Computer and Network Security / Cyber Physical Systems Security

Dr. Chan Yeob Yeun

Week 1

Dr. Chan Yeob Yeun

Education

Royal Holloway, University of London
Ph.D. in Information Security
Royal Holloway, University of London
MSc. in Information Security

Professional Careers

Associate Professor at KU (2016 – Present)
Assistant Professor at KUSTAR (2008 - 2016)
Visiting Professor at KAU (2008 – Present)
Invited Professor at KAIST (2007 - 2008)
Vice President / Research Fellow, LG Electronics, MC R&D, S. Korea (2005 - 2007)
Leader of Wireless Security, Toshiba Telecommunication Research LAB, UK (2000-2004)
Industrial Supervisor at University of London and University of Bristol (2001-2004)
Industrial Security Mentor at Mobile Virtual Centre of Excellence (2001-2004)
Editor-in-Chief of International Journal of RFID Security and Cryptography (2011-Present)
Editor of International Journal of Convergence (2011-Present)
Editor of Journal of Information Security and Applications (2019-Present)

Course

Title : Computer and Network Security (ISEC 615)/
Cyber Physical Systems Security (CSEC 601)

Credit/Hour : 15/ 3.0

Instructors: Dr. Chan Yeob Yeun
Email: chan.yeun@ku.ac.ae
Room: L02030C
Tel: +971 2 5018572

Hours : Mon, 5:00pm – 6:15pm
Wed, 5:00pm – 6:15pm

Course Descriptions

1. Course Aim

To provide students with the concepts of securing modern computer systems and networks and to address common problems that lead to computer and network insecurity.

2. Textbook

A. Main Textbook :

1. Security and Privacy in Cyber-Physical Systems: Foundation, Principles, and Applications.

Houbing Song, Glenn A. Fink, Sabina Jeschke

Wiley-IEEE Press, 2017

ISBN 10:9781119226048

2. Computer Security

Dieter Gollmann

John Wiley & Sons Ltd, 2nd Edition, 2006

ISBN 0-470-86293-9

Course Descriptions

2. Textbook

Recommended Reading Material:

Cryptography and Network Security: Principles and Practice
William Stallings, 2010
Prentice Hall, 5th edition,
ISBN 978-0136097044

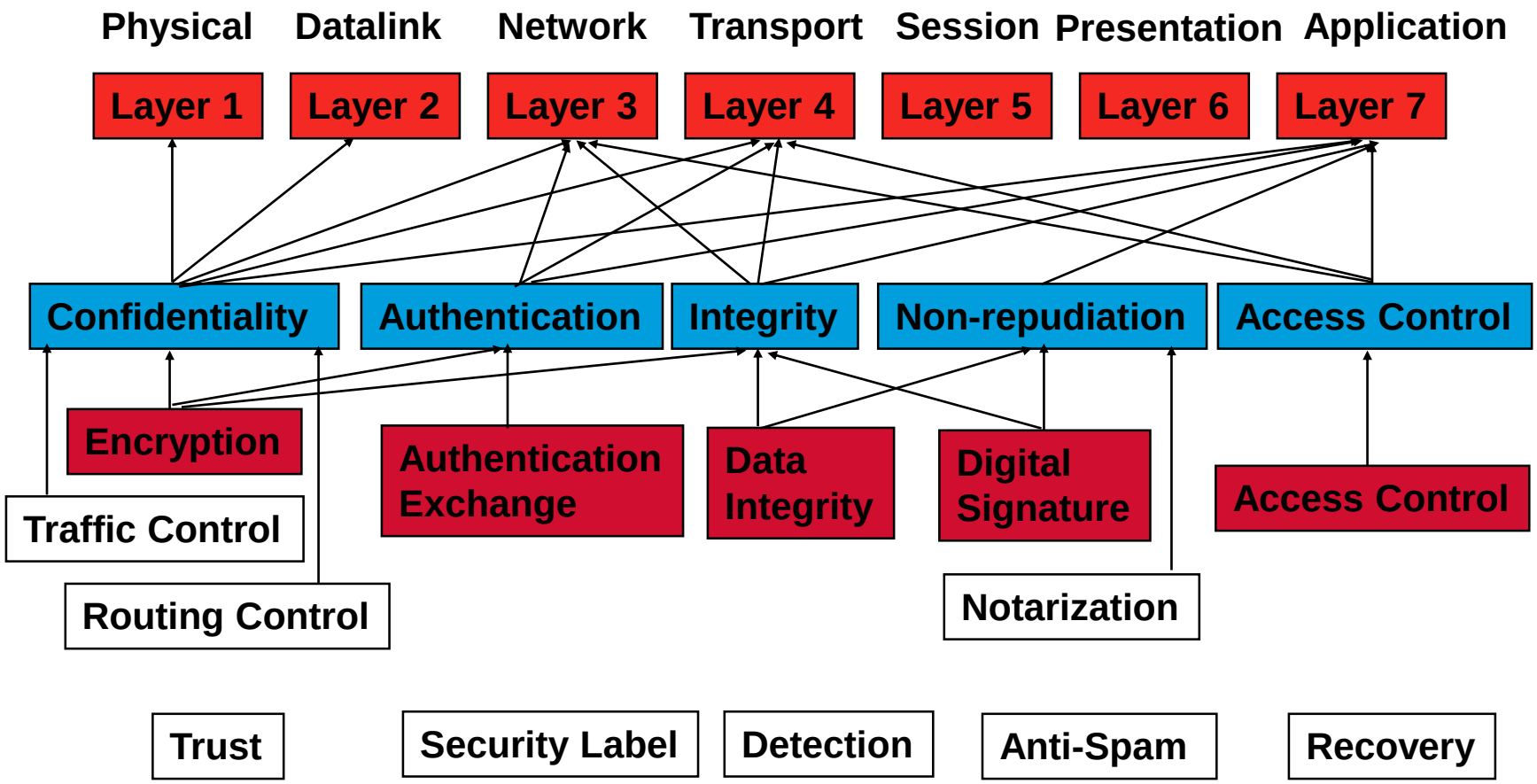
3. Methods of Assessment

Quizzes:	30%
Assignment:	25%
Presentation:	5%
Exam:	40%
Total:	100%

Weekly Lecture Plan

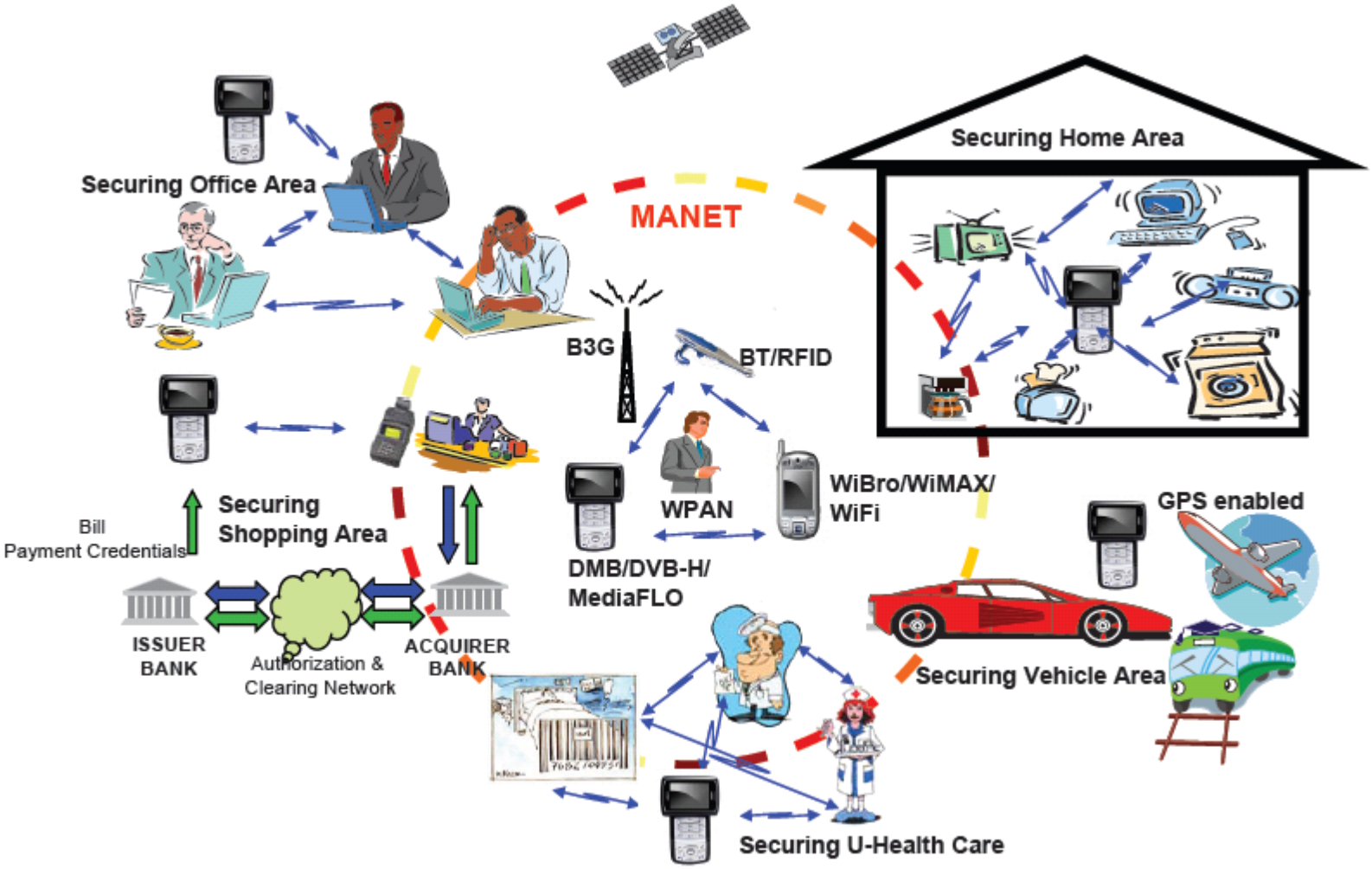
Wk	Contents	Cmt	Wk	Contents	Cmt
1	**Introduction**		9	Foundations of Network Security II	
2	Foundations of Computer Security	Tutorial Assig Plan	10	Network-Based Threats and Attacks	
3	Identification and Authentication I		11	Network Security Protocols I	
4	Identification and Authentication II	Quiz 1	12	Network Security Protocols II	Quiz 3
5	Access Control		13	Firewalls	
6	Modern Computer Attacks		14	IDS / IPS	Assig Submit
7	Malicious Code	Assig Confirm	15	Revision and Presentation	
8	Foundations of Network Security I	Quiz 2	16	Exam	

What is Computer and Network Security ?



Security, Privacy and Trust in U-Network

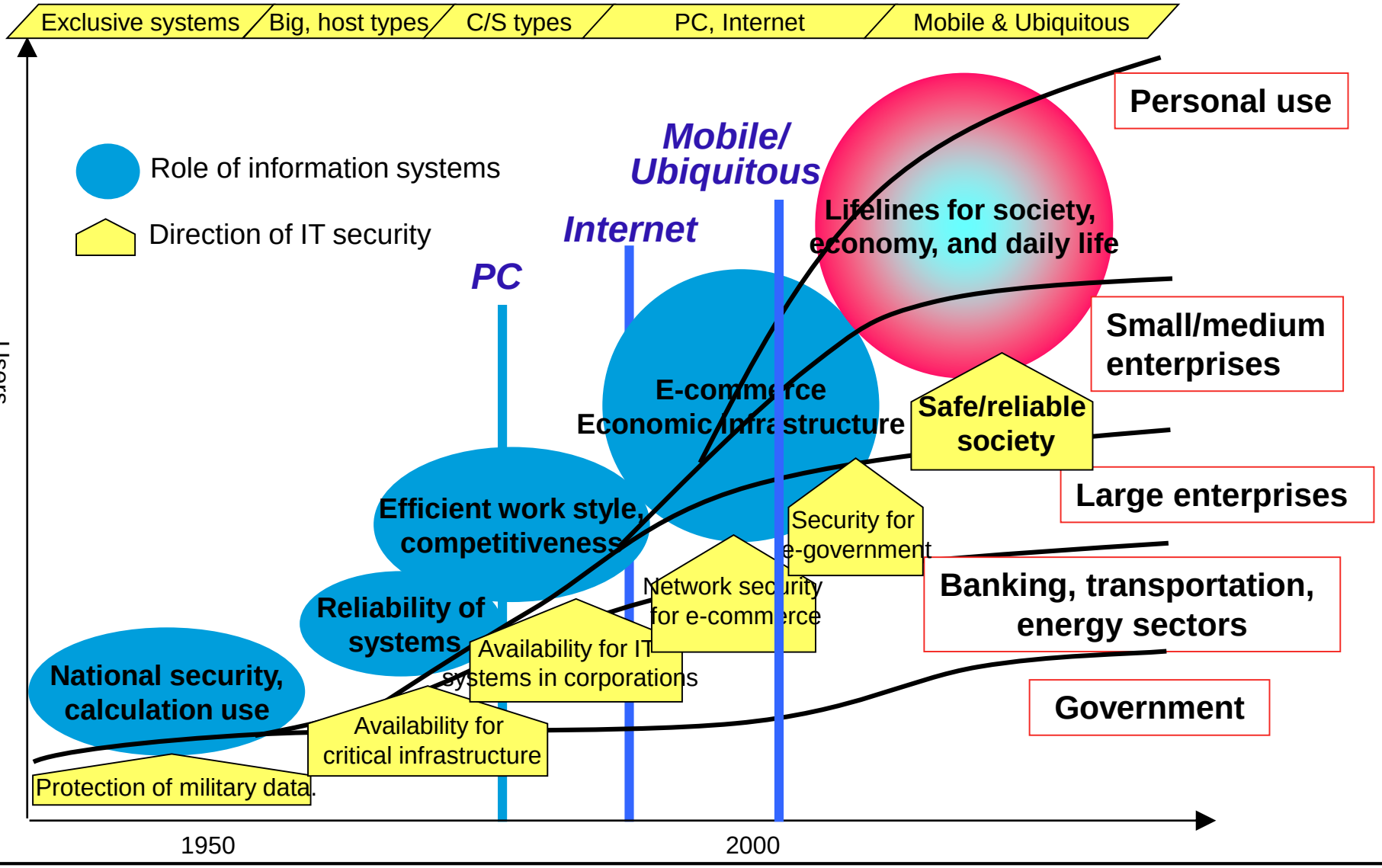
How to manage security, privacy and trust?



What is U-Network?

https://www.youtube.com/watch?v=Mbg8w9IB1H8

Trends of IT Security



Issues in U-Networks

Ubiquity	Infra will be everywhere, affecting everyday life
Invisibility	No idea when or where they use the computer
Sensing	Sense what we do, say, type
Memory Amplification	Every interactions be stored

u-Society

Intervene with Personal, Intimate Experience

Security, Privacy, Trust

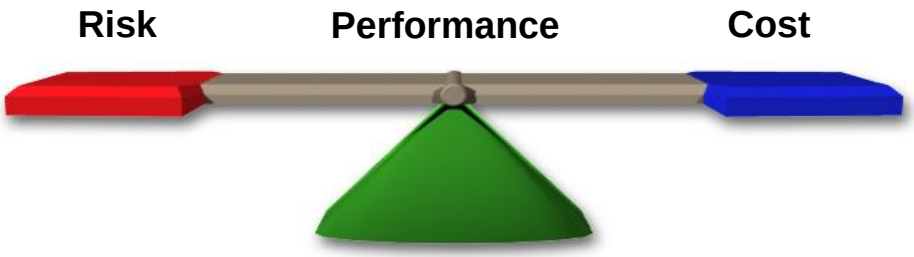
Changes in smart environments

- No physical and cognitive signs for data collections
- Trade off between privacy and usability

New Paradigm in U-Networks

Performance vs. Cost

- Trade-Off : Risk, Cost , Performance
- High Level Dependability without high cost
  - Highly interconnected system



Only the right people get access at any time to the right information with the best possible performance and at the lowest possible cost

New Paradigm in U-Networks

Embedded Security

Patching Security Function after implementation

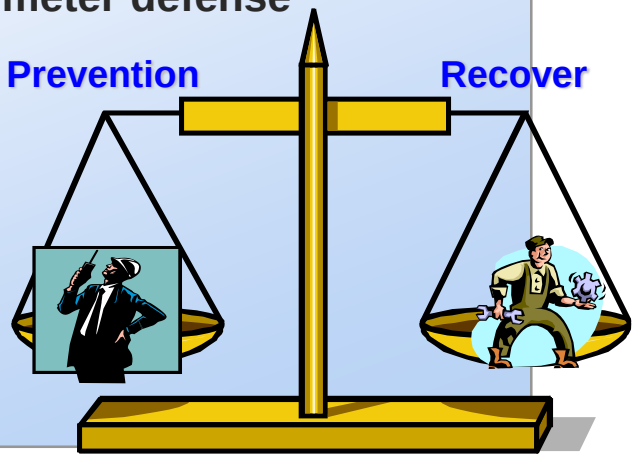
- Endless patches for vulnerability is not answer
- Cause end-user's burden for security

