Introduction to Information Security

Lecture 1: Introduction & Overview

2007. 6.

Prof. Byoungcheon Lee
sultan (at) joongbu . ac . kr

Information and Communications University

About Myself

- **Prof. Byoungcheon Lee**
  - ✓ **Dept. of Information security in Joongbu university**
  - ✓ **E-mail : sultan (at) joongbu . ac . kr**
  - ✓ **Homepage: http://cris.joongbu.ac.kr**
  - ✓ **Mobile : 0 1 7 – 4 1 0 – 9 5 0 9**

  - ✓ **BS and MS in Seoul National Univ.**
  - ✓ **Researcher in LG-CRT**
  - ✓ **Ph.D in information security in ICU, 2002**
  - ✓ **Researcher (visiting professor) in Queensland Univ. of Technology (2003.7-2004.6)**
  - ✓ **Program chair of ICISC2006 conference**
  - ✓ **Asiacrypt Steering Committee member**
  - ✓ **Listed in the Marquis Who's Who in Asia 2007 and in the World 2007**

Contents

1. Basic Terms

Lots of new terminologies in every new fields…

What is Information Security?

- Data
  - recording of “something” measured
  - Raw material, just measured
- Information
  - Information is the result of processing, manipulating and organizing data in a way that adds to the knowledge of the receiver.
  - Processed data
- Knowledge
  - Knowledge is normally processed by means of structuring, grouping, filtering, organizing or pattern recognition.
  - Highly structured information

What is Information Security?

- **Information Systems**
  - **An integrated set of components for collecting, storing, processing, and communicating information.**
  - **Business firms, other organizations, and individuals in contemporary society rely on information systems to manage their operations, compete in the marketplace, supply services, and augment personal lives.**

- **Information Revolution**
  - **A phrase we use to refer to the dramatic changes taking place during the last half of the 20th century in which service jobs based on information are more common than jobs in manufacturing or agriculture.**
  - **Information becomes more and more important than materials, resources.**

- **Competitiveness comes from information**
  - **How much information do you have?**

What is Information Security?

- **Information Security (정보보안, 정보보호)**
  - **Information security is the process of protecting information from unauthorized access, use, disclosure, destruction, modification, or disruption**
  - **The protection of computer systems and information from harm, theft, and unauthorized use.**
  - **Protecting the confidentiality, integrity and availability of information**
  - **Information security is an essential infrastructure technology to achieve successful information-based society**
  - **Highly information-based company without information security will lose competitiveness**

- **What kind of protection?**
  - **Protecting important document / computer**
  - **Protecting communication networks**
  - **Protecting Internet**
  - **Protection in ubiquitous world**

Cryptology = Cryptography + Cryptanalysis

- **Cryptography : designing secure cryptosystems**
  - **Cryptography (from the Greek kryptós and gráphein, "to write") was originally the study of the principles and techniques by which information could be concealed in ciphers and later revealed by legitimate users employing the secret key.**
- **Cryptanalysis : analyzing the security of cryptosystems**
  - **Cryptanalysis (from the Greek kryptós and analýein, "to loosen" or "to untie") is the science (and art) of recovering or forging cryptographically secured information without knowledge of the key.**
- **Cryptology : science dealing with information security**
  - **Science concerned with data communication and storage in secure and usually secret form. It encompasses both cryptography and cryptanalysis.**

Cryptology

- Cryptography is a basic tool to implement information security
- Security goals
  - Secrecy (confidentiality)
  - Authentication
  - Integrity
  - Non-repudiation
  - Verifiability
  - More application-specific security goals
- Achieve these security goals using cryptography
- Without cryptography …. ???

Common Terms (1)

- Cryptography(암호설계): The study of mathematical techniques related to aspects of information security
- Cryptanalysis(암호분석): The study of mathematical techniques for attempting to defeat cryptographic techniques
- Cryptology(암호학): The study of cryptography and cryptanalysis
- Cryptosystem(암호시스템): A general term referring to a set of cryptographic primitives used to provide information security
  - Symmetric key primitives; Public key primitives
- Steganography: The method of concealing the existence of message

❖ Cryptography is not the only means of providing information security, but rather one set of such techniques (physical / human security)

Common Terms (2)

- Cipher: Block cipher, Stream cipher, Public key cipher
- Plaintext/Cleartext (평문), Ciphertext (암호문)
- Encryption/Encipherment(암호화)
- Decryption/Decipherment(복호화)
- Key (or Cryptographic key)
  - Secret key
  - Private key / Public key
- Hashing (해쉬)
- Authentication (인증)
  - Message authentication
  - User authentication
- Digital signature (전자서명)

Security Threats

- Interruption/Denial of service
- Interception: eavesdropping, wiretapping, theft …
- Modification
- Fabrication/Forgery
- Unauthorized access
- Denial of facts

Security Services

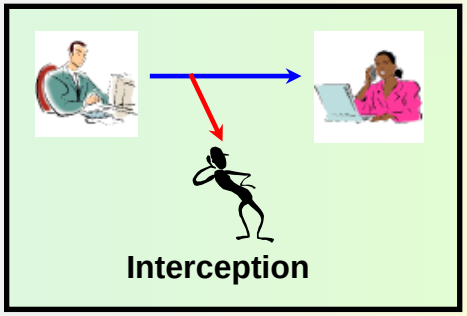
- Security services
  - A service that enhances information security using one or more security mechanisms

- Confidentiality/Secrecy (기밀성) ↔ Interception
- Authentication (인증성) ↔ Forgery
- Integrity (무결성) ↔ Modification
- Non-repudiation (부인방지) ↔ Denial of facts

- Access control (접근제어) ↔ Unauthorized access
- Availability (가용성) ↔ Interruption

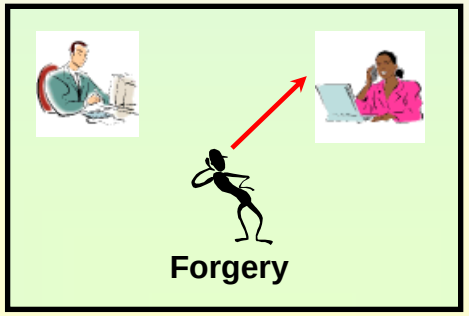
Security Needs for Network Communications

Confidentiality



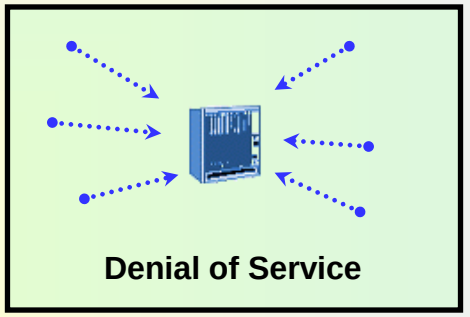
Is Private?

Authentication



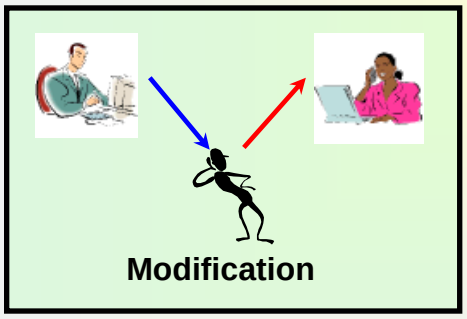
Who am I dealing with?

Availability



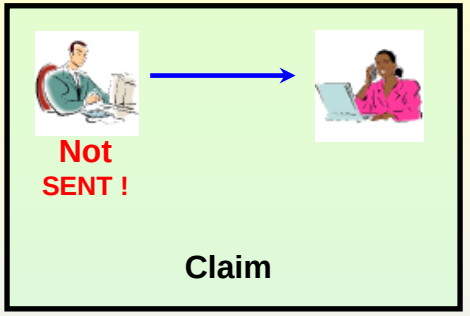
Wish to access!!

Integrity



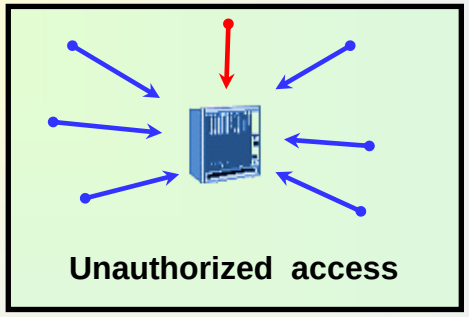
Has been altered?

Non-Repudiation



Who sent/received it?

Access Control



Have you privilege?

Security Mechanisms

- Security mechanism
  - A mechanism designed to detect, prevent, or recover from a security attack

- Encryption
- Authentication
- Digital signature
- Key exchange

- Access control
- Monitoring & Responding

Models for Evaluating Security

- Conditional vs. Unconditional Security
  - Unconditional security
  - Computational security

- Provable vs. Ad hoc Security
  - Provable security
  - Ad hoc security

Attacks

- Attacks
  - An efficient algorithm that, for a given cryptographic design, enables some protected elements of the design to be computed "substantially" quicker than specified by the designer.
  - Finding overlooked and realistic threats for which the design fails
- Attacks on encryption algorithms
  - Exhaustive search (brute force attack)
  - Ciphertext-only attack
  - Known-plaintext attack
  - Chosen-plaintext attack
  - Chosen-ciphertext attack

2. Quick Overview on Information Security

What is the Internet?

- Collection of networks that communicate
  - with a common set of standard protocols (TCP/IP)
  - by multilateral agreement
- Collection of networks with
  - no central control
  - no central authority
  - no common legal oversight or regulations
  - no standard acceptable use policy
- Physical network connections not important
  - leased lines, dial-up, wireless
- Logical connectivity
  - everything is connected to everything else

Internet Security Issues

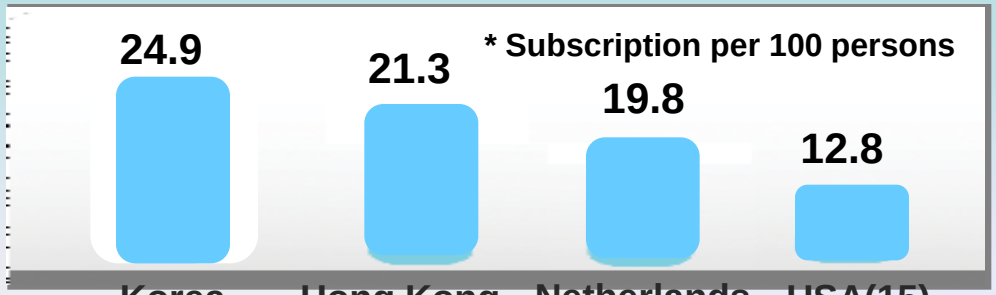
- **Internet Infrastructure is Inherently Insecure**
  - Security was not a design consideration of Internet protocols
  - Unauthenticated routing protocols control Internet reachability
  - Add-on security is hard on users and hard to integrate into applications
- **Increasing Complexity of Network & Applications**
  - Increasing complexity of network connectivity
    - Varying collection of ISPs, Wireless WAN/LAN, Home networking …
    - Dial-up, DSL, Cable modem, Wireless, Satellite, Power line …
  - Increasing complexity of network protocols & applications
    - Peer-to-peer networking protocols, multimedia over IP
  - Internet everywhere: More complexity of management
    - Mobile phones, home appliances ...
  - Complexity is the Worst Enemy of Security & Management

Internet Security Issues

- **More Distributed Networking / Applications Emerging**
  - Distributed file sharing/computing
  - Peer-to-peer networking, Home networking
  - Ubiquitous computing
- **Vulnerable Software Everywhere**
  - Vulnerability in software is inevitable and continues to appear
  - Vulnerable security products deployed
- **Sophistication & Automation of Attack Tools**
  - Attack tools / toolkits are becoming more sophisticated, automated, easy to use & hard to trace back
  - No specific knowledge required to mount attacks
  - Global collaboration is essential

Current IT Penetration in Korea

Global broadband penetration



Korea's broadband penetration

House-holds

- Penetration: 12MM (71%)
- Usage of Internet: 32MM (72%)

Schools

- All primary&secondary schools connected to broadband(2000)

Korea's wireless penetration

- Wireless Internet: 9MM (20%)

1998 → 2005

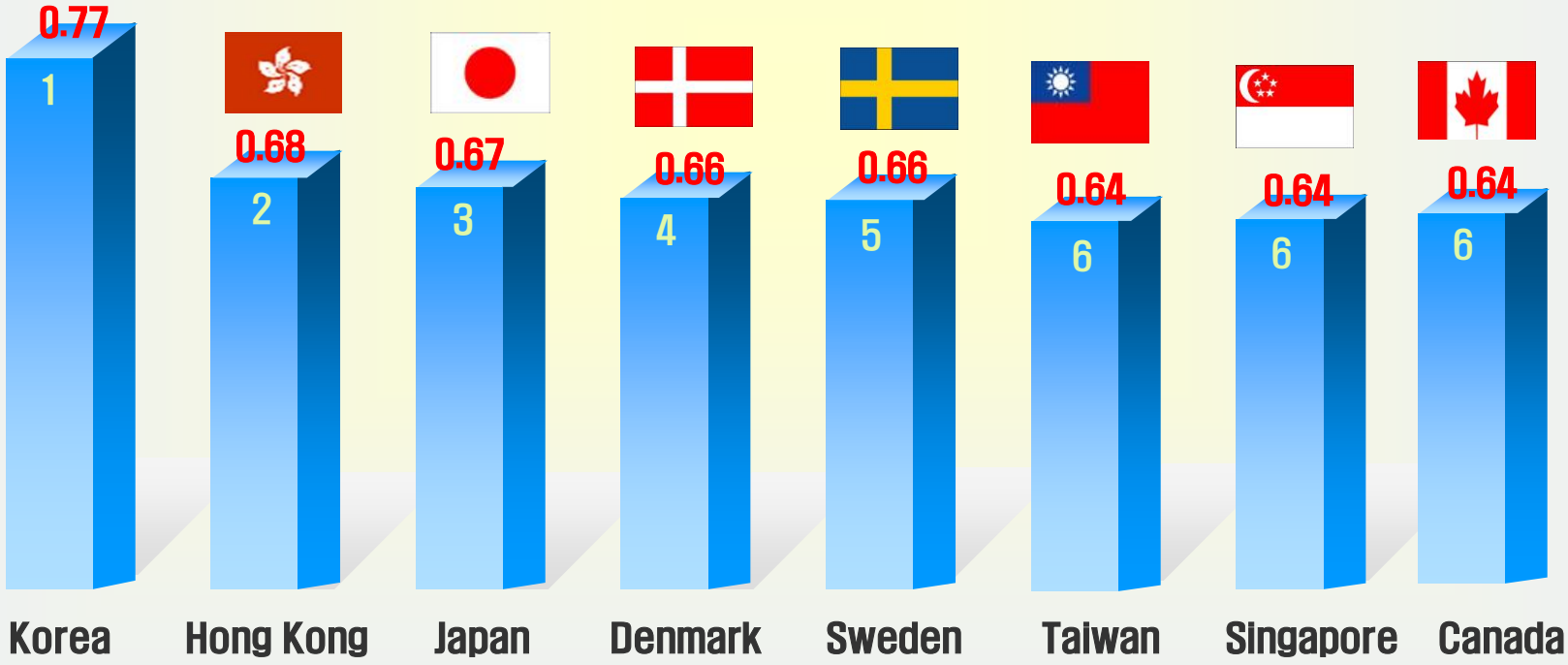
Digital Multimedia Broadcasting (DMB)
Ring back tone service
Location Based Service (LBS)
Short Message Service (SMS)
Mobile game
Ring tone download

