assess and repair any damage caused by that attack. Eg: if the attacker deletes a file, one recovery mechanism would be to restore the file from backup tapes
  - System continues to function correctly while an attack is under way. This type of recovery is quite difficult to implement because of the complexity of computer systems.

Assumptions and Trust

- Opening a door lock requires a key. The assumption is that the lock is secure against lock picking. This assumption is treated as an axiom and is made because most people would require a key to open a door lock. A good lock picker, however, can open a lock without a key. Hence, in an environment with a skilled, untrustworthy lock picker, the assumption is wrong and the consequence invalid.

Saltzer and Schroeder's Security Principles

- Economy of Mechanism
  - Keep all security systems simple
  - Simple is not the same as small
  - Simple systems are easier to understand, debug and maintain
  - Typically less prone to errors
- Fail Safe Defaults
  - Your default security mechanism should be “deny”
  - Provide access to only those people and resources that are required
  - False Negatives are better than False Positives
  - Black listing vs white listing

Saltzer and Schroeder's Security Principles

- Complete Mediation
  - Check EVERY access to EVERY object
  - Sensitive web applications might require you to sign in every 15 minutes
  - If a program requests access to a file, the permissions must be checked every time the file the accessed, not only the first time
- Open Design
  - Diametrically opposite to “Security by Obscurity”
  - Publish all your security mechanisms/algorithm
  - Public scrutiny, early identification of defects and vulnerabilities
  - Open Source Software – fewer security issues
  - All cryptographic algorithms are in the public domain – only the keys remain secret

Saltzer and Schroeder's Security Principles

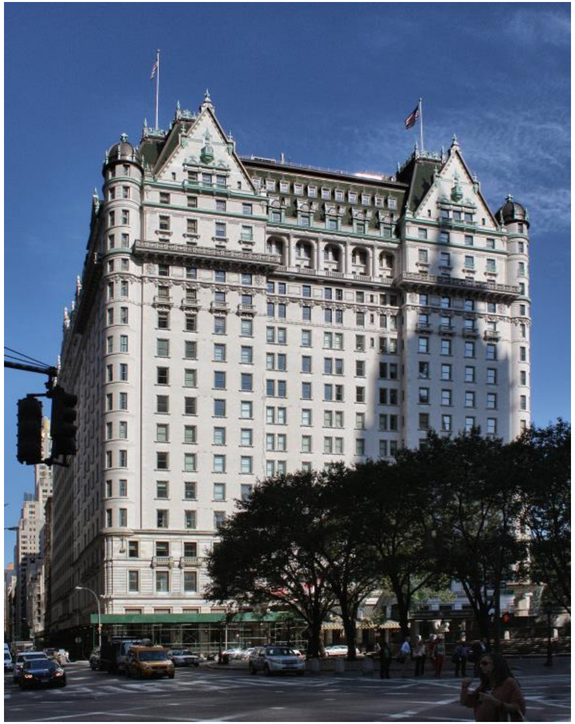
- Separation of Privilege
  - Check multiple conditions before giving access
  - Banking websites check password and OTP
  - One check might fail, but it is highly unlikely that multiple checks would fail
  - Multiple software modules, each requiring separate access is much secure than a monolithic system with a single access check
- Least Privilege
  - Figure out which capabilities are required – grant ONLY those
  - Design principle behind sandboxes
  - Unix concept of root only partially accomplishes this
    - Some programs might need to run as root to perform some action, like binding to a privileged port
    - This leaves them susceptible to buffer overflow exploits

