Principal of Information Security

—— History, Connotations and Concepts

Dr. HU Tianlei

Associate Professor

College of Computer Science, Zhejiang Univ.

htl@zju.edu.cn

Outlines

- History and Evolution of Information Security
- Objectives and Properties of Information Security
- Concepts of Computer Security, Attack and Anti-Attack

History of Information Security

Learn from History

以铜为镜，可以正衣冠；
以古为镜，可以知兴替；
以人为镜，可以明得失。

——唐太宗

What's the meaning of Information Security in History?

- Encryption! Cover the information you want to deliver!
- What was the first cipher in the history of China?
- Who invented the first cipher of CCP?

太公兵法——The 1st Cipher in China

- 武王问太公曰：
  - 引兵深入诸侯之地，三军猝有缓急，或利或害，吾将以近通远，从中应外，以给三军之用。为之奈何?
- 太公曰：
  - 主与将，有阴符，凡八等。
    - 有大胜克敌之符，长一尺。破军杀将之符，长九寸。降城得邑之符，长八寸。
    - 却敌报远之符，长七寸。誓众坚守之符，长六寸。请粮益兵之符，长五寸。
    - 败军亡将之符，长四寸。失利亡士之符，长三寸。
  - 诸奉使行符，稽留者，若符事泄，闻者告者，皆诛之。八符者，主将秘闻，所以阴通言语，不泄中外相知之术。敌虽圣智，莫通识。
- 武王又问太公曰：
  - ... 符不能明；相去辽远，言语不通。为之奈何?
- 太公曰：
  - 诸有阴事大虑，当用书，不用符。主以书遗将，将以书问主。
  - 书皆一合而再离，三发而一知。再离者，分书为三部。三发而一知者，言三人，人操一分，相参而不相知情也。
  - 此谓阴书。敌虽圣智，莫之能识。

豪密 —— The 1st Cipher of CCP

- 由周恩来编写的密码（周总理化名伍豪），三十年代一直用到解放，国民党都没有破解。
  - 周总理是我党和我军无线电工作的鼻祖和直接领导人
  - 早在二十年代末，周总理便在极其艰难的环境中，亲自编写了我党我军的第一部密码——"豪密"。
  - 这部密码直到1949年国民党垮台都没有被破译出来。当时，国民党情报系统的破译力量是相当强大的，他们曾在珍珠港事件前截获破译了日军的进攻计划。

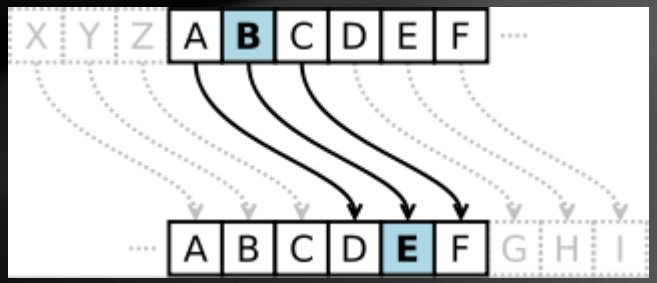
Phaistos Disc

The Phaistos Disc (also spelled Phaistos Disk, Phaestos Disc) is a disk of fired clay from the Minoan palace of Phaistos, possibly dating to the middle or late Minoan Bronze Age (2nd millennium BC). It is about 15 cm (5.9 in) in diameter and covered on both sides with a spiral of stamped symbols.

More Info: http://en.wikipedia.org/wiki/Phaistos_Disc

Caesar cipher

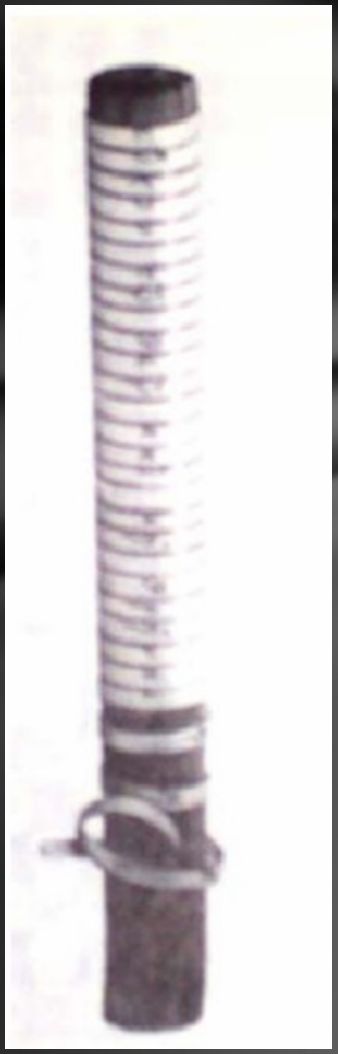
- **The known, earliest Substitution Cipher**
- **Example:**
  - Replace each alphabet with 3 down to it
  - `Plain text:  meet me after the toga party`
  - `Cipher text:  PHHW PH DIWHU WKH WRJD SDUWB`
- **How many different ways of substitution?**
  - 25 possible secret keys



Scytale Cipher

Ancient Greeks, and the Spartans in particular, are said to have used this cipher to communicate during military campaigns.

- Questions:
  - How to encrypt?
  - What's the key?



- What's the difference?
  - Substitution vs Transposition
  - 替代/替换 vs 置换/位移

Information Hiding

- 连城诀
  - 连城剑法的第一招，出自杜甫的‘春归’。他伸手指沾了唾涎，去湿杜甫那首“春归”诗旁的纸页，轻轻欢呼了一声：“是个‘四’字！好，‘苔径临江竹’，第四个字是‘江’
  - 第二招，仍是杜甫的诗，出自‘重经昭陵’。”他又沾湿手指，去湿纸页：“嗯，是‘五十一’！”他一个字一个字的数下去：……‘陵寝盘空曲，熊罴宁翠微’，第51个字，那是个‘陵’字。‘江陵’、‘江陵’，妙极，原来果然便在荆州。”
  - 剑法第三招，出自‘圣果寺’，三十三，第33字，‘下方城郭近，钟磬杂笙歌’中的‘城’字，‘江陵城’。
- 水浒传
  - 《水浒传》中梁山为了拉卢俊义入伙，“智多星”吴用和宋江便生出一段“吴用智赚玉麒麟”的故事，利用卢俊义为躲避“血光之灾”的惶恐心理，口占四句卦歌：

    芦花丛中一扁舟，俊杰俄从此地游。

    义士若能知此理，反躬难逃可无忧。
  - 暗藏“卢俊义反”四字，广为传播。结果，成了官府治罪的证据，终于把卢俊义“逼”上了梁山。

Steganography

http://en.wikipedia.org/wiki/Steganography

Ancient(According to "The Histories" by Herodotus):

- To convince Aristagoras in Miletus to betray the king, Histiaeus had a slave's head shaved and wrote a message on the head. When the hair grew again, the slave could walk around without trouble.
- Demeratus warned the Spartans of the coming invasion of Xerxes: He wrote a message on a wax tablet and recovered the message with wax, making the tablet look blank.

Modern:

- Egg Writing
  - In the 16th Century, the Italy scientist Giovanni Battista Porta wrote ink made of alums and vinegar on the egg and then coddled the egg, which made the ink solidify on the surface of the egg whites. Still, the ink on the shell faded away. So when the eggshell was stripped off, the message was readable.
- Microdot: http://en.wikipedia.org/wiki/Microdot
  - Microdot puts the message on a tiny film, which is made into punctuation so that the film can be hidden in a letter. Microdot cameras can be hidden in a ring, a hallow coin, or other things. To read the message of the microdot, the receiver needs special projection equipment.
- Bacon's cipher: http://en.wikipedia.org/wiki/Bacon's_cipher
  - Cipher, encoded with the font. To encode the message, there should be two fonts and two faked statements with the same words in different fonts, A and B. Then, the faked messages can be A or B, according to their font. In the deciphering, undo it.

The evolution of cryptography

In general, the main objective of cryptography is **Keeping Secret**. The listed ways of keeping secrets in history are the **quintessence** of human wisdom. But the real scientization of cryptography should owe to the coming up of Kerckhoff's Principle and its later development.

- The evolution of cryptography:
  - The first evolution: The Kerckhoffs' Principle
  - The second evolution: Computers
  - The third evolution: Public key ciphers
  - The fourth evolution: The Internet? Mobi-Internet?

The 1st : Kerckhoffs's Principle

"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."

- —— by Auguste Kerckhoffs in 1883

Kerckhoffs's Principle means that cryptography evolves from the prehistoric period to the classic period:

- **Enhance the Safety: Assume that anything invariable will be disclosed**
  - The encryption algorithms themselves can not be kept secret
  - The secrecy is only up to the key
- **It makes the mass production of cipher machines possible**

The 1st Evolution —— Cryptography evolved from Experience to Science.