Digital Opportunity Index

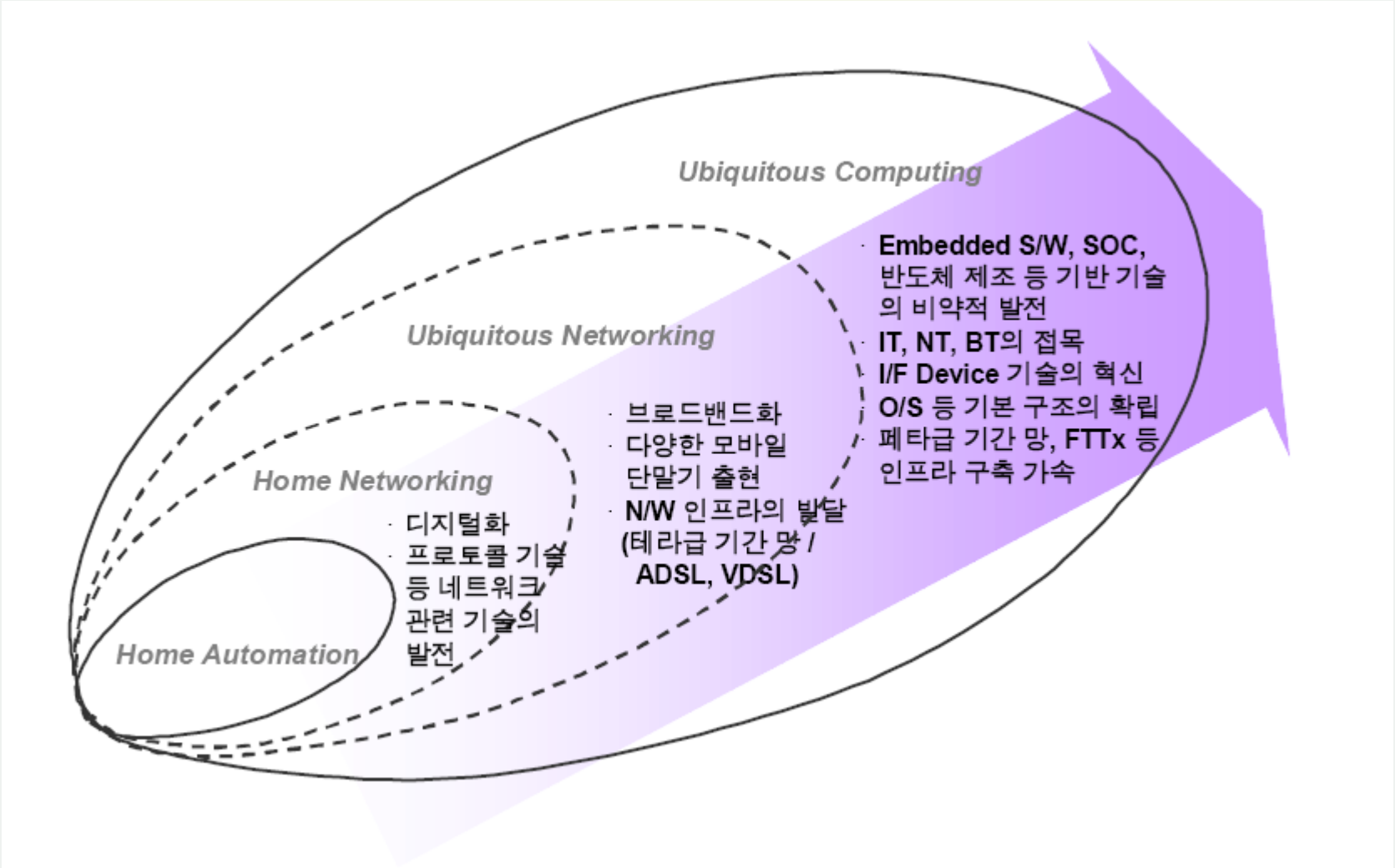
Adoption and Access to ICT

- Excellent in Infrastructure, Utilization, and Opportunity

Source: ITU WSIS (Nov. 2005)



Ubiquitous Computing

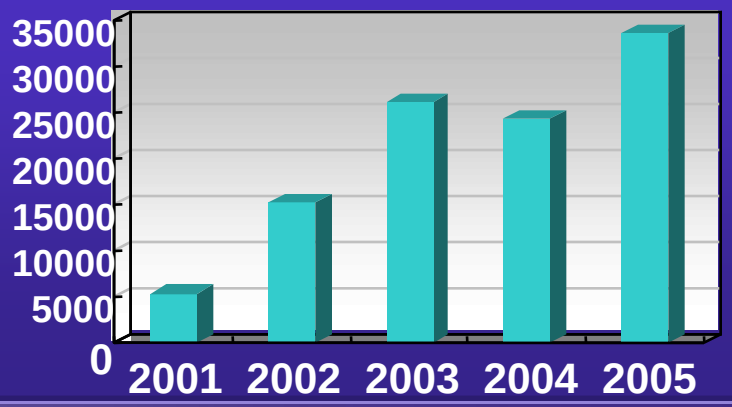


Security Threats

- **Passive**
  - **Sniffing**
  - **Wiretap**
  - **TEMPEST : detecting information from Transient Electromagnetic Pulse**
  - **Social Engineering**
- **Active (Program)**
  - **Worm (independent) : program that replicates itself through network**
  - **Logic bomb : malicious instructions that trigger on some event in the future, such as a particular time occurring**
  - **Trojan horse : program that does something unexpected (and often secretly)**
  - **Trapdoor : an undocumented entry point intentionally written into a program, often for debugging purposes, which can be exploited as a security flaw**
  - **Virus : program fragment that, when executed, attached itself to other programs**

Top Security Problems

Hacking



Web Modification

Rank	04	05
1	USA	USA
2	German	India
3	Korea	China
4	England	Brazil
10	France	Korea

Phishing Hosting

Rank	04	05
1	USA	USA
2	China	Korea
3	Korea	China
4	Japan	German
5	Canada	England

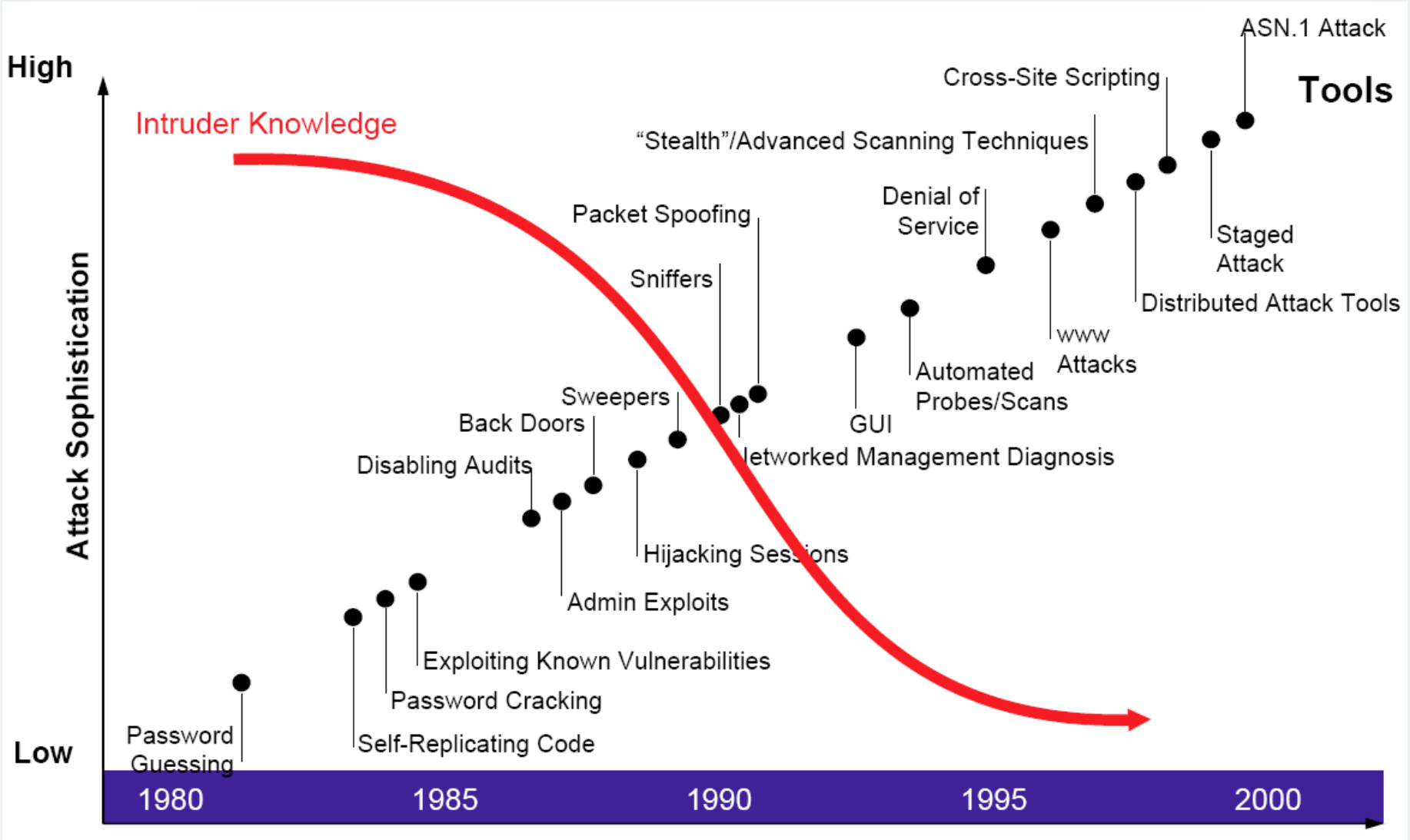
Source: www.antiphishing.org

Bot

Rank	04	05
1	England	USA
2	USA	England
3	China	China
5	Canada	Korea
9	Korea	German