Saltzer and Schroeder's Security Principles

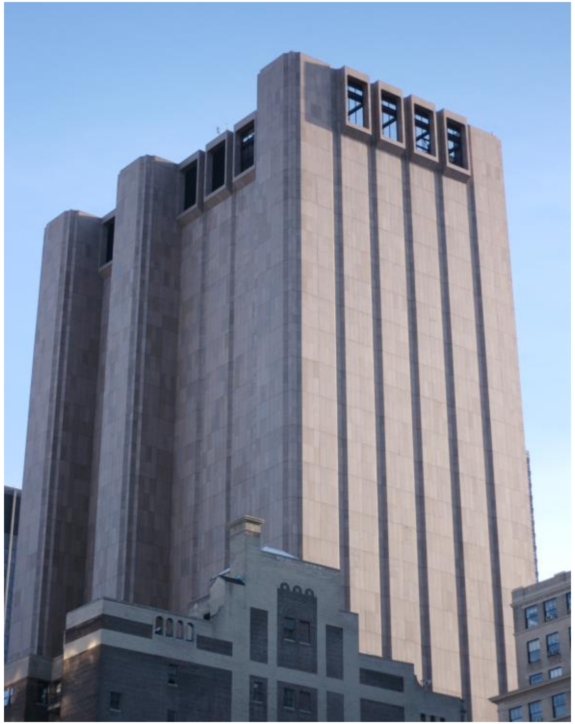
- Least Common Mechanism
  - Mechanisms used to access resources should not be shared
  - Sharing resources provides a channel of communication
- Psychological Acceptability
  - Security mechanisms should be designed for ease of use
  - Eg: Passwords can be guessed for 25 – 80% users. But passwords still continue to be used extensively because they are easy to use
- Work Factor
  - The cost of circumventing a security mechanism must depend on the data being protected
  - Eg: You need less secure mechanisms for protecting student grades than military secrets
- Compromise Recording
  - Sometimes it is more desirable to record the details of an intrusion than to prevent it

Attack Surfaces

Which of the two buildings are more easy to break into?



The Plaza Hotel



The AT&T Long Lines Building
(“Building with No Windows”)

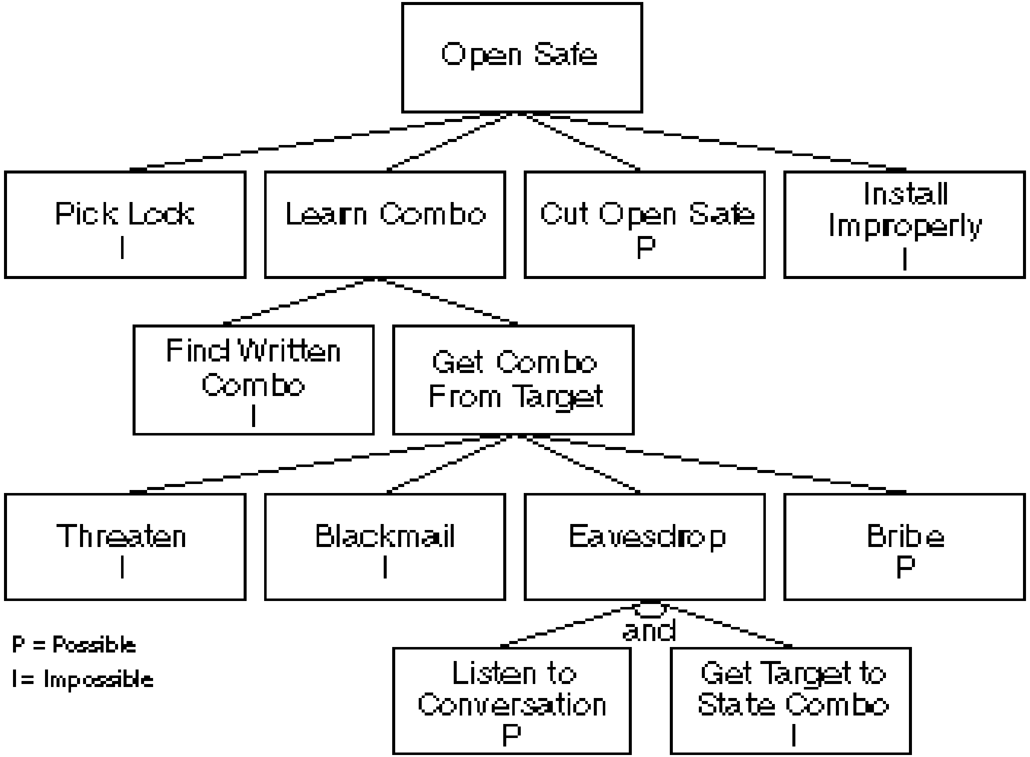
Attack Surfaces

- Attack surface is the total number of points or vectors through which an attacker could try to enter an environment
- In cybersecurity, the concept applies to ways an attacker could send data to and/or extract data from a network/software/system
- Attack surfaces could be physical attack surfaces (such as hard disks, USB drives etc.) or digital attack surfaces (Eg: applications, code, ports, servers, and websites)

