Topic 1

An Introduction

Introducing the course unit and basic concepts of security

- **Home reading: Chapter 1, Cryptography and Network Security,** 7th Edition by William Stallings; You may also be able to live with an older edition of this book.
- Some of the slides/data here are from Cyber *Security Threats* slides by Dr Paul Twomey, the Lowy Institute for International Policy, Argo Pacific Pty Ltd**.**

Overview

- ❑ Introduction to the Course Unit
- ❑ Introduction to Security
  - ❍ What is Security
  - ❍ Security Problems and Challenges
  - ❍ Achieving Security
  - ❍ Security Models
- ❑ Course Roadmap
- ❑ Conclusion

source: Chapter 1 of Cryptography & Network Security

Introduction to the Course Unit

❑ Course Unit Leader, i.e. ME
  - ❍Ning Zhang
  - ❍KB2.113
  - ❍ning.zhang@manchester.ac.uk

  ❑Office hours: Monday pm (after class)

Introduction to the Course Unit

❑ **What this course is about:**
  - ❍Important and commonly used cryptographic methods and techniques
  - ❍Network security
    - ➢Security problems and countermeasures in the transmission of information
    - ➢security problems and countermeasures in networked computer systems

❑ **Who should take this module:**
  - ❍This is a technical module, so if you are interested in security and willing to learn some mathematical stuff, …
  - ❍the prerequisite for networking knowledge is minimal

Introduction to the Course Unit

- ❑ **Reading materials:**
  - ❍ **Main text book: Cryptography and Network Security,** 7ed by William Stallings; An older edition of this book will also be ok.
  - ❍ Many other useful books; you may use the lecture handouts to scope your reading.
  - ❍ There are many useful resources on the Internet, e.g. www.cert.org and www.nist.gov.
- ❑ All the teaching docs are in the Blackboard.

How to Take this Module

- ❑ Attend lectures
- ❑ After lectures
  - ❍ Read notes and recommended textbook
  - ❍ Do the given exercises
  - ❍ Download and install CrypTool available at: http://www.cryptool.org/index.php/en/download-topmenu-63.html (I recommend CrypTool 1.4.30 for Windows, if you run Windows, but there are also versions of JCrypt 1.0 beta for MacOS and Linux). This tool is also available in the third year lab. This is a free e-learning program designed to help you to understand cryptographic algorithms
- ❑ Assessment
  - ❍ 100% exam

Interactions and Feedbacks

- ❑ After every lecture, you are given a couple of exercises, i.e. questions or problems to work on
- ❑ You must do these given exercises – you may work on them yourselves, or in groups
- ❑ In subsequent lectures, I shall invite you to show your work on the board, and
- ❑ I will provide feedback based on your work!

What is Security?

