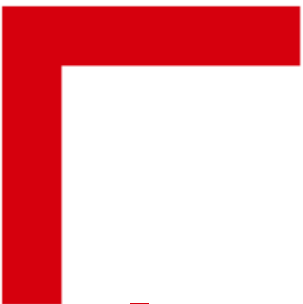





**QUEEN'S
UNIVERSITY
BELFAST**



Introduction to Network Security – Part 1



Dr. Sandra Scott-Hayward

CSC3064 Lecture 02

School of Electronics, Electrical Engineering and Computer Science

Session Overview

- ❑ Threats, Security Goals & Requirements
- ❑ Threat Analysis – message level, communication infrastructure
- ❑ System Security Engineering

Reference:

Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.



Motivation – A Changing World

- Mobile communication networks and ubiquitous availability of the global Internet have already dramatically changed the way we
 - communicate,
 - conduct business, and
 - organize our society
- With current research and developments in sensor networks and pervasive computing, we are creating a new networked world
- However, the benefits associated with information and communication technology imply new vulnerabilities

Increasing dependence of modern information society on availability and secure operation of communication services

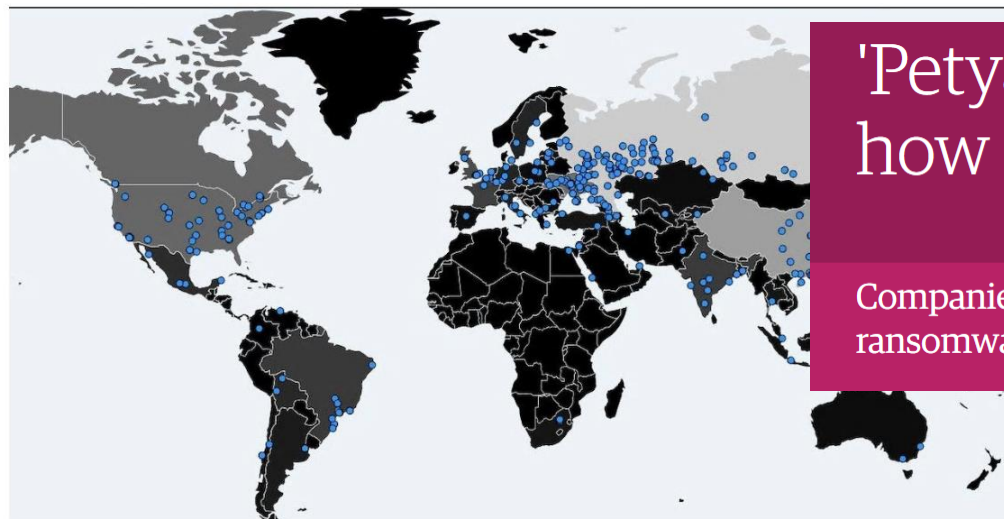
Motivation – Total dependence?

Major cyber attack disrupts internet service across Europe and US

Denial
comp:

A global cyberattack using hacking tools widely believed by researchers to have been developed by the US National Security Agency crippled the NHS, hit international shipper FedEx and infected computers in 150 countries.

More than 300,000 computers were infected while the countries most affected by WannaCry were Russia, Taiwan, Ukraine and India, according to Czech security firm Avast.



Today the web was broken by countless hacked devices – your 60-second summary

IoT gadgets flooded DNS biz Dyn to take down big name websites

By [Chris Williams](#), US editor 21 Oct 2016 at 21:45

222  SHARE ▼

Updated Today a vast army of hijacked internet-connected devices – from security cameras and video recorders to home routers – turned on their owners and broke a big chunk of the web.

'Petya' ransomware attack: what is it and how can it be stopped?

Companies have been crippled by global cyberattack, the second major ransomware crime in two months. We answer the key questions

What is a threat in a communication network?

Abstract Definition:

- A *threat* in a communication network is any possible event or sequence of actions that might lead to a violation of one or more *security goals*
- The actual realization of a threat is called an *attack*

Examples:

- A hacker breaking into a corporate computer
- Disclosure of emails in transit
- Someone changing financial accounting data
- A hacker temporarily shutting down a website
- Someone using services or ordering goods in the name of others
- ...

What is a threat in a communication network?

What are security goals?

- