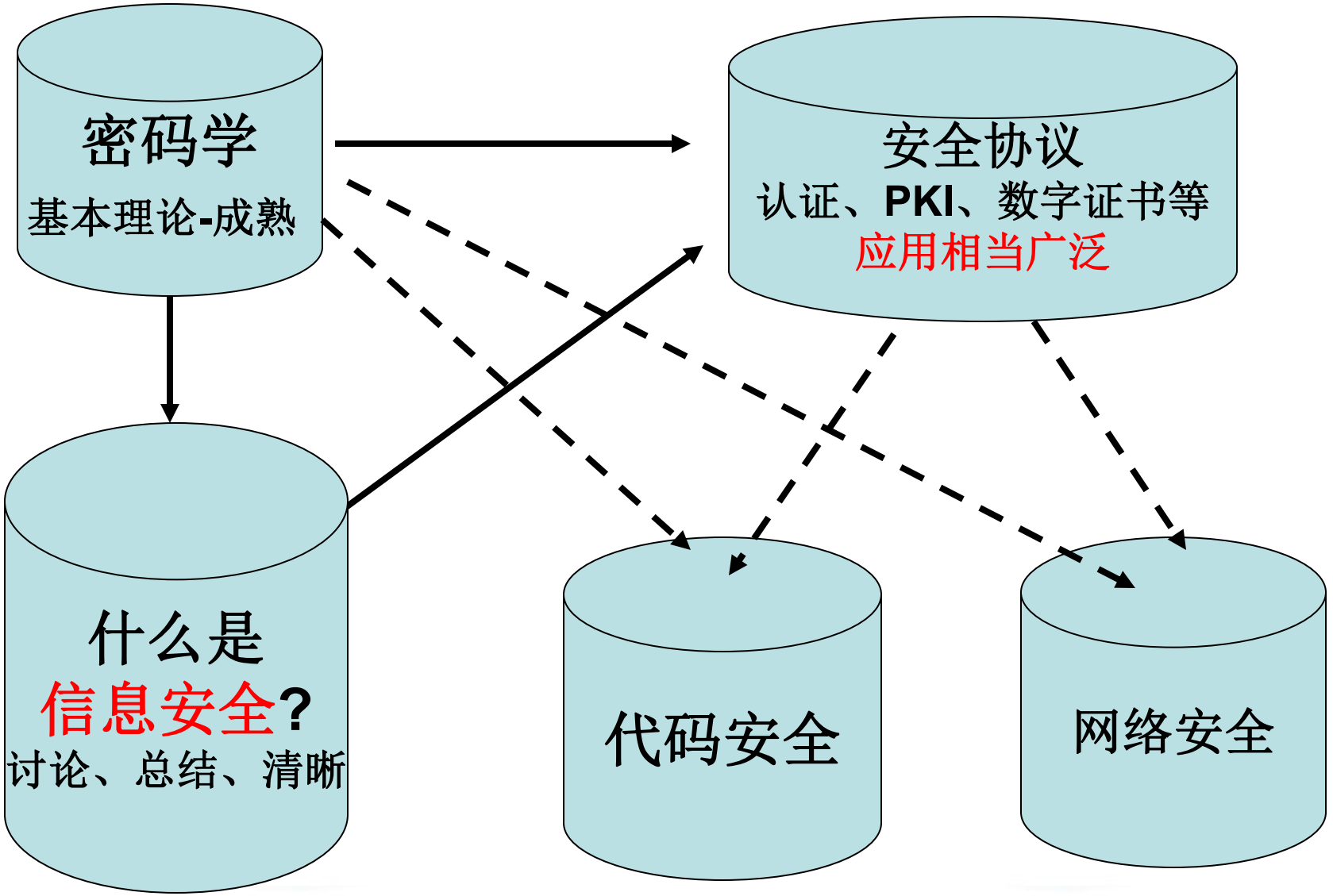
Information Security 06

The Intro to Information Security

—迟到的序言

Chapter1, 2, 3, 9, 11

内容间的联系


密码学
基本理论-成熟
安全协议
认证、PKI、数字证书等
应用相当广泛
什么是
信息安全?
讨论、总结、清晰
代码安全
网络安全

Content

- What is “Information Security”
- A brief history of Info sec
- Threats、Attacks and Defenses

Review

- Classic cipher
- Modern block cipher

→ Symmetric
one secret key

- Public Key cryptography

→ Asymmetric
two keys

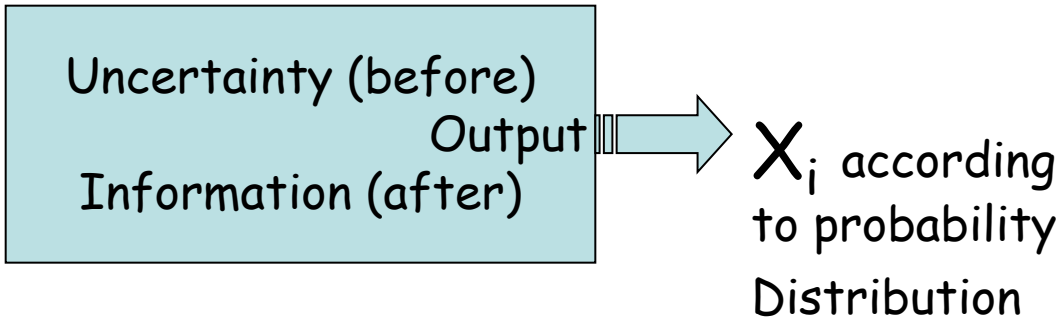
- MAC & Hash function

What is “Information”?

What is "Information"?

- **Definition:** Source is an ordered pair $\Psi = (S, P)$, where $S=\{x_1,\ldots,x_n\}$ is a finite set, the source alphabet, and P is the probability distribution on S. Denote the probability of x_i by p_i or $p(x_i)$

- Amount of
- Amount of



- Shannon 1945, Bell lab

Example for uncertainty

- 1) $\mathrm{p}(x_1) = 1, p(x_i) = 0, i > 1.$ The uncertainty is 0
- 2) $\mathrm{p}(x_i) = \frac{1}{n}, i = 1, \ldots, n.$ The uncertainty is Maxium
- 3) Uncertainty = Information

Example for uncertainty

- 1) $\mathrm{p}(x_1) = 1, p(x_i) = 0, i > 1.$ The uncertainty is 0
- 2) $\mathrm{p}(x_i) = \frac{1}{n}, i = 1, \ldots, n.$ The uncertainty is Maxium
- 3) Uncertainty = Information

$$\mathrm{H_b}(p_1, \cdots, p_n) = -\sum_{i=1}^{n} p_i \log_b p_i, b > 0$$

Units of Entropy

- H_b measures the number of b-ary units of information.
- Example 1. $S=\{x_1,x_2,x_3\}$, $p_i=1/3$, gives

$$H_2(\frac{1}{3},\frac{1}{3},\frac{1}{3}) = \frac{1}{3}\log_2 3+\frac{1}{3}\log_2 3+\frac{1}{3}\log_2 3$$
$$= \log_2 3 \approx 1.585 \text{ bits}$$

- Example 2. $p_1=p_2=1/4$, $p_3=1/2$ gives

$$H_2(\frac{1}{4},\frac{1}{4},\frac{1}{2}) = \frac{1}{4}\log_2 4+\frac{1}{4}\log_2 4+\frac{1}{2}\log_2 2$$
$$= 1.5 \text{ bits}$$

What is “Information System”?