Information hiding eCommerce security

Privacy Malicious code Digital Right Management

Digital signatures Trust

Integrity **eGovernment**

Threats/vulnerabilities

Access control Fraud Encryption **Key management**

POLICY MAKING **Computer forensics**

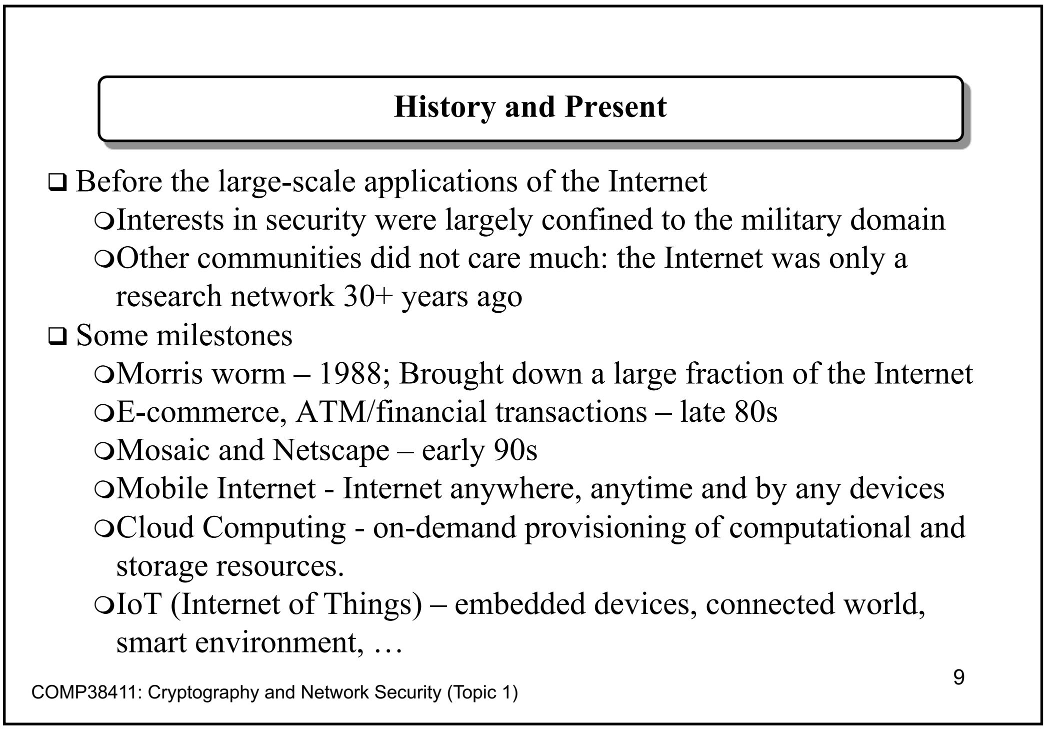
Biometrics

Information security Anonymity

Network security

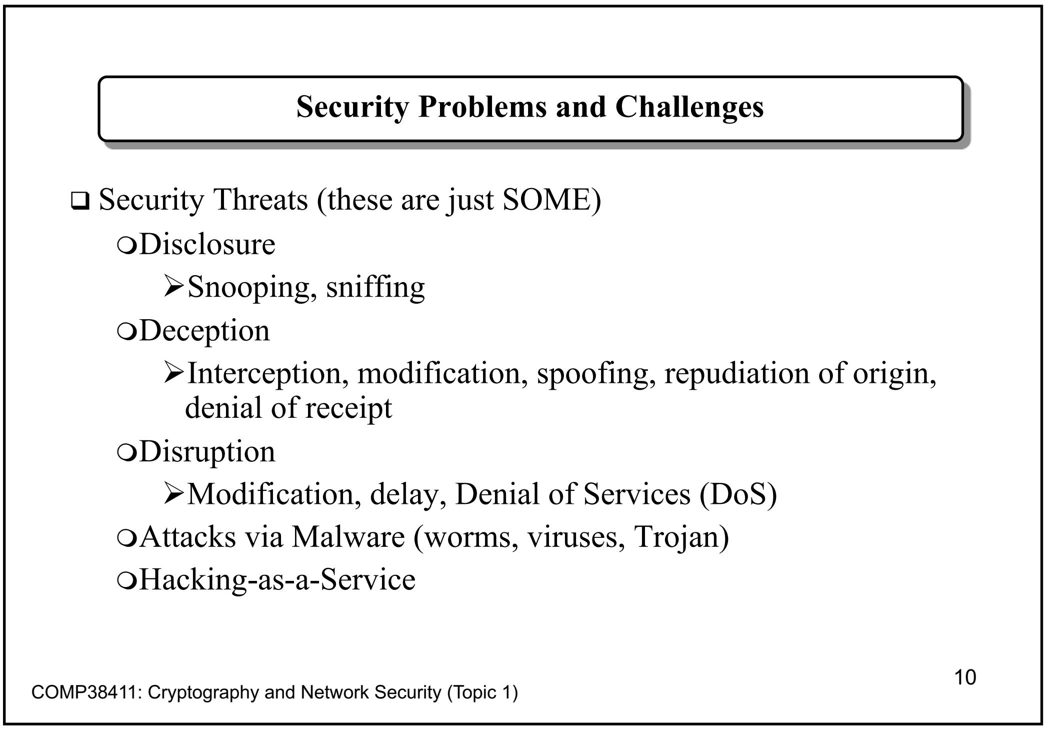
Cryptographic Algorithms & Protocols

Risk assessment



History and Present

- ❑ Before the large-scale applications of the Internet
  - ❍Interests in security were largely confined to the military domain
  - ❍Other communities did not care much: the Internet was only a research network 30+ years ago
- ❑ Some milestones
  - ❍Morris worm – 1988; Brought down a large fraction of the Internet
  - ❍E-commerce, ATM/financial transactions – late 80s
  - ❍Mosaic and Netscape – early 90s
  - ❍Mobile Internet - Internet anywhere, anytime and by any devices
  - ❍Cloud Computing - on-demand provisioning of computational and storage resources.
  - ❍IoT (Internet of Things) – embedded devices, connected world, smart environment, …



Security Problems and Challenges

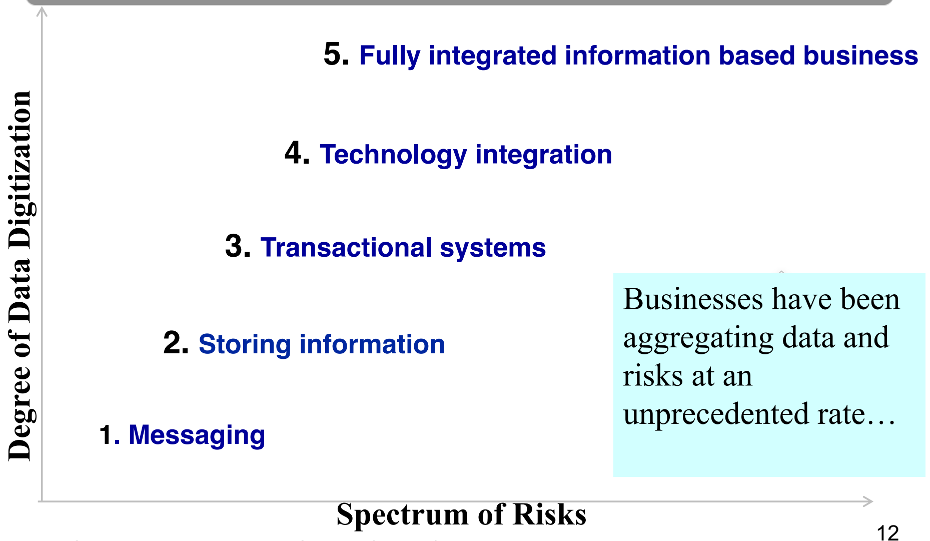
- ❑ Security Threats (these are just SOME)
  - ❍Disclosure
    - ➢Snooping, sniffing
  - ❍Deception
    - ➢Interception, modification, spoofing, repudiation of origin, denial of receipt
  - ❍Disruption
    - ➢Modification, delay, Denial of Services (DoS)
  - ❍Attacks via Malware (worms, viruses, Trojan)
  - ❍Hacking-as-a-Service

Hacking as a Service

- ❑ Consulting services such as botnet setup ($350-$400)
- ❑ Infection/spreading services (~$100 per 1K installs)
- ❑ Botnets & Rentals [Direct Denial of Service (DDoS) $535 for 5 hours a day for one week] , e-mail spam ($40 / 20K e-mails) and Web spam ($2/30 posts)
- ❑ Blackhat Search Engine Optimization (SEO) ($80 for 20K spammed backlinks)
- ❑ Inter-Carrier Money Exchange and Mule services (25% commission)
- ❑ Recruited CAPTCHA Breaking ($1/1000 CAPTCHAs)
- ❑ Crimeware Upgrade Modules: Using Zeus Modules as an example, range anywhere from $500 to $10K

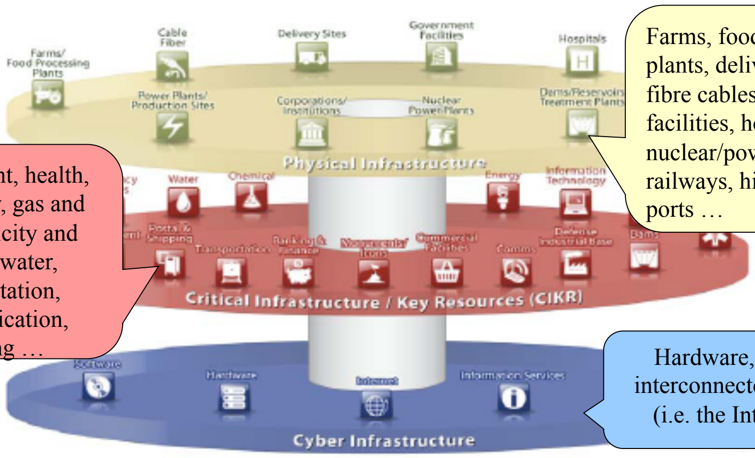
Source: Fortinet 2013 Cybercrime Report

Security Problems and Challenges


5. Fully integrated information based business
4. Technology integration
3. Transactional systems
2. Storing information
1. Messaging
Degree of Data Digitization
Spectrum of Risks

Businesses have been aggregating data and risks at an unprecedented rate…

Security Problems and Challenges



Government, health, emergency, gas and oil, electricity and energy, water, transportation, communication, banking …

Farms, food processing plants, delivery site, fibre cables, gov facilities, hospitals, nuclear/power plants, railways, highways, ports …

Hardware, software, interconnected networks (i.e. the Internet), …

Figure 2-3. Infrastructure relationships in cyberspace[10]

Source: DHS, "Securing the Nation's Critical Cyber Infrastructure

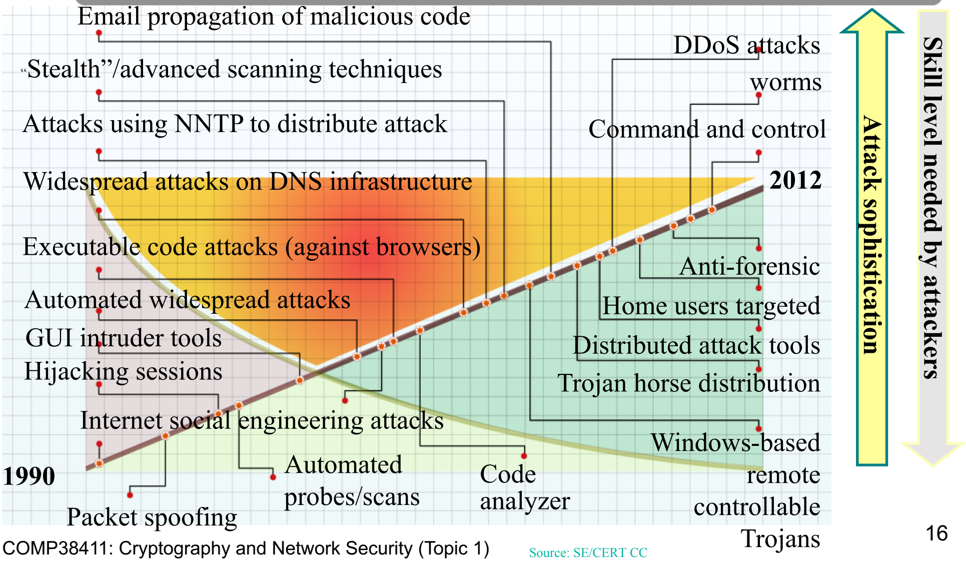
Threat Types	Motivation	Targets	Methods
Information Warfare	Military or political dominance	Critical infrastructure, political and military assets	Attack, corrupt, exploit, deny, conjoint with physical attack
Cyber Espionage	Gain of intellectual Property and Secrets	Governments, companies, individuals	Advanced Persistent Threats
Cyber Crime	Economic gain	Individuals, companies, governments	Fraud, ID theft, Extortion, Exploit
Cracking	Ego, personal enmity	Individuals, companies, governments	Attack, Exploit
Hactivism	Political change	Governments, Companpeis	Attack, defacing
Cyber Terror	Political change	Innocent victims, recruiting	Marketing, command and control, computer based violence

Source: analysis, Dr Irv Lachov

Security Problems and Challenges

- ❑ Naïve users - Lack of security awareness
- ❑ Inadequate management procedures
  - ❍Insecure system set-up and configuration
  - ❍Lack of proper policy making, implementation and enforcement procedures
- ❑ Global networks without national boundaries
- ❑ Heterogeneous devices, e.g. laptops, iPhones and PDAs, with universal connections
- ❑ Wireless and open channels
- ❑ Anonymous nature of many Internet-based services

Security Problems and Challenges



Email propagation of malicious code

"Stealth"/advanced scanning techniques

Attacks using NNTP to distribute attack

Widespread attacks on DNS infrastructure

Executable code attacks (against browsers)

Automated widespread attacks

GUI intruder tools

Hijacking sessions

Internet social engineering attacks

1990

Packet spoofing

Automated probes/scans

Code analyzer

DDoS attacks

worms

Command and control

2012

Anti-forensic

Home users targeted

Distributed attack tools

Trojan horse distribution

Windows-based remote controllable Trojans

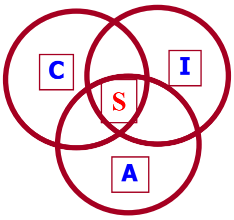
Attack sophistication

Skill level needed by attackers

Source: SE/CERT CC

Achieving Security – Basic security components

- ❑ Securing information: CIA
  - ❍Confidentiality
    - ➢Keeping data and resources hidden
  - ❍Integrity
    - ➢Data integrity (making sure data is authentic)
    - ➢Origin integrity (authentication)
  - ❍Availability
    - ➢Ensuring data/service is available to authorised users



Comment on C, I and A for these cases:
(1) Disconnect a computer from the Internet;
(2) Have extensive data checks by different people/systems.

Achieving Security – Life-cycle

- ❑ Threats analysis and identification
  - ❍Decide what to protect
- ❑ Policy specification: defining security goal
  - ❍Define what is, and is not, allowed
- ❑ Design and implementation: enforce policies (achieve security goal)
  - ❍Decide how to protect in order to satisfy the specification
    - ➢Technical measures
    - ➢Procedural measures
- ❑ Operation and maintenance: security assurance
  - ❍assess how well the implementation has achieved its security goal

Achieving Security – Threats analysis

- Identify assets, threats and vulnerabilities
- Assess the levels of risks on the assets based upon
  - Values of assets
  - Threats to assets and their importance
    - vulnerabilities and likelihood of exploitation
  - Not all threats are worth defeating (cost vs benefit)
- This may be carried out by using an Attack Tree

- Cost-benefit analysis
  - Is it cheaper to prevent (using security mechanisms) or recover (e.g. using restoration from backup) or just ignore?

