# Lecture 1

1

INFORMATION SECURITY

# Information Security Today



- Emergence of the Internet and distributed systems
- Digital information needs to be kept secure
  - Competitive advantage
  - Protection of assets
  - Liability and responsibility
- Financial losses
  - The FBI estimates that an insider attack results in an average loss of $2.8 million
  - There are reports that the annual financial loss due to information security breaches is between 5 and 45 billion dollars

# ตัวอย่าง สถานการณ์ภัยคุกคามไซเบอร์ ที่เกิดในประเทศไทย



- **ปี 2555 เจาะระบบ THNIC:** ผู้ให้บริการโดเมนเนมไทย (.th) ถูกเจาะระบบและแก้ไขข้อมูลที่อยู่ของเว็บไซต์ขององค์กรใหญ่หลายแห่ง
- **ปี 2556 DDOS ตลาดหลักทรัพย์:** โจมตี DDOS โดยกลุ่ม Anonymous กับเว็บไซต์ตลาดหลักทรัพย์ในอเมริกา **และ**เอเชียตะวันออกเฉียงใต้ ทำให้บริการขัดข้องหลายชั่วโมง ส่งผลกระทบด้านเศรษฐกิจจากปัญหา Cybersecurity
- **ปี 2557 Sony Pictures Hack:** ระบบคอมพิวเตอร์ของมหาลัยชื่อดังแห่งหนึ่งของไทย ถูกกลุ่ม GOP (Guardians of Peace) ใช้เป็นฐานการโจรกรรมข้อมูลจากบริษัท Sony Pictures สหรัฐอเมริกา

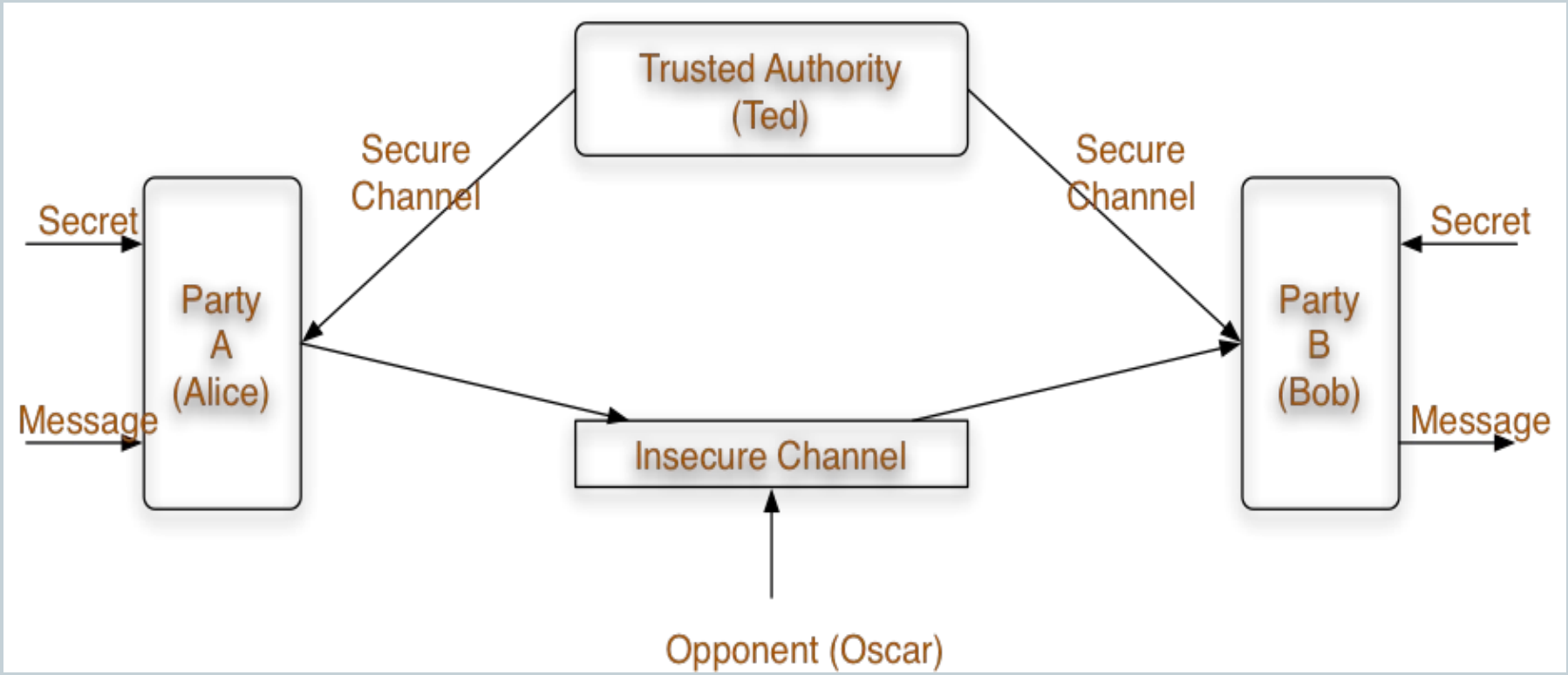
# ตัวอย่าง สถานการณ์ภัยคุกคามไซเบอร์ ที่เกิดในประเทศไทย



