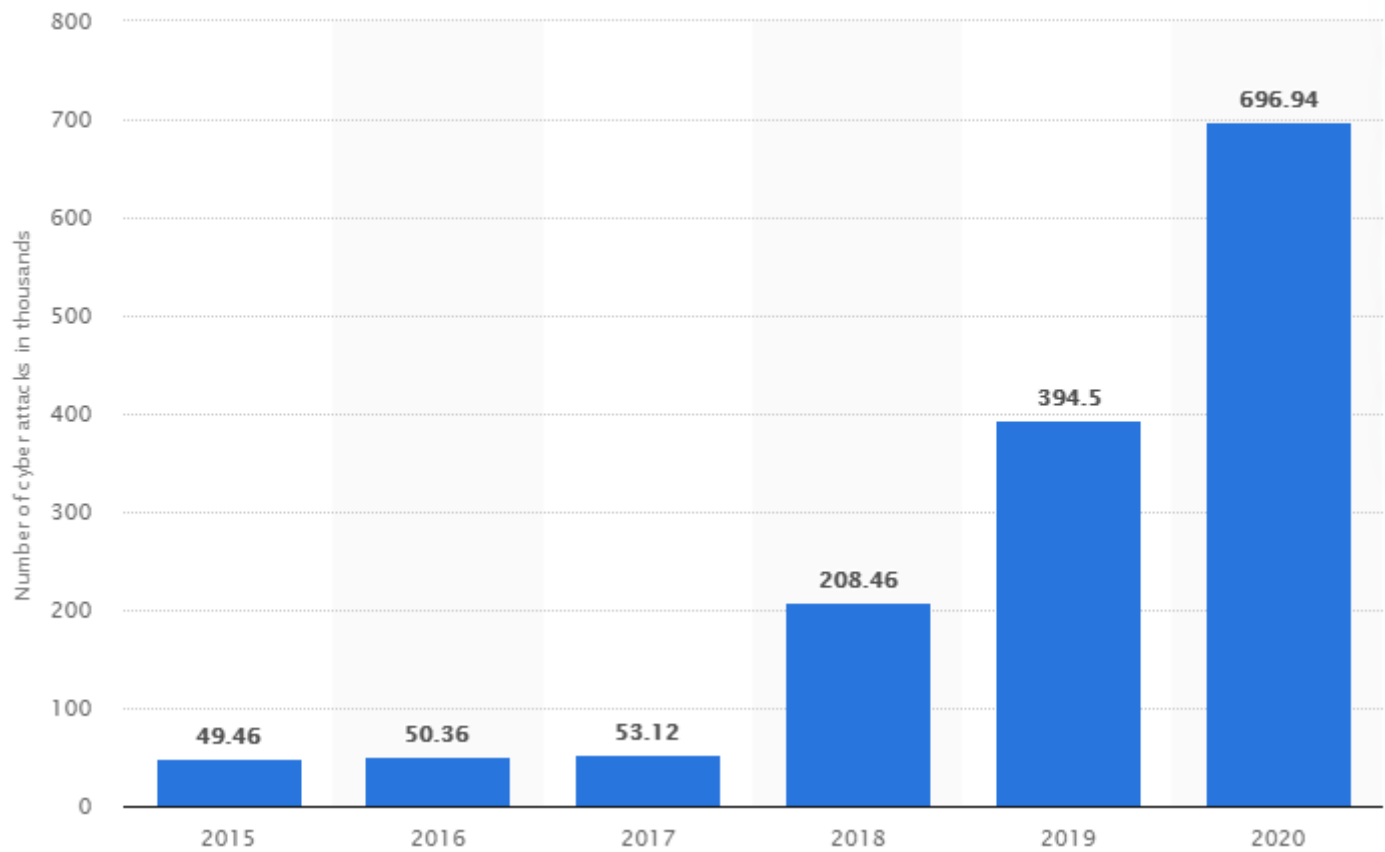




INTRODUCTION TO CYBER SECURITY

Dr. Amit Praseed



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

THREATS AND ATTACKS

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

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



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 is 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 more 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