Needs for new Security Model, Method

- Principal of mutual suspicion vs. Concept of perimeter defense
- end-to-end Security

100% Prevention is not possible

- Need prevention and recovery system
- Minimize damage & Quick Recovery



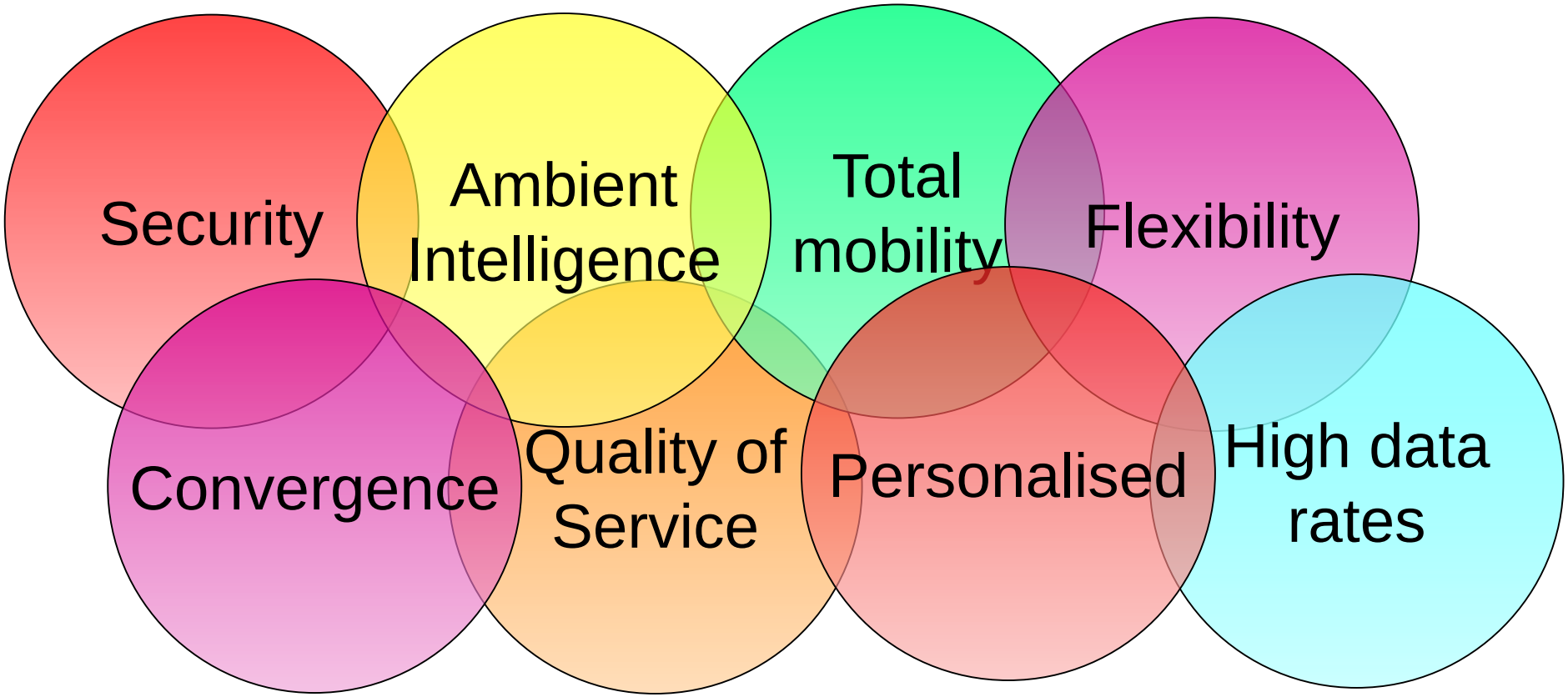
Security Requirement in U-Network

Security requirement		Special Requirement in U-network
Basic	Availability	DoS attack, Priority management in access control, Differentiated service
	Confidentiality	Key management, light weight cryptography, secure DB, mobile cryptography
	Integrity	Integrity mechanism for U-network
Additional	Authentication	Mutual authentication, use of dynamic key, Wireless PKI, device authentication, Central authentication, QoS
	Control of delegate	Entity authentication and authorization Access control
	Anonymity	Transfer of real ID information
	Safe roaming	Global roaming, DRM, Seamless secure roaming

Vulnerabilities in U-Network

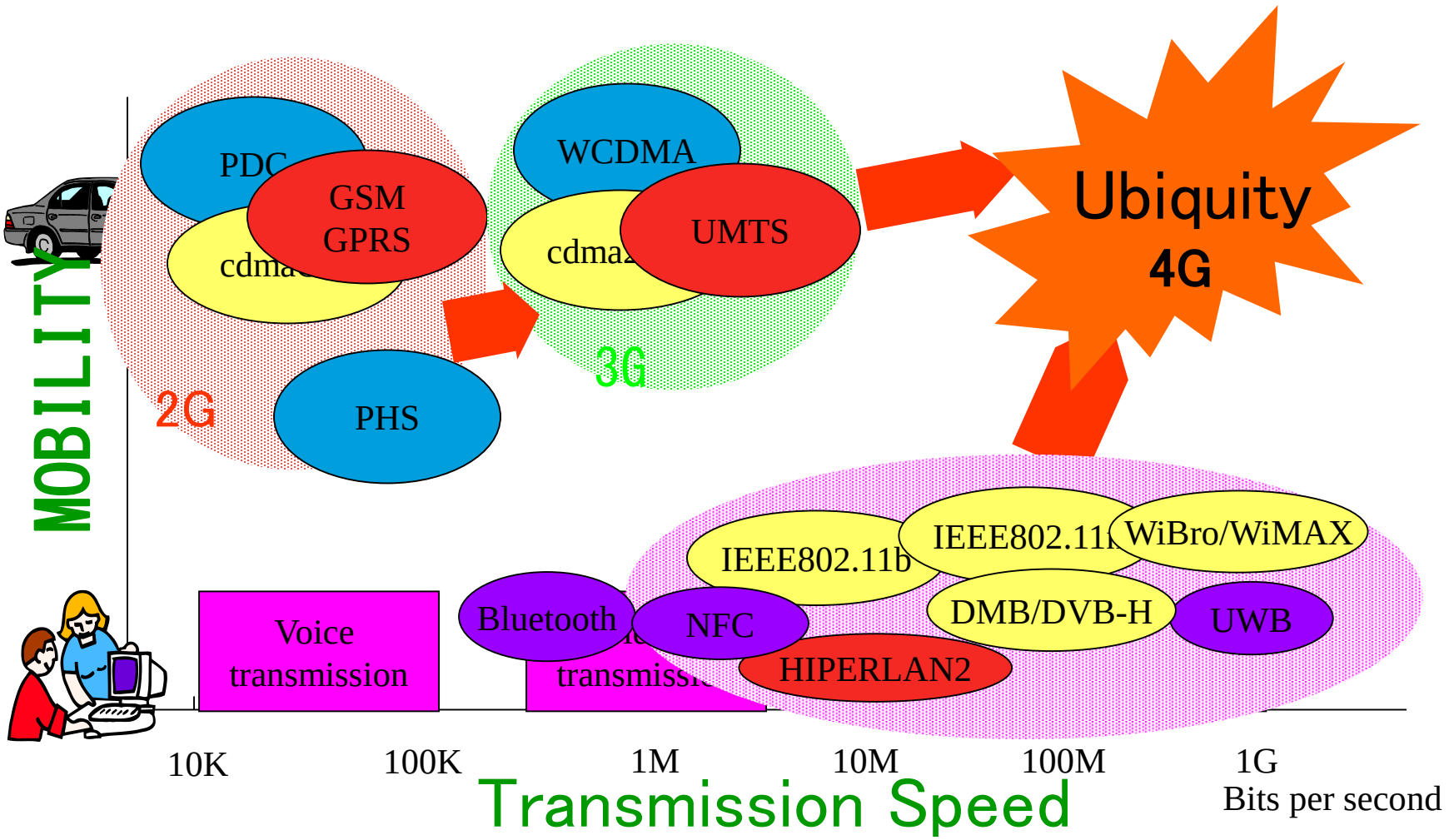
Risks	Type of Intrusion	Problem	Countermeasures
Theft or Stolen	Confidentiality Authentication	Device holders have authentication information	Entity (or device) authentication/Cryptography
Illegal Access Point	Authentication	1-way authentication	Mutual authentication
IP Spoofing	Confidentiality	Radiation of RF signal to unwanted user	Cryptography
(D)DoS	Availability	Degraded availability	Availability
Trojan Horse, Worm, Virus	Availability, Confidentiality, Integrity	Degraded availability & integrity	Anti-Virus program
Attack by harmful signal	Availability	Interfered communication channel	Spread Spectrum-Frequency Hopping
Resource consumption attack	Availability	Out of battery power	Availability
Revealing Location or ID-information	Confidentiality	Privacy	Anonymity

