Topic 1: An Introduction

Give course unit structure and an introduction of security

- **Main textbook: Cryptography and Network Security,** 7th Edition by William Stallings.
- Supplementary textbook: Computer Security: Art and Science, 2nd Edition, Matt Bishop.
- 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

- Part 1
  - Introduction to the Course Unit
- Part 2
  - What is Security
  - Security Problems and Challenges
- Part 3
  - Achieving Security
  - Security Models
  - Course Roadmap
  - Conclusion

Home Reading: Stalling's book, Chapter 1

Introduction to the Course Unit

- This course is about Cryptography and System Security
  - Cryptography:
    - important and commonly used cryptographic methods and techniques
  - Applied cryptography:
    - apply cryptography methods and techniques to solve security problems in a networked/distributed system setting
  - Access control

- Who should take this module
  - This is a technical module, so if you are interested in security and willing to learn some mathematical stuff, …
  - No prerequisite

Introduction to the Course Unit

- Course Unit Leader
  - Ning Zhang
  - ning.zhang@manchester.ac.uk

Introduction to the Course Unit

- Reading materials
  - **Main textbook: Cryptography and Network Security,** 7ed by William Stallings.
  - Computer Security: Art and Science, 2nd Edition, Matt Bishop.
  - Many other useful books; you can use the topics covered in the lecture handouts to scope your reading.
  - Lot of useful resource on the Internet, e.g. www.cert.org and www.nist.gov.
- All the teaching docs (except for the videos) are hosted in the Blackboard.

Course Unit Structure

- New materials are structured into topics
  - One topic per week; multiple parts per topic
  - One lecture handout per topic
- 5 sets of Quiz questions for formative assessment purpose
- Exercise questions for enhancing understanding of lecture contents and problem-solving skills
- Two-hour synchronous sessions per week via Blackboard Collaborate
  - For addressing any questions you may have on the lecture contents
  - For working on the exercise questions

Course Unit Structure

- Download and install CrypTool available at: http://www.cryptool.org/ (I recommend CrypTool 1.4.30 for Windows: https://www.cryptool.org/ct1download/SetupCrypTool_1_4_30_en.exe. There are also versions for MacOS and Linux). This is an e-learning tool for cryptographic algorithms. Other tools are fine, as long as they do the job.
-
- Assessment
  - 70% exam and 30% coursework

Part 2 Overview

- What is Security
- Security Problems and Challenges

What is Security?

Information hiding

eCommerce security

Location based authentication

Digital Right Management

Privacy

Malicious code

Trust

Digital signatures

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 in its early stage
- 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, …
  - Crypto currencies, smart contract signing, getting rid of third parties - blockchain technologies

Security Threats and Challenges

- Threats in a generic context (Confidentiality, Integrity and Availability, or CIA)
  - Disclosure (threats to confidentiality):
    - Snooping, sniffing (data in transit)
    - Unauthorised access (systems, data at rest)
  - Deception (fraud and forgeries):
    - Spoofing (identity theft)
    - Unauthorised data modification
    - Replay (intercept and retransmit)
    - Repudiation (false denial) of origin, repudiation of receipt
  - Disruption (threat to availability): modification, delay, Denial of Services (DoS)

Security Threats and Challenges

- Specific Threats (e.g. Top 5 Cyber Threats/Attacks)
  1. Social Engineering Attacks
     - What is our social media threat profile?
     - Who is monitoring it?
     - What tools are available for such monitoring?
     - What are our social media use policies? How do we implement them?
  2. Supply Chain Attacks
     - What sensitive information am I sharing with my vendors?
     - How do I assess the risk of each vendor?
     - What tools and services can I use to effectively control the threats posed by such a risk?

https://www.softwareone.com/en-gb/blog/articles/2019/01/24/biggest-cyber-security-challenges-in-2019

Security Threats and Challenges

3. IoT and Infrastructure Attacks
   - How are IoT and infrastructure devices impacting my risk?
   - Who is managing and controlling the risk?
   - What are the remediation protocols and policies that will help me to mitigate the risk?
4. Identity and Mobile Authentication
   - How should I control authentication and access across multiple devices, almost all connected to the Internet and with a varying degree of trust?
   - What kind of biometric and MFA (multi-factor-authentication) solutions are appropriate for my environment?
   - What cloud-based solutions should I use to access sensitive information?

Security Threats and Challenges

5. Rise of Zero-Day Threats and Polymorphic Attacks
   - What should I do if zero-day vulnerabilities are discovered for a mission-critical system?
   - Which security vendors and products should I trust for effective countermeasure to polymorphic attacks?
   - What is the status of my systems for known vulnerabilities? Who manages this?
   - Should I take a cyber-insurance?