Achieving Security – Threat analysis

- What is an **Attack Tree (Threat Tree)**
  - is a **“**conceptual diagrams showing how an asset, or target, might be attacked”.
  - is consisted of one root node, children and leaf nodes.
- The root node representing the Attack Goal.
- Child nodes are conditions which must be satisfied to make the direct parent node true.
- Conditions may be ‘OR’ or ‘AND’: ‘OR’ represents alternative attack methods or avenues to succeed in the attack, whereas ‘AND’ represents multiple steps in launching an attack.

  - Reference: https://en.wikipedia.org/wiki/Attack_tree

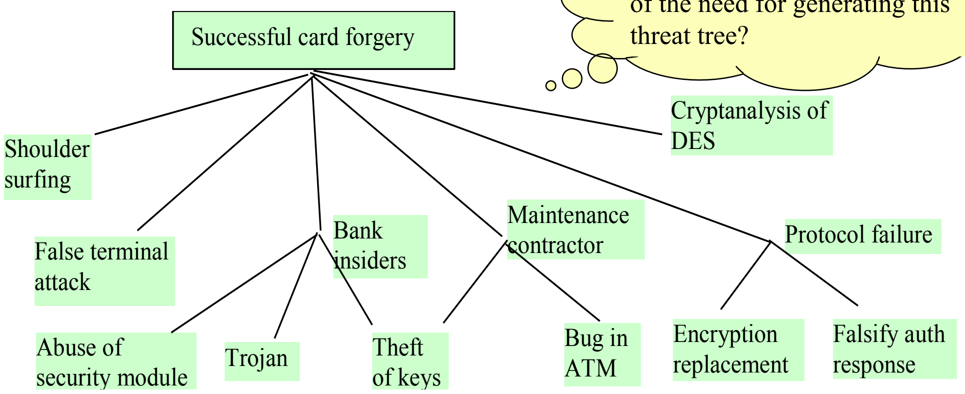
Achieving Security – Threat analysis

- ❑ Each node may be given a value to indicate, e.g.
  - ❍**likelihood** that an attacker will mount the attack, or **probability** of succeeding the attack
  - ❍**cost** in succeeding the attack, in terms of monetary cost, or time taken to accomplish the attack, etc.
- ❑ In this way, you could identify and make a decision as
  - ❍What, Where and How to protect your asset
- ❑ How to produce an Attack Tree
  - ❍Identify an attack goal
  - ❍Identify all the possible attack methods or avenues to achieve this goal

Achieving Security – Threat analysis

- ❑ An example of threat analysis using a **Threat Tree:**

Q: What can you see in terms of the need for generating this threat tree?



Successful card forgery

Shoulder surfing

False terminal attack

Abuse of security module

Trojan

Bank insiders

Theft of keys

Maintenance contractor

Bug in ATM

Cryptanalysis of DES

Protocol failure

Encryption replacement

Falsify auth response

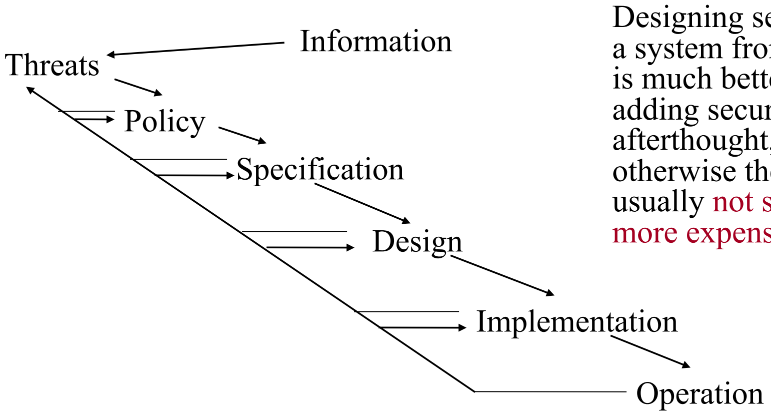
Achieving Security – Defining & achieving security goal

- Security measures: a method, protocol, tool, or procedure used to address the risks identified (or to enforce a security policy)
  - Prevention
    - Block attacks by closing vulnerabilities
    - Reduce the level of risks by making attack harder
    - Make another target more attractive than this target
    - E.g. access control (firewalls), encryption, digital signatures
  - Detection
    - Measures taken during or after the attacks
    - E.g. auditing and intrusion detection
  - Recovery
    - Stop attack, assess and repair damage
    - Continue to function correctly even if attack succeeds
  - Accept it and do nothing

Achieving Security - Operation and maintenance

- Assurance
  - Testing to check the correct implementation of policies.
  - Formal evaluation of the implementation.
  - Standards
    - US Security Evaluation Criteria (the Orange Book).
    - European ITSEC (Information Technology Security Evaluation Criteria).
- Human Issues
  - Organizational issues
    - Power and responsibility
    - Financial benefits
  - People problems
    - Outsiders and insiders
    - Social engineering

Tying It All Together



Designing security into a system from the start is much better than adding security as an afterthought, as otherwise the solution is usually not secure and more expensive.