Key concepts for the ubiquitous networks future

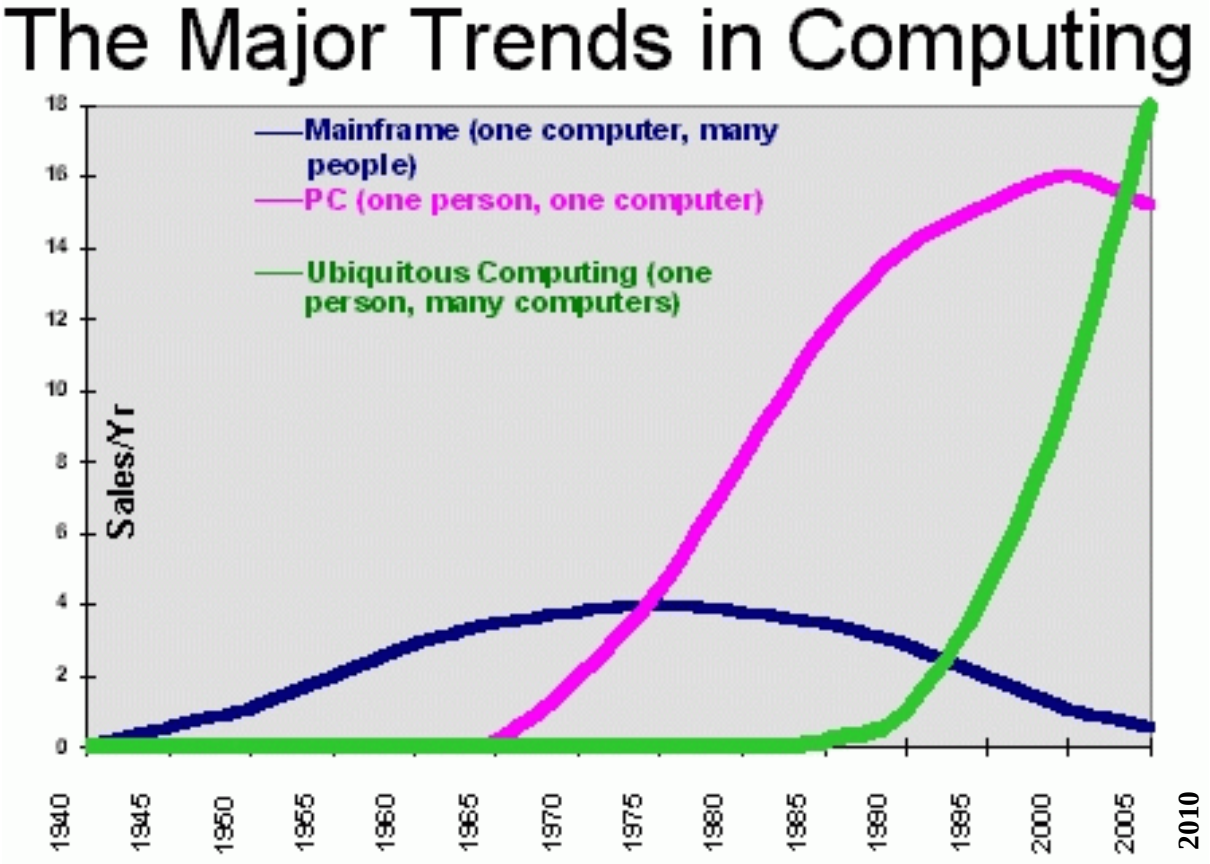


Introduction – Ubiquitous networks Vision

User is able to access any service anywhere, on any device, at any time and across any network



Introduction – Major Trends in Computing and Communications



Reference: Alan Daniel, Georgia Institute of Technology.
http://www.cc.gatech.edu/classes/cs6751_97_fall/projects/gacha/daniels_essay.html

Introduction – What is Ubiquitous Networks?

Smart environments for Ubiquitous Society will ensure secure communications with

- Anyone,
- Any organisations,
- Anytime,
- Anywhere,
- Any networks and
- Any devices (A6)

Example projects

AT&T Active bat/badge, HP Cooltown, Microsoft Aura, Intel Place Lab, Berkeley Smart Dust and PersonalServer, MIT AutoID

Introduction – Characteristics of Ubinet

- Heterogeneous nature of the UbiNet Environment.
  - A diversity of security mechanisms and credentials have to be integrated and managed.
- Dynamic nature of the UbiNet Environment
  - It challenges maintaining continuity of security as the topology changes
- Trust
  - It is difficult to establish trust in new devices as they join/leave the UbiNet Environment including Mobile Ad hoc Networks (MANET).
  - MANETs with a very limited coverage and without the need for infrastructure
- Where do we currently stand?
  - Ubiquitous services such as currently mostly “location-based”, home networking, Remote monitoring, home/office/shopping/healthcare applications.

Introduction – Security challenges of Network/Ubinet

What is the security properties we want in Network/Ubinet?

Confidentiality
Integrity
Availability
Authentication and Accountability
Increased mobility results in interesting security challenges
Dynamic Key Management (NP-Hard Problem) in MANET and Wireless Sensor Networks (WSN)
Overcome Malicious insider attacks
Single log on security with biometric techniques

Introduction – Security challenges of Ubinet

Confidentiality

Cryptography

Authentication

Digital Certificates

Integrity

Digital signatures and MAC

Non-repudiation

Digital signatures and certificates

Introduction – Security challenges of Ubinet

Global availability of UbiNet management functions

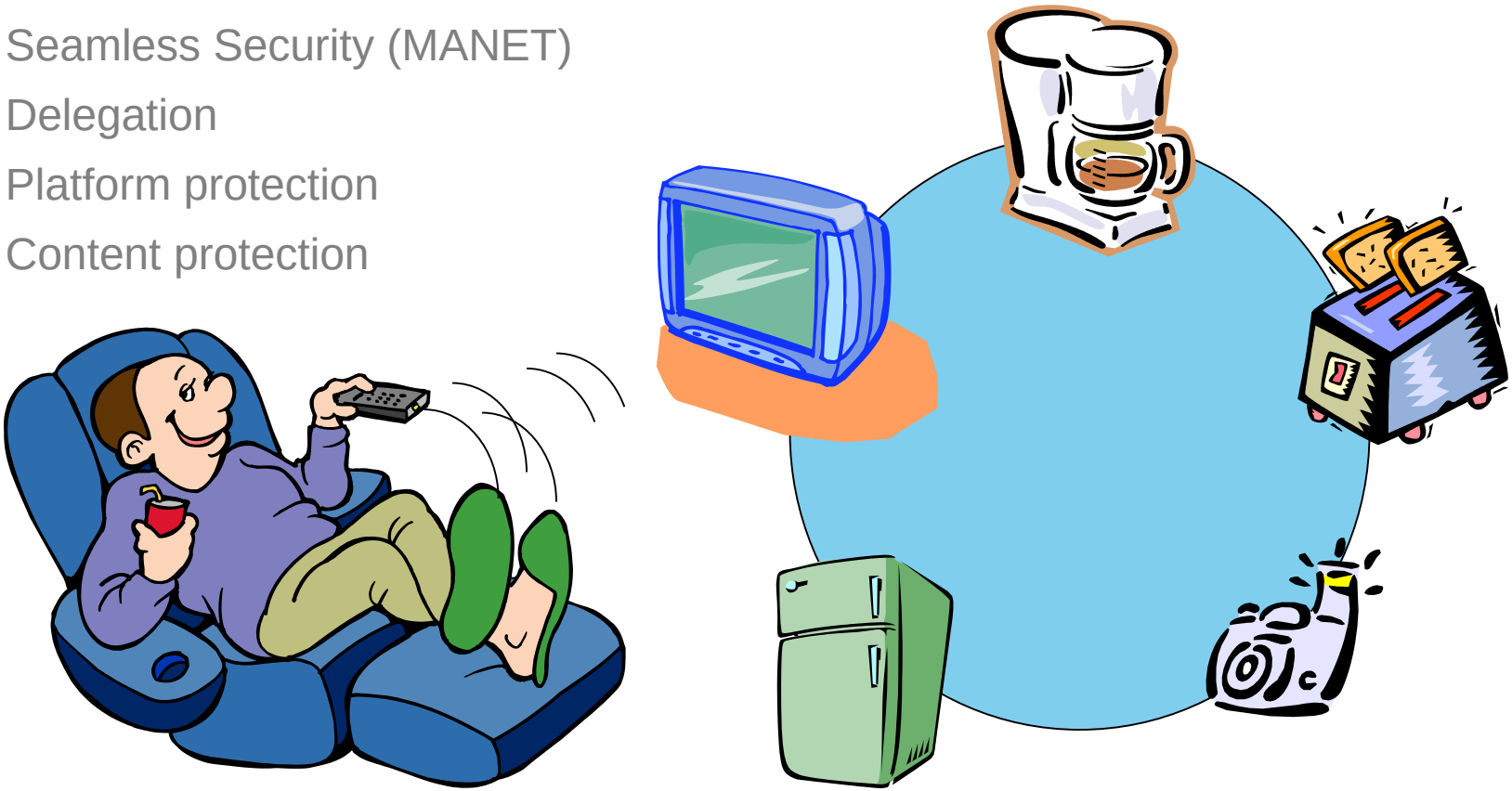
Best efforts operation of UbiNet environment