What is “Information System”?

- Bearer of Info
  - 例: 烽火台
    - 周幽王烽火戏诸侯

What is “Information System”?

- Computer system is the one
- All aspects (bearer of Info)
  - Hardware
  - Software
  - Data (at rest and in transit)
  - People?

- ***C, I, A + Authentication & Non-repudiation***

What is “Information System”?

- Computer system is the one
- All aspects (bearer of Info)
  - Hardware
  - Software
  - Data (at rest and in transit)
  - People?
- **Assets** – the valuable stuff (not everything is an asset)

What is “Security”

- Confidentiality
  - **assets** *accessed* only by authorized parties
- Integrity
  - **assets** *modified* only by authorized parties or in authorized ways
  - Information is *precise, accurate, consistent, meaningful*
- Availability
  - **assets** *accessible* to authorized parties *at appropriate times*
  - provide *timely response*, *fair allocation of resources*, *quality of service*
  - opposite? denial of service

What is “Security”

- Basic Goals
  - ***C*onfidentiality**
  - ***I*ntegrity**
  - ***A*vailability**

- Added when people talk about “Information Assurance”
  - **Non-repudiation**: Messages or actions are accompanied by proof which cannot be denied
  - **Authentication**: Establishing the validity of a transmission, message, or originator (including verifying the identity of a participant)

Questions

- Which security services can be provided by the cryptography techniques?
- Why?

Other Terminologies

- *Vulnerability*
  - weakness in security system
- *Threat*
  - a set of circumstances with potential to cause harm
- for example
  - wall, crack (vulnerability), water (threat), person

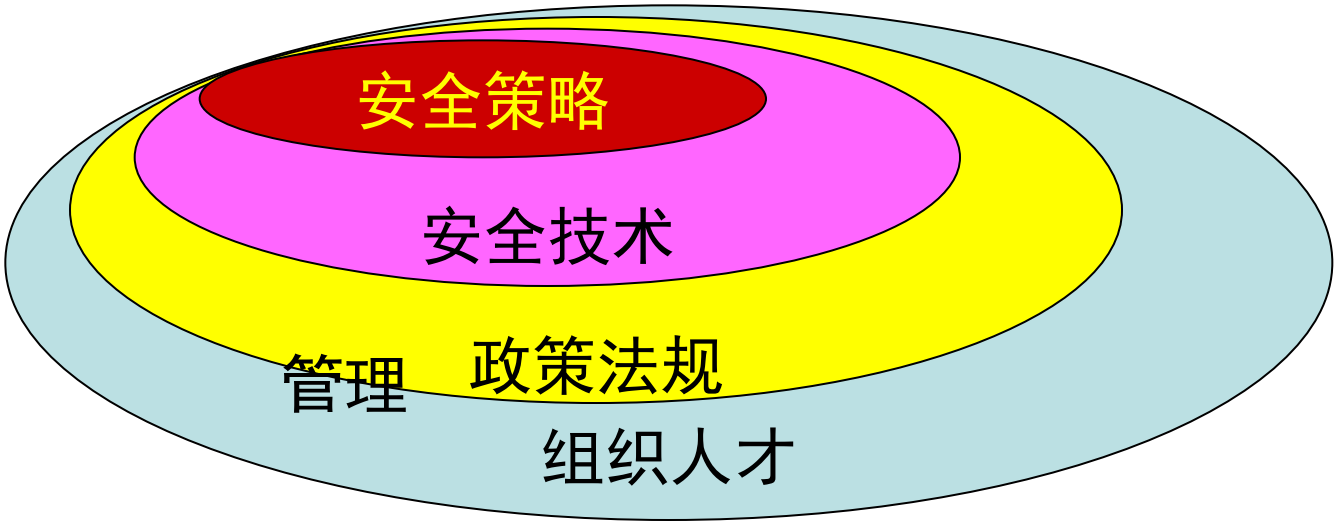
- *Attack* – exploit of a vulnerability
- *Control* – action, device, procedure or technique that removes or reduces vulnerability
- *Threat blocked by control of a vulnerability*

Content

- What is “Information Security”
  - **Security policy**
- A brief history of Info sec
- Threats、Attacks and Defenses

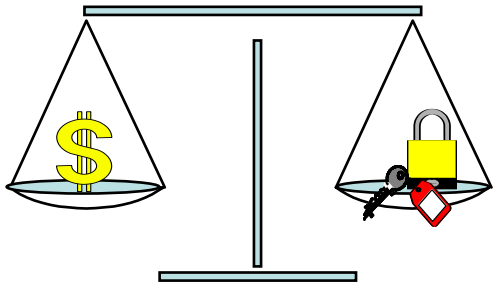
信息安全理念

- 安全不是纯粹的技术问题，是一项复杂的系统工程—信息安全工程论
- 安全是策略，技术与管理的综合



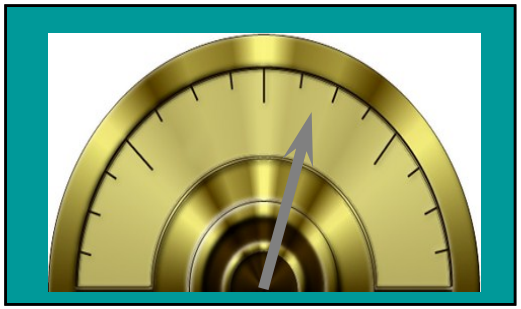
正确理解安全理念

- 两对“舍与得”



Access **Security**

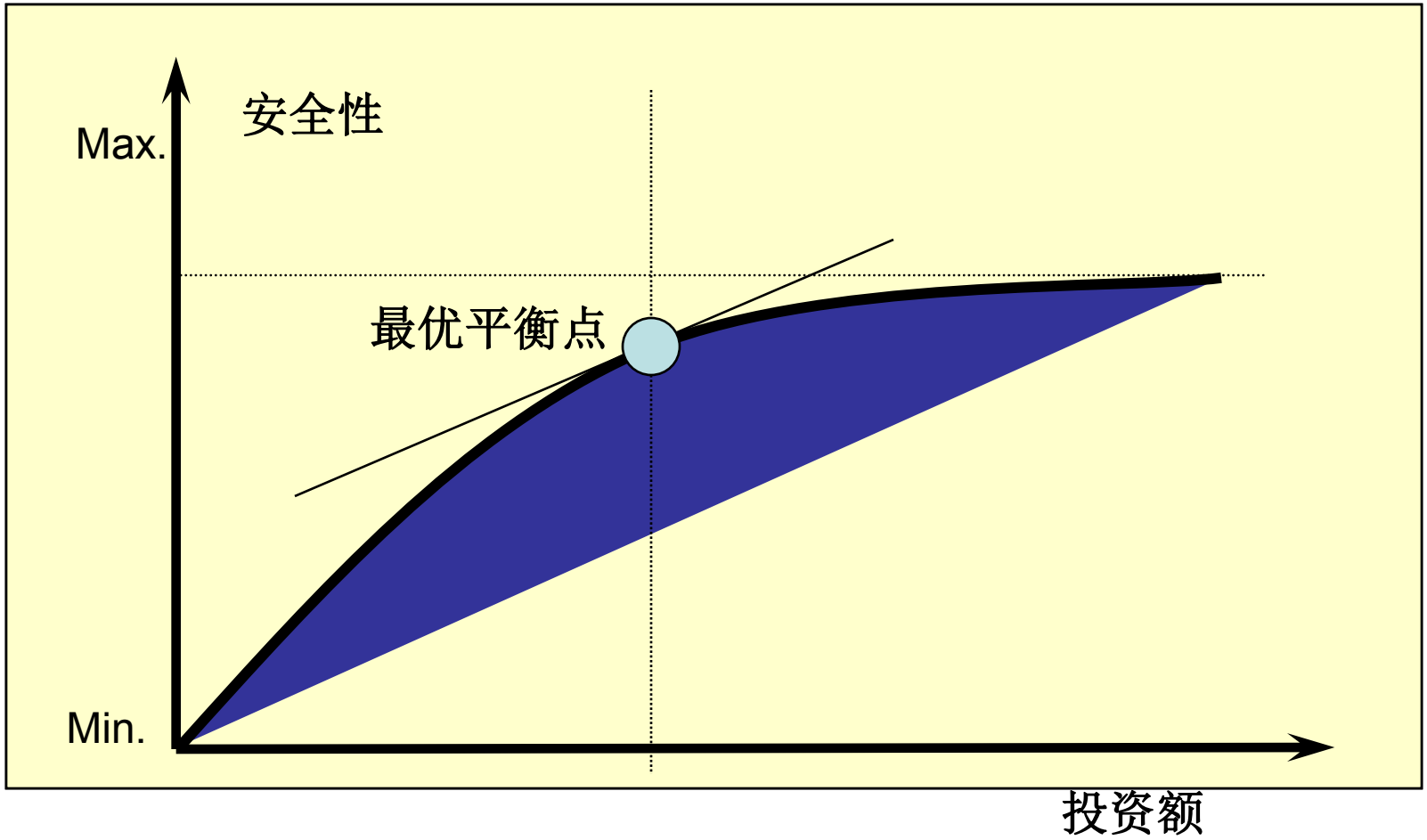
Connectivity
Performance
Ease of Use
Manageability
Availability



Authentication
Authorization
Accounting
Assurance
Confidentiality
Data Integrity

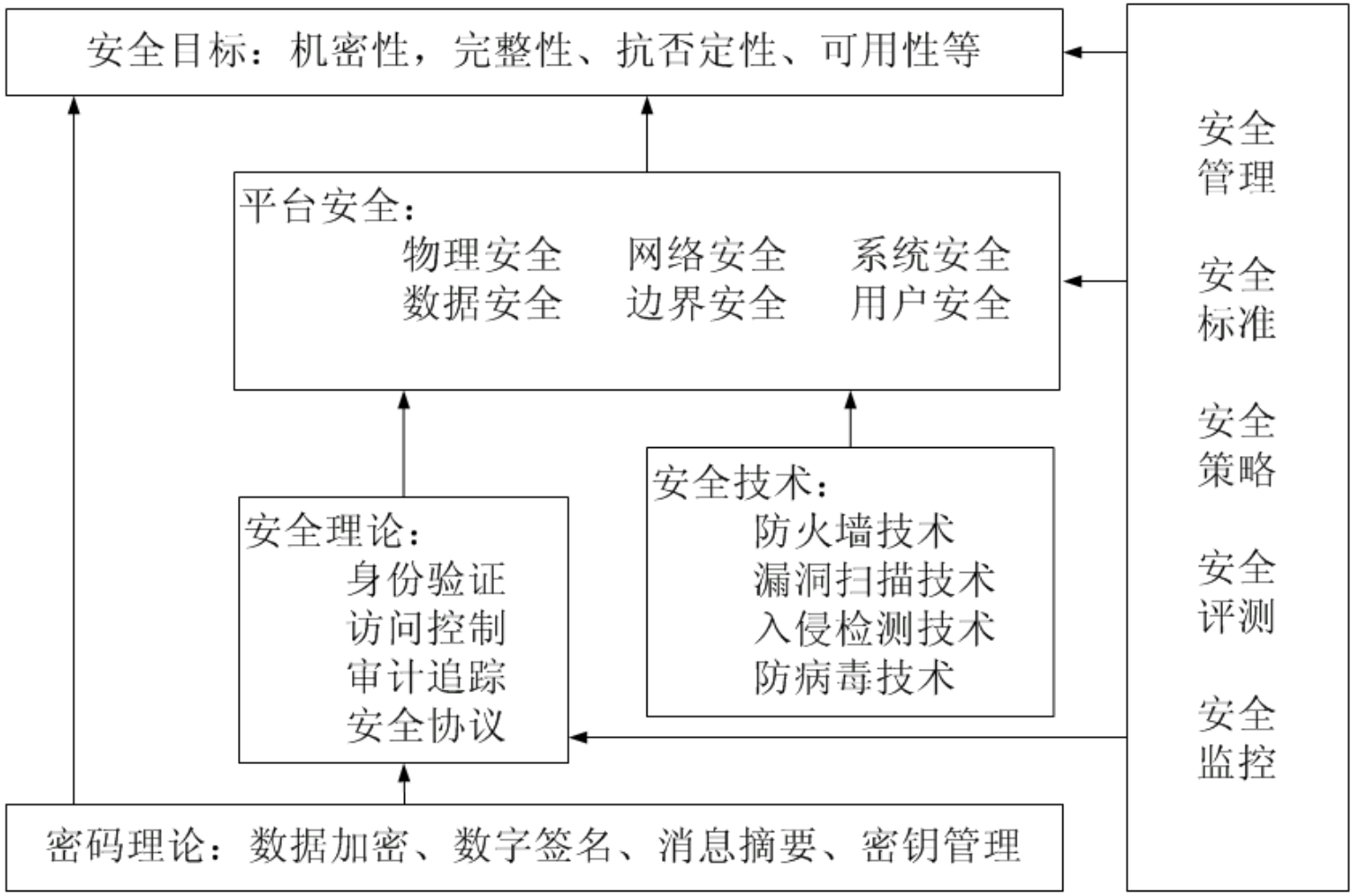
安全策略管理

理解安全理念...