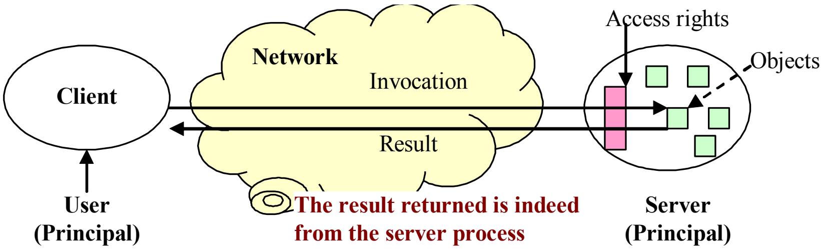
Security Models: A distributed system security model

- ❑ A quick question:
  - ❍Identify security threats in this model
  - ❍Name security properties/services necessary to counter the identified threats

User/client should be identified

Messages should be secured during transit

Access to the objects should be controlled



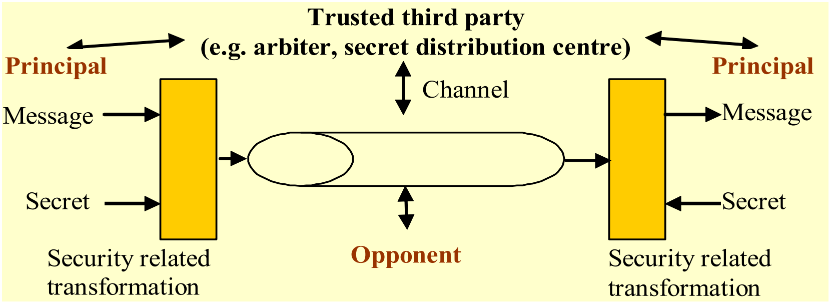
The result returned is indeed from the server process

Security Models: A distributed system security model

- ❑ In this model, following issues arise:
  - ❍Could the server be certain about the identity of the principal behind the invocation?
  - ❍Could the client be certain about the invocation response message
    - ➢Is it from the intended server?
    - ➢Has it been altered during transit?
  - ❍The channel should be secured
    - ➢A perpetrator on the network could read, copy, alter, or inject messages as they travel across the network and gateways.
    - ➢A perpetrator may attempt to save copies of messages and to replay them at a later time.
  - ❍etc …

Security Models: A communication security model

- ❑ Here, the emphasis is on protecting **data while in transit**.
- ❑ Security questions: authenticity (*prove the origin of a message + integrity*) and confidentiality.



Trusted third party
(e.g. arbiter, secret distribution centre)