Seamless Security (MANET)

Delegation

Platform protection

Content protection



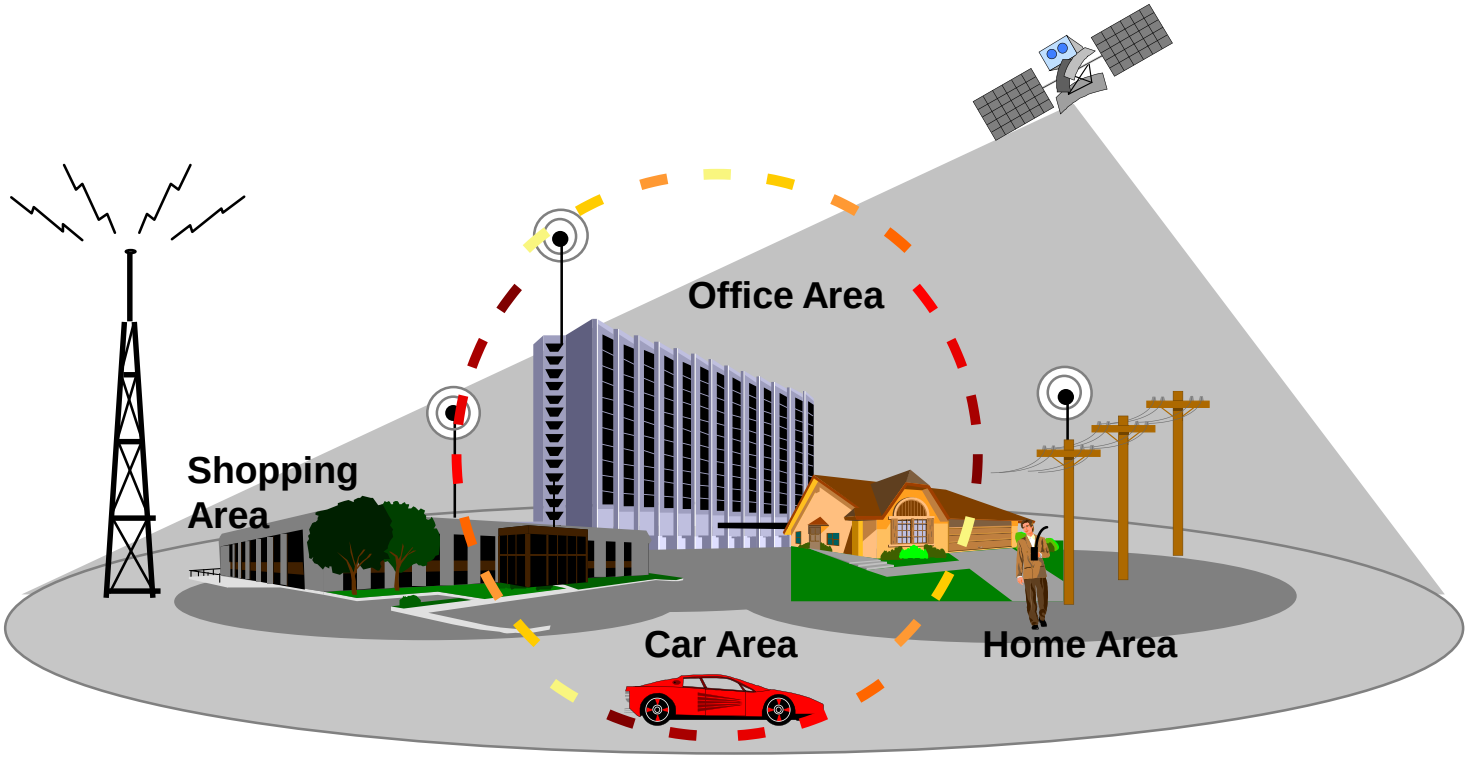
Introduction – Security mechanisms

- Most critical and complex issue:
  Key Establishment
  - Key Agreement (e.g. Diffie-Hellman key agreement)
  - Key Transport (Transfer of a specific key chose a priori by one party)

- Symmetric key transport and derivation with a server
  - Symmetric Key Transport with Server-Based Protocols

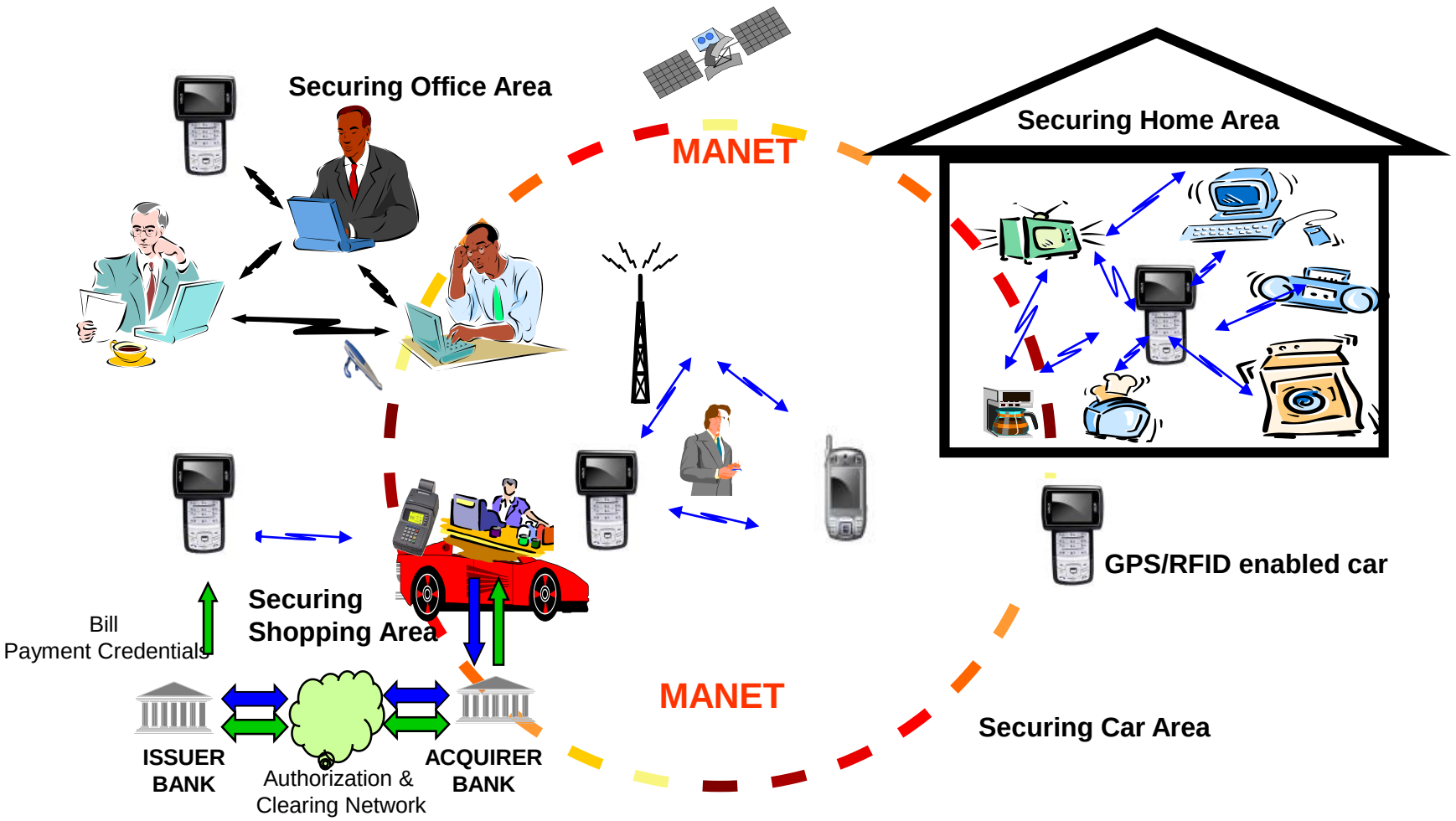
- Asymmetric or ID-based cryptography is appropriate for Mobile Ad hoc Networks (MANET) to authenticate nodes
  - Authenticated Group Key Agreement Protocols