信息安全学科内容

- 信息安全是一门交叉学科



Content

- What is “Information Security”
- A brief history of Info sec
  - **Controls-防御**
  - **Attacks-攻击**
- Threats、Attacks and Defenses

从“信息安全”概念的发展来看

- Communication Secrecy, 50s, 60s，
- Computer Security, 70s, 80s
- Information Security, 80s, 90s
- Information Assurance

军用 → 民用

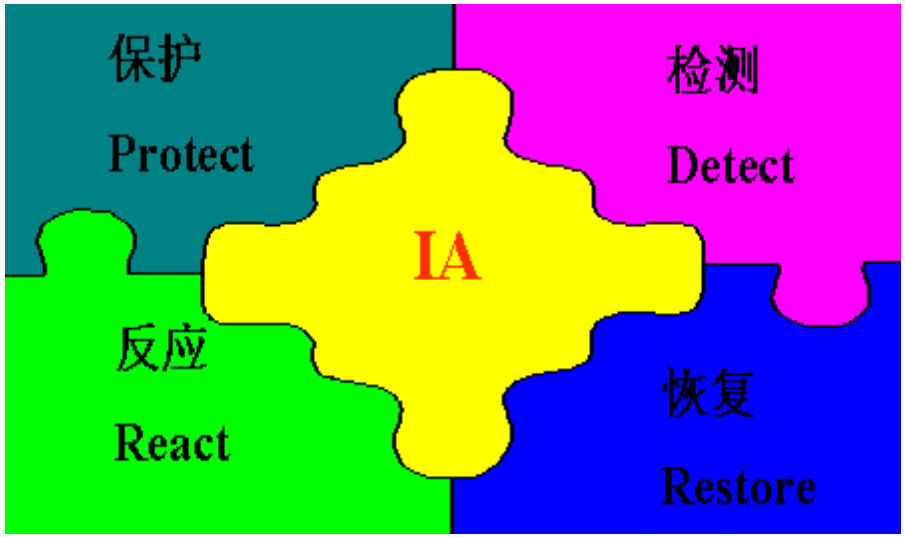
安全技术 = 军火

出口限制

注意两个时间点

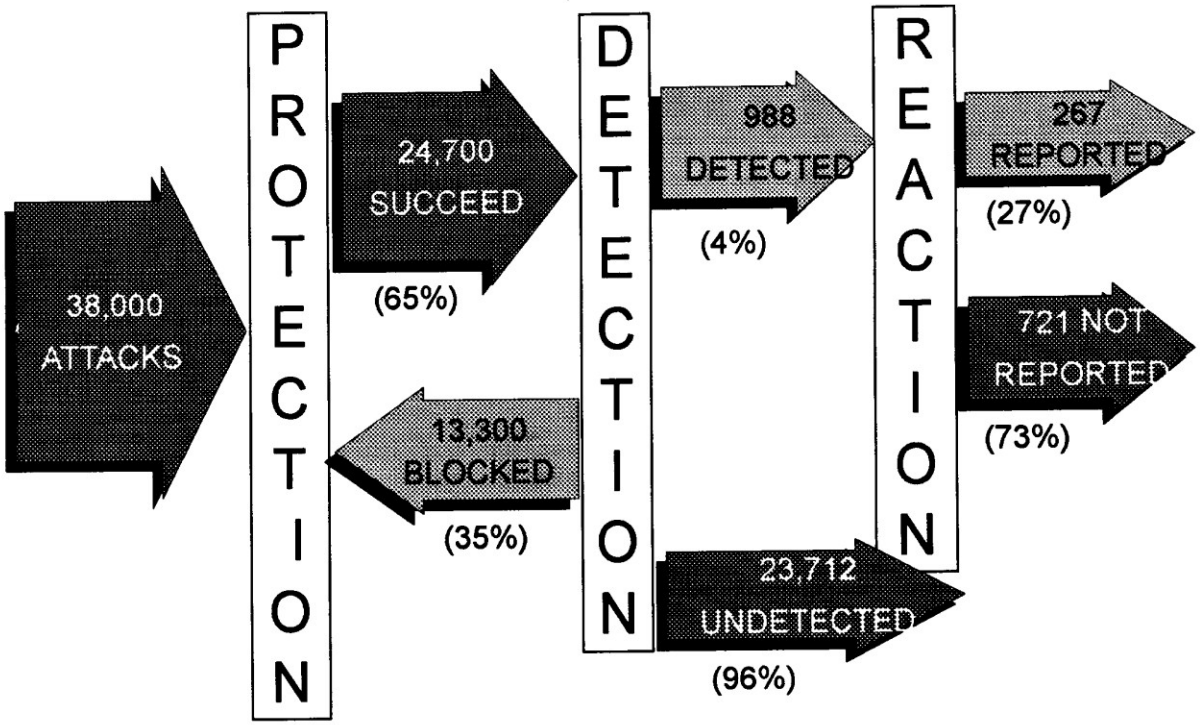
信息保障-PDRR模型

- 安全（security）：侧重于“防范潜在的威胁”。
- 保障（assurance）：更侧重于可用性和业务的连续性
- 信息保障（IA，Information Assurance）的核心思想是对系统或者数据的4个方面的安全要求（注意是有纵深的）：



PDRR保障体系

From RAND Report



Defense in Depth

- ***Definition***: Using multiple layers of security to protect against failure of individual controls.
- Non-computer example:
  - Multi-walled (or concentric) castles
- Computer security example:
  - Internal systems with access control protections, on an internal network with an intrusion detection system, with connections from outside controlled by a firewall.