Principal

Principal

Message

Message

Channel

Secret

Secret

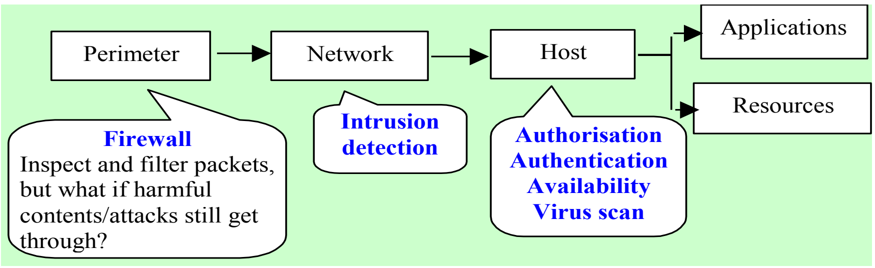
Opponent

Security related transformation

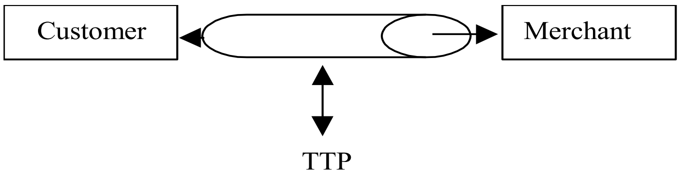
Security related transformation

Security Models: A network security model

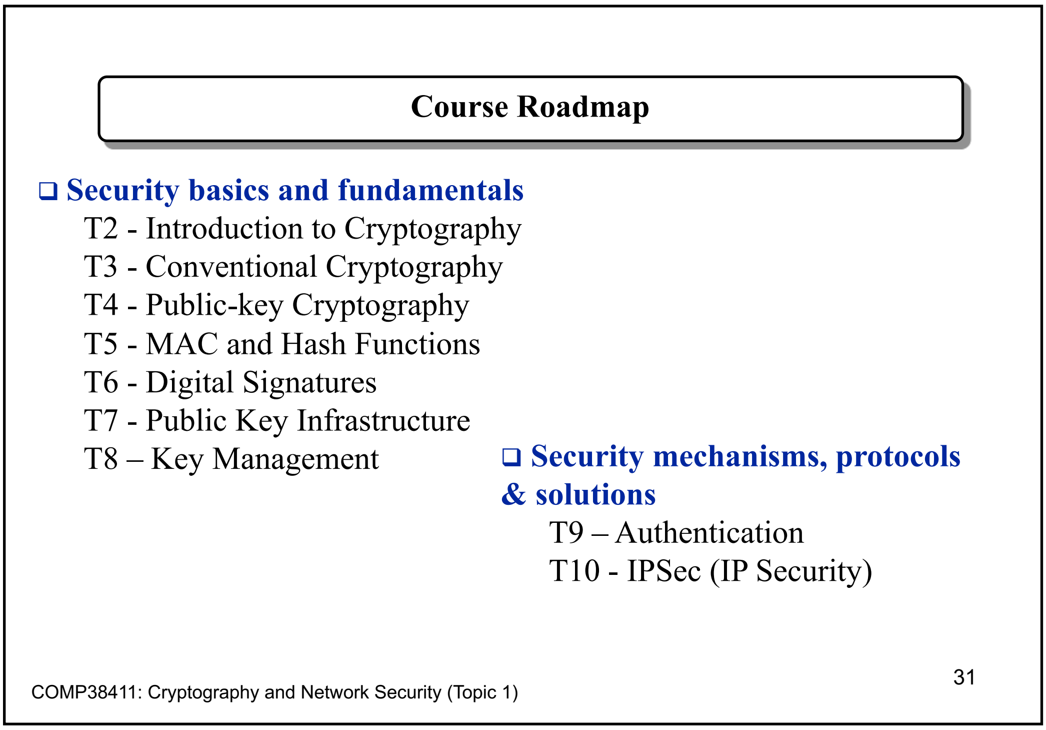
- ❑ Here the focus is on protecting data and services on a network against external attacks or unauthorised usage.
- ❑ Multi-level security measures.
- ❑ However, the use of mobile devices will make the boundary hard to define.



Security Models: An e-commerce security model

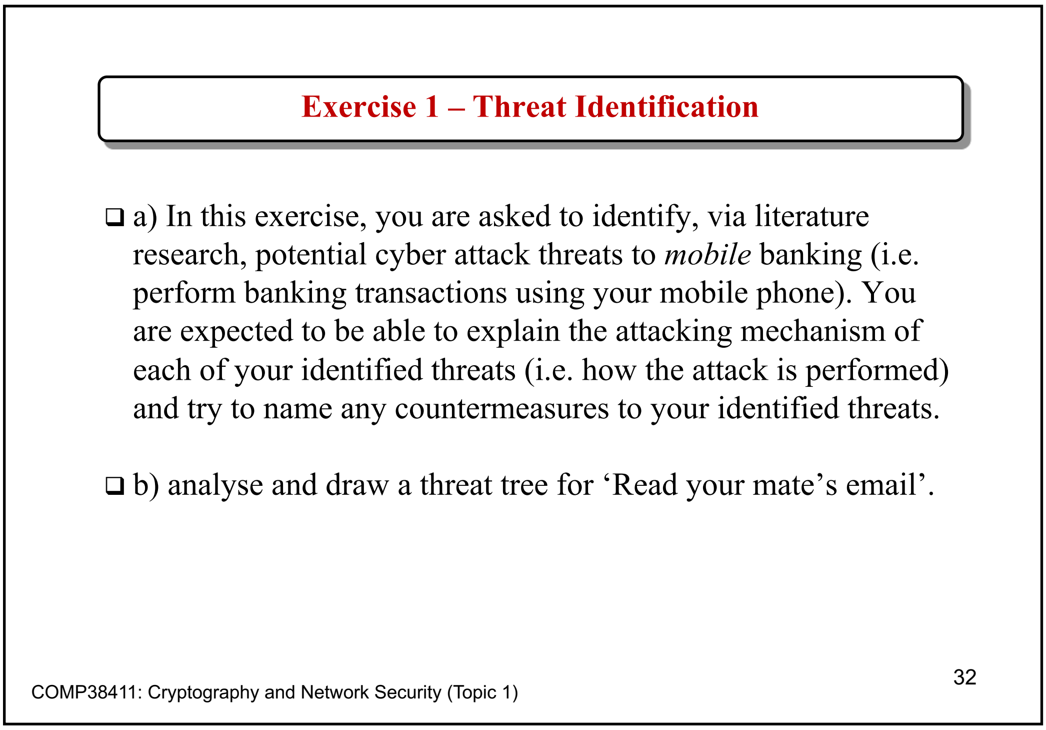


- ❑ The opponent now is a misbehaving insider.
- ❑ The third party is now a trusted third party (TTP), e.g. an arbitrator, that offers some services.
- ❑ Non-repudiation services generate the evidence the arbitrator will consider when resolving a dispute.



Course Roadmap

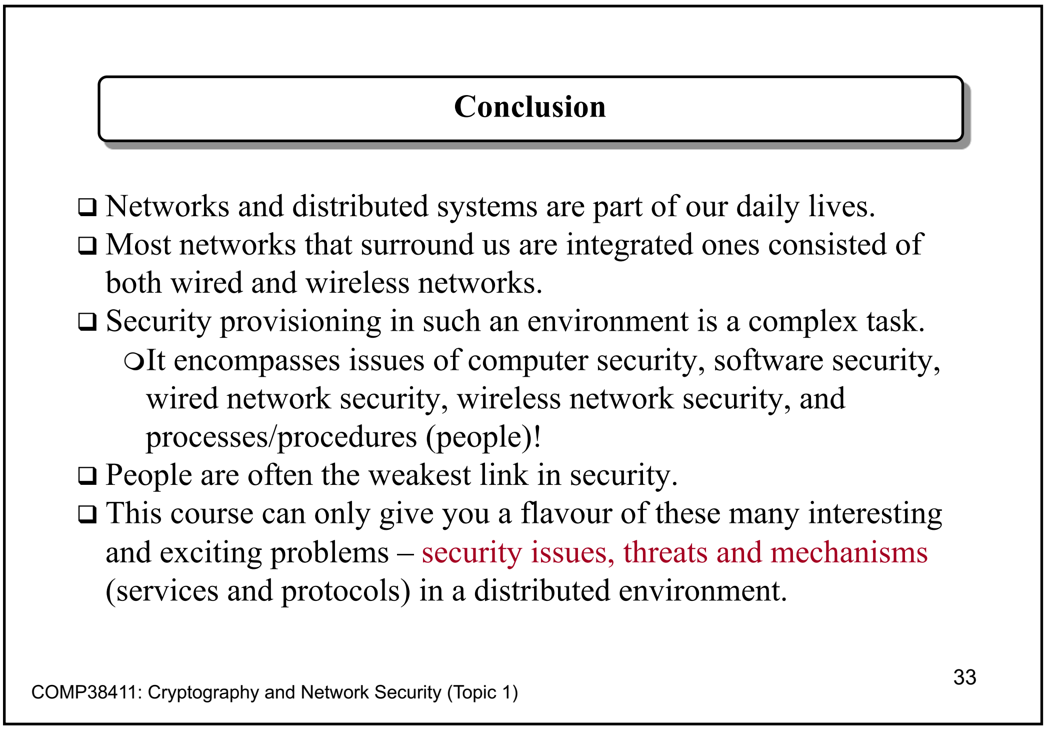
- ❑ **Security basics and fundamentals**
  - T2 - Introduction to Cryptography
  - T3 - Conventional Cryptography
  - T4 - Public-key Cryptography
  - T5 - MAC and Hash Functions
  - T6 - Digital Signatures
  - T7 - Public Key Infrastructure
  - T8 – Key Management
- ❑ **Security mechanisms, protocols & solutions**
  - T9 – Authentication
  - T10 - IPSec (IP Security)



Exercise 1 – Threat Identification

❑ a) In this exercise, you are asked to identify, via literature research, potential cyber attack threats to *mobile* banking (i.e. perform banking transactions using your mobile phone). You are expected to be able to explain the attacking mechanism of each of your identified threats (i.e. how the attack is performed) and try to name any countermeasures to your identified threats.

❑ b) analyse and draw a threat tree for ‘Read your mate’s email’.



Conclusion

- ❑ Networks and distributed systems are part of our daily lives.
- ❑ Most networks that surround us are integrated ones consisted of both wired and wireless networks.
- ❑ Security provisioning in such an environment is a complex task.
  - ❍ It encompasses issues of computer security, software security, wired network security, wireless network security, and processes/procedures (people)!
- ❑ People are often the weakest link in security.
- ❑ This course can only give you a flavour of these many interesting and exciting problems – security issues, threats and mechanisms (services and protocols) in a distributed environment.