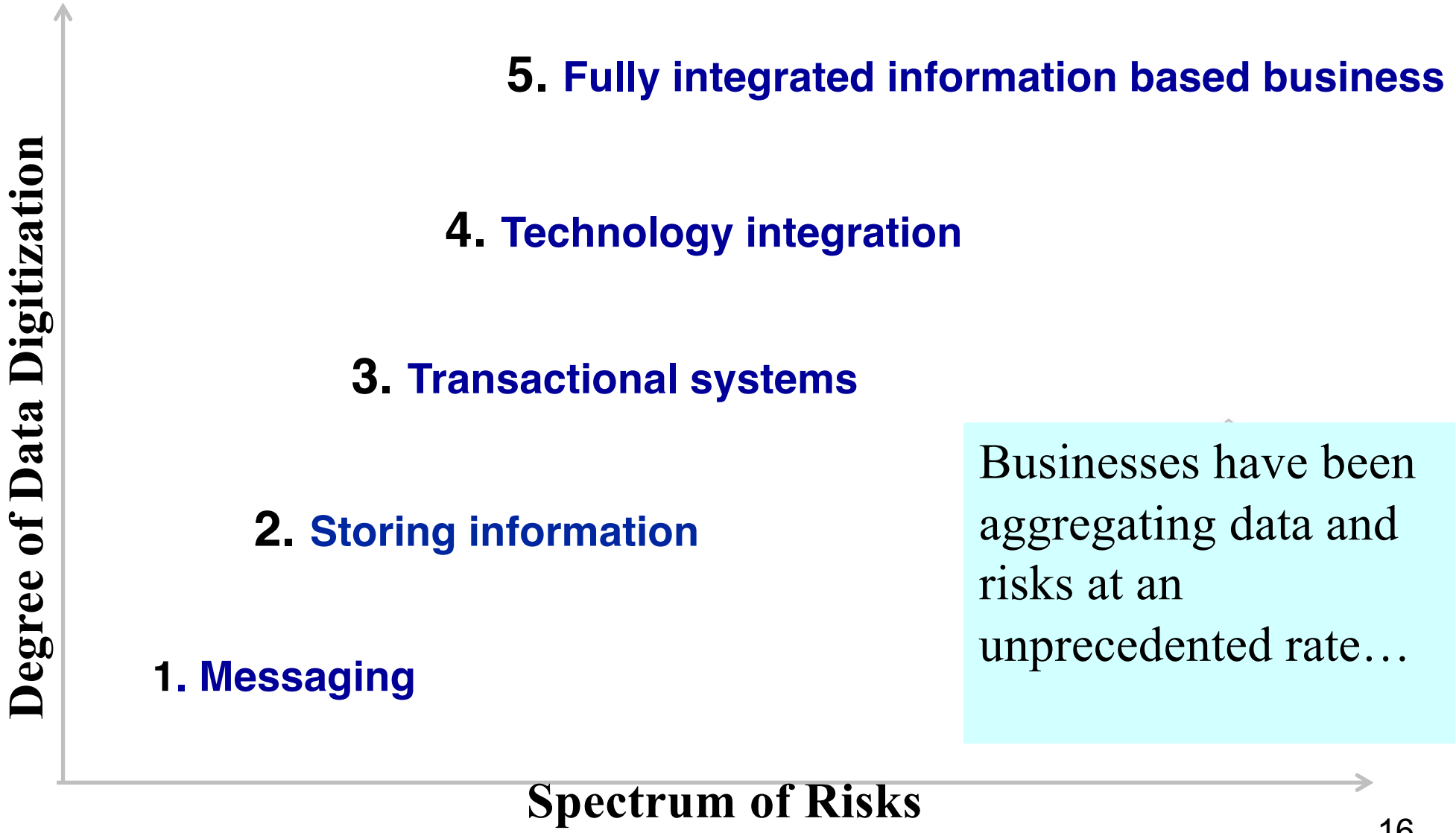
- Most attacks are done by using Malware (worms, viruses, Trojan, …)
- Hacking-as-a-Service

Security Threats and Challenges: Hacking as a Service

- 444,259 ransomware attacks took place worldwide in 2018.
- Hackers create 300,000 new pieces of malware daily.
- There is a hacker attack every 39 seconds.
- Hackers steal 75 records every second.
- You can purchase a consumer account for $1 on the dark market.
- More than 6,000 online criminal marketplaces sell ransomware products and services.
- Consulting services such as botnet setup ($350-$400).
- Infection/spreading services (~$100 per 1K installs).
- 73% of black hat hackers said traditional firewall and antivirus security is irrelevant or obsolete.