- **ปี 2558 DDoS 4 Bitcoin:** 5 ธนาคารพาณิชย์ได้รับอีเมลข่มขู่ เรียกเงินเป็น Bitcoins เพื่อแลกกับการไม่ถูกโจมตี DDOS จากกลุ่ม Armada Collective
- **ปี 2559 ATM Malware:** ATM 21 ตู้ ของธนาคารแห่งหนึ่งของไทย ถูกโจมตีด้วยมัลแวร์ และลอบขโมยเงิน 12 ล้านบาท ซึ่งพบว่าเป็นมัลแวร์คล้ายกันกับที่เคยโจมตี ATM ที่ไต้หวัน
- **ปี 2560 Ransomware ระบาด:** มัลแวร์ WannaCry และ Petya แพร่ระบาด เครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Microsoft Windows จำนวนหนึ่งในไทย ทำให้ถูกเข้ารหัสข้อมูล

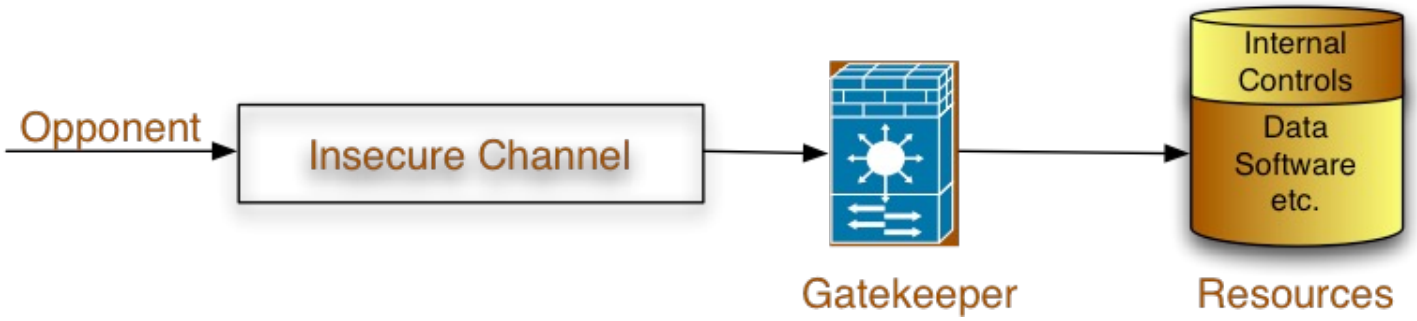
# Model 1: Security of Information Transmission