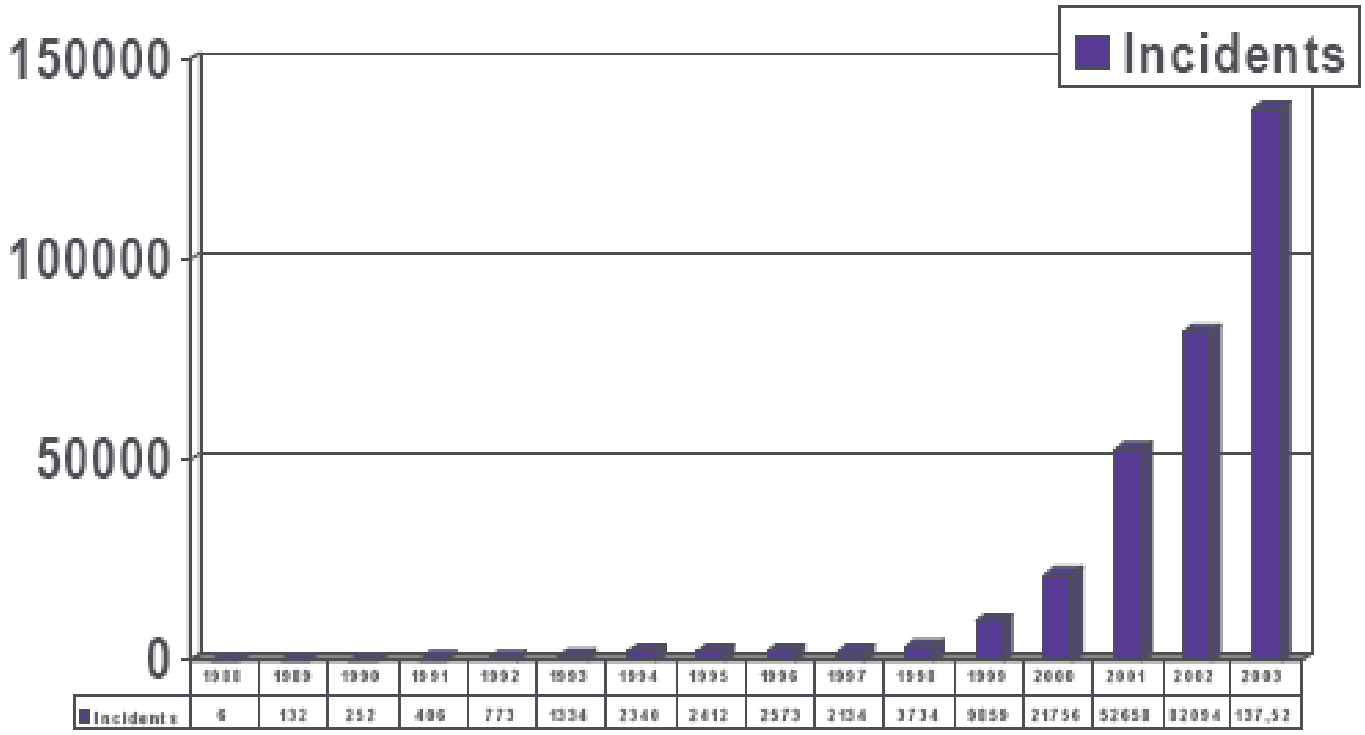
Some History

- **1967**: People starting to publish papers on computer security
- **1970**: Influential (in some circles!) RAND report: "Security Controls for Computer Systems"
  - Originally classified – declassified in 1979
- **1964—1974**?: MULTICS system development
- **Mid-70's**: Many influential papers published in open literature
- **Mid-70's**: Cryptography takes off in public research
- **1985**: Department of Defense publishes "Trusted Computer System Evaluation Criteria" (Orange Book)
- **1994**: Publication of "Common Criteria for Information Technology Security Evaluations"
- **2003**: Publication of "The National Strategy to Secure Cyberspace"

Content

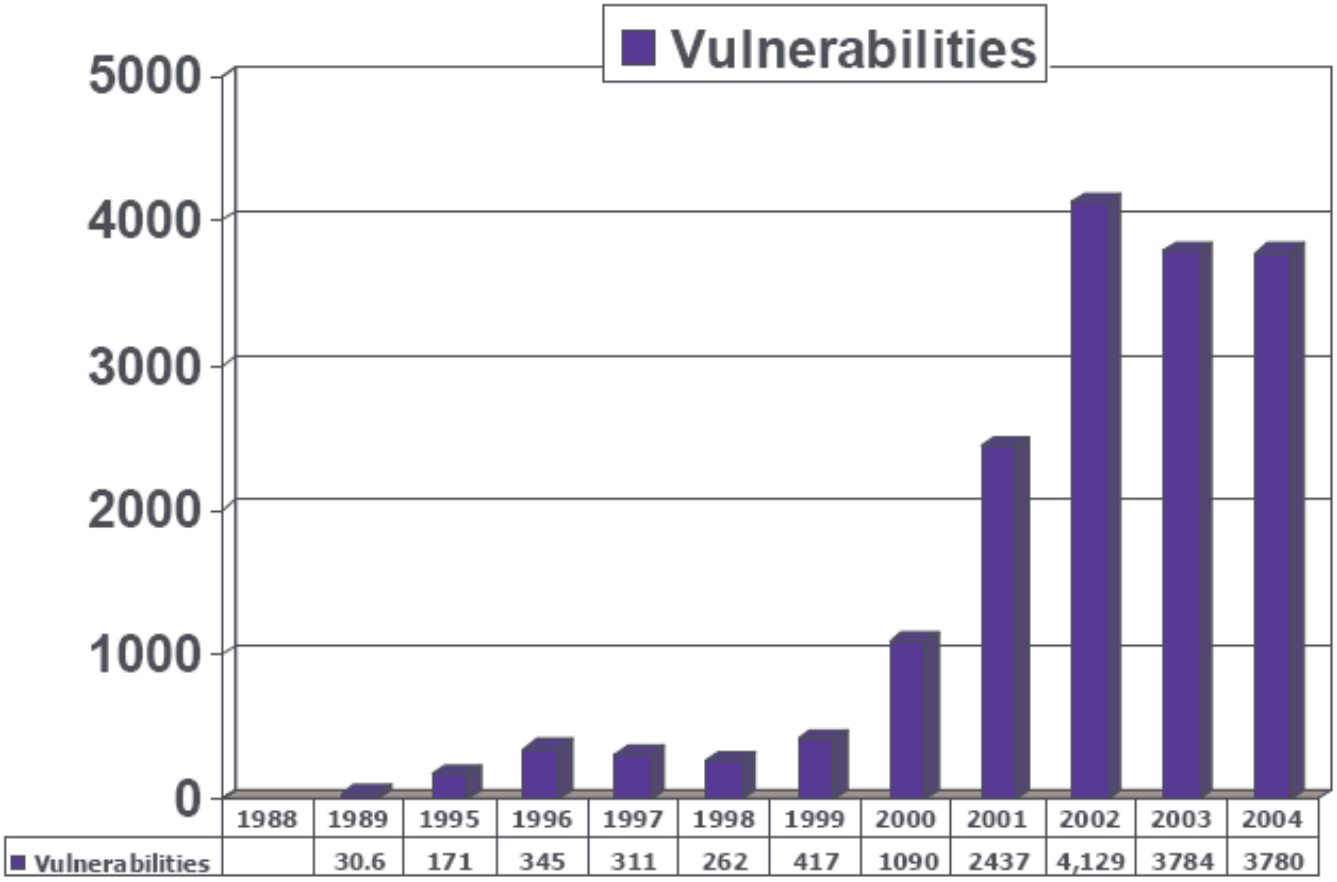
- What is “Information Security”
- A brief history of Info sec
  - Controls-防御
  - **Attacks-攻击**
- Threats、Attacks and Defenses