Ubinet Security Research



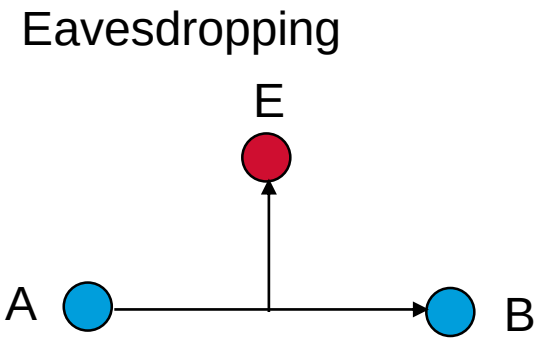
In Ubiquitous Society we envisage a continuous, secure and seamless use of wireless networking and broadband technologies in mobile communication, office networking, car networking and home networking.

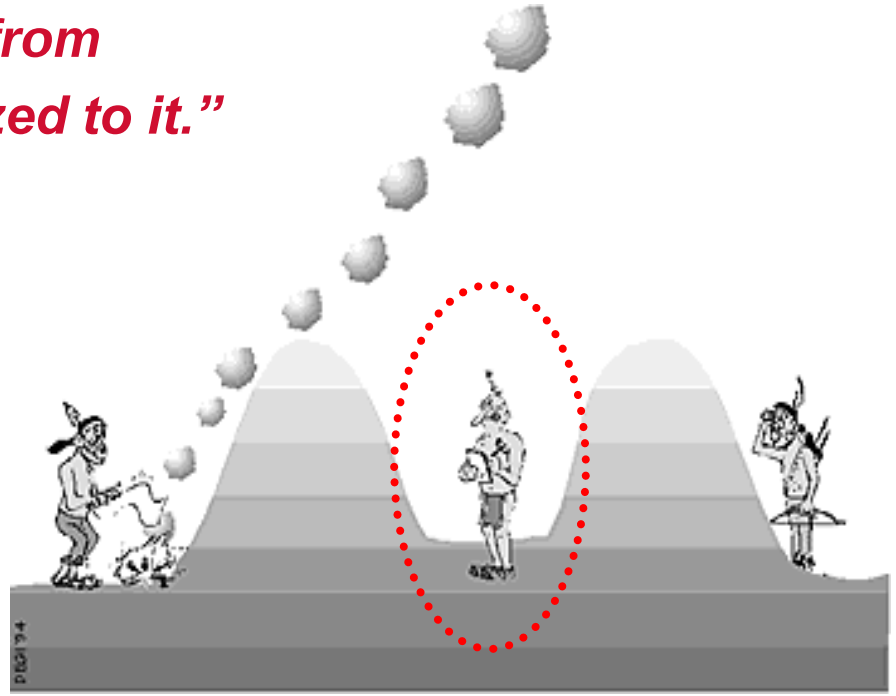
Ubinet Security Research – Securing UbiNet



Security Requirements - Confidentiality

"Keeping information secret from all but those who are authorized to it."





Attacker (Eavesdropper)

※ *Pictures are taken from the CryptMail User's Guide, Copyright (C) 1994 Utimaco Belgium,*

Security Requirements - Authentication

✓***Entity authentication (or identification)*** **:**

Corroboration of the identity of an entity

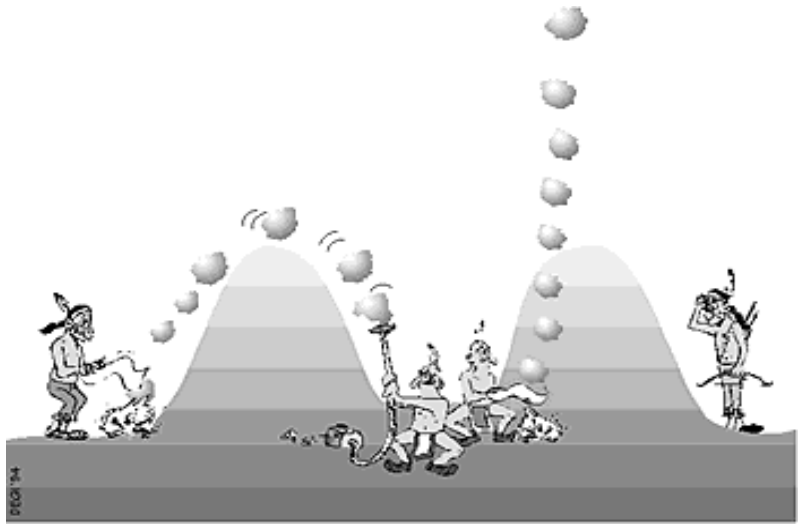
(e.g., a person, a computer terminal, etc)

✓***Message authentication :***

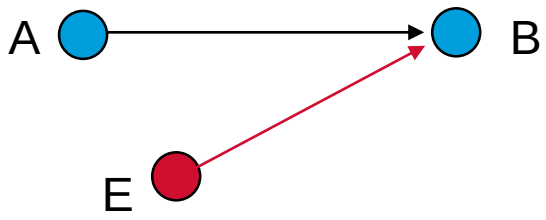
Corroboration the source of information

also known as data origin authentication

= data integrity

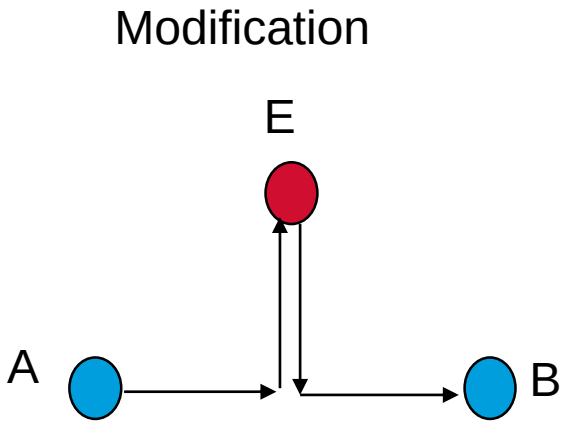


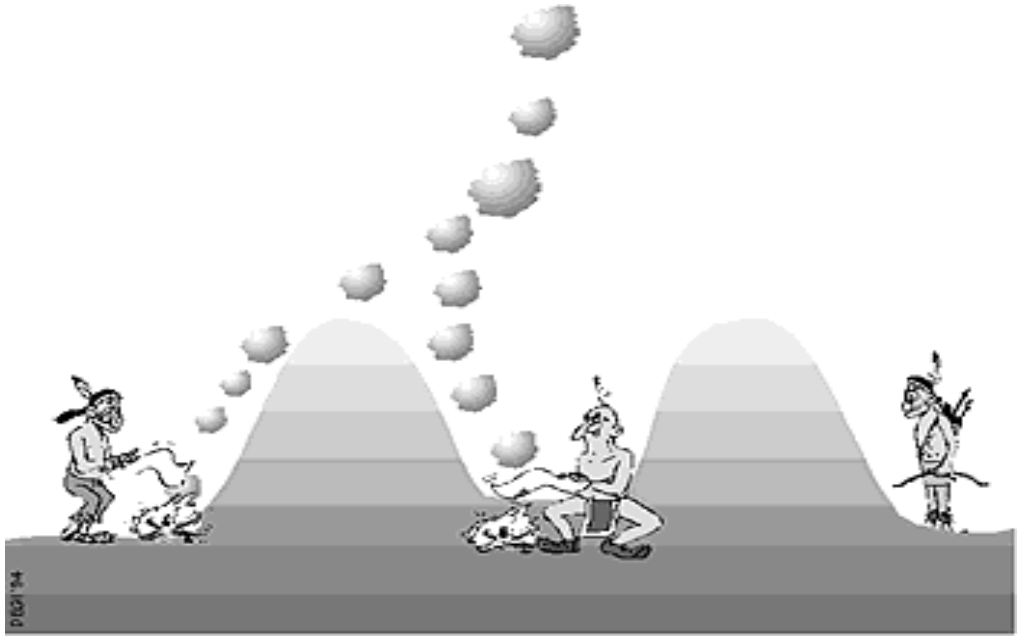
Impersonation



Security Requirements - Integrity

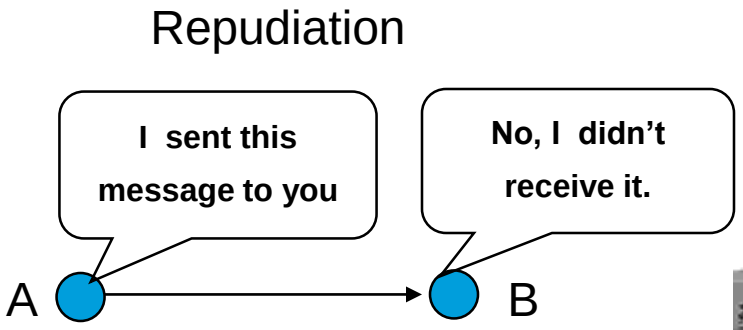
"Ensuring information has not been altered by unauthorized or unknown means."