Source: www.symantec.com

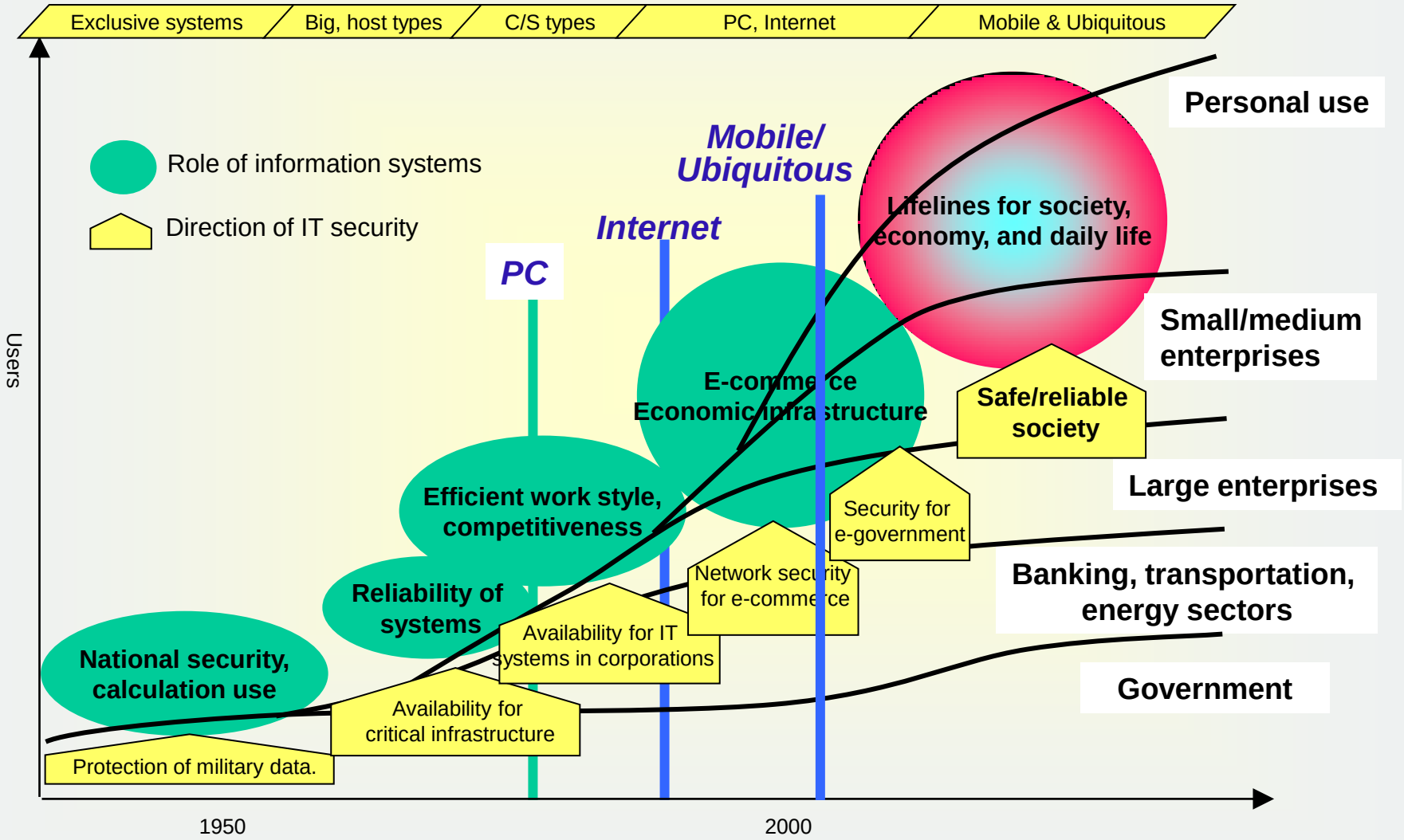
Evolution of Attack



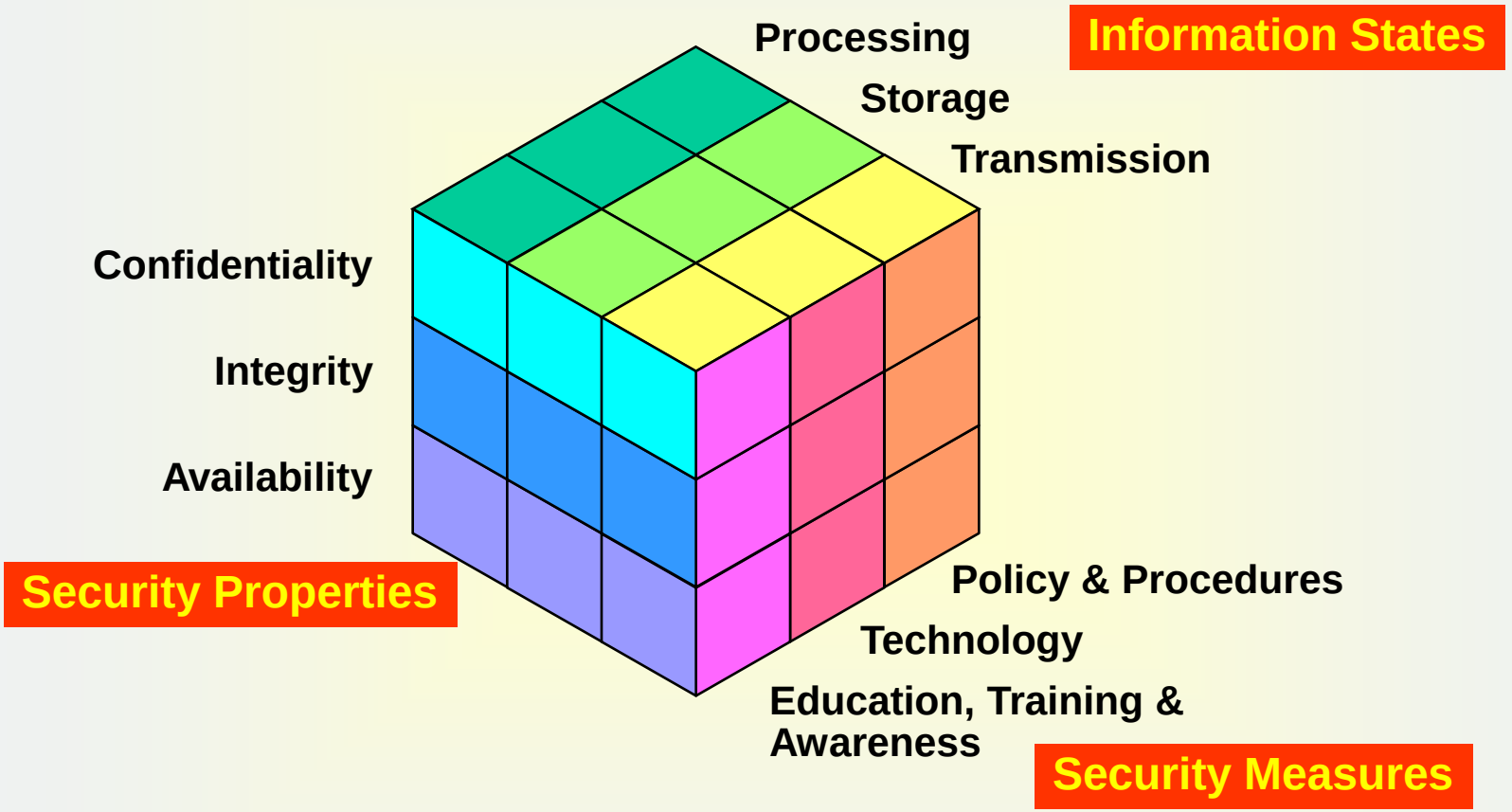
Top Corporate Security Threats

1. External hackers attacking your systems' availability
2. Security defects / vulnerabilities in hardware and software
3. External hackers attacking your corporate information
4. Employee errors in software and computer use
5. Employee actions that are intentionally harmful
6. Natural disasters
7. Theft of physical assets
8. Unauthorized wireless network access
9. Terrorism

Trends of IT Security



What is Information Security?



NSTISSI 4011: National Training Standard for Information Systems Security Professionals, 1994

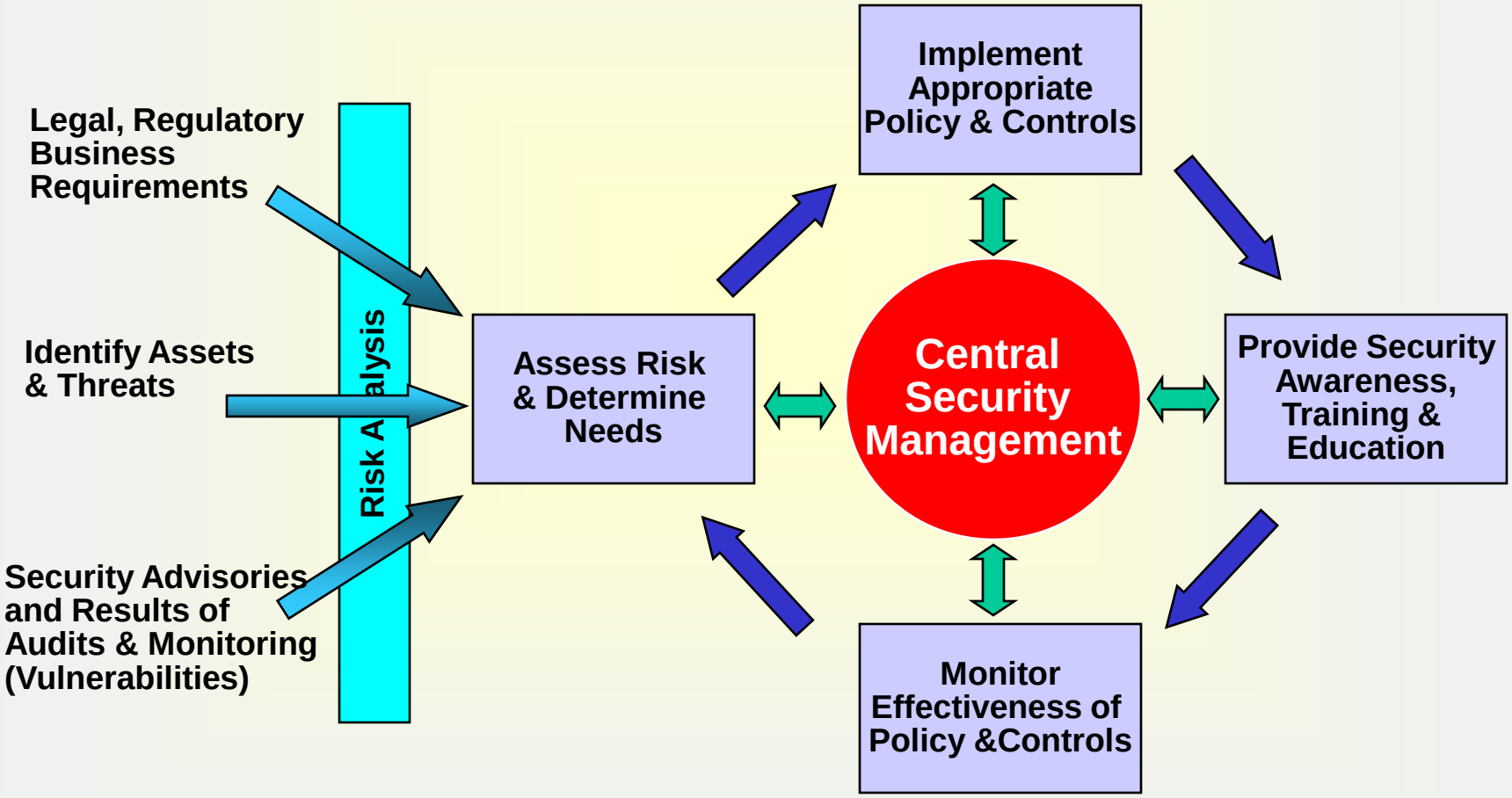
Information Security C.I.A.

- **Information Security**
  - **Discipline that protects the Confidentiality, Integrity & Availability of information, during processing, storage & transmission, through Policies, Technologies & Operations**
  - **Network/Communication security, Host/Computer security**

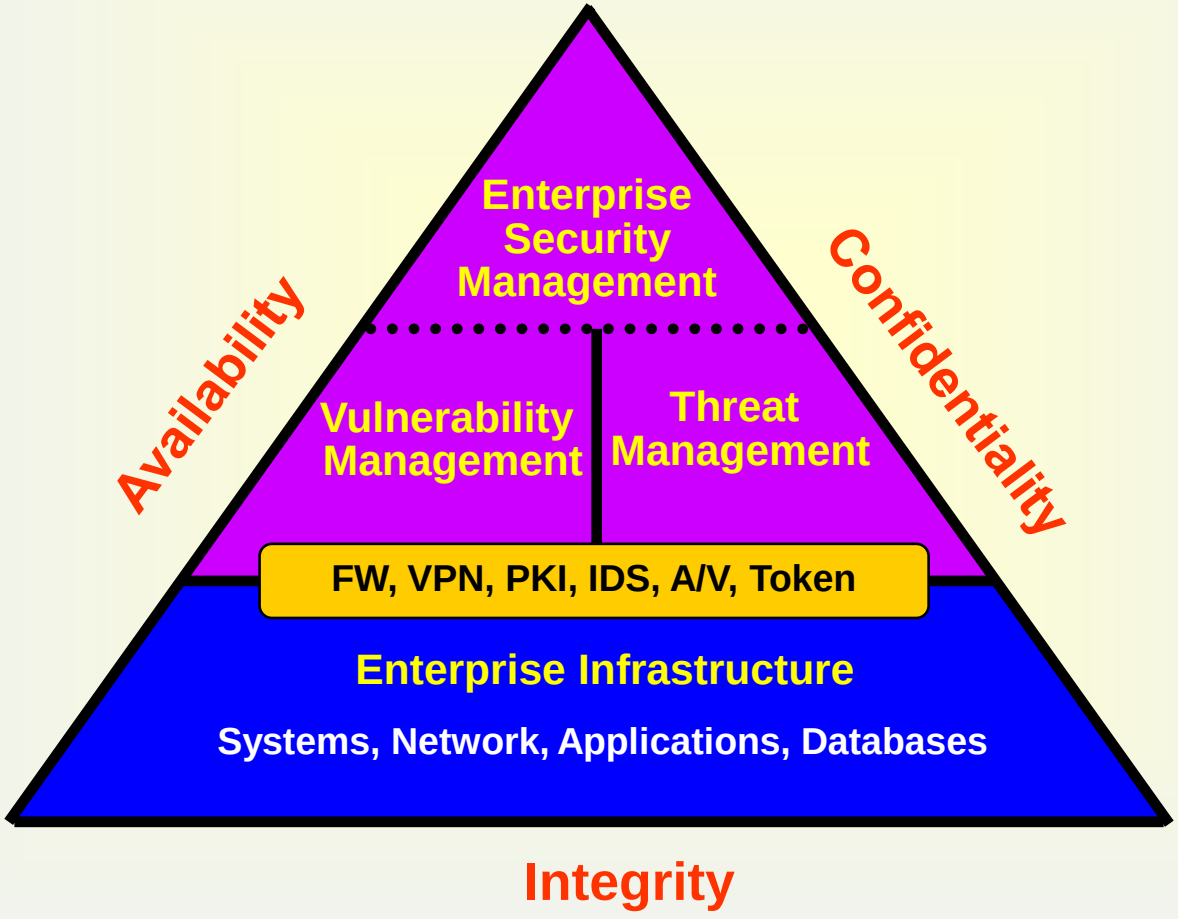
- **C.I.A. of Information Security**
  - **Confidentiality: Protecting from unauthorized disclosure**
  - **Integrity: Protecting from unauthorized modification**
  - **Availability: Making information accessible/available when needed**

- **How to Achieve Information Security**
  - **Policies : what should do, what should not do, etc., for information security**
  - **Technologies: implementing the policies**
  - **Operations: assessment & improvement on the implemented technologies**