# Model 2 - Network Access Security

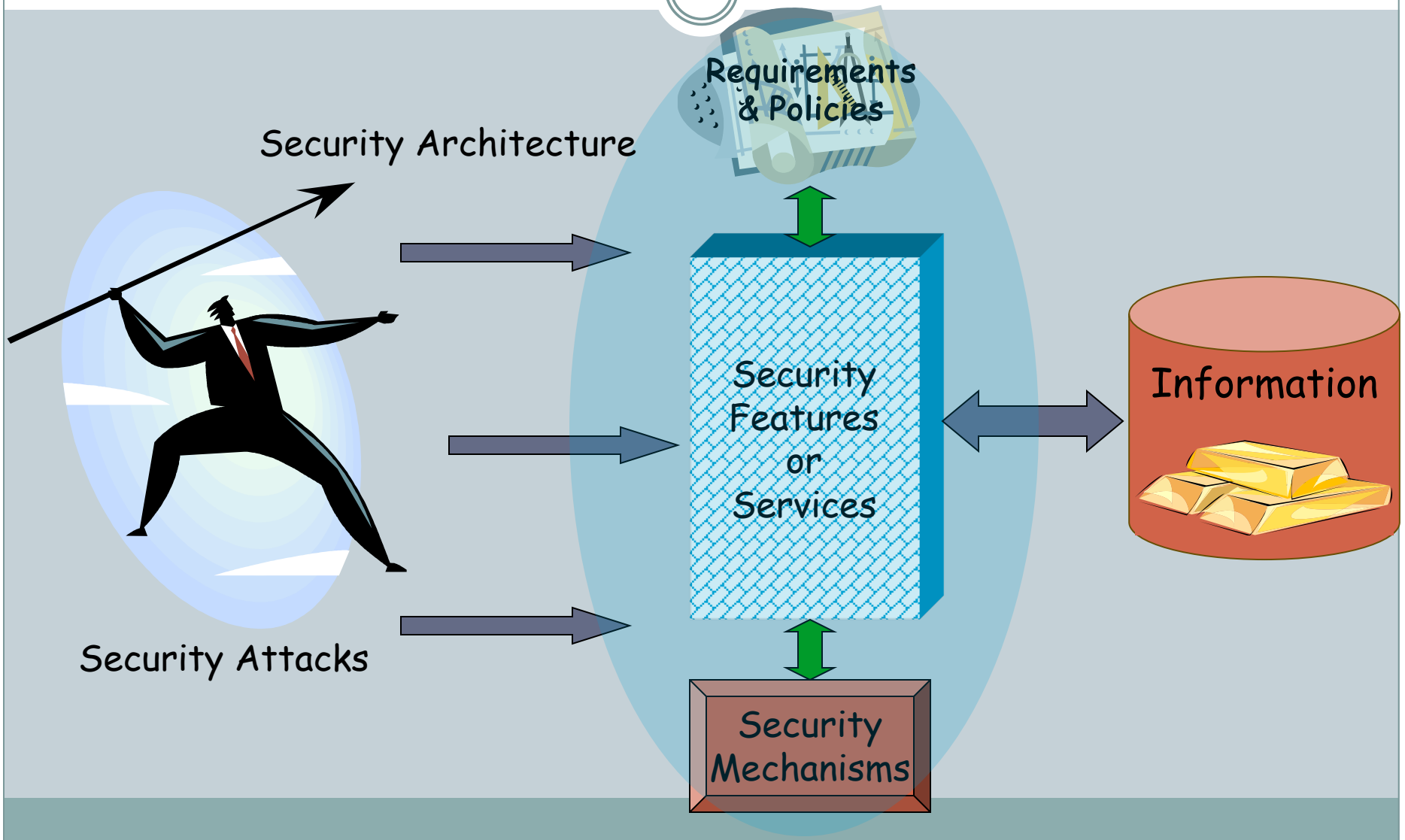





- Gatekeeper
  - Firewall, application gateway, packet filter etc.
- Internal control
  - Logs, Monitoring, IDS, audits, virus scans, etc.

# Terminology -I





# Terminology - II



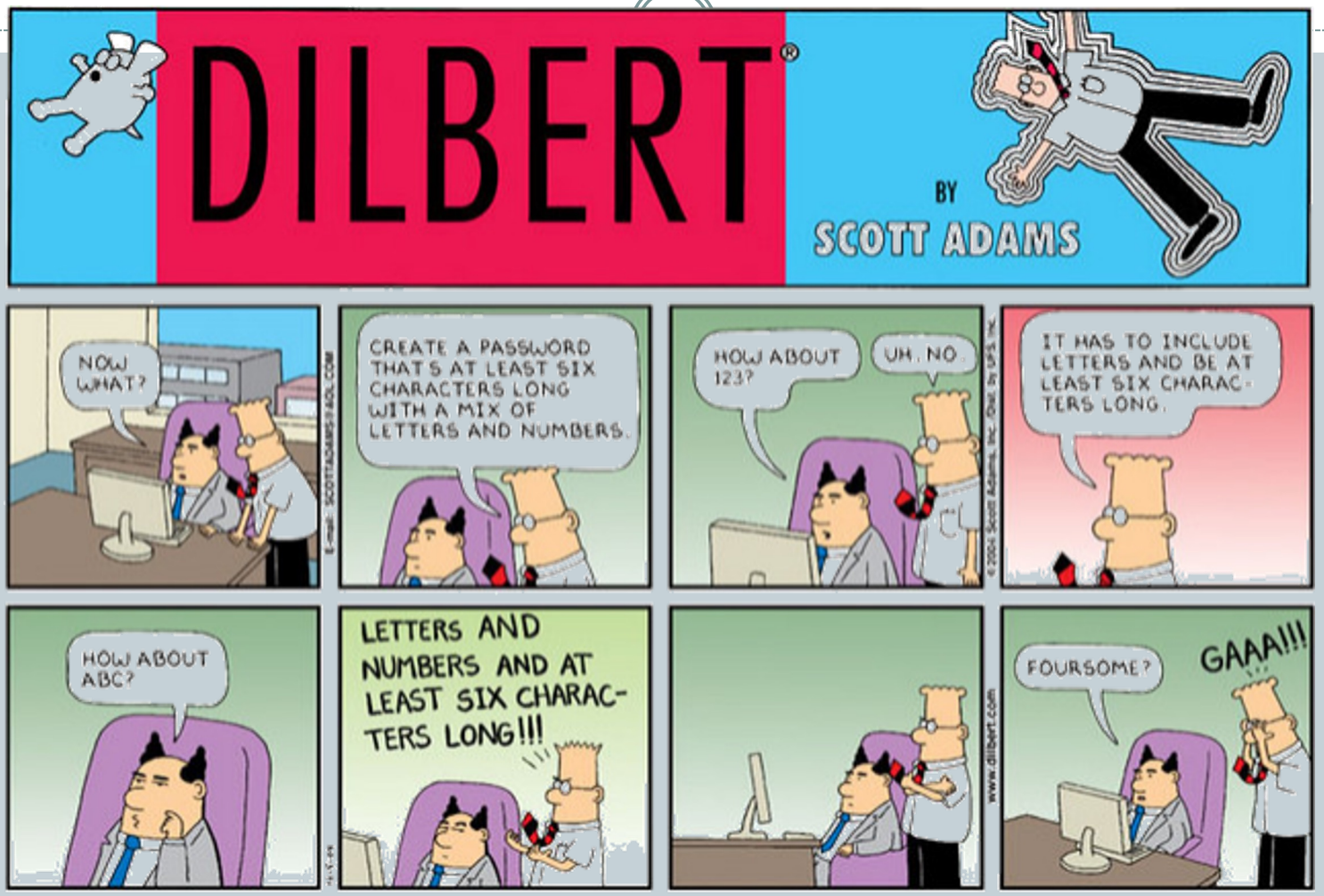
- Asset
  - Network or system resource that has value
    - Examples - bandwidth, web server, CPU cycles, database with credit card numbers, e-mail with confidential data
- Vulnerability
  - Weakness in the asset that can be exploited
    - Example - Access to network bandwidth for anyone without authentication or controls
- Threat
  - Someone capable of and wanting to exploit a vulnerability in an asset
  - Sometimes it is expressed as an abstract event that could occur rather than specifically identifying someone who is a threat