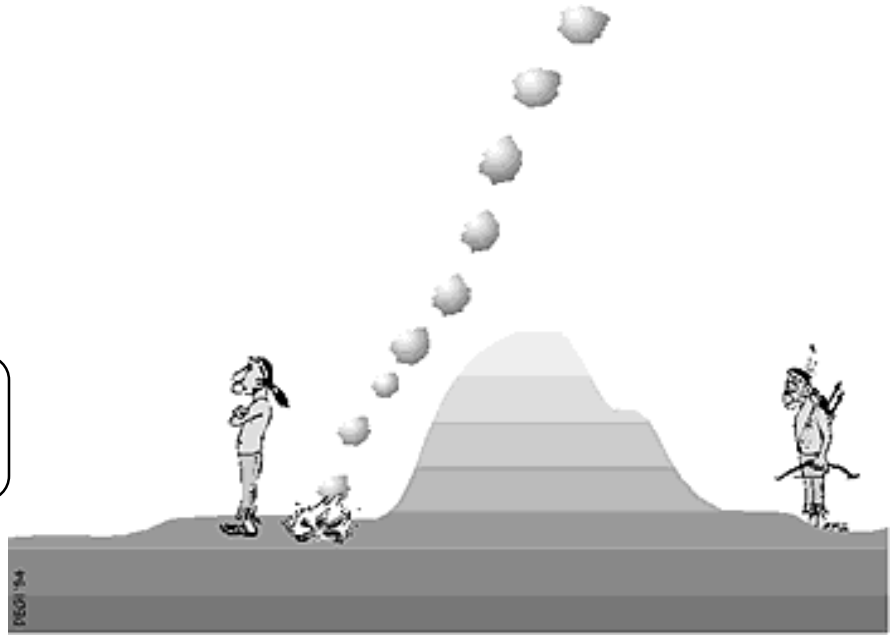




Security Requirements - Non-repudiation

"Preventing the denial of previous commitment or actions."





Types of Attacks

Access

An attempt to gain unauthorised access to information that the attacker is not authorised to see

Modification

- An attempt to modify information that the attacker is not authorised to modify

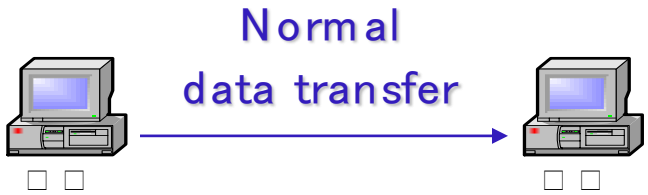
Denial-of-Service

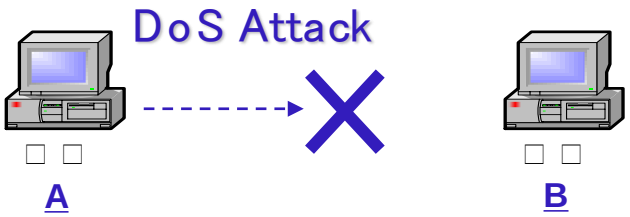
An attempt to deny the use of resources to legitimate users.

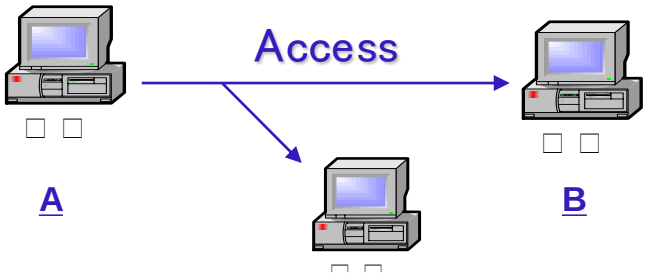
Repudiation

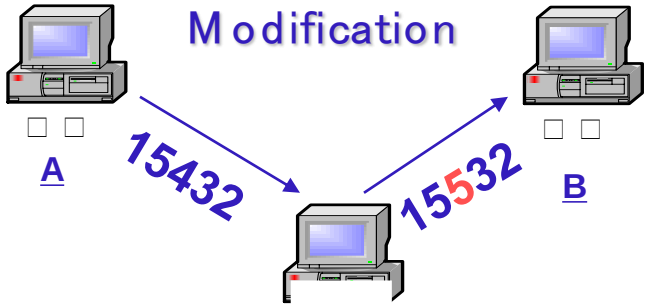
An attempt to give false information or deny that a real event or a transaction has occurred.

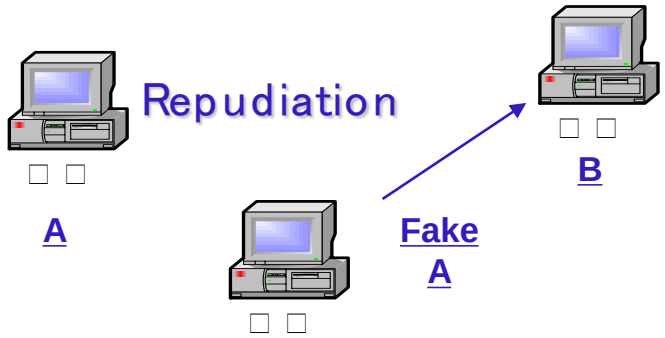
Types of Attacks











Note: These attacks could apply to network traffic as well as to data on standalone systems.

Attacks Vs. Security Services

- **Each of these attacks can mainly affect one or more security service**

Attack	Security Service			
	Confidentiality	Integrity	Availability	Accountability
Access	X			X
Modification		X		X
Denial of Service			X	
Repudiation		X		X

Introduction to Cryptology Concepts (1/3)

The word Cryptology stems from Greek meaning "hidden word".

Cryptology splits into two: Cryptography and Cryptanalysis.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, integrity, authentication, availability, accountability and non-repudiation.

History of Cryptography Research (I) (2/3)