Security Incidents



Source: CERT

Security Vulnerabilities



	1988	1989	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004
Vulnerabilities		30.6	171	345	311	262	417	1090	2437	4,129	3784	3780

Some History – The Other Side

- **1970's**: Age of phone phreaking
- **1986**: First PC virus in the wild (the "Brain virus")
- **1988**: The "Morris worm"
  - Automated spreading across the Internet
  - Exploited several bugs, including the first highly-visible "buffer overflow" exploit (of fingerd)
  - Around 6000 computers affected – 10% of the Internet at the time!
  - Morris convicted in 1990
  - CERT created largely because of this

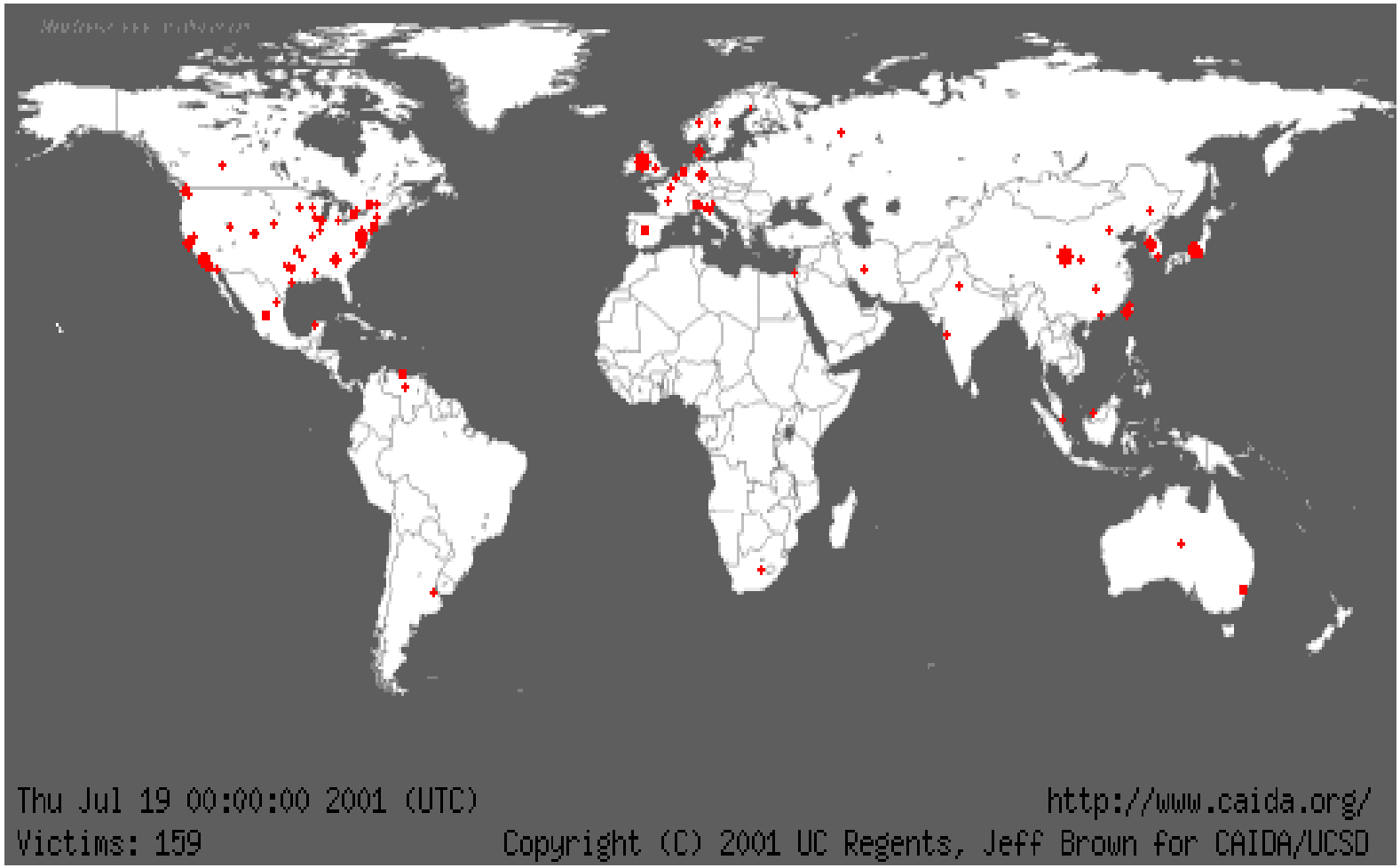
Some History – The Other Side

- **1999** – **present**: Widespread worms/viruses
  - 1999: Melissa (Word macro virus/worm)
  - 2000: Love Letter (VBScript – did damage!)
  - 2001: Nimda (hit financial industry very hard)
  - 2001: Code Red (designed to DoS the White House, but hard-coded IP address so defeated!)
  - 2003: "Slammer" (spread astoundingly fast!)
- **1999**: DDoS networks appear
  - 2000: Big attacks on Yahoo, eBay, CNN, …
  - Today: "Bot-nets" with 10's of thousands of bots

How bad is it?

- September 2001 - Nimbda worm spread nationwide in less than an hour and attacked 86,000 computers
- January 2003 – Sapphire/Slammer SQL worm was able to spread nationwide in less than 10 minutes, doubling in size every 8.5 seconds. At its peak (3 minutes after its release) it scanned at over 55 million IP addresses per second, infecting 75,000 victims

Geographic Spread of Code Red Worm



Why is it so bad?

- Computers are everywhere
- Internet has become a mission-critical infrastructure for business, government, and financial institutions
- Today's networks are very heterogeneous, highly critical applications run side by side with noncritical systems
- Cyber attacks against non-critical services may produce unforeseen side-effects of devastating proportions

Why is it so bad?

- Home Users Increase Vulnerabilities
- Today most homes are connected, particularly with the advent of DSL and cable modems
- Most home users:
  - are unaware of vulnerabilities
  - don't use firewalls
  - think they have nothing to hide or don't care if others get their data
  - don't realize their systems can serve as jump off points for other attacks (*zombies*)

Why is it so bad?