# Vulnerabilities



- Cannot get rid of all of them
- Reasons
  - Poor design - buggy code
  - Architectural weaknesses - in software and hardware
  - Poor implementation - users do not deploy assets in the right way
  - Poor containment - asset can be used for things it was not meant to be

# Why do vulnerabilities exist?




Poor Implementation - Customer deploys a product incorrectly

# Some more fun :-)



# Threats



- Insider and External
  - General belief that insiders are the predominant cause of security breaches is not true anymore
  - An external threat CAN get insider access
- Structured and Unstructured [6]
  - Does the threat have a formal methodology, financial sponsor and defined objective?
    - More dangerous, could be long term and subtle
  - Threat is one of intellectual curiosity or mindless instantiation of automated code
    - Recreational crackers, script kiddies and the like - seek notoriety

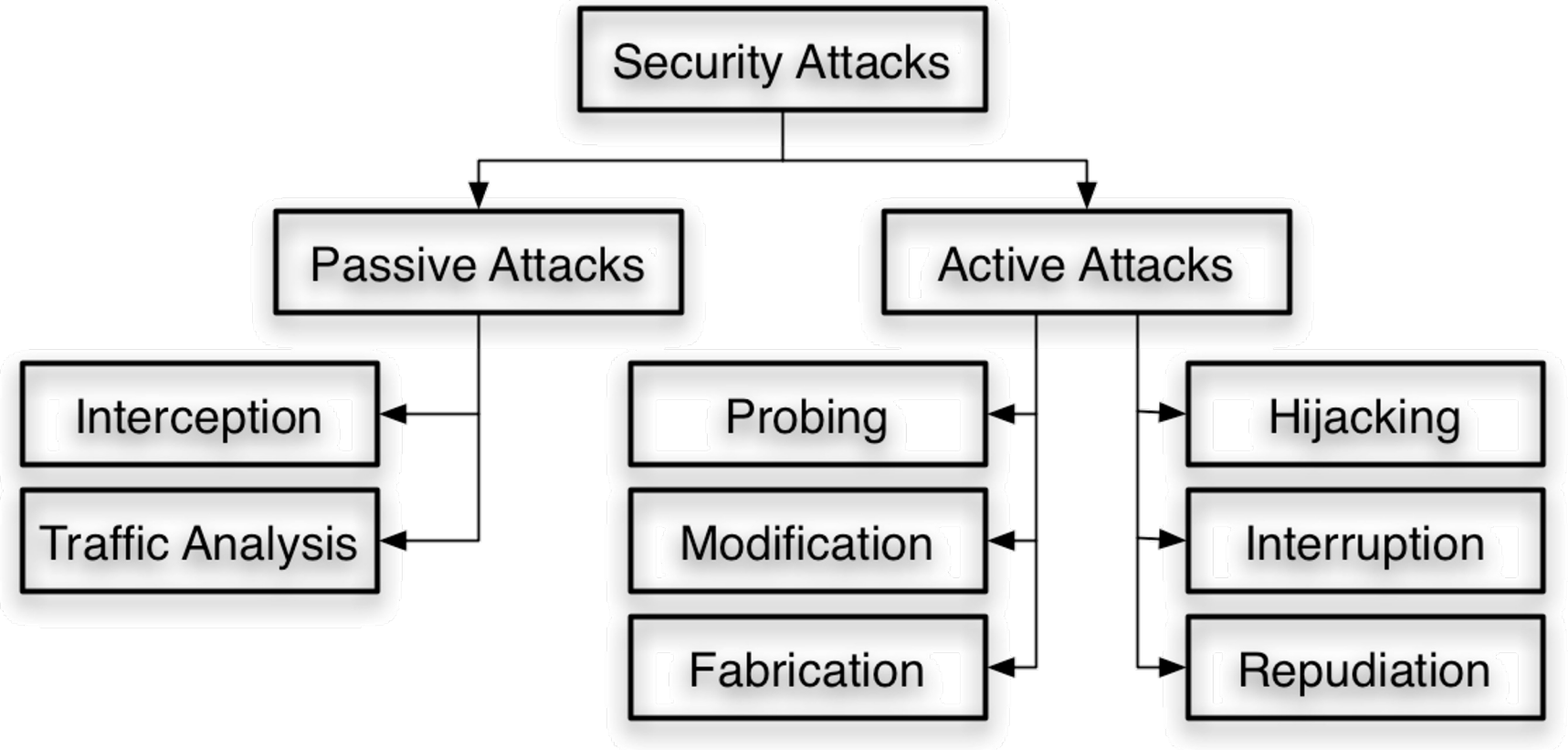
# Threats and Attacks



- A threat is a potential violation of security
  - Violation may not actually occur, but it might occur
  - Need to be prepared against threats
  - Typical threats - disclosure, deception, disruption, usurpation
- An attack is any action that compromises the security of information
  - It is an actual violation!
  - Can be classified based on information flow or nature of attack

# Types of Attacks






- Passive attacks are hard to detect - they must be prevented
- Active attacks are hard to prevent - they must be detected rapidly

# Examples of Attacks



- Zombies
  - Take over several vulnerable machines and use them as Zombies to launch DoS attacks or send SPAM e-mail
- Steal information
  - Break into systems and databases and steal credit card and identity information
- Extortion
  - Threaten companies that their cyberinfrastructure will be attacked if they do not pay up

**Most attacks are on hosts running vulnerable software. But not all of them are such attacks**

# Policies and Requirements



- Policy - a statement of what is allowed and what is not
  - It should take into account
    - What resources are being protected
    - Who may attack these resources (Risk)
    - How much of security can be afforded (Cost)
- Often involves procedures that cannot be implemented solely through technology