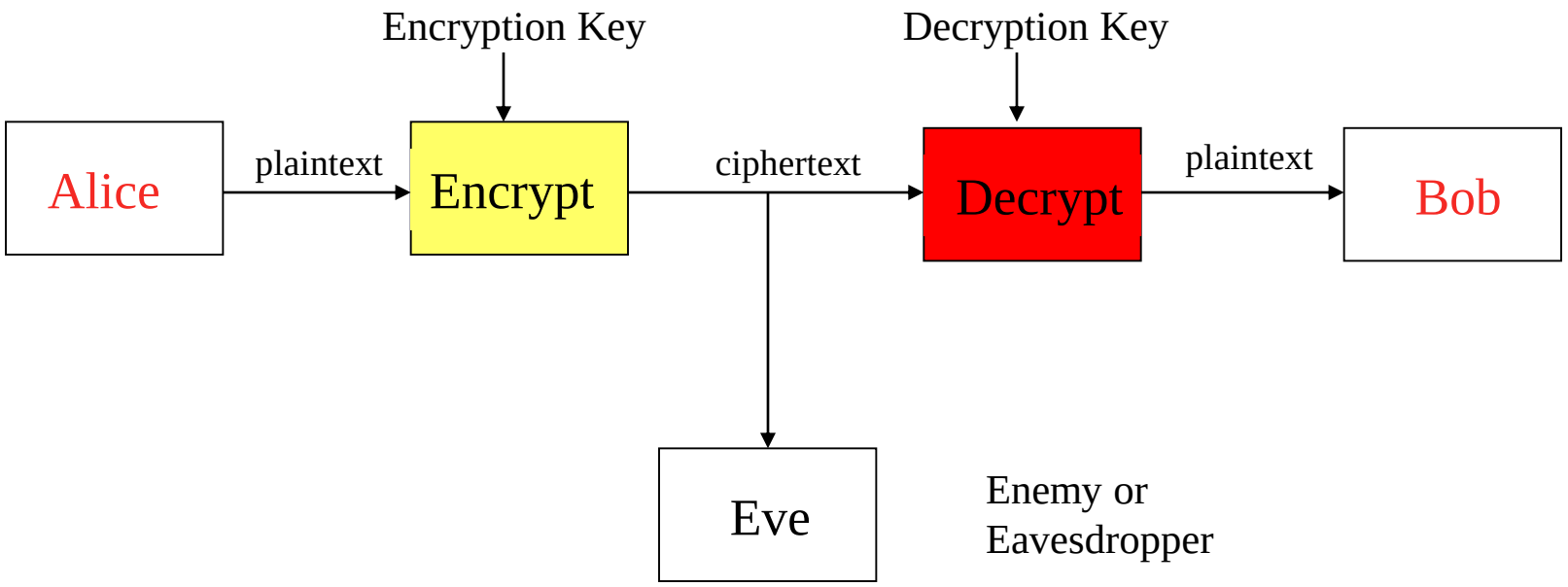
1900BC : Non-standard hieroglyphics
1500BC : Mesopotamian pottery glazes
50BC : Caesar cipher
1518 : Trithemius' cipher book
1558 : Keys invented
1583 : Vigenere's book
1790 : Jefferson wheel
1854 : Playfair cipher
1857 : Beaufort's cipher
1917 : Friedman's Riverbank Labs
1917 : Vernam one-time pads

History of Cryptography Research (II) (3/3)

1919 : Hegelin machines
1921 : Hebern machines
1929 : Hill cipher

1973 : Feistel networks
1976 : Public Key Cryptography
1977 : DES
1979 : Secret Sharing
1985 : Zero Knowledge
1990 : Differential Cryptanalysis
1994 : Linear Cryptanalysis
1997 : Triple-DES
1998 ~ 2001 : AES
2001 ~ : Side Channel Attacks
2005 : Collusion Search Attack of SHA-1

Secure Communications



Basic Communication Scenario

Symmetric Key Cryptography

Encryption and decryption keys are known to both
i.e. Encryption key = Decryption key

communicating parties (Alice and Bob).

All of the classical (pre-1970) cryptosystems are symmetric.

Examples : DES and AES (Rijndael)

A Secret should be shared (or agreed) between the communicating parties.

Asymmetric Key Cryptography

Public key encryption (invented in the late 1970s), involves a different model.

Private Key - known only to the owner

Public Key - known to anyone in the systems with assurance

Sender encrypts the message by the Public Key of the receiver

Only the receiver can decrypt the message by her/his Private Key

Encryption key ≠ Decryption Key

Message Authentication Codes (MACs)

MACs are designed to enable the recipient of a message to verify its origin and integrity.

A MAC algorithm takes a secret key and a message as input and outputs a MAC (appended to the message as a type of integrity check).

If recipient has the same secret key, the MAC can be computed on received message and compared with sent value.

Hash Functions

Given arbitrary length m, compute constant length digest d = h(m)

Desirable properties

- h(m) easy to compute given m
- One-way: given h(m), hard to find m
- Weakly collision free: given h(m) and m, hard to find m' s.t. h(m) = h(m')
- Strongly collision free: hard to find any x, y s.t. h(x) = h(y)

Example use: password database, file distribution

Common algorithms: MD5, SHA

Digital signatures

Digital signatures are also a kind of public key cryptography.

For a digital signature algorithm, keys are again generated in pairs: public verification keys and private signing keys.

Private signature key of sender applied to message to yield a digital signature of the message.

Sent with message.

Any recipient with public verification key can check origin and integrity of the message.

MACs and Signatures

Whilst both MACs and signatures provide integrity and origin protection for data, they have different characteristics.

A MAC relies on shared secrets, and hence is appropriate in a point-to-point environment.

A signature enables the origin and integrity of a message to be independently checked by many recipients, and hence fits well to a broadcast or multicast environment.

Non-repudiation

Digital signatures can also provide non-repudiation.

Since verifier has only the public key, they cannot create signatures (compare with MACs).

Hence a digitally signed message may be of value as long term evidence of an event, which cannot be repudiated by the originator of the signature.

Authentication protocols

An authentication protocol is a cryptography-based exchange of messages, designed to enable participants to verify who it is they are communicating with.

Typically the protocols use MACs or signatures to protect individual messages.

However, apart from use of cryptography, means are required to verify that messages are not replays of old (valid) messages.

Security threats and services

All cryptographic schemes are designed to counter security threats.

Threats include:

- ***Eavesdropping on communications***
- ***Masquerade***
- ***Manipulation of communications***
- ***Repudiation***
- ***DoS***

Addressing threats by Cryptanalysis

A 'Security service' is a term for the provision of protection against a threat.

Examples include:

- *Confidentiality (to defeat eavesdropping);*
- *Entity authentication (to defeat masquerade);*
- *Integrity protection (to defeat manipulation);*
- *Non-repudiation (to defeat repudiation).*

Security services include as follows:

- *Encryption can provide confidentiality;*
- *Authentication protocols can provide entity authentication;*
- *MACs or digital signatures can provide integrity protection;*
- *Digital signatures can provide non-repudiation.*

Key management and PKIs

Any use of cryptography requires the generation and distribution of Key material (key management).

Key management for public key cryptography rather different than for 'secret key' cryptography.

Key management for secret key cryptography involves confidential and reliable transfer of secret keys.

Key management for public key cryptography is simpler – public keys are not secret.

However public keys still need to be reliably transferred.

Public key certificates

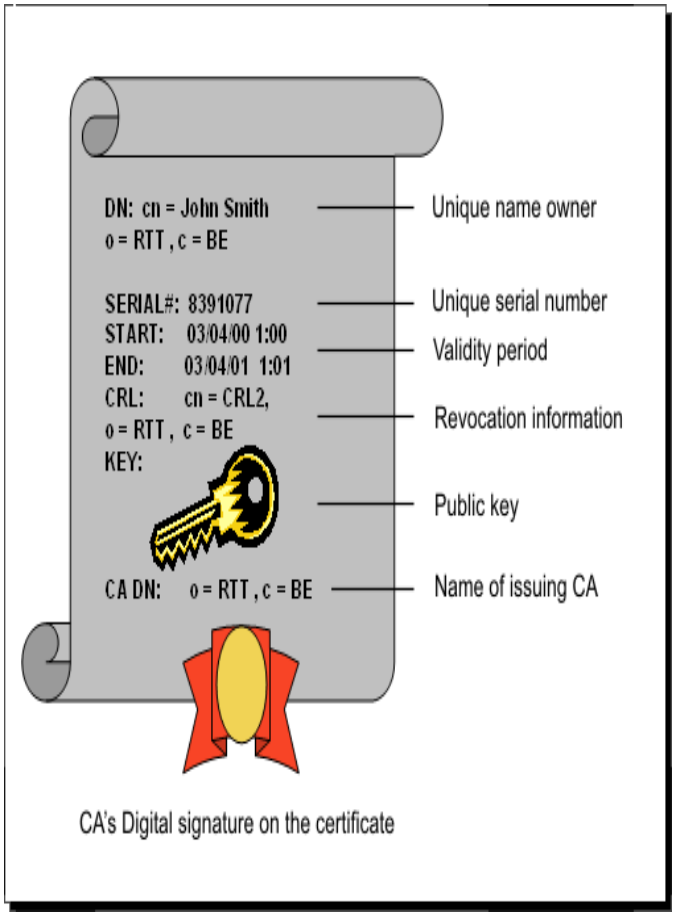
The Certificate Authority (CA) signs a concatenation of the public key, client name, and expiry date to form a public key certificate.

Anyone who verifies a public key certificate then has a reliable copy of the public key of the certificate owner.

Certificates (i.e. data structures signed by a Trusted Third Party, i.e. CA) can be used for things other then public keys.

An Attribute Authority can create Attribute Certificates, granting the owner privileges.

E.g. a network operator could sign an attribute certificate saying that a particular software vendor is reliable.



Authorisation and access control

Authorisation is a term relating to the notion of access control.

Any system will often need to make a decision about whether another entity should be allowed to perform a particular action.

This is normally referred to as access control.

Summary of Basic Definitions

Confidentiality

Cryptography

Authentication

Digital Certificates

Integrity

Digital signatures and MAC

Non-repudiation

Digital signatures and certificates