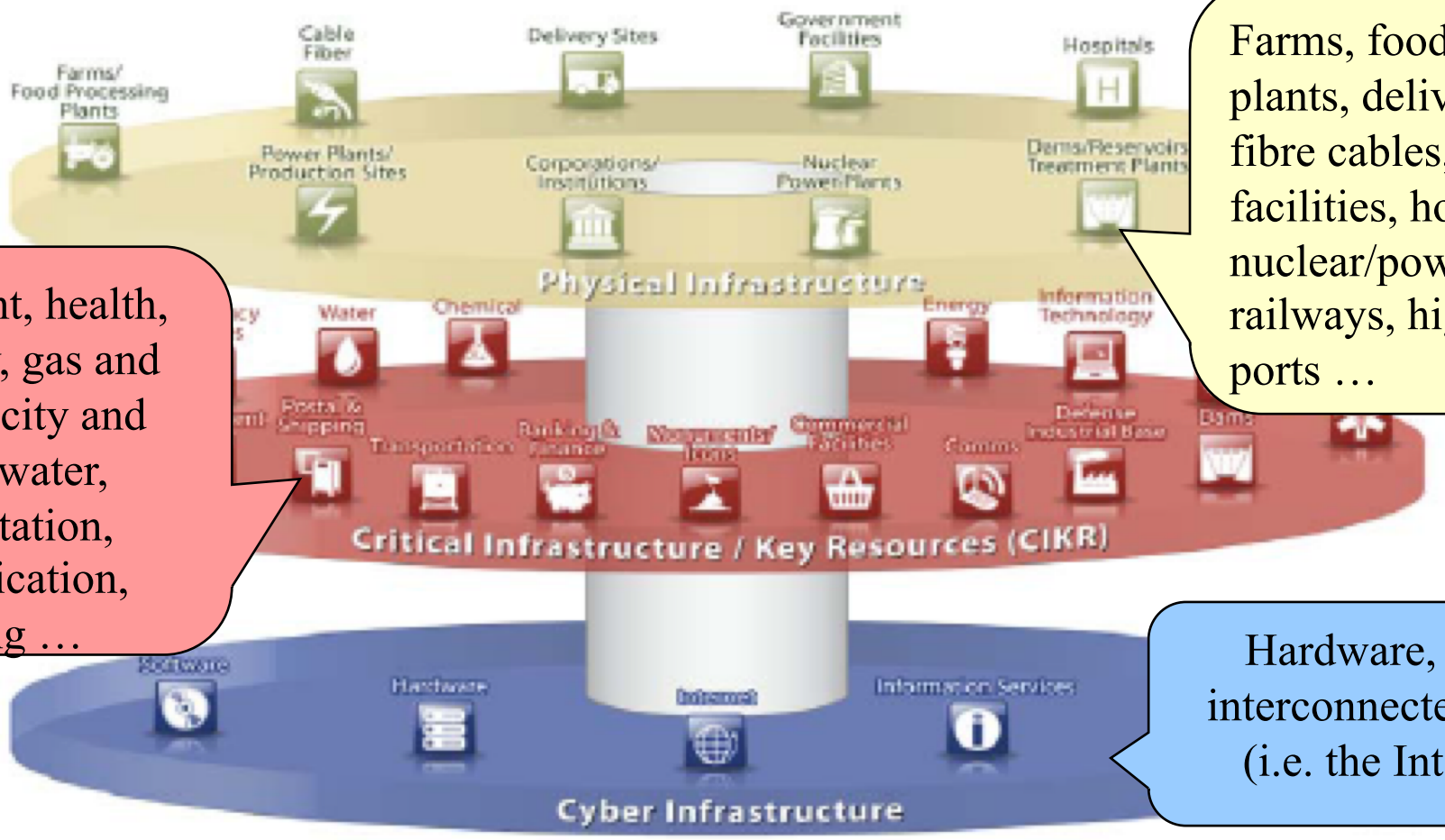
Source: Hostingtribunal.com

Security Threats and Challenges



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

Security Threats and Challenges



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

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

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

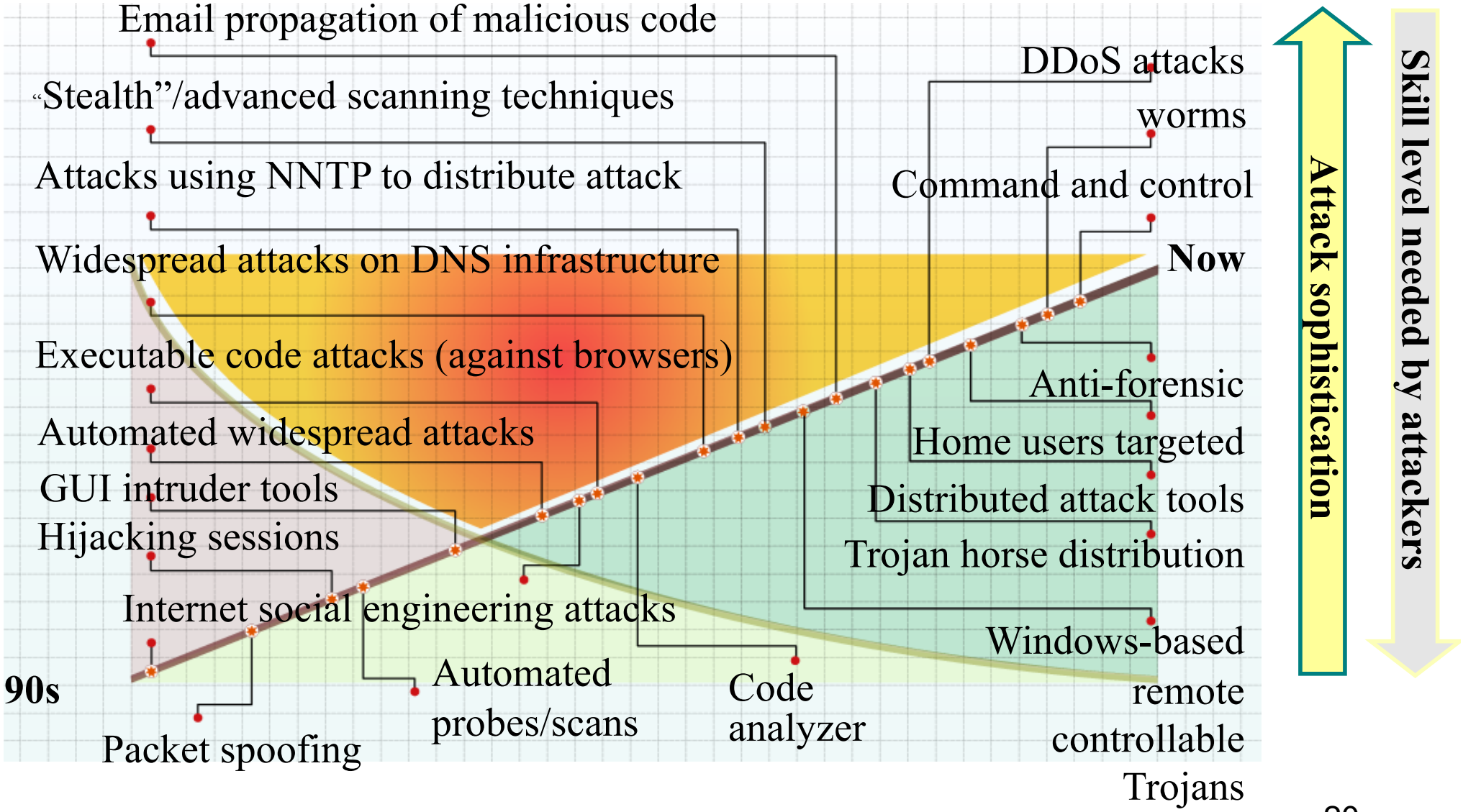
Threat Types	Motivation	Targets	Methods
Information Warfare	Military or political dominance	Critical infrastructure, political and military assets	Attack, corrupt, exploit, deny, conjoint with physical attack
Cyber Espionage	Gain of intellectual Property and Secrets	Governments, companies, individuals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

Source: analysis, Dr Irv Lachov

Security Threats 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 Threats and Challenges



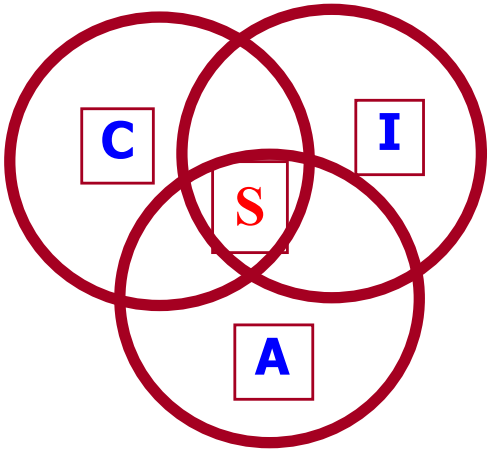
Source: SE/CERT CC

Part 3 Overview

- Achieving Security
- Security Models
- Course Roadmap
- Conclusion

Achieving Security – Basic security properties

- Securing information: CIA
  - Confidentiality
    - Keeping data and resources hidden
  - Integrity/Authenticity/Authentication (making sure data is authentic)
    - Content integrity (any unauthorised modification and replay of data can be detected)
    - Origin integrity (data is indeed from a claimed source)
  - Availability
    - Ensuring data/service is available to authorised users



Achieving Security – Advanced security properties

- Freshness
  - Ensuring data is not a replay/retransmission of 'old' data
- Non-repudiation
  - Protecting against repudiation (false denial)
- Fairness
  - Either all the parties have received what they expect to receive or none of them receives anything useful

Achieving Security – Life-cycle

- Define your security goal
  - Threats analysis and identification
    - Decide what to protect against
  - Policy/Requirement specification
    - 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