The 2nd : Electronic Computer

Why & when do computers appear?

- To decrypt ENIGMA, in World WAR II

Computers accelerate both encryption and decryption

Theoretical basis—— Shannon's Information Theory :

- "A mathematical theory of communication," 1948
- "Communication theory of secrecy systems," 1949

The emergence of Modern ciphers: DES

The 2nd Evolution —— Cryptography evolved from Manual to Mechanical and Electronic.

The 3rd : Public Key Ciphers

"New Directions in Cryptography"

- Whitfield Diffie and Martin E. Hellman, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976
- http://www-ee.stanford.edu/~hellman/publications/24.pdf

Public key ciphers make it possible to exchange a large number of secret messages without sharing any secret key between the sender and receiver.

The most widely used Public Key Ciphers Algorithm:

- RSA, http://en.wikipedia.org/wiki/RSA_(algorithm)

The 3rd Evolution —— Revolutionary Evolution of Cryptography Mechanism

The 4th : (Mobile) Internet? AI?

- **Expansion of the Connotation of Cryptography:**
  - Not only "Secret," but also other problems;
- **Expansion of the Extension of Cryptography:**
  - Application: Military Field-> Civil Field-> Personnel Field
  - Protect: Simple PTP Protocol -> Complicated PTP Protocol-> Various of Internet Protocol & Application -> 5G, Blockchain, IoT & AI
- **The challenge of the development of hardware and software**
  - Promotion of hardware performance and capacity & reduction of cost;
  - Mass distributed computing, cloud computing, cipher analysis, and so on;

The 4th Evolution —— The Expansion of Cryptography Connotation and Extension derived by Technologies and Applications.

Connotation of Computer Security

—— Significance and Properties

Significance of computer security

We have experienced the following:

- **In the PC Era, Virus ravages —— To show off or destroy**
  - Jerusalem@1987 "Black Friday," the first malignant Computer Virus
  - MICHELANGELO @1992 On March 6th, clear the first 100 blocks of the HDD
  - CONCEPT @1995 Office Macro Virus
  - CIH @1998 Virus to Damage the hardware

Significance of computer security

We have experienced the following:

- **In the Internet Era, hackers, worms, and DOS burst out —— To benefit & to monetize**
  - Sino-US hacker wars@1999，2001 — The bombing of the Yugoslavia Embassy and the Sino-US South China Sea collision led to the cyber hacker war.
  - Melissa @1999 — The first Virus spread from email, a combination of Macro Virus and Worm
  - Nimda @2001 — The most famous worm, spreading all over the world in fifteen minutes, led to more than 2.6 billion dollars in losses;
  - Blaster, Sasser @2003, 2004 — Blaster Worm / Sasser Worm, lead to the jam of the Internet
  - 熊猫烧香 @2006 — Troy Virus code by Chinese
  - Storm Worm @2007 — most giant botnet, with more than 15 million computers in control
  - CSDN @2011 — Most serious security-related event in China

Significance of computer security

We have experienced the following:

- **In the Post-Internet Era, when the Internet/mobile is a part of our life:**

PRISM @2013	The headache of the U.S.A. government
iOS 7越狱“太极门”@2014	Mobile devices promote the privacy issues
Xcode Ghost @2015	Distributing trojans by developing tools affecting Weixin, Didi, Netease Music, …
Krack on WPA2 @ 2017	Affecting almost every device using WIFI
Meltdown/Spectre @ 2018	Exploiting the CPU Architecture, affecting nearly every device
Huawei & Tiktok @2019 – now	Data security is the major conflict of interest among major countries
Blockchain / Bitcoin / …	Blockchain will be the infrastructure of the future. Lots of cryptocurrencies are primarily deceptive.
Rumors / Fake news / …	Information itself can cause severe disaster.
Privacy issues	More and more public awareness of privacy all over the world.

Distinctness of computer security

Security has always been critical to business, diplomacy, the military, and other human activities. However, "computer-based information security" differs from traditional "paper-based information security."