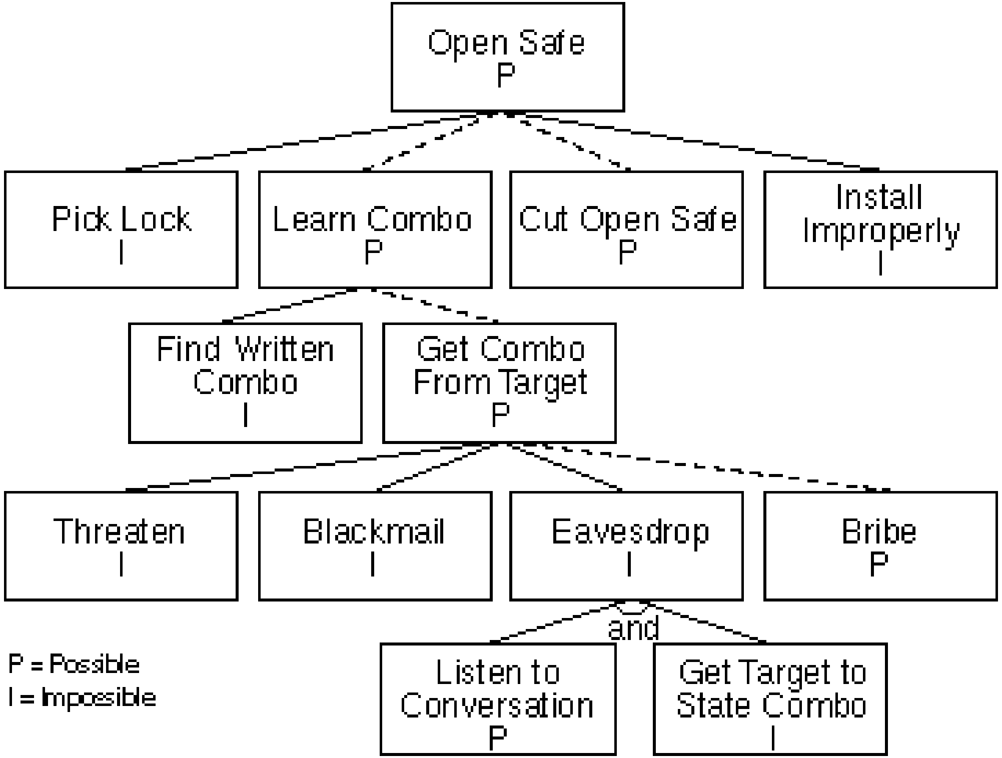
Reducing your Attack Surface

- Less code, less software attack surface
- Remove unnecessary OS software and services
- Scan your network ports
- Create a subdomain map
- Analyze your SSL certificates
- Segment your network
- Audit your software, network and traffic
- Train all your employees to avoid getting tricked

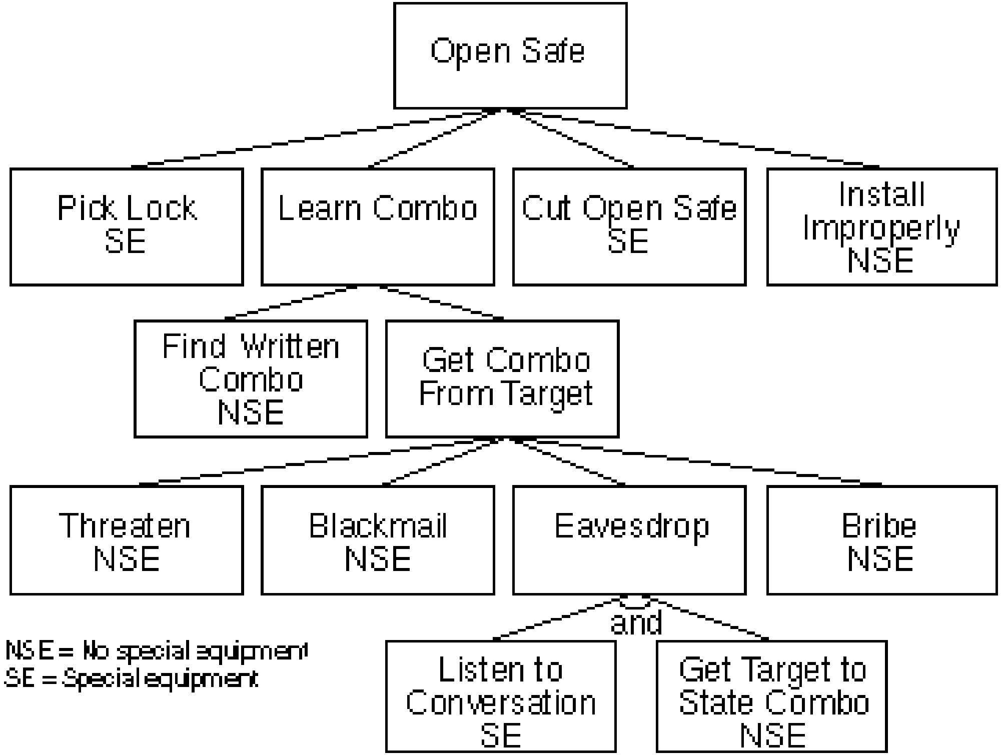
Attack Trees



ATTACK TREES



ATTACK TREES



Open Safe

Pick Lock SE

Learn Combo

Cut Open Safe SE

Install Improperly NSE

Find Written Combo NSE

Get Combo From Target

Threaten NSE

Blackmail NSE

Eavesdrop

Bribe NSE

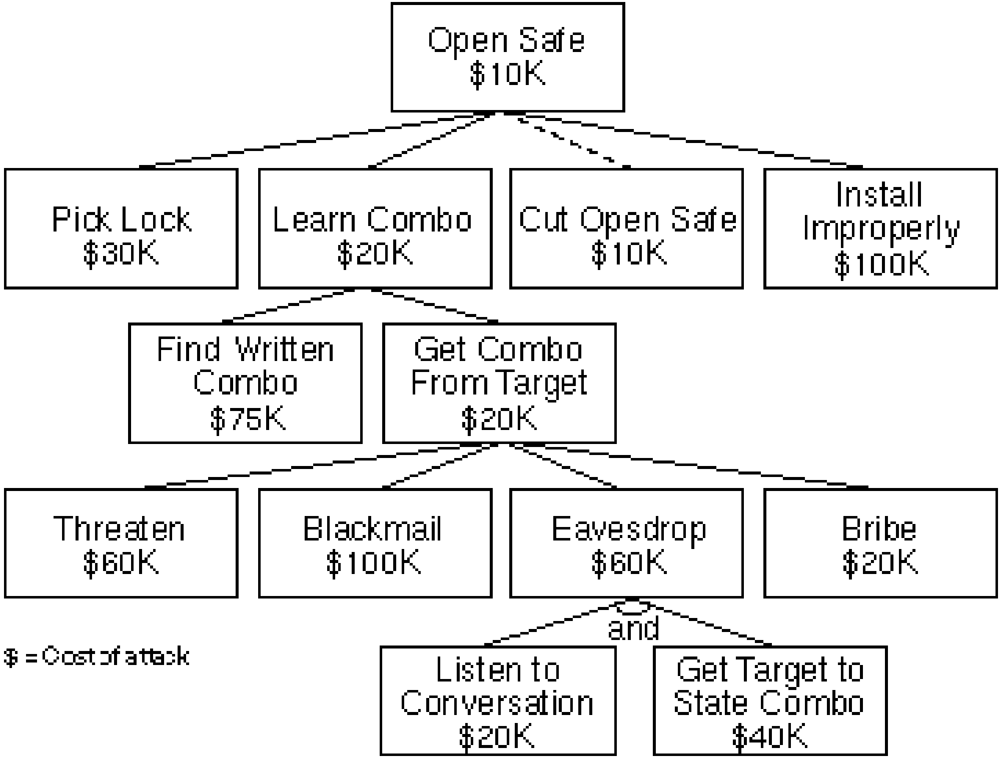
and

Listen to Conversation SE

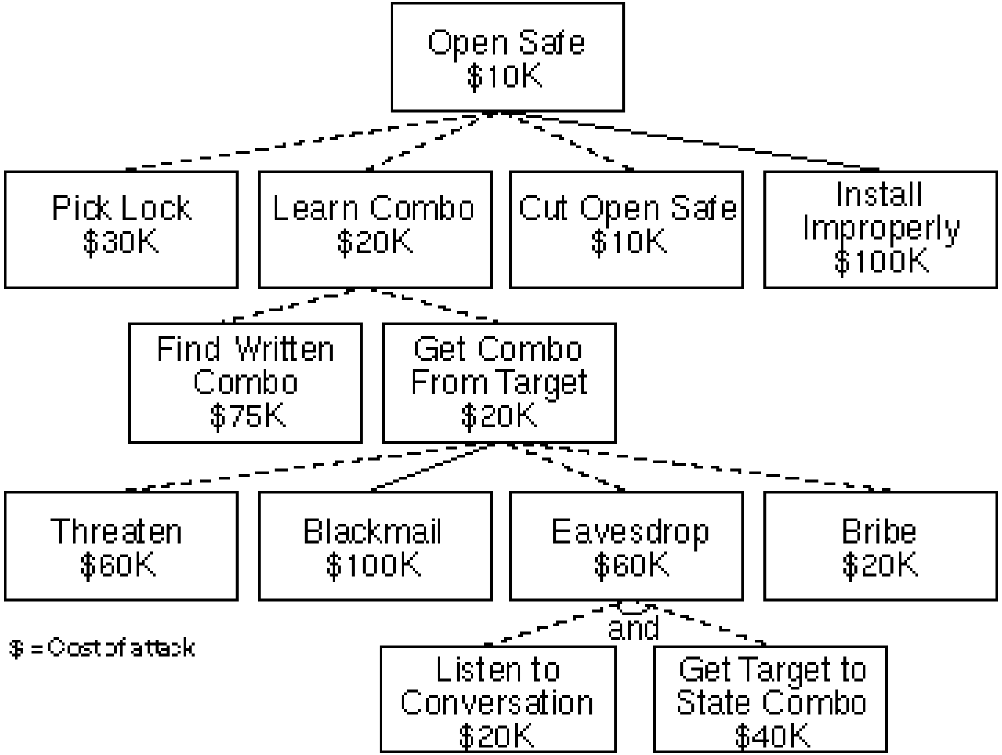
Get Target to State Combo NSE

NSE = No special equipment
SE = Special equipment

Attack Trees



Attack Trees



Open Safe
$10K

Pick Lock
$30K

Learn Combo
$20K

Cut Open Safe
$10K

Install Improperly
$100K

Find Written Combo
$75K

Get Combo From Target
$20K

Threaten
$60K

Blackmail
$100K

Eavesdrop
$60K

Bribe
$20K

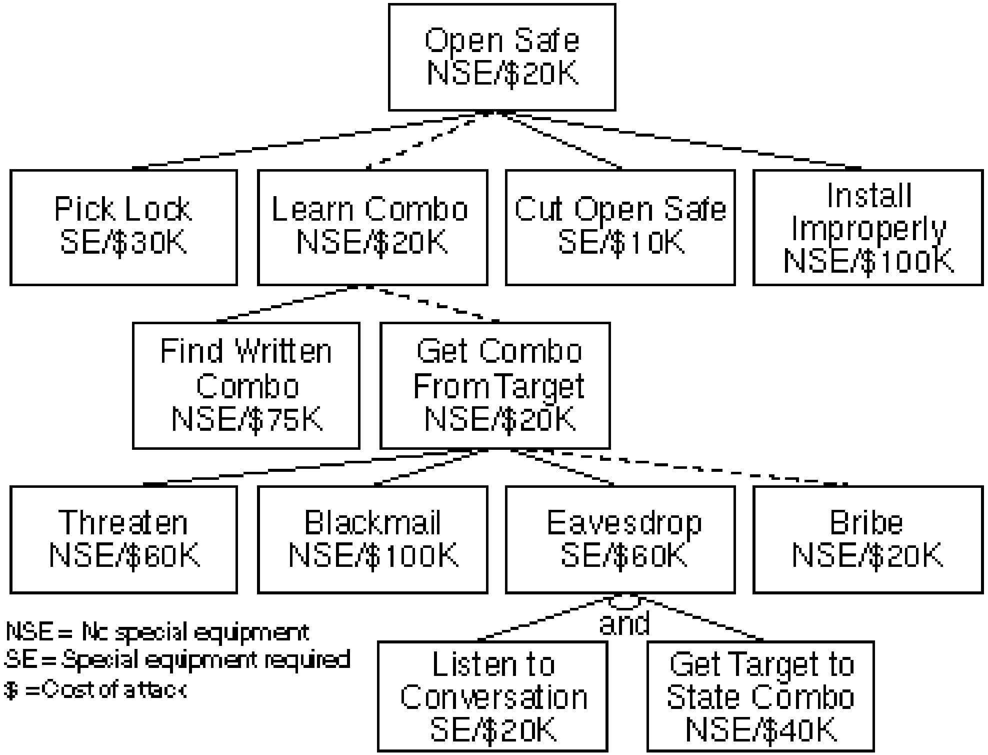
and

Listen to Conversation
$20K

Get Target to State Combo
$40K