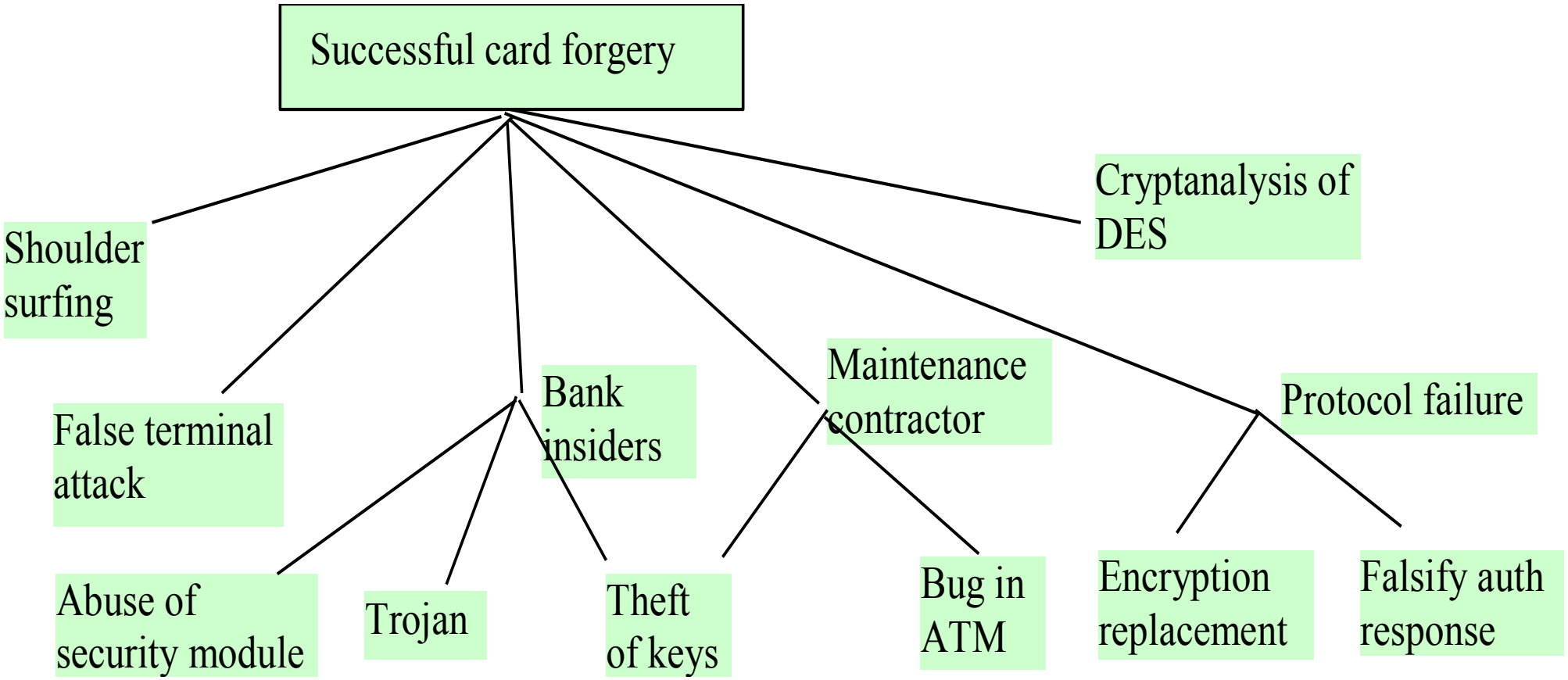
Achieving Security – Threat analysis

- 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.

- How to produce an Attack Tree
  - Identify an attack goal
  - Identify all the possible attack methods or avenues to achieve the goal