- We can tell the difference between an original and a copy of paper documents,
  - But, for digital documents, we can't distinguish between the original and the copy;
- Alterations on paper will leave physical marks,
  - But, alteration on digital paper will leave nothing;
- Paper documents are relatively difficult to destroy,
  - But, digital documents are really easy to delete;
- Handwritten signatures and stamps are verified depending on their physical characteristics;
  - But, digital Information only depends on binary information ;

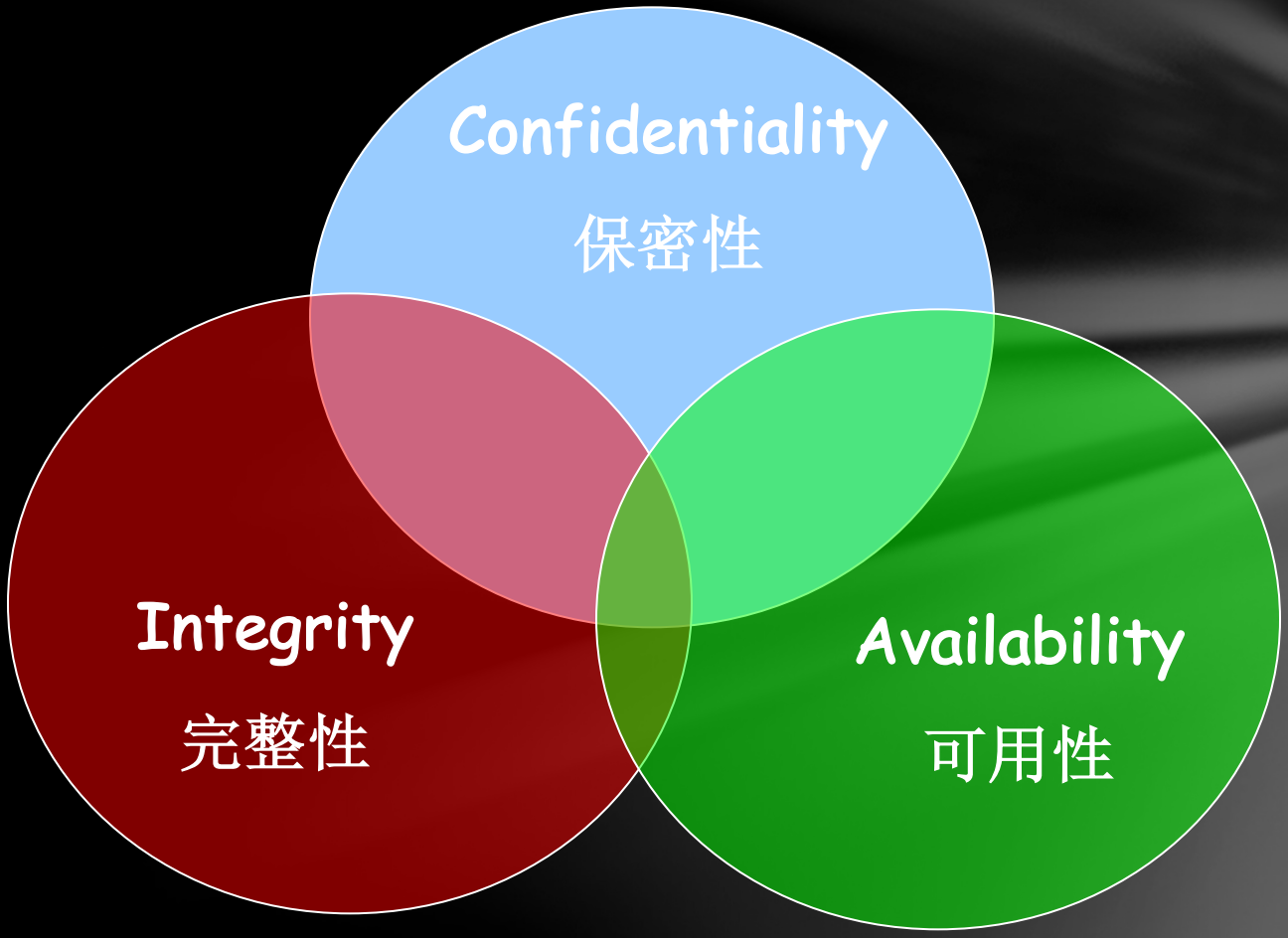
Characteristics of computer security

- Comprehensiveness
  - System Security depends on the weakest link
- Procedural
  - It's a constant back-and-forth rising spiral security model
- Dynamic
  - The entire security system is in the process of constantly updating, improving, and progressing.
- Hierarchy
  - Have to use multi-level security technologies, methods, and ways to resolve security risk
- Relativity
  - Security is relative, and no absolute security

Concepts of Computer Security

—— concept, attack and confront

3 Elements of Computer Security



The 1st, Confidentiality

Confidentiality: can others see your data?