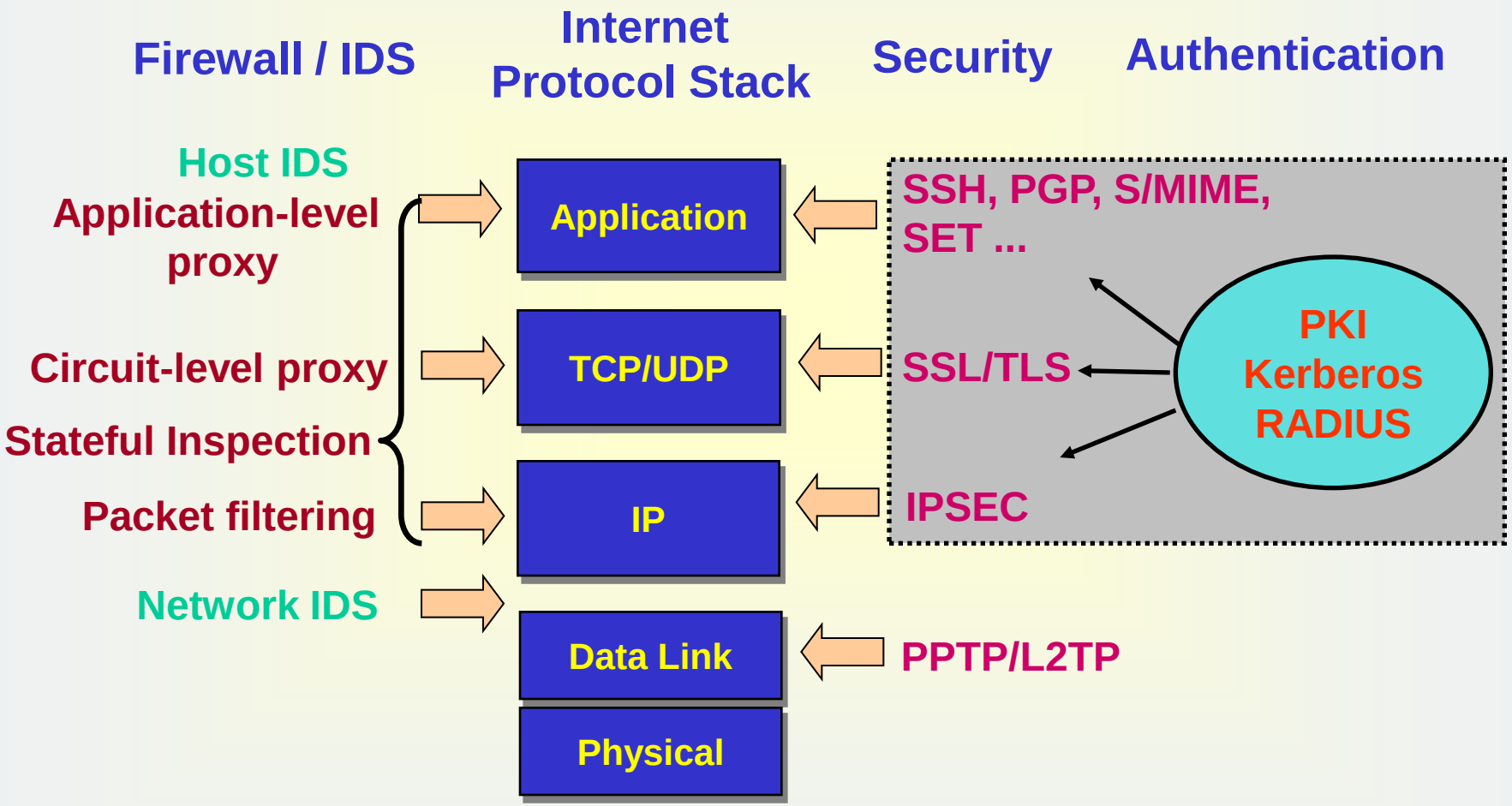
Managing Security



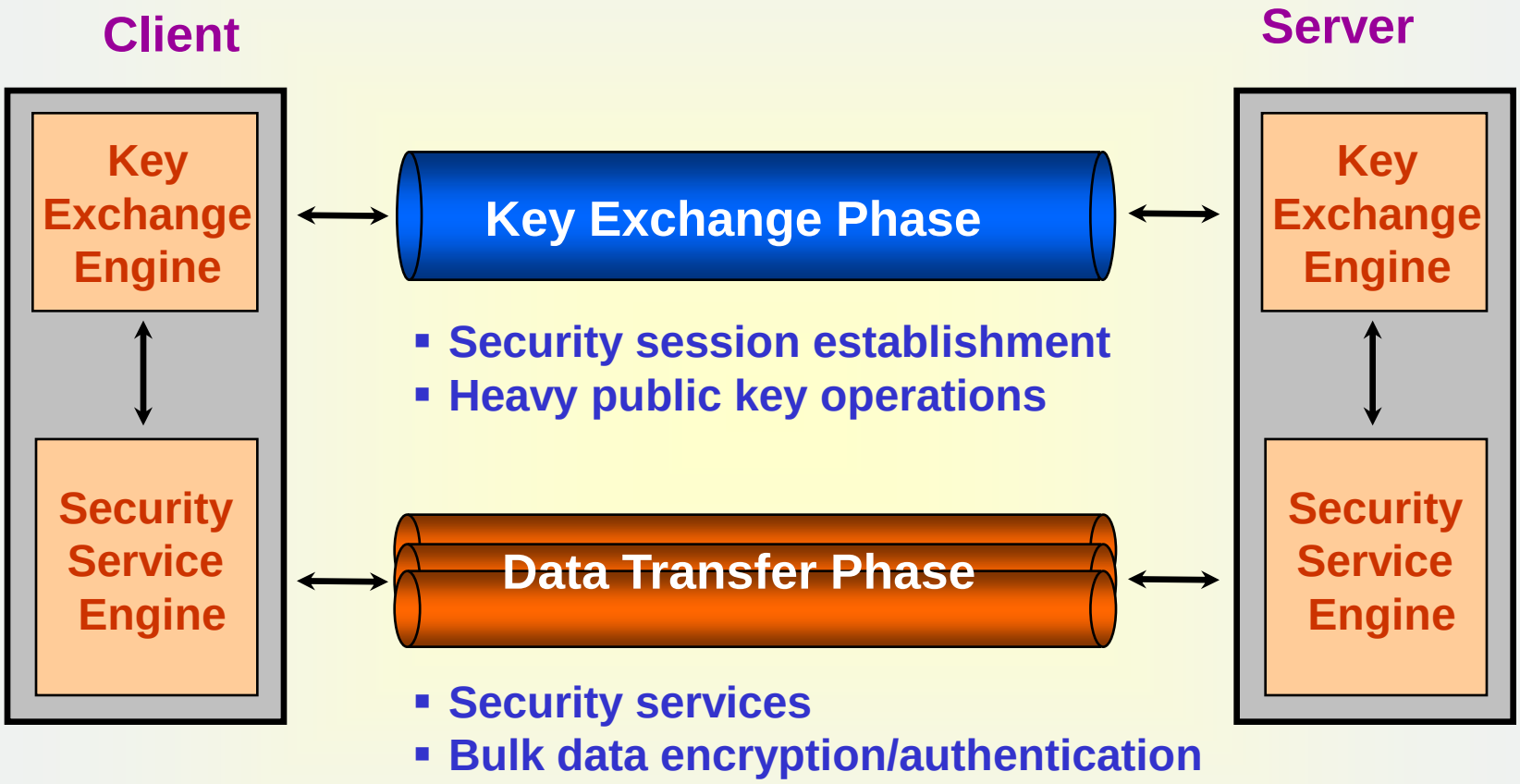
Enterprise Security Management



Major Internet Security Technologies

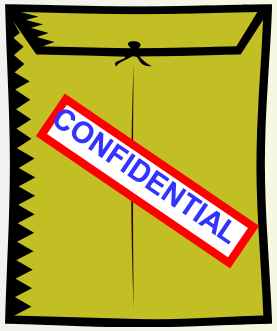


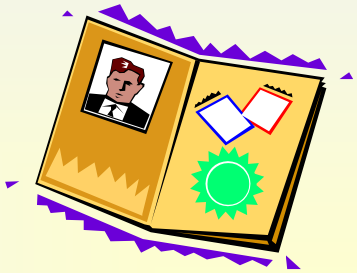
Network Security Protocols



❖ Examples: IPSec, SSL/TLS/WTLS, SSH …

Solutions for Security Needs





Physical Solutions

- Temper-evident sealed envelope
- ID-card, Passport, Drivers license
- Signature

Cryptographic Solutions (for communications over open network)

- Encryption with MAC : Confidentiality, Authentication, Integrity Protection
- Digital Certificate : Identification
- Digital Signature : Authentication, Integrity Protection, Non-Repudiation
- Security mechanisms are combined to provide a security service
  - ✓ Virtual Private Network(VPN), Firewall, IDS, etc.

3. Quick Overview on Cryptology

Classical Encryption Techniques

- Basic building blocks of all encryption techniques
  - Substitution: replacement
  - Transposition: relocation

- Substitution ciphers
  - Caesar cipher
  - Monoalphabetic ciphers
  - Playfair cipher
  - Hill cipher
  - Polyalphabetic ciphers: Vigenere cipher
  - Vernam cipher/One-time pad: perfect cipher

- Transposition techniques
  - Rotor machines: Enigma, Purple

Confusion and Diffusion

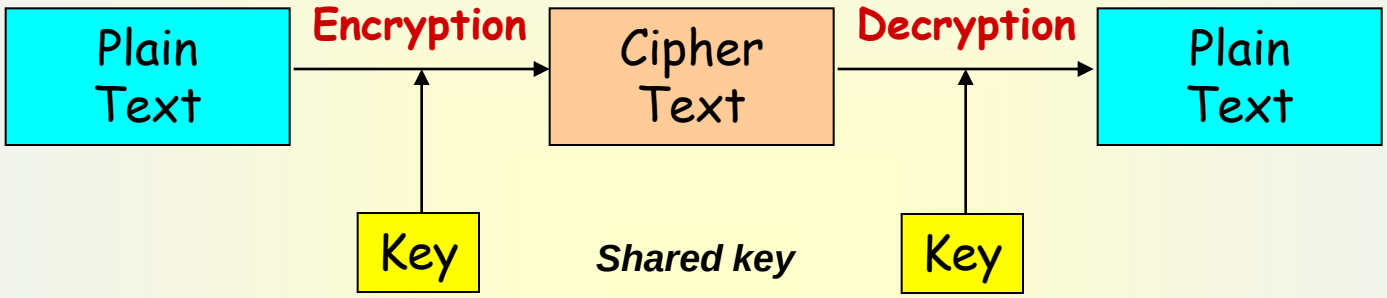
- **Diffusion**
  - Ideally, ciphertext should look as if it is a random string of letters.
  - Distributes or disperses the statistical structure of plaintext over the ciphertext.
  - Hides the statistical relationships between the ciphertext and the underlying plaintext.
  - Changes in the plaintext should affect many parts of the ciphertext.
  - Substitution + Transposition
- **Confusion**
  - The principle of confusion prevents the cryptanalyst from using ciphertext to figure out the secret encryption key.
  - Hides the statistical relationship between ciphertext and secret key.
  - The interceptor should not be able to predict what changing one character in the plaintext will do to the ciphertext.
  - Substitution (Well-designed & Complex)

Secret Key vs. Public Key Systems

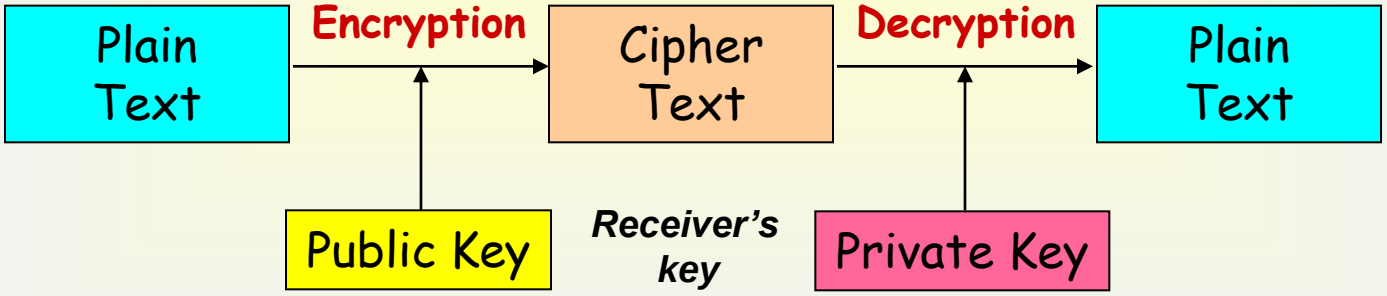
- **Symmetric Key Cryptosystem**
  - ✓ Both parties must share the same secret key
  - ✓ Encrypt/Decrypt & MAC generate/verify
  - ✓ Very fast : Bulk data encryption, User/message authentication
  - ✓ Block/Stream Cipher : AES, DES, IDEA, SEED, Crypton…; RC4, SEAL…
  - ✓ MAC schemes: Keyed hash (HMAC), CBC-MAC …
  - ✓ Problem of Key Sharing ; Cannot provide Non-repudiation
- **Public Key Cryptosystem**
  - ✓ A pair of (Public Key, Private Key) for each user
  - ✓ Encrypt/Verify with peer's Public Key; Decrypt/Sign with its own Private Key
  - ✓ Encryption scheme: RSA, ElGamal
  - ✓ Key exchange: DH(Diffie-Hellman), ECDH
  - ✓ Signature schemes: RSA, DSA, KCDSA, ECDSA, EC-KCDSA …
  - ✓ Slow : Key exchange, Authentication, Non-repudiation
  - ✓ Problem : How to get the right peer's Public Key

Secret Key vs. Public Key Systems

- **Symmetric Key Cryptosystem**

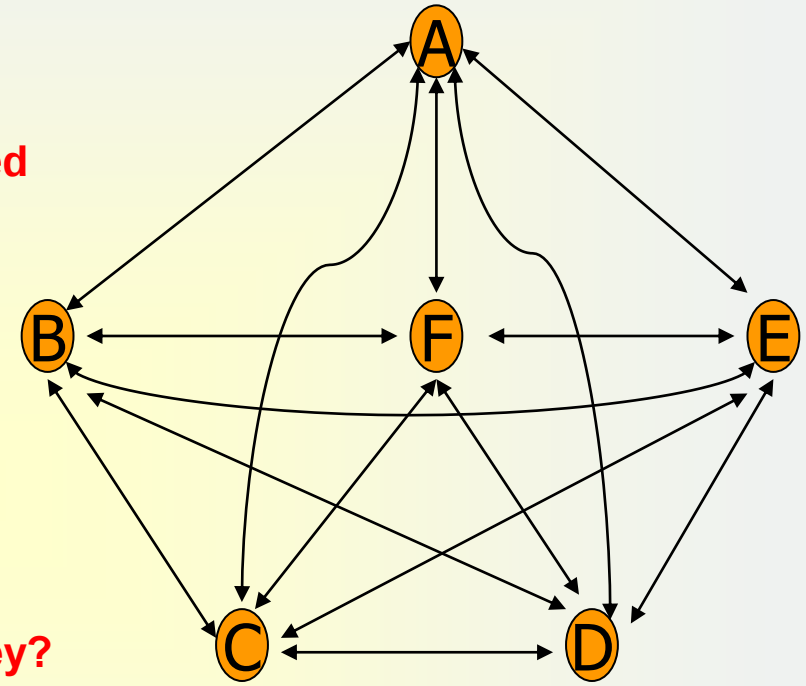


- **Public Key Cryptosystem**



Key Distribution Problem

- **Symmetric Key Cryptosystem**
  - ✓ $_nC_2 = n(n-1)/2$ secret keys are required



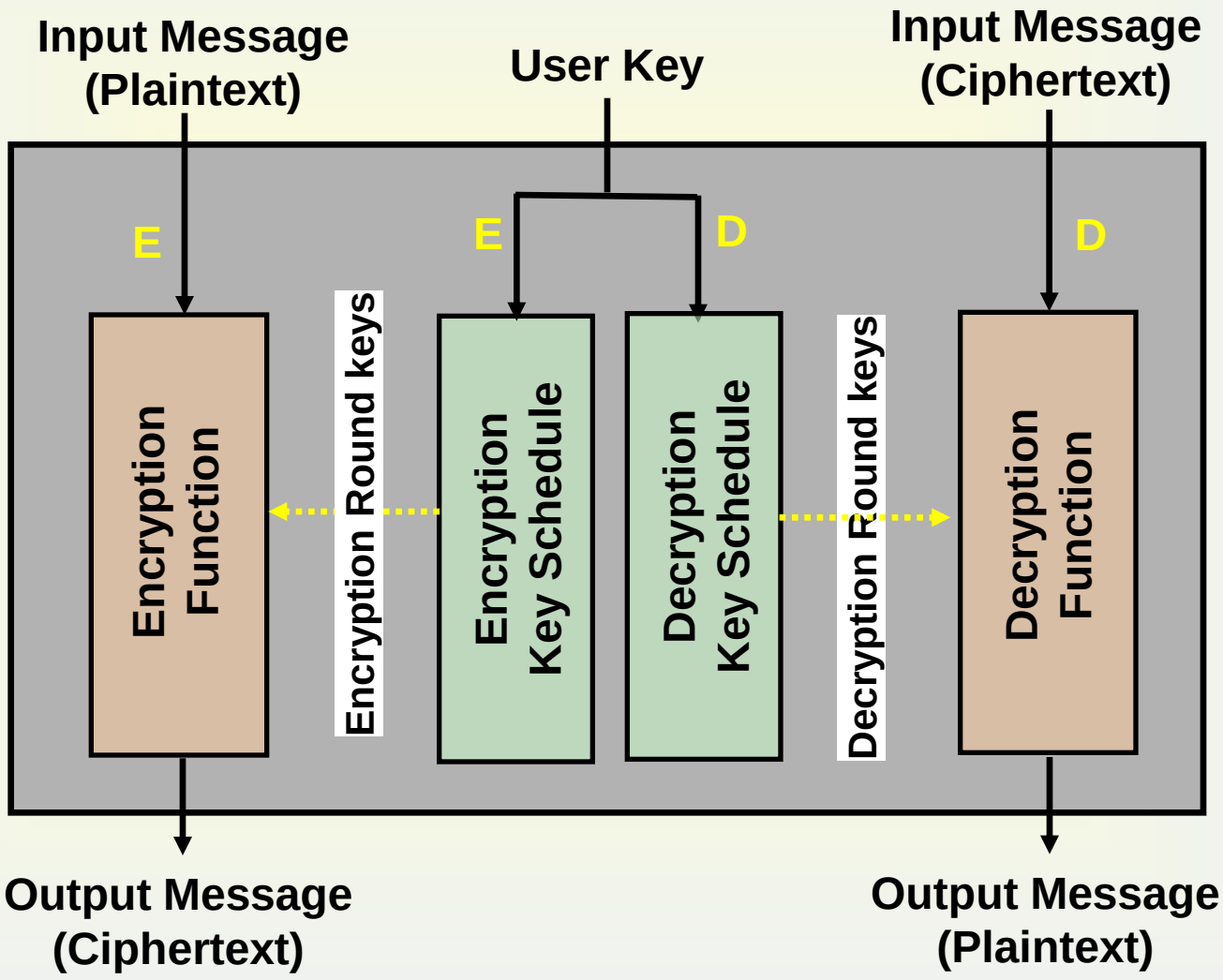
- **Public Key Cryptosystem**
  - ✓How to get the right peer's Public Key?

Cryptographic Primitives

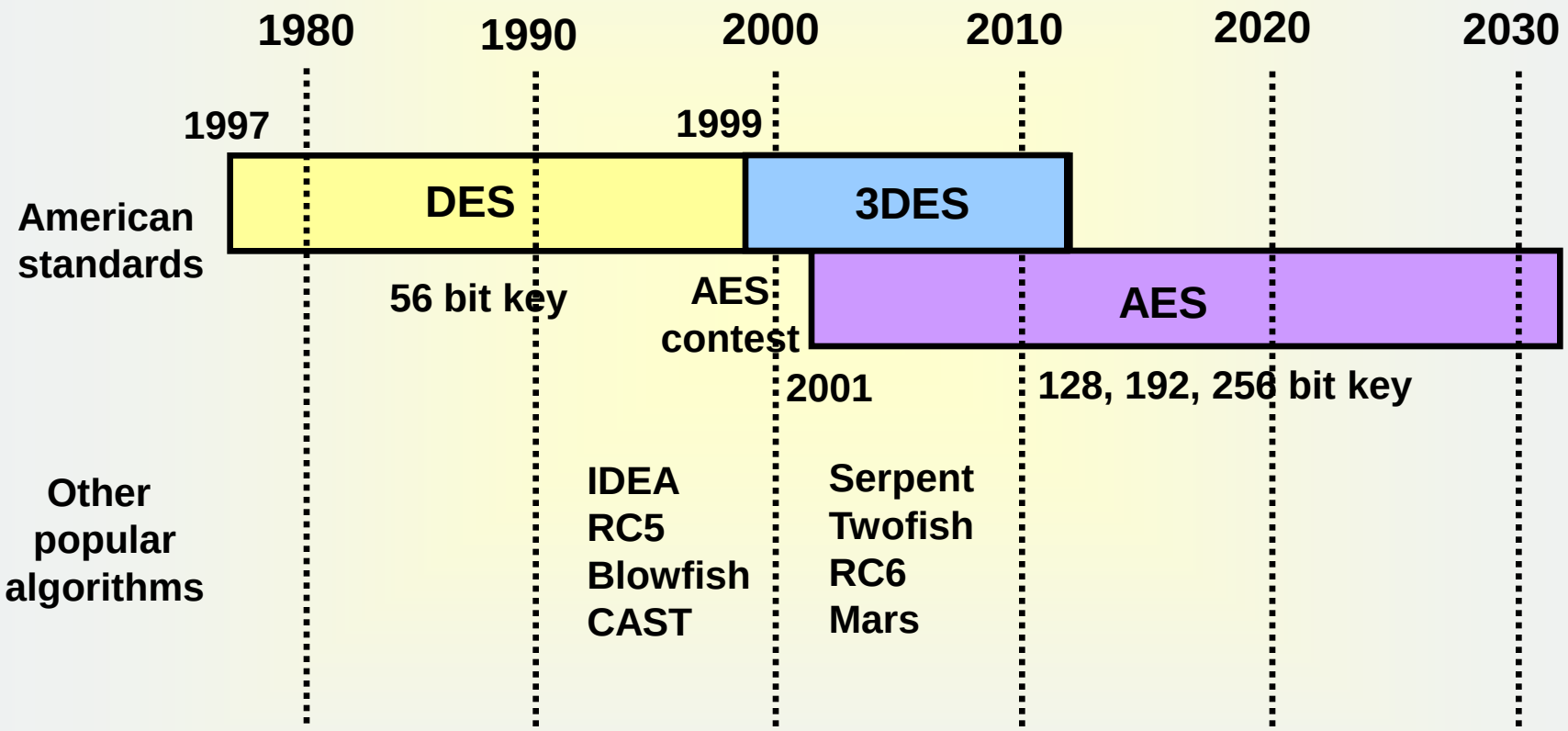
- Block / Stream Cipher
  - 3DES, AES, SEED, RC2, RC5, … / RC4, SEAL …
- Hash Function
  - MD5, SHA1/SHA2, HAS160, RMD160, Tiger …
- Message Authentication Code (MAC)
  - HMAC, CBC-MAC, UMAC

- Public Key Ciphers
  - RSA, ElGamal
- Digital Signature
  - RSA, DSA/ECDSA, KCDSA/EC-KCDSA …
- Key Exchange
  - Diffie-Hellman, ECDH, RSA key transport

Block Cipher – A Simplified View



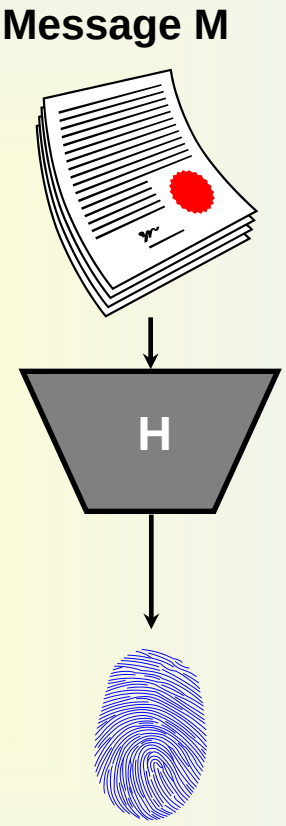
Most Popular Symmetric Ciphers



Hash Functions

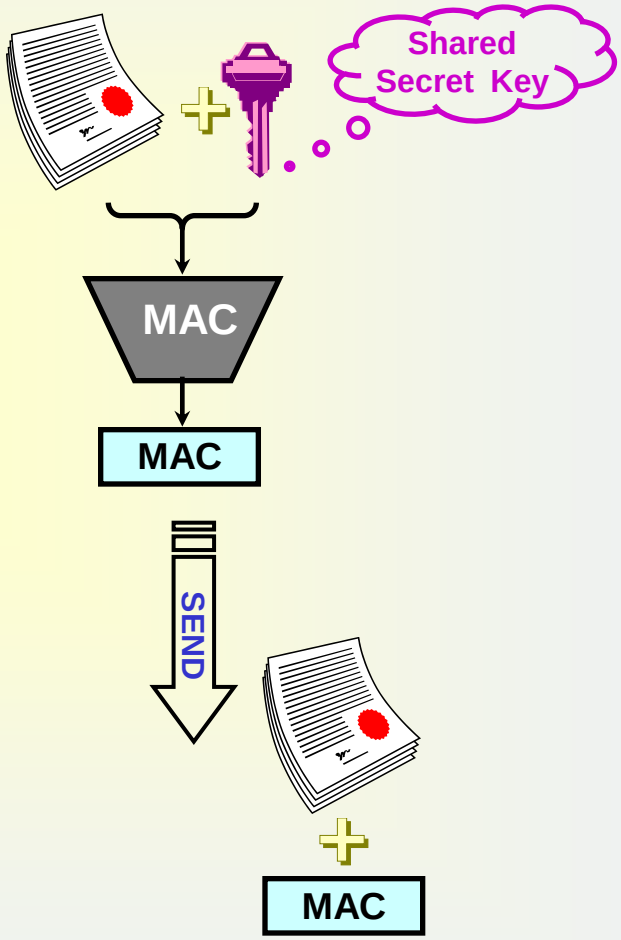
- **Hash Function**
  - ✓ Generate a fixed length "Fingerprint" for an arbitrary Message
  - ✓ No Key involved
  - ✓ One Way Function
  - ✓ MD5, SHA1, SHA2, HAS160

- **Applications**
  - ✓ Keyed hash: used to generate/verify MAC(Message Authentication Code) or Integrity Check Value(ICV) → HMAC
  - ✓ Unkeyed hash: used to produce Digital Signature

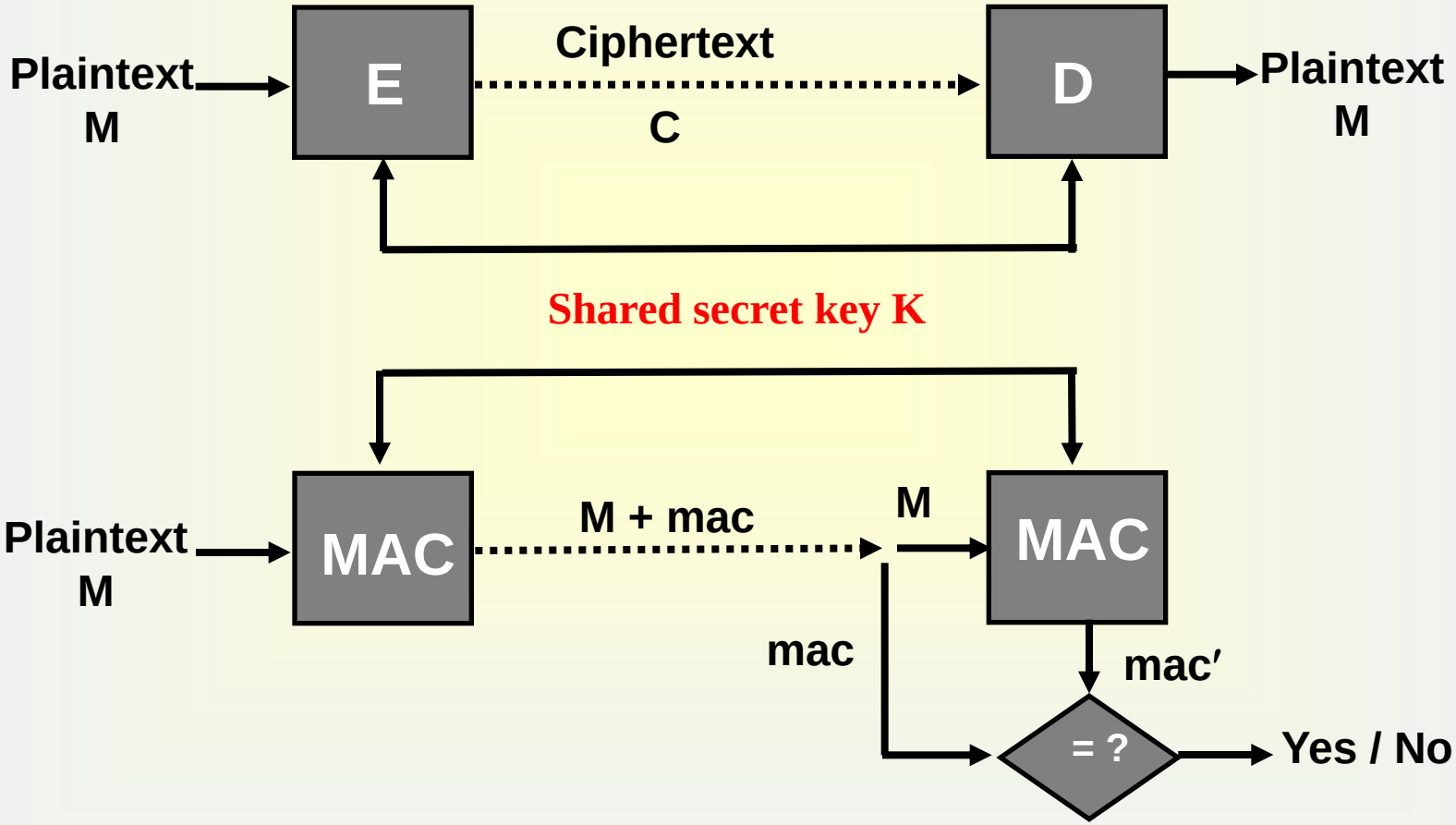


Message Authentication Code (MAC)

- **Purposes**
  - ✓ Secure tag for authentication
  - ✓ Message origin authentication
  - ✓ User authentication
  - ✓ Message integrity
- **Schemes**
  - ✓ Keyed hash: HMAC
  - ✓ Block cipher: CBC-MAC, XCBC-MAC
  - ✓ Dedicated MAC: UMAC

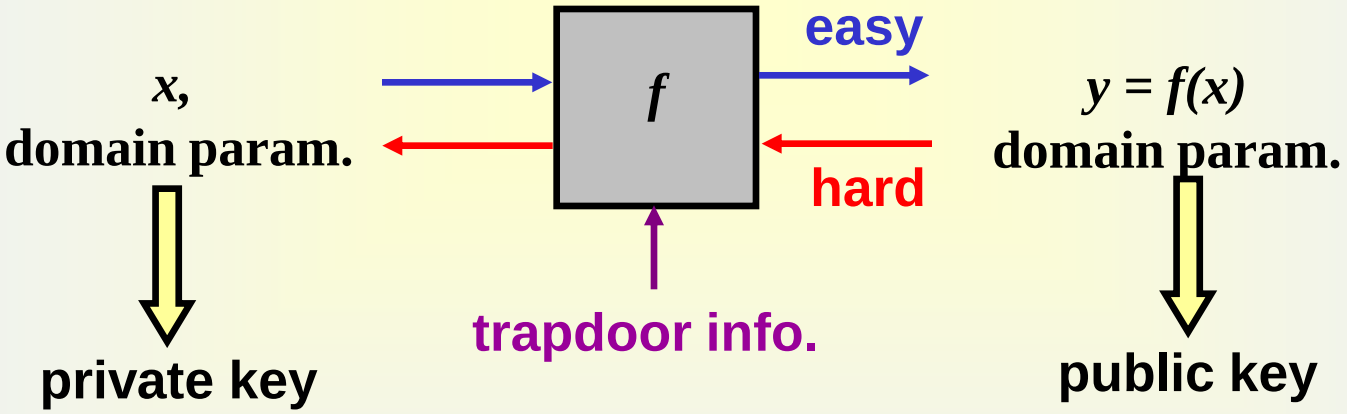


Symmetric Encryption vs. Authentication



Public Key Cryptography Concept

- Invented by Diffie and Hellman in 1976
- Solve the secret key sharing problem in symmetric cryptosystems
- Two keys used: public key & private key
- Also known as two-key cryptography or asymmetric cryptography
- Based on (trapdoor) one-way function

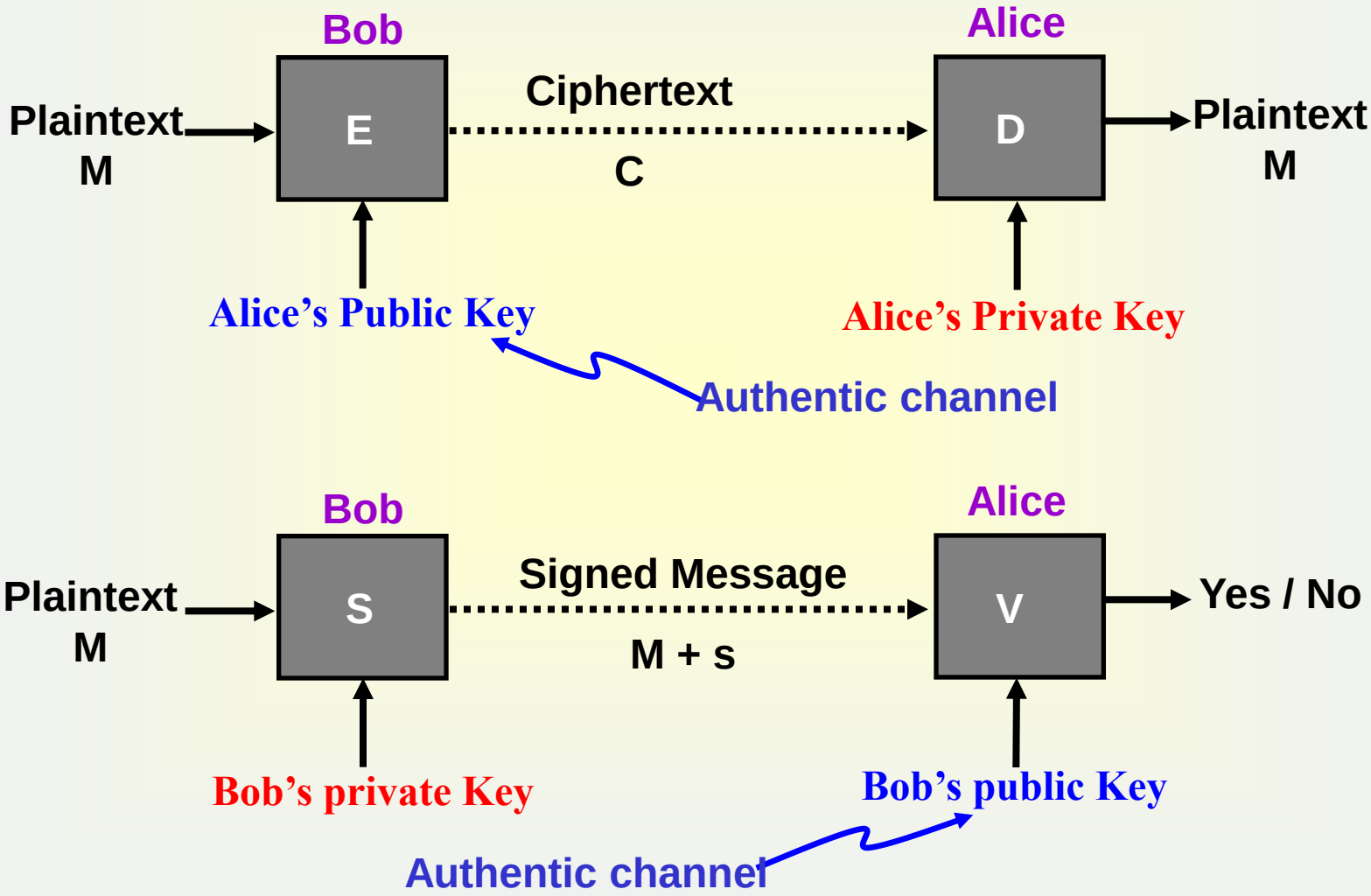


But, easy if trapdoor info. is given.

Public Key Cryptography

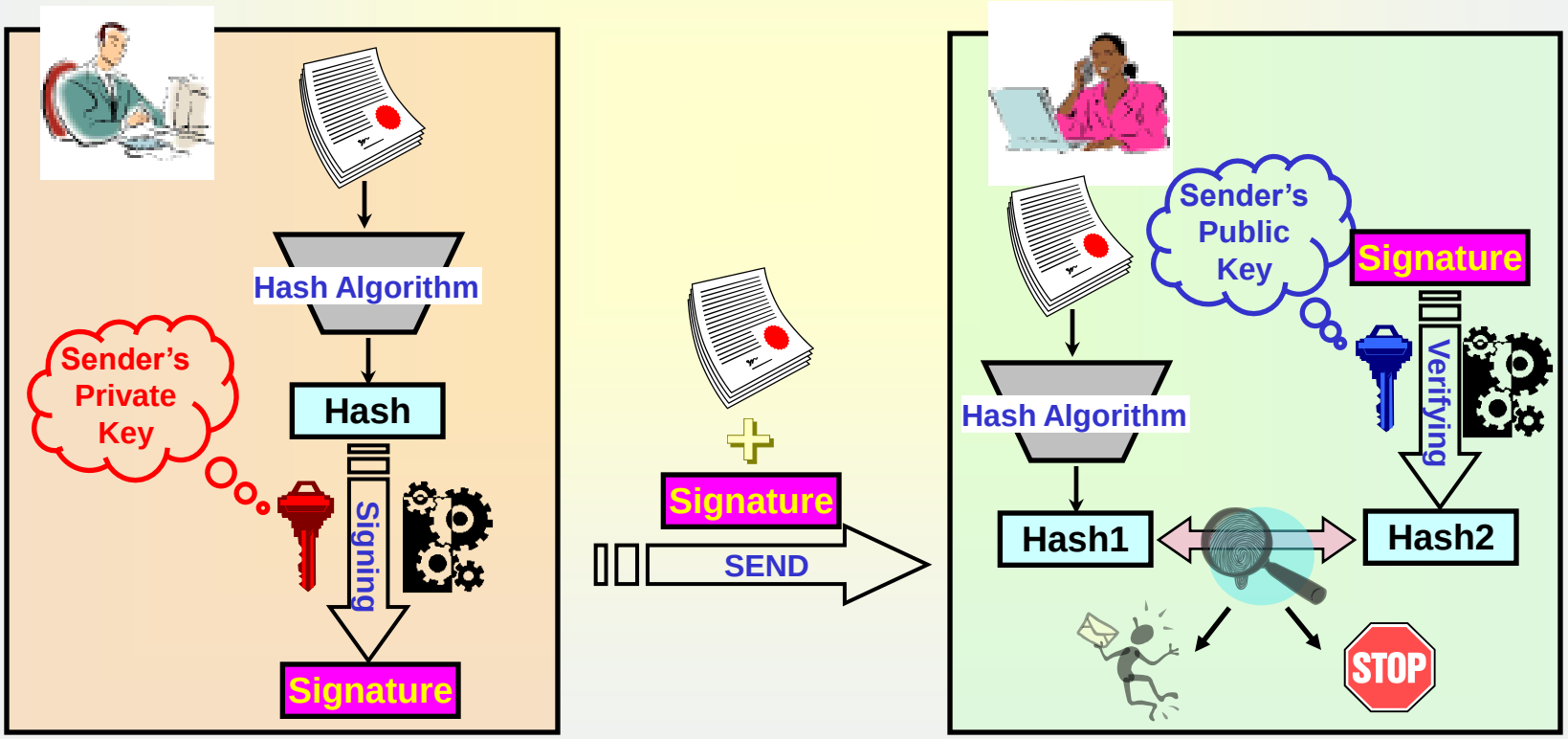
- Keys
  - ✓ A pair of (Public Key, Private Key) for each user
  - ✓ Public keys must be publicly & reliably available
- Public Encryption
  - ✓ Encrypt with peer's Public Key; Decrypt with its own Private Key
  - ✓ RSA, ElGamal
- Digital signature
  - ✓ Sign with its own Private Key; verify with peer's Public Key
  - ✓ RSA, DSA, KCDSA, ECDSA, EC-KCDSA …
- Key exchange
  - ✓ Key transport or key agreement for secret-key crypto.
  - ✓ RSA; DH(Diffie-Hellman), ECDH

Public Key Encryption vs. Signature



Digital Signature

- **Digital Signature**
  - ✓ Combine Hash with Digital Signature and use PKC
  - ✓ Provide Authentication and Non-Repudiation
  - ✓ RSA; DSA, KCDSA, ECDSA, EC-KCDSA

