Topic 2: Security Basics

Introduce some security basics

Overview

- Cybersecurity Threats
- Security Properties
- Achieving Security
- Security Models
- Conclusion

Home Reading: Main textbook, Chapter 1

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, Companies	Attack, defacing
Cyber Terror	Political change	Individuals, companies	Marketing, command and control, computer based violence

Source: analysis, Dr Irv Lachov

Cybersecurity Threats

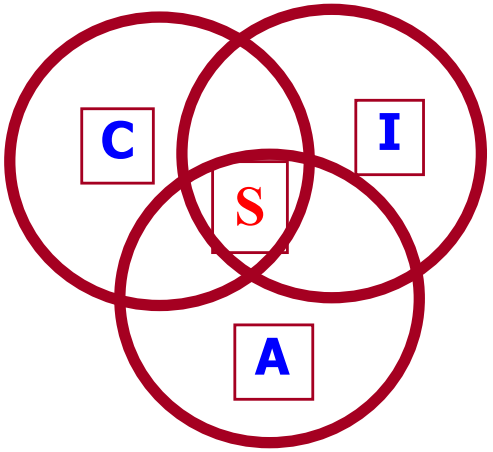
- Malware (virus, trojan, worm, …)
- Ransomware
- Adware
- Hacking
- Spoofing
- Phishing
- Pharming
- DDoS (Distributed Denial of Service) attacks (Botnets attacks)
- Identity theft
- SQL injection
- Social engineering
- Cryptojacking (Cryptocurrency Hijacking)
- etc, the list goes on …

Cybersecurity Threats

- 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; threats to integrity):
    - 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 Properties

- CIA triad
  - Confidentiality
    - Keeping data and resources hidden
  - Integrity/Authenticity/Authentication (making sure data is authentic)
    - Entity integrity (entity indeed has the claimed identity)
    - Content integrity (any unauthorised modification and replay of data can be detected)
    - Origin integrity (data is indeed from a claimed source)
  - Availability
    - Ensuring data/services/systems are available to authorised users



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

- There is no perfect security; security is about risk management.

- The **Life-cycle** consists of three main steps:
  - Define your security goal and threat analysis: to identify what to protect against and to specify security policy.
  - Design and implement security measures: to decide how to protect so as to achieve your goal.
  - Security assurance (operation, monitoring and maintenance): to assess how well the implementation has achieved the goal.

- **Define your security goal**
  - Threats analysis: to identify and decide what to protect against.
  - Policy/Requirement specification: to define what is, and/or is not, allowed.

Achieving Security: threats analysis

- Identify assets, threats and vulnerabilities: to find out what are the most likely avenues in which an attack will succeed at a relatively low cost to the attacker.
- Find answers to these questions:
  - What are the assets to protect?
  - What is the value of each asset (to see if it is worth protecting)?
  - What are the threats?
  - Where are they from or how are they mounted?
  - Where are the vulnerabilities? What are the likelihood of their exploitation?
  - Who are the adversaries, and what are their resources?
- Not all threats are worth defeating (cost vs benefit).
- Typically carried out by using an Attack Tree Analysis method.

Achieving Security: threats analysis

- An **Attack Tree (Threat Tree)**
  - is a "conceptual diagram showing how an asset, or target, might be attacked".
  - is consisted of one root node, child nodes, and leaf nodes.
- The root node representing the Attack Goal.
- Child and leaf nodes are conditions under which, or ways/methods by which, one may obtain the goal. If a method in turn requires other intermediate steps, then under each of these child nodes, branch off as appropriate.
- Relationship between branches may be 'OR' or 'AND':
  - 'OR' represents alternative attack methods to succeed in the attack.
  - 'AND' represents multiple steps required to launch the attack.

Achieving Security: threats analysis

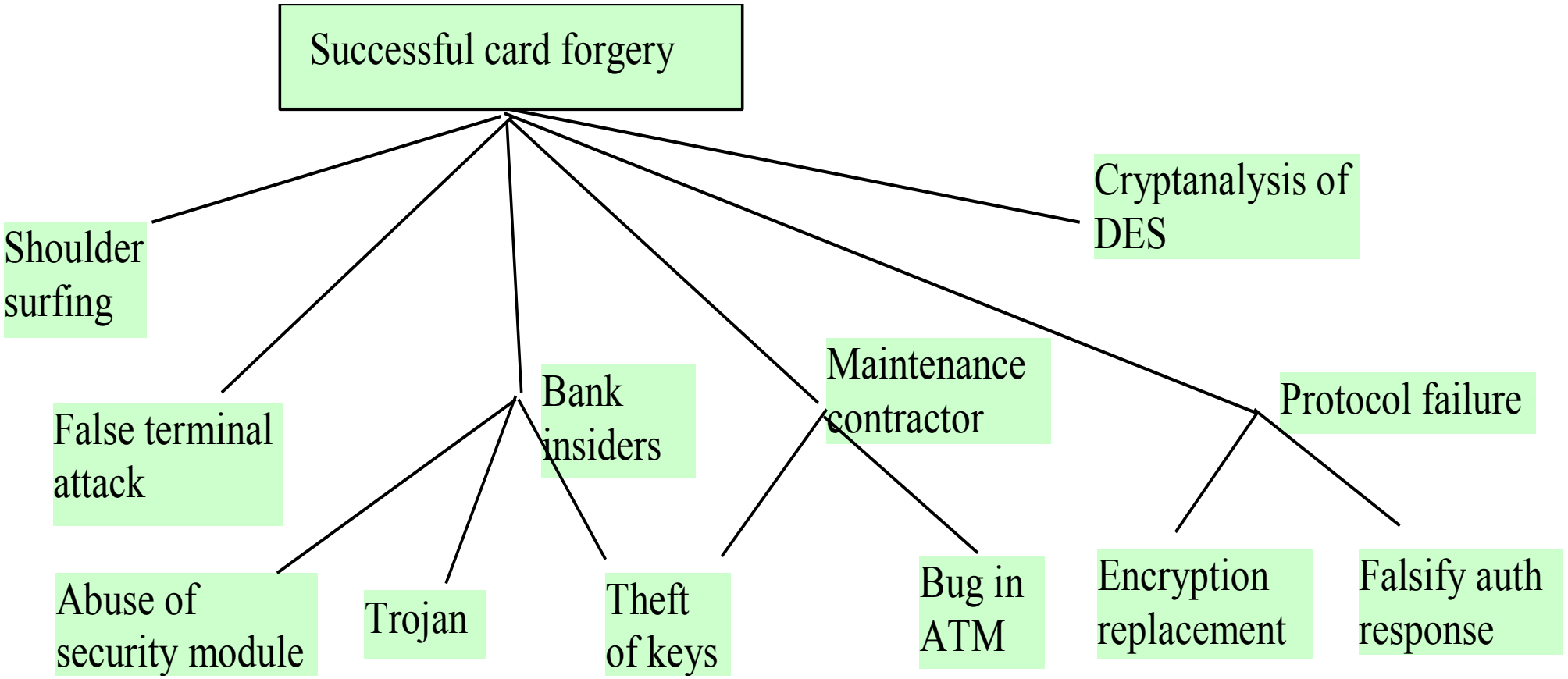
- Each node may be given a value to indicate, e.g.
  - **likelihood** that an attacker will mount the attack, or **probability** of succeeding the attack
  - **cost** in succeeding the attack, in terms of monetary cost, or time taken to accomplish the attack, etc.

- Once done, any path from a leaf node to the goal is a potential attack marked with likelihood, or cost ...