1940s~1950s：

- U.S. National Security Agency（NSA）
  - U.S. National Security Agency came from Cipher Departments, which was created in 1952
  - It is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis
- The NATO Multilateral Export Control Coordinating Committee (CoCom)
  - Prevent exporting computers, Precision Machine Tools, Cipher Systems, and others to Socialist countries.

At that time, there were few computers and no Internet, which meant no modern hacking.

- The objective of Security is Confidentiality, preventing information data leakage, including information technologies.
- Without computers, the information system consists of paper documents whose objective is confidentiality.

The 2nd , Integrity

Integrity: can your data be illegally changed?

Since the 1960s: the emergence of database technologies inspires the requirements:

- Confidentiality: unauthorized read
- Integrity: unauthorized write (insert, delete, modify)

Need to distinguish the "valid user" and the "illegal user," for example:

- Illegally modification of School Management Information Systems
- Illegally change of bank account
- Modify data transferred on the network

The 3rd, Availability

Availability: will the resource be accessible?

Since the 1980s, many social functions have been built on massively deployed computers and networks. The availability of those information systems directly affect our daily life; imagine that:

- If you cannot withdraw cash with your bank card …
- If your email box is full of junk and spam …
- If Alipay cannot guarantee a response because of network congestion …
- If Weixin is attacked and down for half a month …

In the 1980s-1990s, a virus became famous because of its "novelty," but after the 1990s, a virus or worm became famous only because of its "damage."

The 4th, Authenticity / Non-repudiation

However, not addressed in formal textbooks, Authenticity / Non-repudiation is a critical security issue in the Internet Era.

Authenticity is the assurance that a message, transaction, or other exchange of information is from the source it claims to be from. Authenticity involves proof of identity.

Non-repudiation implies one's intention to fulfill their obligations to a contract. It also means that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction.

Concepts of Computer Security

- Asset (资产) – People, property, and information.
  - An asset is what we're trying to protect.
- Threat (威胁) – Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.
  - A threat is what we're trying to protect against.
- Vulnerability (漏洞) – Weaknesses or gaps in a security program that threats can exploit to gain unauthorized access to an asset.
  - A vulnerability is a weakness or gap in our protection efforts.
- Risk (风险) – The potential for an asset's loss, damage, or destruction due to a threat exploiting a vulnerability.
  - Risk is the intersection of assets, threats, and vulnerabilities.

Asset + Threat + Vulnerability = Risk.

A + T+ V = R

Types of security threat

By method:

- Natural threat —— earthquake, fire, flood, lightning, hurricane …
- Physical threat —— improper usage, careless damage
- Hardware/Software threat —— improper design, backdoor, logical bomb, system conflict…
- Media threat —— HDD damage, careless delete, careless demagnetization …
- Leak threat —— electromagnetic leakage, video surveillance of screen
- Communication threat —— capture, modify, and fake in the process of communication
- Personal threat —— careless delete damage, intentional destroy and leakage …

Meant or Unmeant:

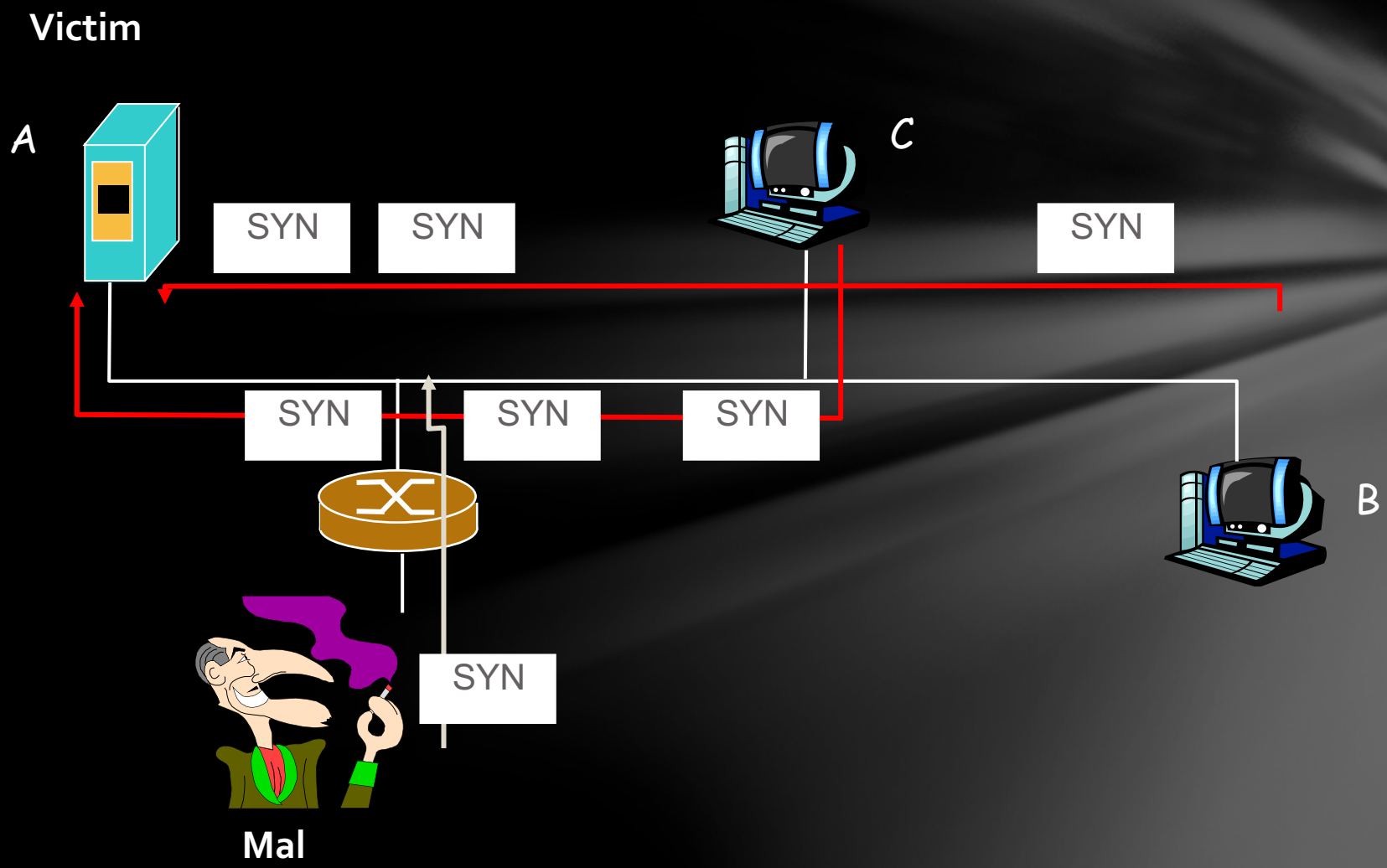
- Unmeant threat —— careless loss of HDD, delete and operation …
- Meant threat:
  - threat from outside the organization (hacker, industrial spy, terrorist, criminal …)
  - threat from inside of the organization(fired , corrupt, unsatisfied staff …)
  - The most effective threat comes from internal and external collaboration

Types of security attack — Interruption

- **Interruption:**
  - **An asset of a system is destroyed, unavailable, or unusable**
  - Attack —— “Availability”
  - Easy to detect

- **Ways of interruption:**
  - Hardware damage
  - Damage to the communication chain in physical
  - Introduce noise
  - Delete routine
  - Remove the program or file
  - denial of service attack (DOS)

Active Attacks: Denial of Service



Types of security attack — Interception

- **Interception:**
  - **An unauthorized party gains access to an asset**
  - Attack —— "Confidentiality"
  - Difficult to detect a silent Interceptor

- **Ways of Interception:**
  - Wiretap eavesdropping
  - Link monitoring
  - Packet capturing
  - System hacking & compromising

- **It can't be avoided entirely.**

Types of security attack — Modification

- **Modification：**
  - **Unauthorized parties gain access as well as tamper with asset**
  - Attack —— “Integrity”
  - Can be prevented: digital watermarking and other technologies

- **Ways of modification：**
  - Modify a record in the database
  - System hacking
  - Delay of communication
  - Modify hardware