  - Human factor is very important
  - Conflicting policies may exist
- Extremely important for legal recourse

# Security Services - 1



- Measures intended to counter security attacks by employing security mechanisms
  - Like physical procedures, but increasingly automated
  - Examples - signatures, documents, ID cards, endorsements, etc.
- Typical services that are considered are confidentiality (privacy), authentication, integrity, non-repudiation, availability

# Security Services - 2



- Confidentiality
  - Protects against interception and traffic analysis
- Message Authentication
  - Combination of authentication and integrity
  - Protects against fabrication and modification
- Non-repudiation
  - Protects against repudiation
- Availability - Protects against interruption and denial of service

# Confidentiality



- Information should be accessible only to authorized parties
- Related to “concealing” of resources or information
- It can be broad
  - Including all possible data or the very existence of data
- It can be narrow
  - Taking into account only certain fields or parts of the data
- Attacks are mostly passive
  - Interception leading to disclosure or traffic analysis
  - Active attacks are also possible and increasingly common

# Authentication and Integrity



- Authentication
  - Identity of the source of information is not false
    - During initiation of connection
    - During ongoing interaction
  - Attacks are active – fabrication, masquerade, replay, session hijacking etc.
- Integrity
  - Information has not been modified by unauthorized entities
    - Not reordered, inserted, delayed, or changed in any other way
  - Attack is active: modification, alteration

# Authentication and Integrity (II)



- Evaluating and assuring integrity is hard
  - There are several issues
    - Verifying that the source of the information is right
    - Verifying that the source is trustworthy or credible
      - How was the data protected before it arrived?
      - How is the data currently protected?
      - Where has the data passed through?
- Non-repudiation
  - Neither the sender nor the receiver should deny the transmission or its contents
    - A user should not be able to deny that he created some files
    - Another user should not be able to deny that he received a notification