Achieving Security – Threat analysis

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



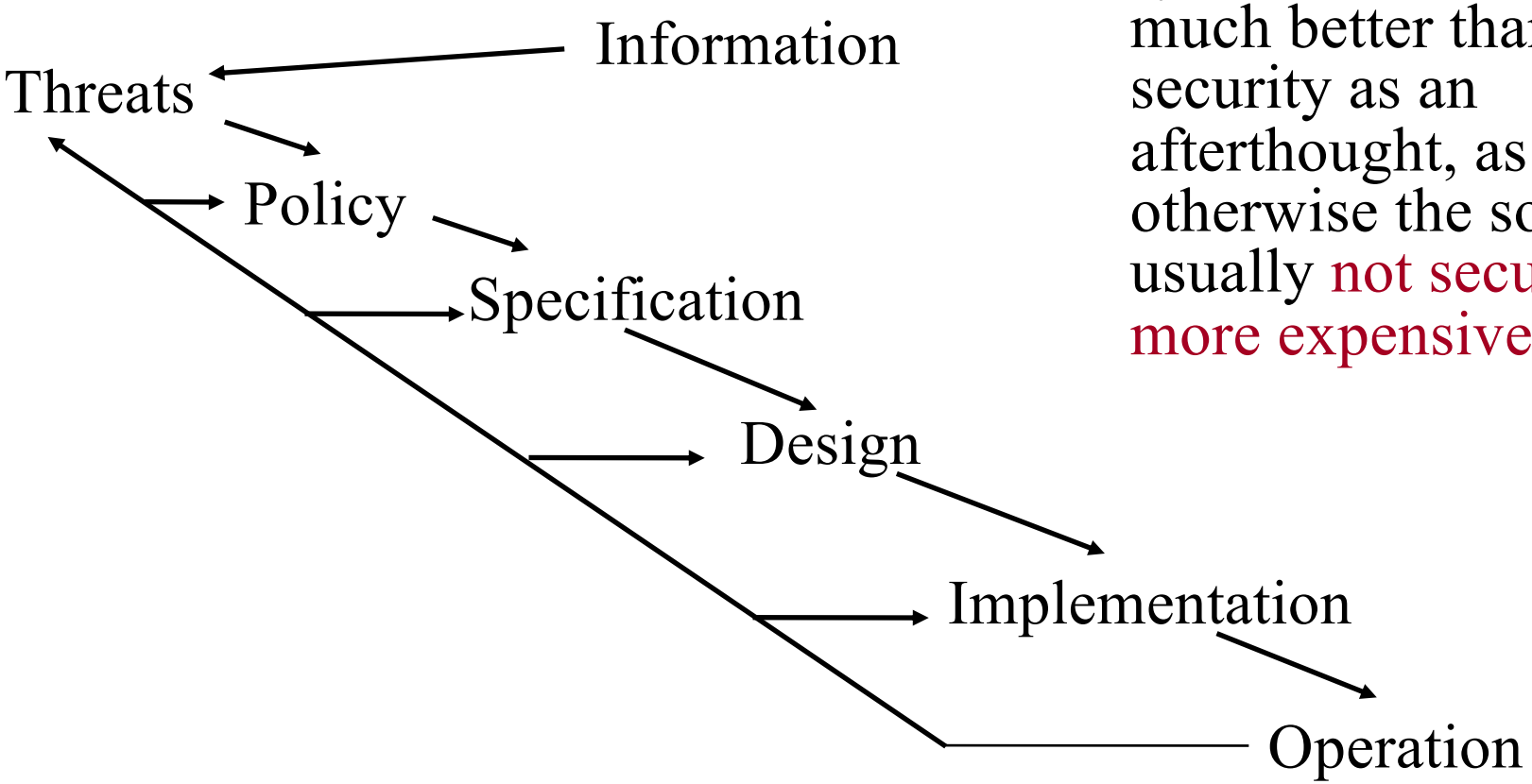
Achieving Security – Defining & achieving security goal

- 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, honey pots …
  - Detection
    - Measures taken during or after the attacks
    - E.g. logging, auditing and intrusion detection
  - Recovery
    - 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