- Computer security is reactive
  - usually too slowly to react to latest attack
  - offense is easier than defense
- Security is expensive both in dollars and in time
- There is not now, and never will be, a system with perfect security
  - the capacity of human beings
    - Windows 3.1 →3,000,000 lines
    - Windows 2000 → 50,000,000 lines

Content

- What is “Information Security”
- A brief history of Info sec
- Threats、Attacks and Defenses
  - Attacks
  - Threats
  - controls

Other Terminologies

- *Vulnerability*
  - weakness in security system
- *Threat*
  - set of circumstances with potential to cause harm
- for example
  - wall, crack (vulnerability), water (threat), person

- *Attack* – exploit of a vulnerability
- *Control* – action, device, procedure or technique that removes or reduces vulnerability
- *Threat blocked by control of a vulnerability*

Who are the attackers?

- **Script kiddies** download malicious software from hacker web sites
- **Hackers** trying to prove to their peers that they can compromise a specific system
- **Insiders** are legitimate system users who access data that they have no rights to access
- **Organizational level attackers** use the full resources of the organization to attack

Attacks and Attackers

- An *attack* is when a vulnerability is exploited to realize a threat
- An *attacker* is a person who exploits a vulnerability
- Attackers must have *M*eans, *O*pportunity, and *M*otive (*MOM*)
  - Means: Often just an Internet connection!
  - Opportunity: Presence of vulnerabilities
  - Motive may be complex, or not what you think!

Attackers – Motives

- Intellectual challenge
  - Some people see it as a game
- Espionage (government or corporate)
- Financial reward
  - Credit card numbers sold, spam-nets rented, fraud, ...
- Revenge
- Showing off
  - DDoS attacks on CNN, eBay, Yahoo, etc.
- Civil disobedience
  - Basic vandalism
  - “Hactivism”

Attackers – Types

- Amateurs
  - Could be ordinary users (insiders) exploiting a weakness
  - Sometimes accidental discoveries
- Crackers
  - People looking specifically to attack
  - Motive is often challenge, not malice
  - Skill level ranges from very low (script kiddie) to high
- Career criminals
  - Organized crime beginning to get involved
  - Terrorists? (Cyber-terrorism)
- Government/military information warfare

Threats to Confidentiality

- Interception/Eavesdropping/Wiretapping (sniffers)
  - Used to be commonly installed after a system break-in
  - Can (could?) capture passwords, sensitive info, ...
  - Has always been a problem with wireless transmission!
  - Electromagnetic emanations (TEMPEST security)
- Illicit copying (proprietary information, etc.)
  - Copied company documents, plans, ...
  - Copied source code for proprietary software
  - Non-electronic: “dumpster diving”, social engineering

Threats to Integrity

- Modification
  - Changing data values (database)
  - Changing programs
    (viruses, backdoors, trojan horses, game cheats, ...)
  - Changing hardware (hardware key capture, ...)
  - Can be accidental corruption (interrupted DB transaction)
  - Many small changes can be valuable (e.g., salami attack)
- Fabrication
  - Spurious transactions
  - Replay attacks
- Identity spoofing
  - Somewhat related: fake web sites and “phishing”

Threats to Availability

- Denial of Service (DoS)
  - Commonly thought of as network/system flooding
  - Can be more basic: disrupting power
  - Deleting files
  - Hardware destruction (fire, tornado, etc.)
- Distributed Denial of Service (DDoS)
  - Bot-nets of zombie machines that can be commanded to flood and disable “on-command”
  - Discovery of botnets with 10-100 systems is a daily occurrence; 10,000 system botnets are found almost weekly; and one botnet with 100,000 hosts has even been found (according to Johannes Ullrich, CTO of the Internet Storm Center).

Defenses and Controls

- Business motivation: Manage risk
  - Risk is the possibility for harm to occur
  - Main purpose: Balance risk with costs
- Risk Analysis:
  - Determine what controls are most cost-effective
  - Most “bang for the buck”
- Security policy:
  - a statement of what is and what is not allowed,
  - May be informal (English statements) or formal (mathematical logic statements)
- Methods of Controls
  - Risks can be prevented, deterred, detected and responded to, transferred, or accepted

Controls – Examples

- A Web Site for a Small Company
  - Business requirements
  - Risk analysis?
  - Security policy?
  - Controls?

Controls – Examples

- Cryptography
- Access Control
  - Operating System controls (file rights, capabilities, ...)
  - Application access restrictions (DB, web server, ...)
  - Network boundary (firewall, VPN, ...)
  - Authentication (pw, advanced: smart cards, tokens, ...)
- Network Security
  - Detection programs (IDS, virus scanners)
  - Regularly test/evaluate (called “penetration testing”)
- Software Security
  - Development controls (secure software development)
- Physical controls (door locks, media management)
- ??

We have done

- Cryptography
  - mathematical foundation of many controls

- Project 1
  - terminology (need to know definitions)
  - application of terms (can you use terms)
  - class material (are you paying attention)

C, I, A分类

- 小李拷贝了小王的作业
- 小李让小王的计算机崩溃了
- 小李将小王的支票从100元修改到1000元
- 小李冒用死去的老张的签名
- 小李注册了一个域名www.fudan.org，并拒绝复旦大学购买并且使用这个域名
- 小李得到小王的信用卡卡号并让信用卡公司删除这个卡，然后重新办理了新的卡，并使用原有卡的信用
- 小李哄骗小王计算机的IP检测，得到了访问小王计算机的访问许可