# Availability



- Information is available to authorized parties when needed
  - Important aspect of reliability and system design
  - A system that is not available is as bad as no system at all
- Impact on availability
  - There may be deliberate attempts to deny access to data and service
  - There may be natural failures in information systems
  - Patterns of usage can be manipulated to affect availability
- Network design, protocol design

# Access Control



- Only authorized people have access to the network resources and information
- There may be varying levels of access and control
- Requires good policies to be in place
- Affects all other security services

# Security is a process



- It is a process NOT an absolute or measurable quantity
  - It is ongoing and uncertain
- Four components in security
  - Assessment
  - Prevention
  - Detection
  - Response

# Components of security



- Assessment
  - What is the status?
    - Are there the right policies and procedures, are right technical pieces in place, are we legal…
- Prevention
  - Measures taken to reduce the chance of security breaches
    - Includes architectural placements, deployment of components like firewalls, use of secure protocols… both host-based and perimeter-based
- Detection
  - Process of identifying security breaches and violations of policies
    - Automatic methods like IDS and IPS, manual - monitoring and logs, procedures like audits
- Response
  - Making sure that detection of a security breach is actually a security breach
  - Process to ensure similar breaches do not occur again (patch, clean-up, restore)
  - Process to take legal and other steps (report to DoJ, sue, etc.)

# Security breach is also a process!



- A security breach due to a “structured threat” does not occur instantaneously
- Phases [6]
  - Reconnaissance
  - Exploitation
  - Reinforcement
  - Consolidation
  - Pillage

# Reconnaissance



- Attacker confirms a variety of properties of the victim
  - Connectivity, services, vulnerable applications
  - Network architecture, IP address space, operating systems, versions of software applications
- Could be technical or non-technical
- Helps the attacker accomplish his objectives in a better way
  - Less obtrusive, more efficient, helps planning

# Reconnaissance - II



- Many Windows based attacks do not perform reconnaissance
  - Commonality of the vulnerabilities
  - Increases speed of attack - reduces time to attack
- Reconnaissance methods need to appear to be normal
  - Make use of commonly available protocols and information services through the information they “leak”
  - Social engineering
- Defense
  - Possible to detect reconnaissance in some cases
    - Some probes are not very stealthy

# Exploitation



- Attacker breaches services on the target using normal protocols
  - Mostly through bugs in software tools and in design
    - Buffer overflows, authentication failures, misconfiguration
  - Sometimes other vulnerabilities are exploited - protocol failures, fooling IDSs, breaching firewalls etc.
- Types
  - Abuse - use stolen material to illegitimately obtain access
    Subversion - make a service do what it is not supposed to do
  - Breach - take control over a service, stop it, or get its privileges
- Defense
  - Possible to detect some of the message exchanges by IDS

# Reinforcement



- After exploitation, increase the level of control over victim
  - Example - attacker gets user-level access to some services
  - Attacker elevates it to administrative or root access
- Also introduce tools in the victim hosts that may aid the attacker further
  - Perhaps create some backdoors and close the vulnerabilities

# Consolidation and Pillage



- Attacker has complete control over the victim host
  - Communications are possible covertly through the backdoor
  - The victim host may initiate communications with the attacker
- Pillage
  - Use the victim host as desired
    - Steal sensitive information
    - Use as a base for other attacks, etc.

# Some Security "Truisms"



- Security is always a question of economics and it is a tradeoff with convenience
- Keep the level of all of your defenses at the same height
- An attacker does not go through security, but around it
- Put your defenses in layers but keep it simple
- It is a bad idea to rely on security through obscurity
- A program or protocol is insecure until proven otherwise
- Don't give a person or a program any more privileges than necessary to do a given job
- Security should be an integral part of the original design