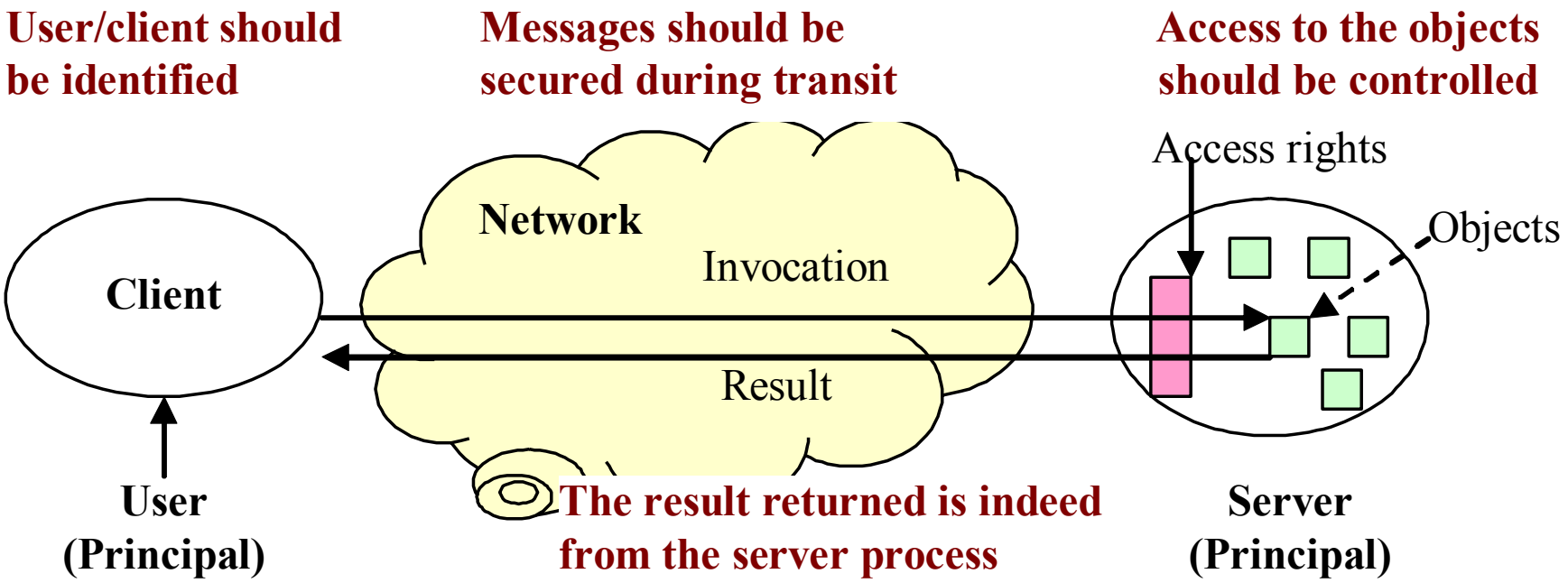
Tying it all together



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

- What are the security threats in this model?
- What are the security properties/services that are necessary to counter the threats?