机密性

- **机密性**是指保证计算机相关的有价值财产（信息）只能被授权过的用户所访问。
- 机密性的保护
  - 认证和访问控制
  - 加密

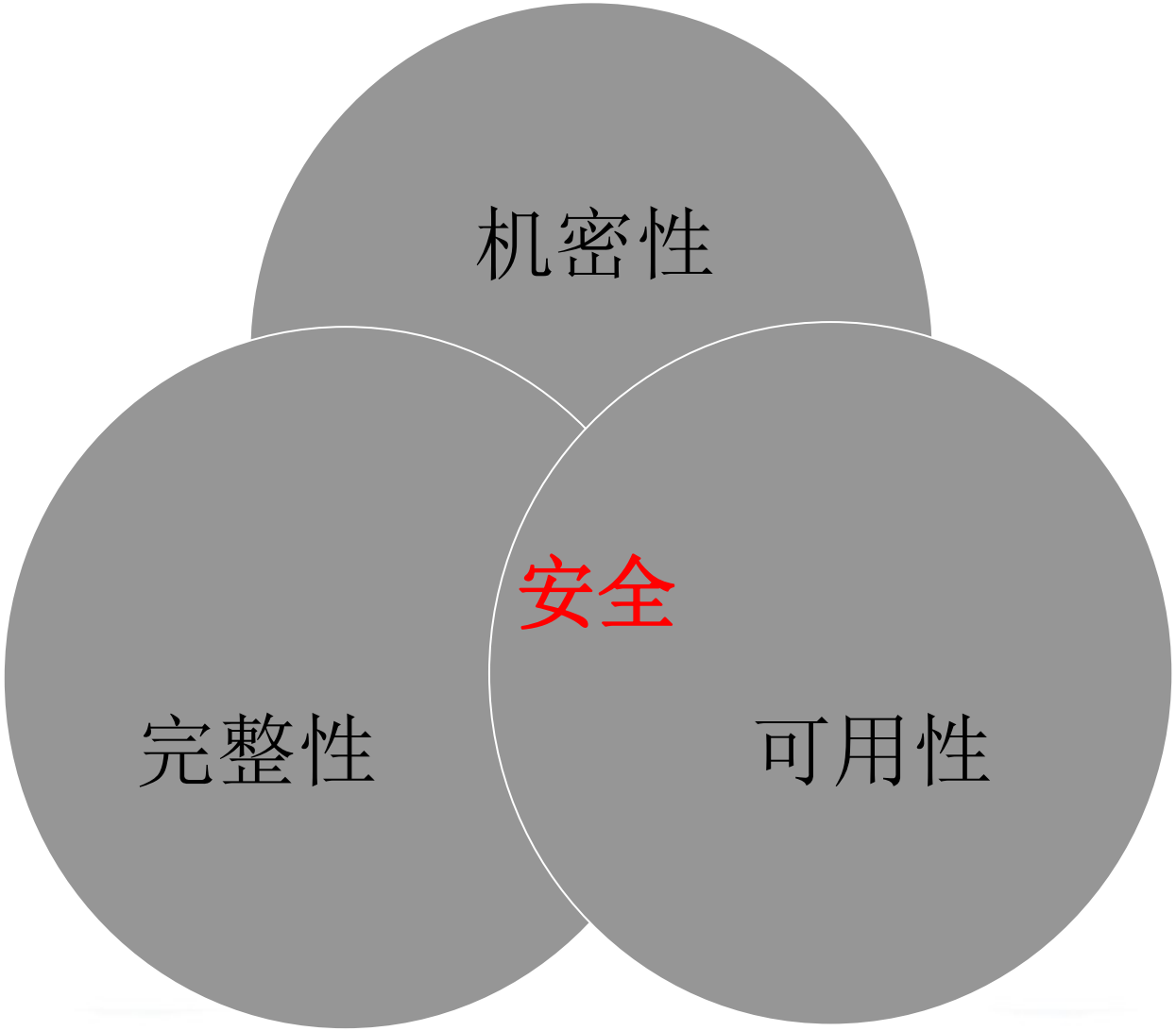
完整性

- **完整性**是指这些计算机相关的有价值财产（信息）只能被授权过的用户所修改，或者通过授权过的过程所修改。
- 完整性的保护
  - 认证和访问控制
  - 加密

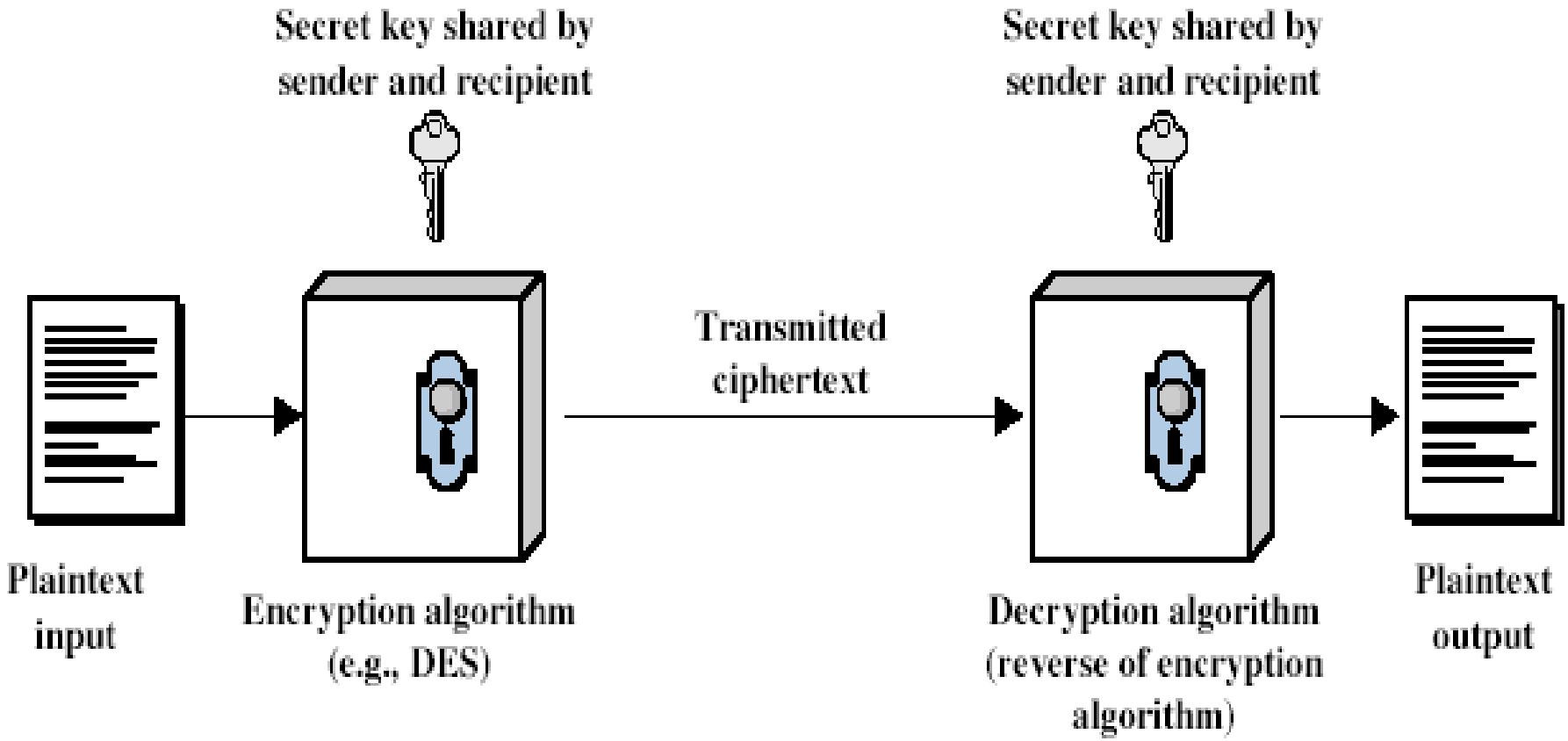
可用性

- **可用性**是指这些有价值的财产（信息）在需要的时候必须能够被授权的用户访问或者修改。
- 可用性的破坏
  - DOS: Denial Of Service

机密性，完整性和可用性及其之间的关系



Review: Symmetric Model



Asymmetric Model