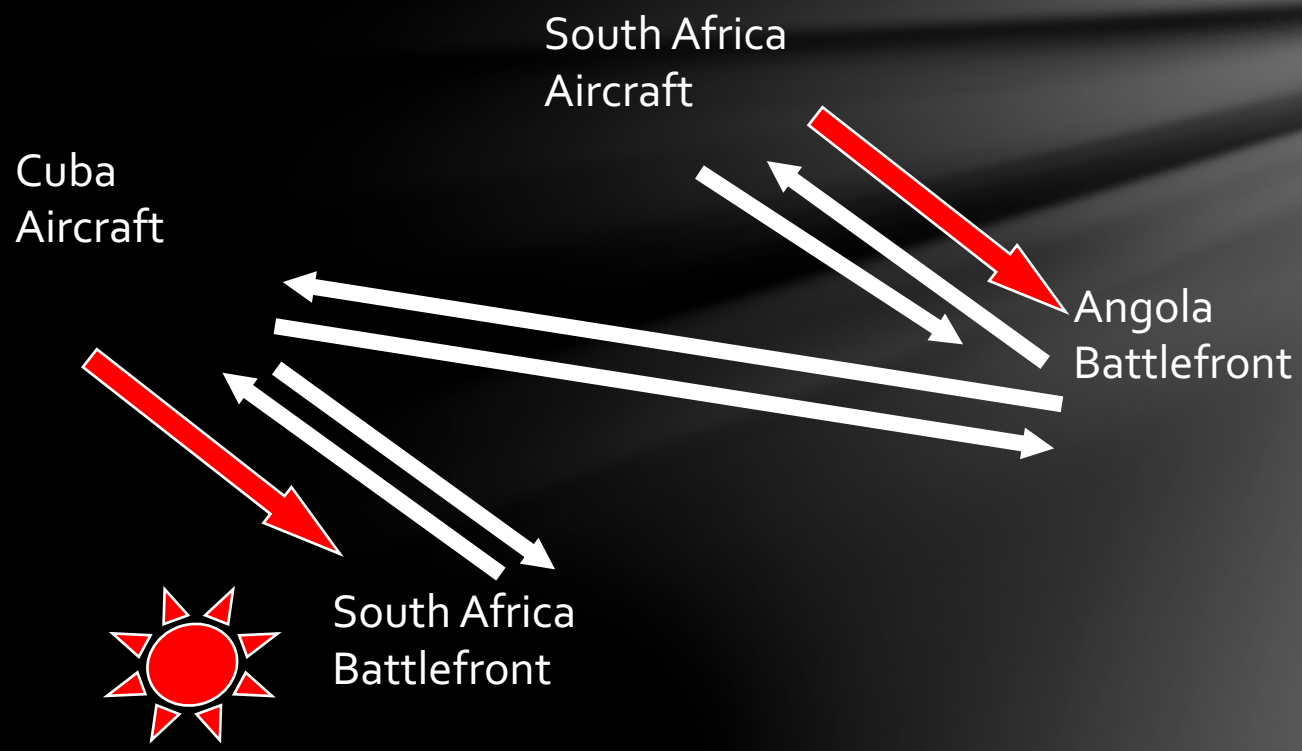
Types of security attack — Fabrication

- **Fabrication:**
  - **An unauthorized party inserts counterfeit (fake) objects into the system and pretends an authorized party sent them.**
  - Attack —— "Authenticity"
  - Associate with non-repudiation

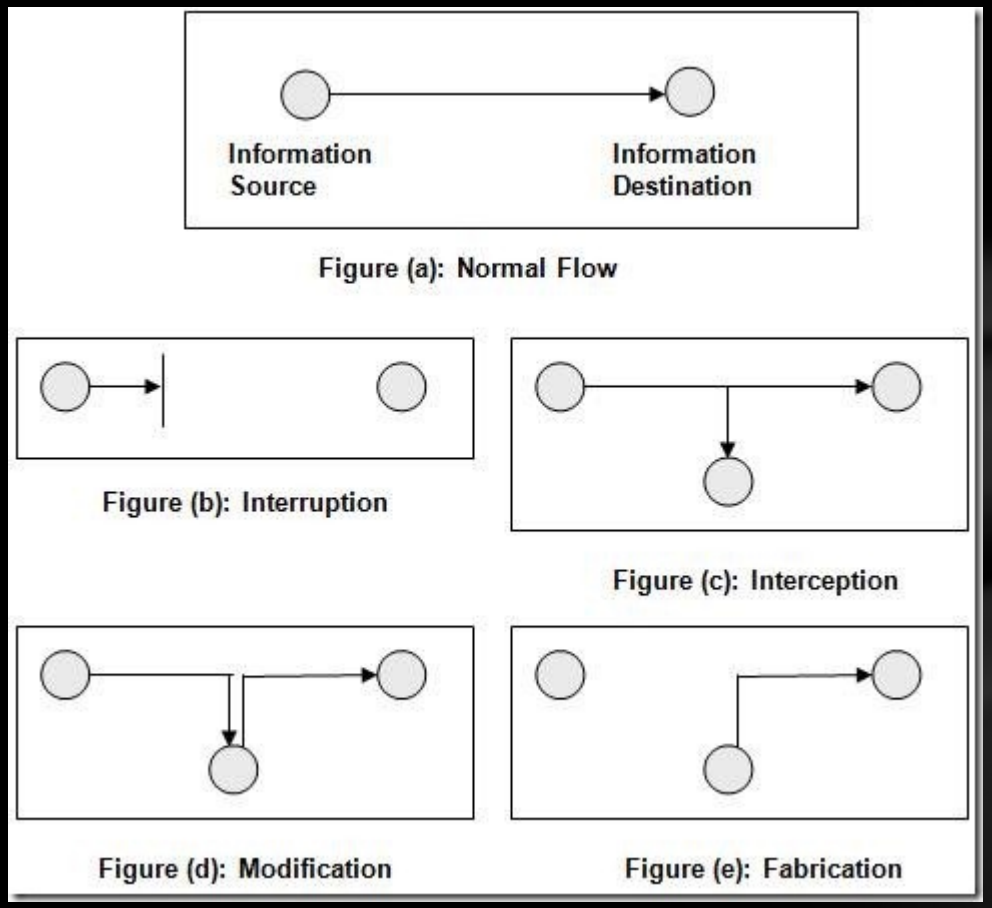
- **Ways of fabrication:**
  - Insert a record in the database
  - Insert a packet(with faked IP address)
  - Fishing with faked email or web address