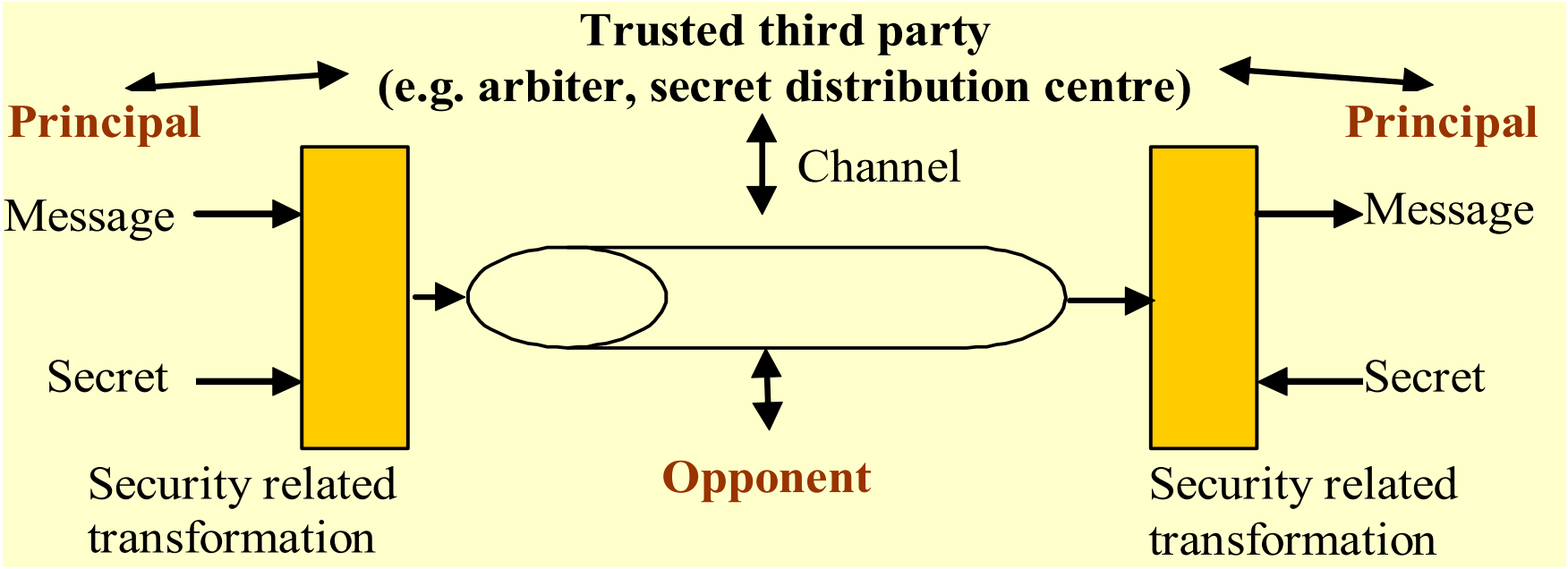


Security Models: a distributed system security model

- 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 …

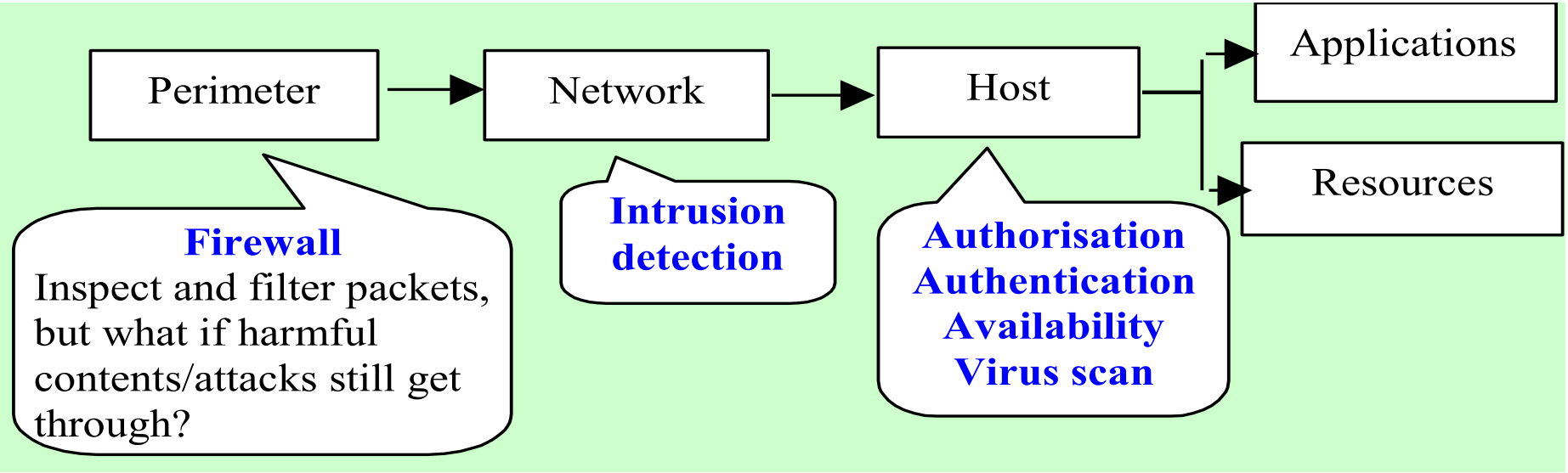
Security Models: Communication security model

- Here the emphasis is on protecting **data over the channel**.
- Security questions: authenticity (*prove the origin of a message + its integrity*) and confidentiality.



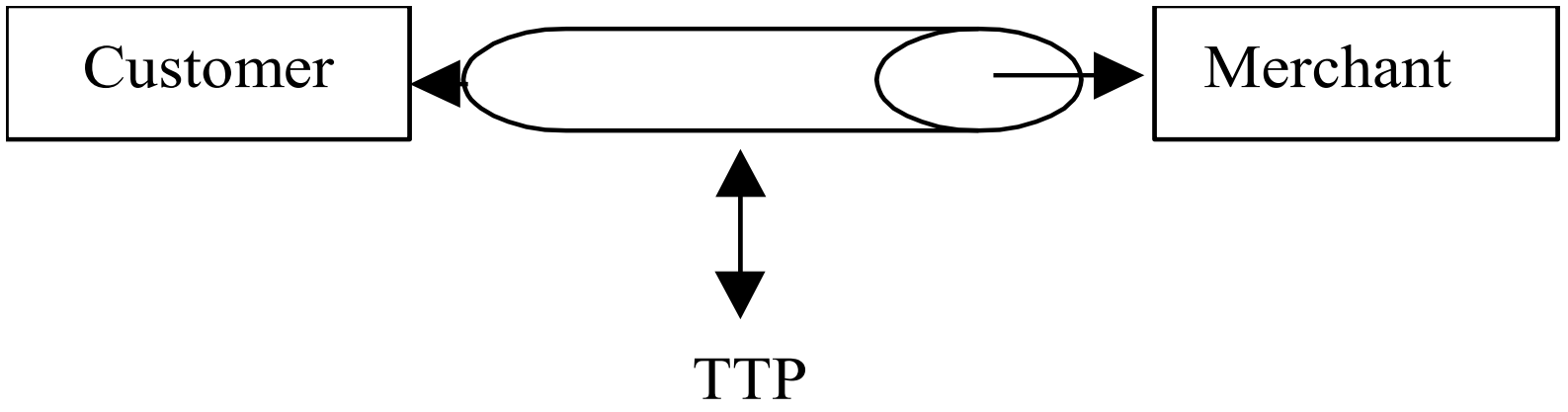
Security Models: Network security model

- 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: 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 service generates evidence for dispute resolution.



Course Roadmap

- **Security basics and fundamentals**
  - T2 – Classical Ciphers
  - T3 – Symmetric-key Ciphers
  - T4 - Asymmetric-key Ciphers
  - T5 – Cryptographic Checksum
  - T6 - Digital Signatures
  - T7 - Public Key Infrastructure
  - T8 – Key Management Issues
- **Security systems**
  - T9 – Entity Authentication
  - T10 – More Security Solutions
  - T11 – Access Control

Exercise Question – E1.1

Comment on the implications to risks (i.e. whether risks are increased or decreased) in terms of Confidentiality, Integrity and Availability in each of the following cases:

i. Disconnect a computer from the Internet;
ii. Have extensive data checks by different people/systems.

Exercise Question – E1.2

i) 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.

ii) Draw a threat tree for ‘Read your mate’s email’.

Conclusions

- Networks and distributed systems are part of our daily lives.
- Most systems that surround us are networked via the Internet which is open to many attacks and threats.
- 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.