$ = Cost of attack

Attack Trees



Open Safe
NSE/$20K

Pick Lock
SE/$30K

Learn Combo
NSE/$20K

Cut Open Safe
SE/$10K

Install Improperly
NSE/$100K

Find Written Combo
NSE/$75K

Get Combo From Target
NSE/$20K

Threaten
NSE/$60K

Blackmail
NSE/$100K

Eavesdrop
SE/$60K

Bribe
NSE/$20K

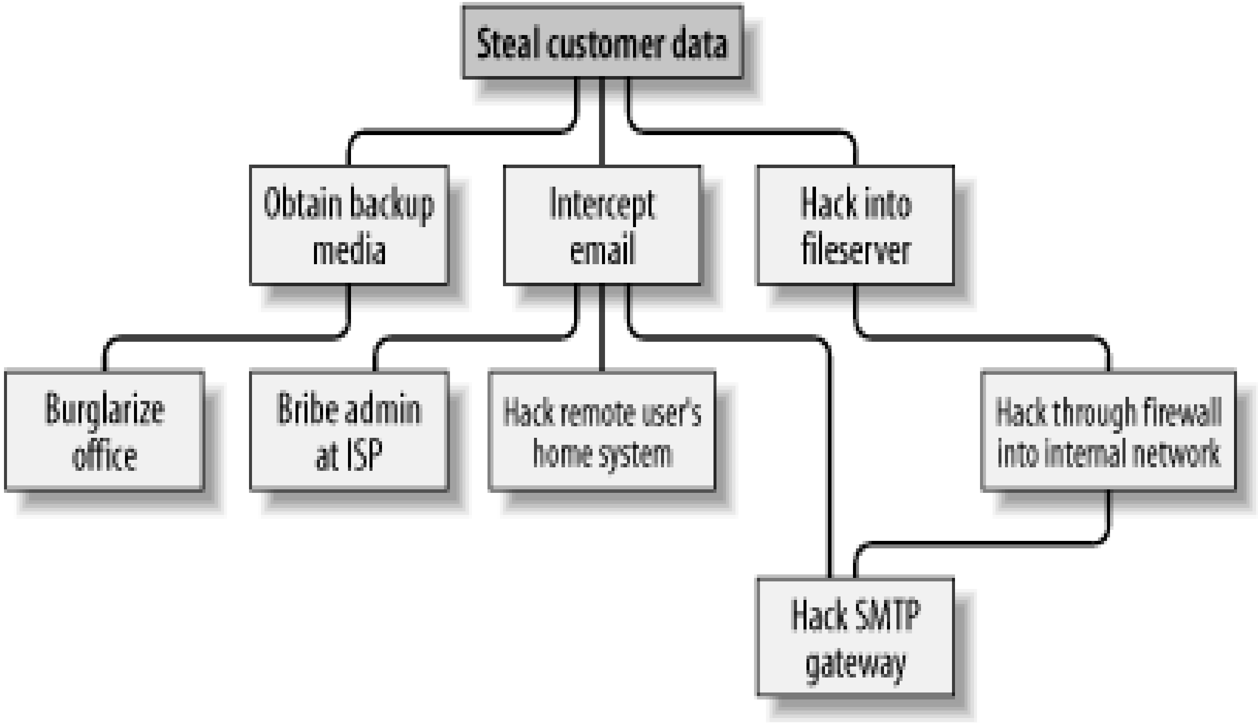
and

Listen to Conversation
SE/$20K

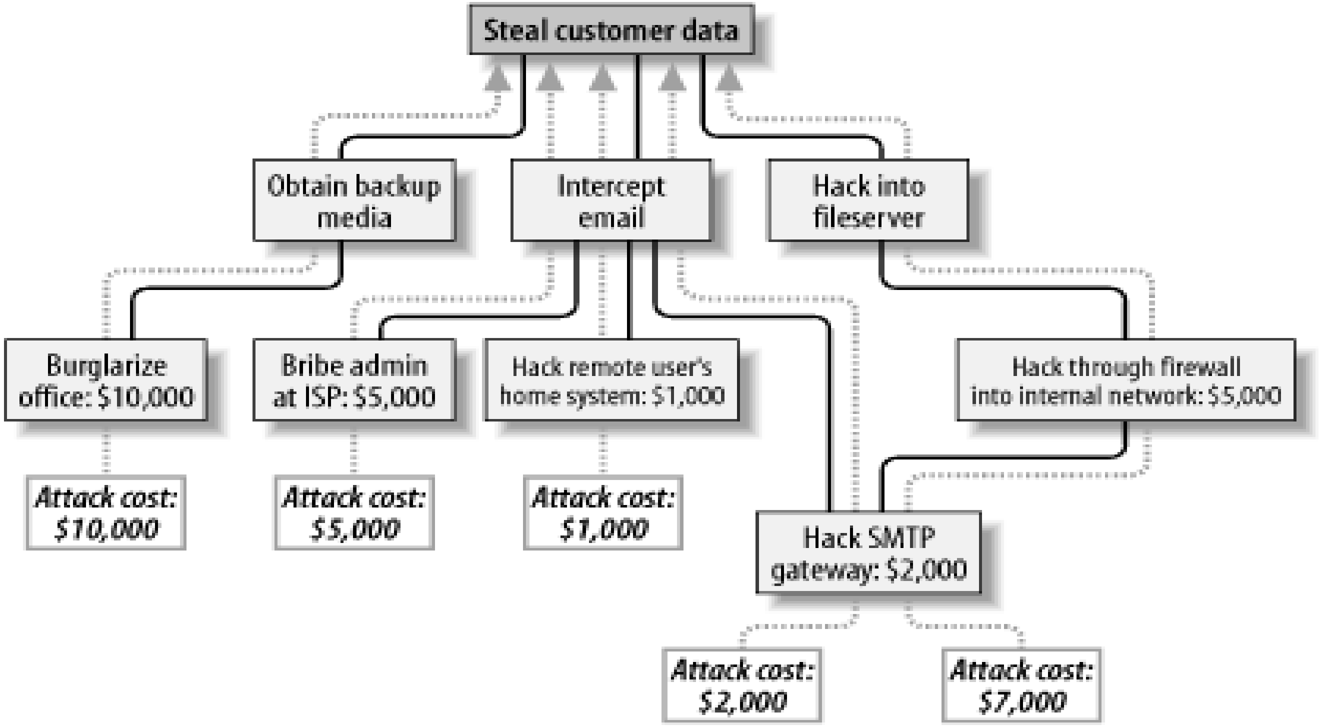
Get Target to State Combo
NSE/$40K

NSE = No special equipment
SE = Special equipment required
$ = Cost of attack

Attack Trees – A Technical Example



Attack Trees – A Technical Example



Security Functional Requirements

- Access Control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
- Awareness and Training: (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
- Audit and Accountability: (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.
- Certification, Accreditation, and Security Assessments: (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Security Functional Requirements

- Configuration Management: (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.
- Contingency Planning: Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations. Identification and Authentication: Identify information system users, processes acting on behalf of users, or devices, and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- Incident Response: (i) Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user-response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Security Functional Requirements

- Maintenance: (i) Perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- Media Protection: (i) Protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.
- Physical and Environmental Protection: (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
- Planning: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Security Functional Requirements

- Personnel Security: (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
- Risk Assessment: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
- Systems and Services Acquisition: (i) Allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that thirdparty providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

Security Functional Requirements

- System and Communications Protection: (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.
- System and Information Integrity: (i) Identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.