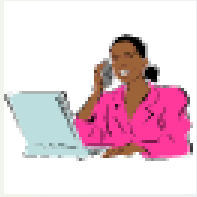


Digital Enveloping : Key Transport + Encryption

Bob's Public Key/Private Key

Alice's Public Key

Randomly Generated Session Key



Hash Algorithm

Hash

Signing

Signature

Signature

Encryption

Encrypted Message

Symmetric Key Cryptosystem

Encrypted Session Key

Encrypted Message

SEND

Encryption

Encrypted Session Key

Public Key Cryptosystem

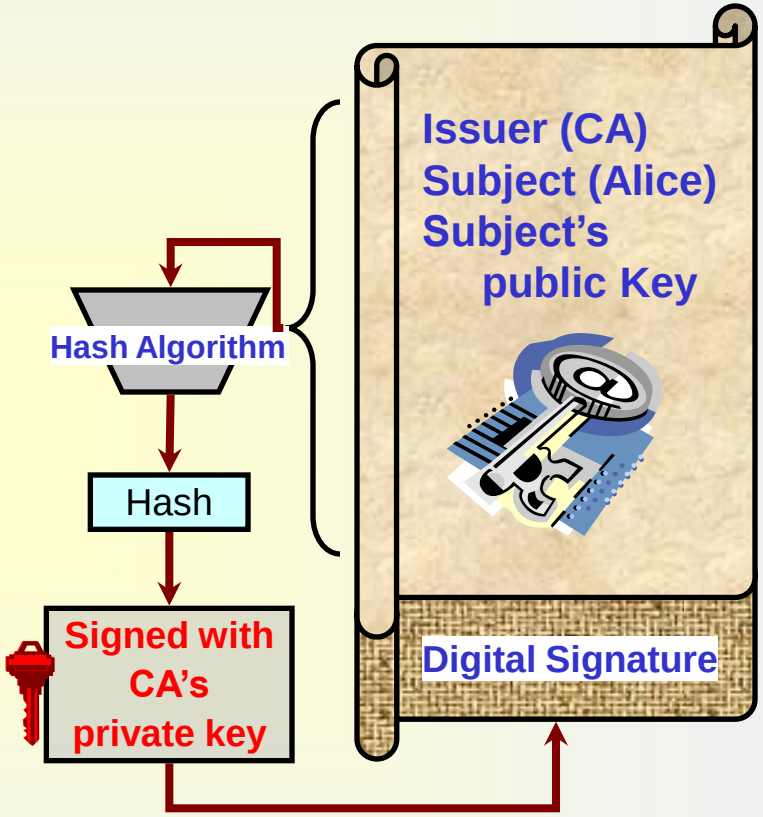
Cryptographic Protocols

- **Cryptographic algorithms**
  - ✓ Algorithm executed by a single entity
  - ✓ Algorithms executing cryptographic functions
  - ✓ Encryption, Hash, digital signature, etc…
- **Cryptographic protocols**
  - ✓ Protocols executed between multiple entities through pre-defined steps of communication
  - ✓ Protocols executing cryptographic functions
  - ✓ Primitives: Key agreement, secret sharing, blind signature, coin toss, etc …
  - ✓ Complex systems: e-commerce, e-voting, e-auction, etc …

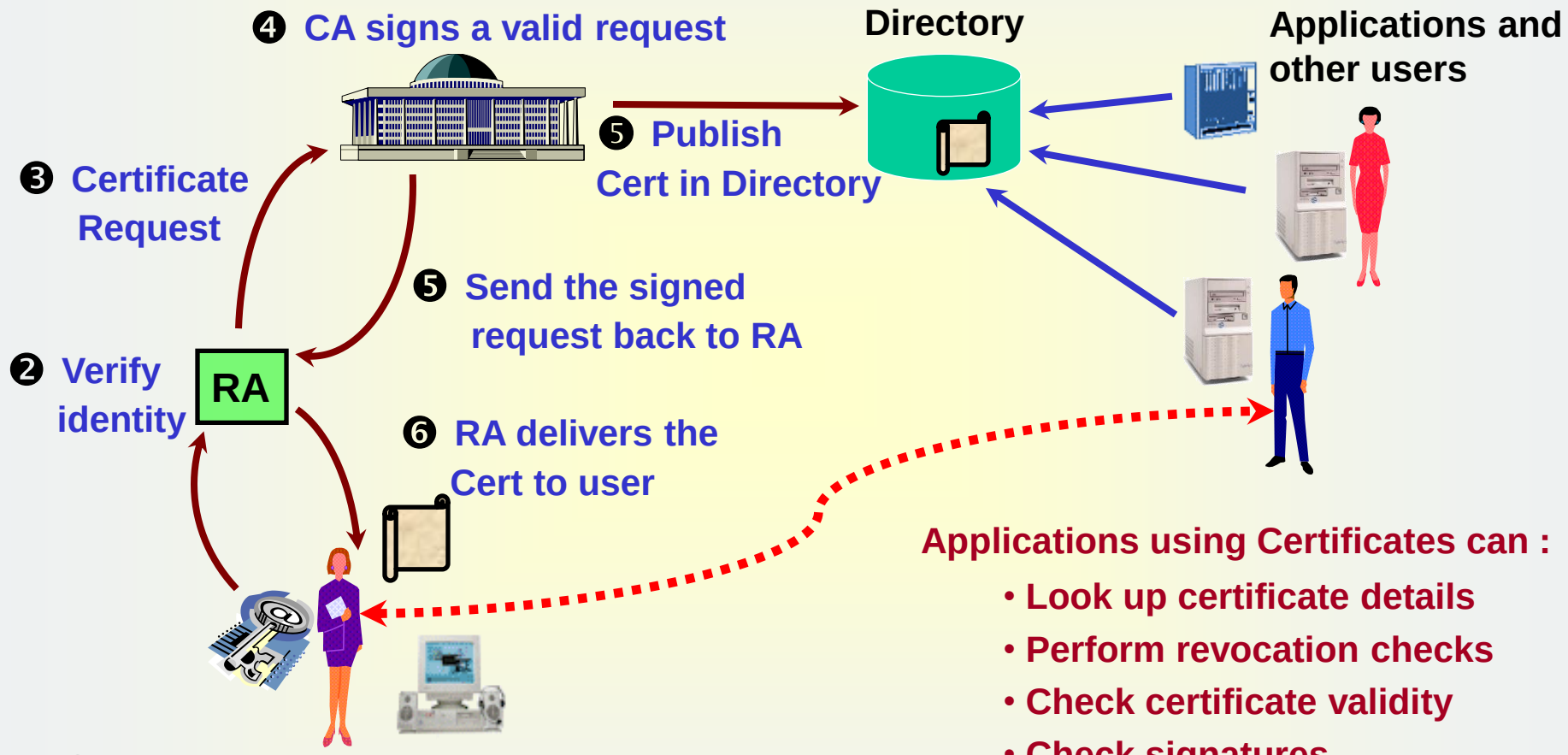
What is a Digital Certificate?

- **Digital Certificate**
  - ✓ A file containing Identification information (CA's name (Issuer), Alice's name (Subject), valid period, Alice's public key, etc) and digital signature signed by trusted third (CA) party to guarantee its authenticity & integrity

- **Certificate Authority (CA)**
  - ✓ Trusted third party like a government for passports
  - ✓ CA has authenticated the public key belongs to Alice
  - ✓ CA creates Alice's a Digital Certificate



How PKI Works



Applications using Certificates can :

- Look up certificate details
- Perform revocation checks
- Check certificate validity
- Check signatures
- Decrypt data

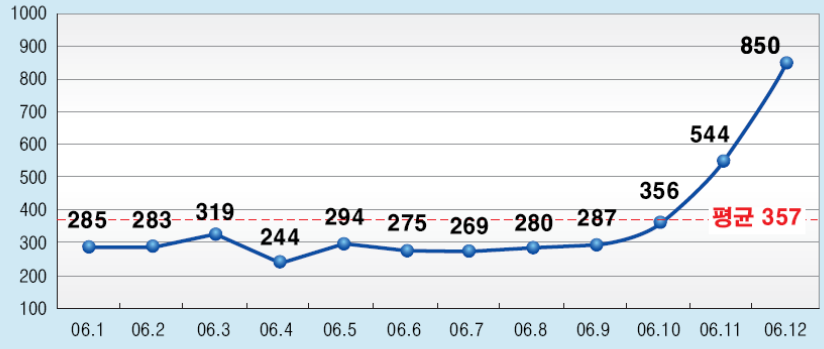
4. Real World

Information Security Industry

Security Violations

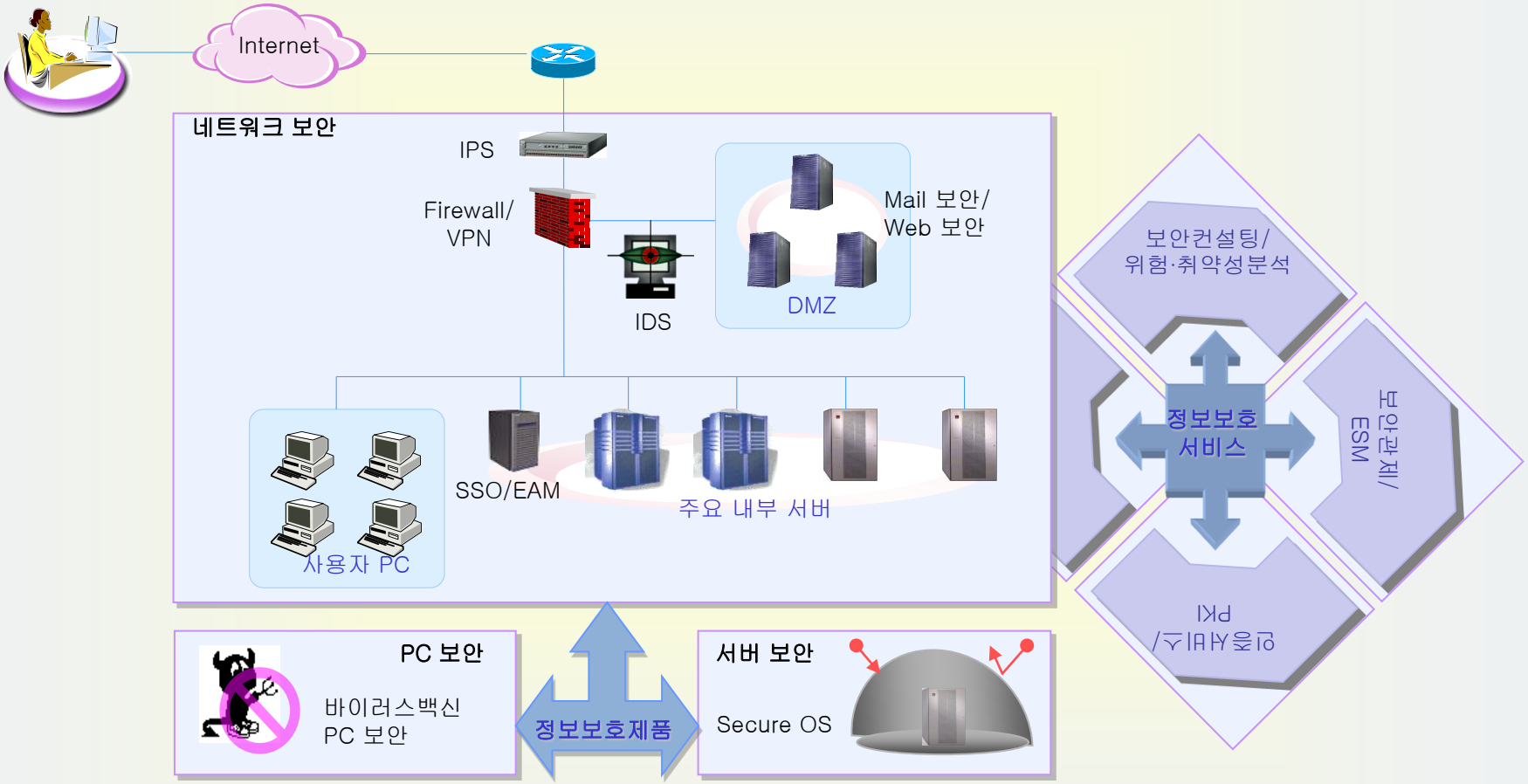
구분	2005년 총계	2006년												2006년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
웜·바이러스	16,093	606	859	556	395	427	745	396	683	865	892	773	592	7,789
해킹신고처리	33,633	2,225	1,968	2,032	1,799	2,175	2,433	2,284	2,787	2,263	2,503	2,409	1,930	26,808
- 스팸릴레이	6,334	782	682	957	788	1,162	1,418	1,314	1,685	1,318	1,336	1,407	1,206	14,055
- 피싱경유지	1,087	78	118	125	120	130	114	85	119	97	97	83	100	1,266
- 단순침입시도	-	161	218	225	365	285	227	327	353	444	561	350	195	3,711
- 기타해킹	9,520	330	358	248	325	444	556	406	530	355	380	325	313	4,570
- 홈페이지변조	16,692	874	592	477	201	154	118	152	100	49	129	244	116	3,206
봇(Bot)	18.8%	10.0%	11.8%	14.6%	10.1%	9.1%	11.4%	14.1%	13.1%	13.1%	16.9%	12.6%	13.2%	12.5%

* From KrCERT/CC



2006년 월별 사이버 침해사고 발생 추이

Information Security Industry

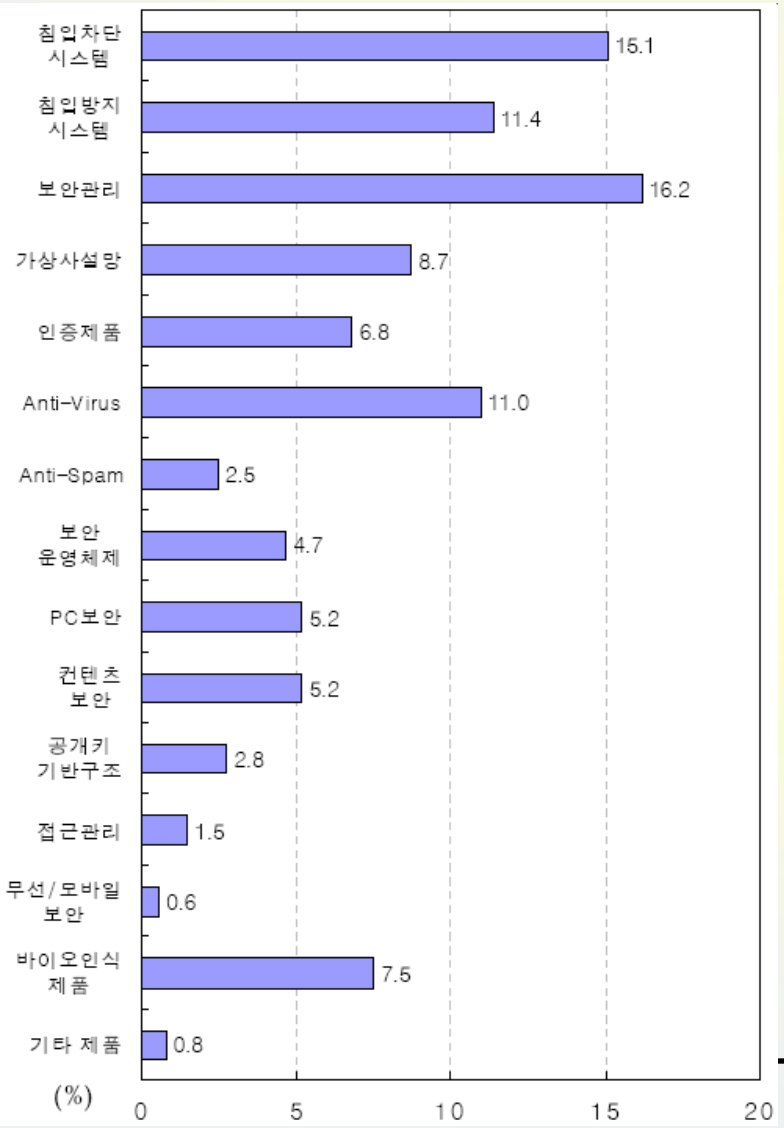


Information Security Industry

Current view

대분류	소분류	기호	세부 항목 예시
정보보호 H/W	침입차단	A	1. 침입차단시스템 2. 웹방화벽 3. 통합보안제품**
	침입방지	B	1. 방화벽 기반 2. 침입탐지시스템 기반 3. 네트워크장비 기반 4. 통합보안 제품**
	가상사설망	C	1. VPN 단일제품 2. 통합보안제품**
	망 전환 장치	D	1. 망 전환 장치
	H/W 인증	E	1. 보안 스마트카드 2. H/W 토큰
	생체인식	F	1. PC/네트워크보안 2. 출입통제/근태관리 3. 법 집행용 4. 금융/결재 시스템 5. 신원인증 6. 기타
정보보호 S/W	보안 관리 S/W	G	1. 통합보안관리 툴 2. 로그 관리/분석 툴 3. 취약점 분석 툴
	침입탐지 S/W	H	1. HIDS 2. HIPS 3. NIDS
	방화벽 S/W	I	1. 개인용 2. 기업용
	Anti Virus	J	1. Virus 백신 2. Anti 스파이웨어
	Anti Spam	K	1. 스팸차단 S/W
	시스템 보안	L	1. Secure OS 2. 서버 보안
	PC 보안	M	1. PC 보안
	어플리케이션 보안	N	1. 내부정보유출방지 2. DB보안 3. DRM(문서/이메일)
	3A	O	1. PKI 2. EAM 3. SSO 4. IM/IAM
	무선/모바일 보안	P	1. WPKI 2. WLAN 보안 3. 모바일 백신
정보보호 서비스	인증 서비스	Q	1. 공인/사설 인증 서비스
	보안 관제	R	1. 보안관제 서비스
	보안 컨설팅	S	1. 안전진단 2. 인증 3. 기반보호
	유지 보수	T	1. 판매 후 유료서비스
	기술 공급	U	1. 기술/ DB 제공
	기타서비스	V	1. 교육 훈련 서비스 2. 보안 제품 렌탈/임대

Information Security Industry



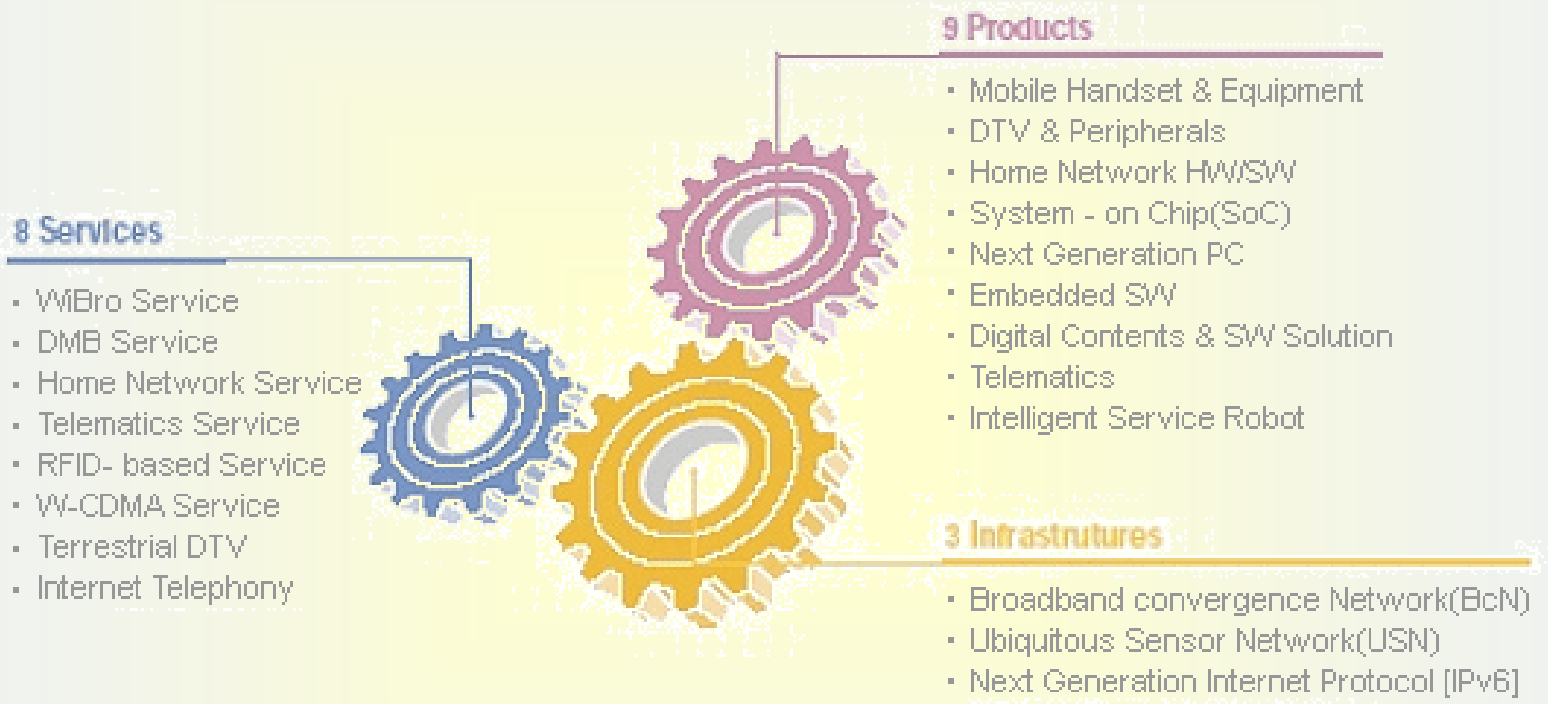
[단위 : 백만원]

대분류	소분류	2005년	2006년	증감율(%)
시스템 및 네트워크 정보보호 제품	침입차단(방화벽)시스템	89,108	94,554	6.1
	침입방지시스템(IPS)	62,406	71,469	14.5
	보안관리	87,957	101,038	14.9
	가상사설망(VPN)	53,776	54,558	1.5
	인증제품	56,736	42,691	-24.8
	Anti-Virus	57,935	68,671	18.5
	Anti-Spam	10,756	15,438	43.5
	보안운영체제(Secure OS)	28,652	29,144	1.7
	PC 보안	29,500	32,662	10.7
	컨텐츠 보안	27,329	32,554	19.1
	공개키기반구조(PKI)	16,085	17,735	10.3
	접근관리	11,221	9,087	-19.0
	무선/모바일 보안	2,516	3,646	44.9
	바이오인식 제품	43,195	46,725	8.2
	기타 제품	6,251	5,210	-16.7
	소 계	583,423	625,182	7.2
정보보호 서비스	인증서비스	6,549	7,465	14.0
	보안관제	22,241	26,602	19.6
	보안컨설팅	26,331	31,093	18.1
	유지보수	40,051	43,186	7.8
	기타서비스	2,110	1,264	-40.1
	소 계	97,282	109,610	12.7
합 계		680,705	734,792	7.9

IT839


2007년 생산 380조원, 수출 1,100억불
해외진출 지원, 선도기술개발
기업
수출, 고용창출
산업전반 시너지 확산
재투자
정부
방식결정
주파수 분배
사업자허가
법제도 정비
경쟁체제 유지
서비스 준비
국내외 시장확대
기반 구축
원가절감
기술개발
시범사업 추진
표준화
애로기술 지원
공공시범 사업추진
8대 서비스
WiBro
DMB
홈 네트워크
텔레매틱스
RFID
W-CDMA
지상파 DTV
VoIP
9대 신성장동력
차세대 이동통신
디지털 TV
홈 네트워크
IT SoC
차세대 PC
임베디드 S/W
DC · S/W솔루션
텔레매틱스
지능형로봇
표준화 선도, 기반기술개발
초기시장 창출, 투자자금 지원
3대 인프라
BcN
USN
IPv6

IT839



- **Information Security in the future**
  - **One of the basic tool/service to realize IT839**
  - **Information Security is working together in wide areas in IT839**
  - **Ubiquitous world is coming**

Wide Spectrum of Lecture Topics

- Security related departments in Korean universities (undergraduate)
  - Dept. of Information Security – 5
  - Security related departments – total about 20

- Lecture topics (very diverse)
  - Cryptography
  - System security
  - Network security, Internet security
  - E-commerce security
  - Security management, policy
  - Hacking and virus
  - Projects on security related topics
  - Security programming
  - Cryptographic protocols
  - Cyber warfare

Specialist on Information Security (SIS)

구 분	시스템 분야	네트워크 분야	어플리케이션 분야	정보보호 일반분야
컴퓨터 관련과목	· 컴퓨터구조 · 논리회로 · 마이크로프로세서 · 운영체제 이론 및 실습 · 시스템 프로그래밍	· 데이터통신 · 컴퓨터 네트워크 · 네트워크 이론 및 실습 · 통신공학 · 무선/이동 통신 · 네트워크 프로그래밍 · 인터넷 프로토콜 · 인터넷 프로그래밍 · 분산처리 시스템	· 데이터베이스 · 파일처리론 · 자료구조론 · 소프트웨어/정보공학 · 멀티미디어 · 컴파일러 · 인공지능 · 프로그래밍 언어론 · 각종 프로그래밍언어 (실습포함) · 비주얼 프로그래밍	· 알고리즘 · 계산이론 · 오토마타 · 수치해석 · 이산수학
정보보호 전공과목	· 운영체제 보안 · 악성 소프트웨어 · 시스템 기반 침입 탐지 시스템 · 시스템 기반 취약점 · 재해 및 재난복구 시스템	· 네트워크 보안 · 네트워크 기반 침입 탐지 시스템 · 네트워크 기반 취약점 분석 · (무선)통신 보안 · 침입차단시스템 · 침입추적시스템 · 암호/보안 프로토콜 · 인터넷 보안	· 데이터베이스 보안 · 전자상거래 보안 · 인증시스템 · 컨텐츠 보안 · 업무영속성기획 · 생체인식 · 프로그래밍 보안	· 정수론 · 대수학 · 확률/통계론 · 정보/부호이론 · 암호론 · 정보보호개론 · 정보보호관련윤리 · 정보보호관련법률 · 정보보호 기술표준화

http://www.kisa.or.kr/kisa/notics/jsp/sis_1010.jsp

Wide Spectrum of Job Opportunity

- Security Manager of Information Systems
  - We are depending more and more on information systems
  - National security / corporate security / organization security
  - CIO (chief information officer) and CSO (chief security officer)
- Engineer and developer of security products
  - Security needs to be incorporated into wide range of IT products
  - Wide spectrum of security applications
- Advanced Researcher
  - Cryptography
  - Information security

5. Lecture Outline

Objectives of this Lecture

- Understanding the basic concepts on
  - information security
  - cryptography (as a basic tool for information security)
  - Internet security mechanism
  - Electronic commerce security
- Can try to solve security problem in my area
- What is your objective? To be a security expert?

Textbook and References

- ✓ **Textbook**
  - ✓ **Wade Trappe, Lawrence Washington, "Introduction to Cryptography with Coding Theory", 2nd Ed, 2005, Prentice Hall ISBN 0-13-186239-1**
- ✓ **References**
  - ✓ **Richard A. Mollin, "An Introduction to Cryptography", Chapman & Hall/CRC, 2001, ISBN 1-58488-127-5**
  - ✓ **Josef Pieprzyk, T. Hardjono, J. Seberry, "Fundamentals of Computer Security", Springer**
  - ✓ **Douglas R. Stinson, "Cryptography – Theory and Practice", CRC press**

- ✓ **You need to have the textbook! Since cryptology is not an easy topic, your study should be firmly based on a textbook.**

Lecture Schedule

1. Introduction and overview
2. Classical Ciphers
3. Block / Stream Ciphers
4. Hash Functions / MAC
5. Number Theory

❖ Midterm Exam

6. Public Key Cryptosystems
7. Network Security
8. Cryptographic Protocols
9. Electronic Commerce

❖ Final Exam

Lecture Notes

- ✓ Introduce large spectrum of security topics
  - ✓ Introduction to information security
  - ✓ Cryptology
  - ✓ Network security
  - ✓ Cryptographic protocols
  - ✓ E-commerce

- ✓ Some parts of this lecture notes are originally from material by
  - ✓ prof. Kwangjo Kim (ICU)
  - ✓ prof. Chaehoon Lim (Sejong Univ.)

- ✓ TA : Hyunrok Lee (tank@icu.ac.kr)

- ✓ Webpage : http://caislab.icu.ac.kr/Lecture/data/2007/summer/ice1212/

Homework #1

Write a free-style essay on the following topics

1. **Introduction of yourself**
2. **Your interest on information security**
3. **Your study plan and its relevance to information security**