Reference: http://www.attack-tree.com/

Achieving Security: threats analysis

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



Achieving Security: design and implementation

- **Design and implementation**: to enforce policies by deciding how to protect (deploying security measures).
- Security measures:
  - are methods, protocols, tools, or procedures used to mitigate the risks identified.
  - can be technical measures or procedural measures.
  - can be preventive, detective or response/recovery measures.
- Preventive measures
  - Block attacks by closing vulnerabilities, e.g. penetration testing, ethical hacking, …
  - Make successful attacks harder, e.g. access control, firewalls, encryption, digital signatures, malware scanning, …
  - Make another target more attractive than this target, e.g. Honeypots.

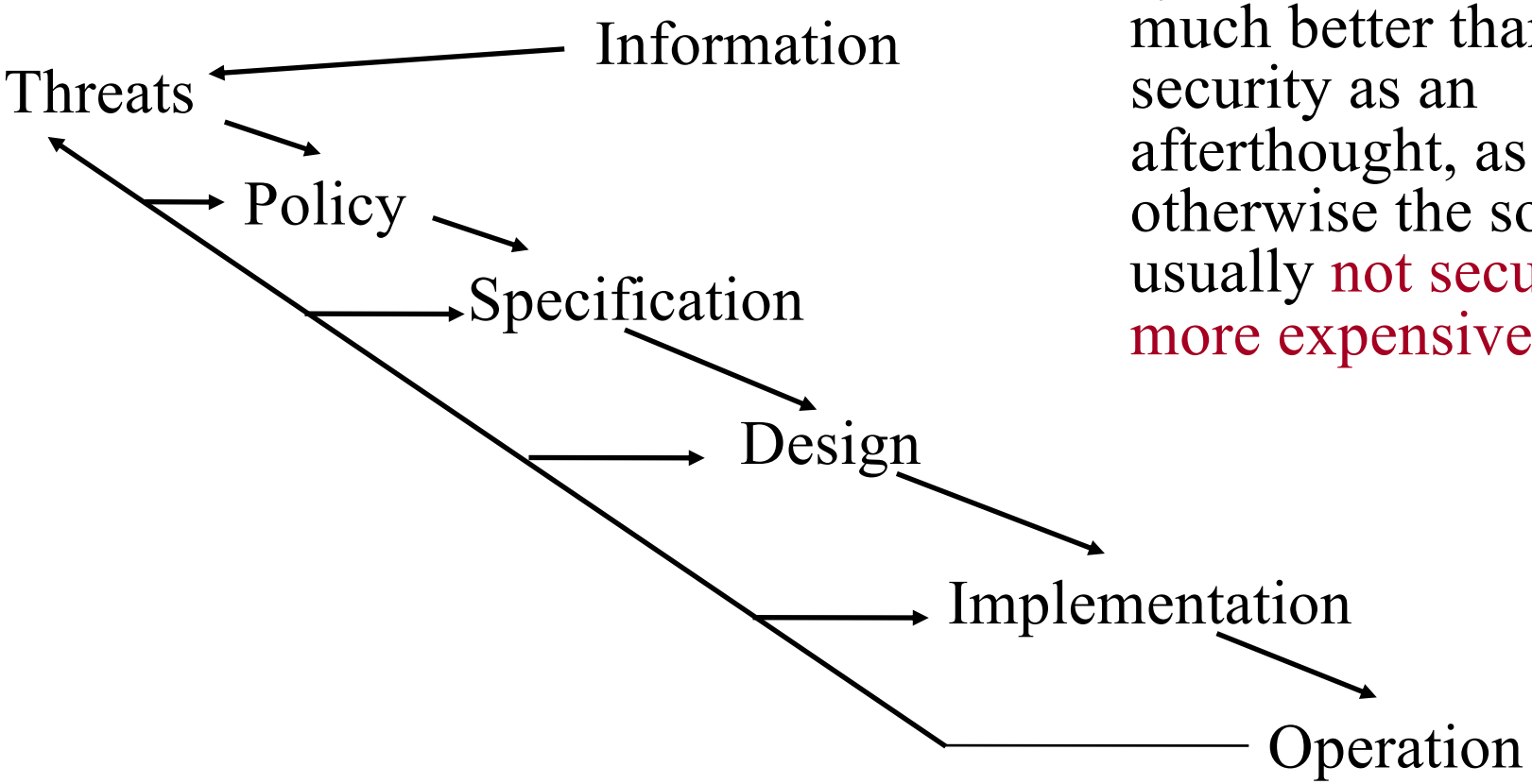
Achieving Security: design and implementation