Active Attacks: Replay

- Time: late in 1980s
- Subject: Cuba vs. South Africa Airforce



Types of security attack



Passive Attacks

- Goal: interception
- Difficult to detect
  - prevention will be more effective than detection in countering passive attacks

Active Attacks

- Goal: interruption, modification, and fabrication
- Easy to detect
  - difficult to prevent, and can be restored from damage

Against Security Threats —— The Goal

Prevention

- Prevent attackers from violating security policy.

Detection

- Detect attackers' violation of security policy.

Recovery

- The attack is stopped, the system is fixed, and operations resume.
- (Advanced Version) Continue to function correctly even if an attack succeeds.

Against Security Threats —— Policies and Mechanisms

The policy says what is allowed and what is not allowed

- This defines “security” for the site/system/*etc*.
- Policy definition: Informal? Formal? POLICY-LANGUAGE
- Ex. No internet users can access the internal database server

Mechanisms enforce policies

- Technical? Procedural?
- Ex. Firewalls

Composition of policies

- If policies conflict, discrepancies may create security vulnerabilities
- Ex. Student/faculty; partition

Against security threats ——Security Service

- **Authentication**
  - Ensure that the communication entities are the ones they claimed, including peer entity authentication and data origin authentication.
- **Access control**
  - Prevent the unauthorized visit to the resource
- **Data Confidentiality**
  - Prevent data leakage, including linked confidentiality, unlinked confidentiality, selected field confidentiality, and flow confidentiality.
- **Data Integrity**
  - Ensure the received data is sent from an authorized entity, and insert, delete, and replay without modification.
- **Non-Repudiation**
  - Prevent repudiation in communication from any entity
- **Availability**
  - Make sure the availability of the service

Against security threats
—— Operational Issues

Cost-Benefit Analysis

- Is it cheaper to prevent or recover?

Risk Analysis

- Should we protect something?
- How much should we protect this thing?

Laws and Customs

- Are desired security measures illegal?
  - Ex1. export control of the US government (DES)
  - Ex2. key-escrow regulation by France, → US
- Will people do them?
  - Ex1. use urine specimens to determine identity.

Against security threats
—— Human Issues

30% technical, 70% management

Organizational Problems

- Power and responsibility
- Financial benefits

People problems —— by far the primary source of security problems

- Outsiders and insiders
  - *Which do you think is the real threat?*
- Untrained People, ex. Unverified backup tape
- Social engineering, ex. Night call from an executive

Against security threats —— Altogether

- The Goals
- The Policies
- The Mechanisms / Services
- The Operation
- The People

Review of key points

- **History of info security and evolution**
  - The earliest info security?
  - The landmarks of four evolution of computer security?
- **Significance and properties of computer security**
  - What's unique about computer security?
- **Concepts, attacks, and confront of computer security**
  - Three elements of computer security
  - Concepts of computer security: vulnerabilities, threats, attacks, control
  - Ways of a computer attack and their classification
  - Security system, security services, security mechanisms, operational and human issues