- Detective measures
  - Measures taken during or after the attacks, e.g. logging/auditing, intrusion detection systems (host-based, network-based, hybrid …).
- Response and Recovery
  - Measures to repair any damage so that the system can continue to function correctly even if an attack succeeds, e.g. backup.
- Accept it and do nothing
- Cost-benefit analysis
  - Is it cheaper to prevent (using security mechanisms) or recover (e.g. using restoration from backup) or just ignore?

Achieving Security: security assurance

- **Security assurance**: to assess how well the implementation has achieved the goal.
  - 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

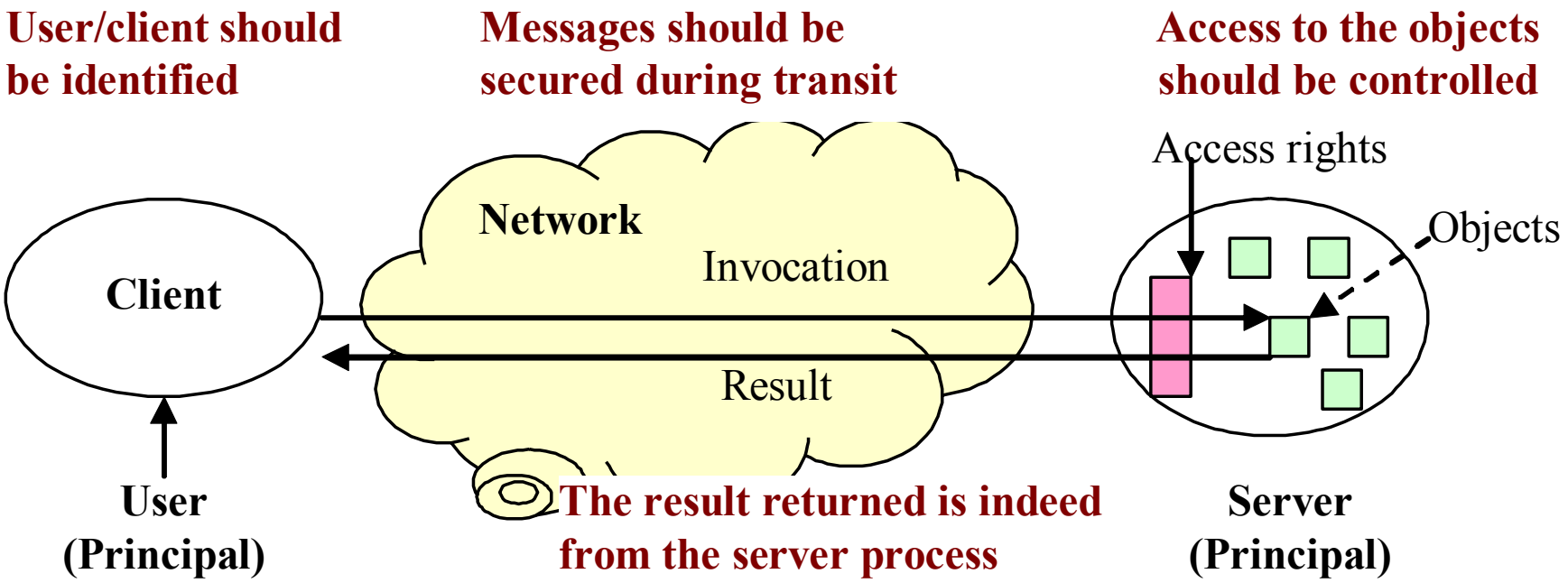
Achieving Security: putting it all together



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?

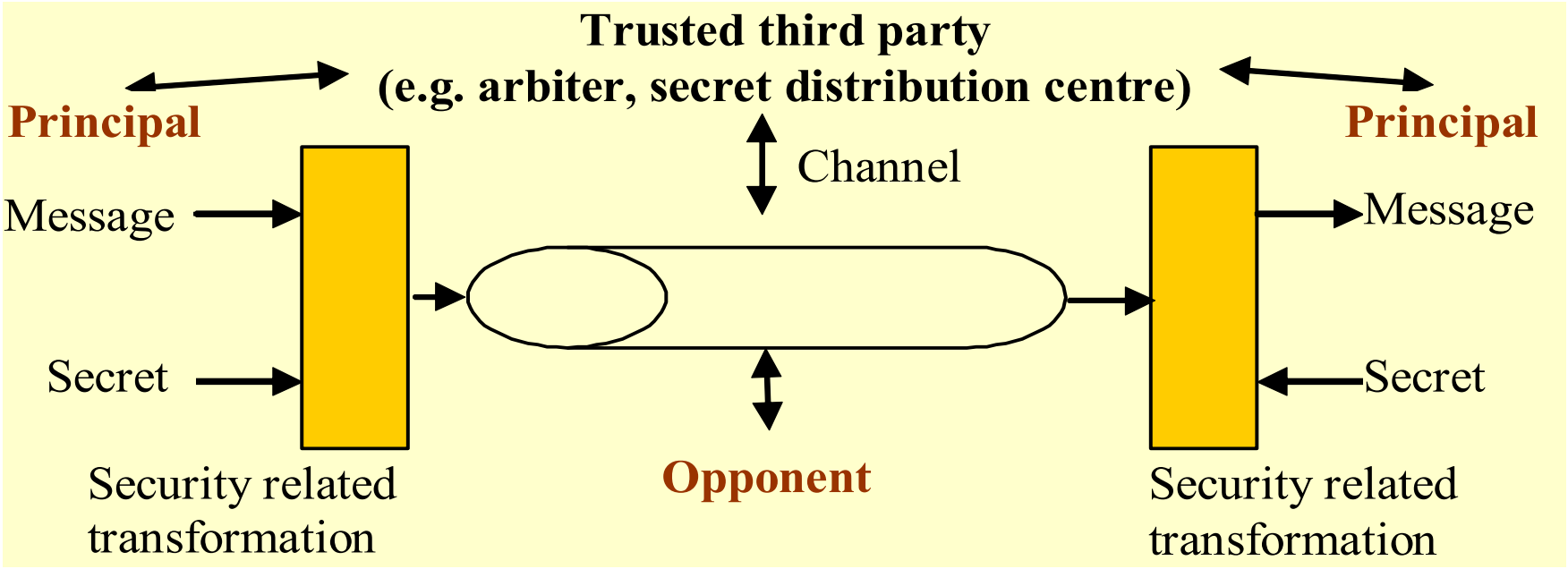


Security Models: a distributed system security model

- 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 …

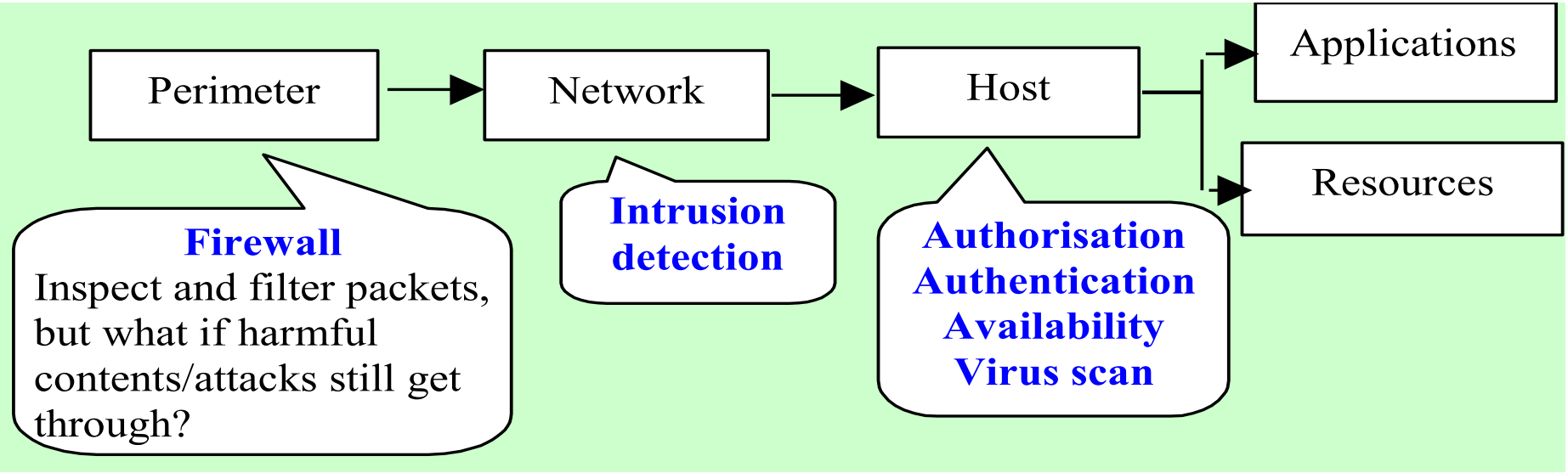
Security Models: A communication security model

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



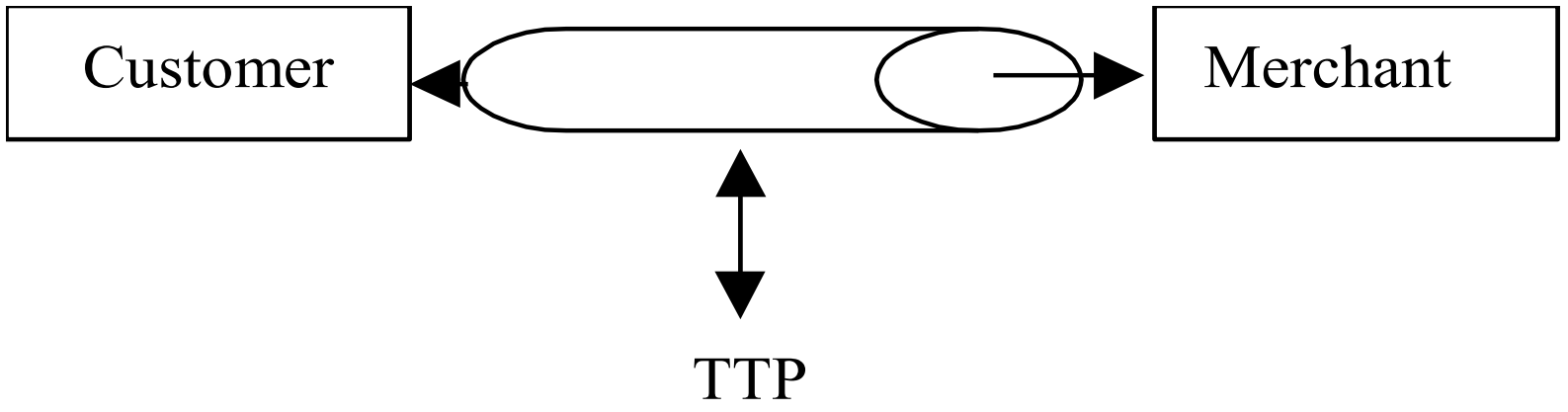
Security Models: a networked system security model

- 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 service generates evidence for dispute resolution.



Exercise Question – E2.1

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 – E2.2

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 'reading your best friend's email without authorisation'.

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.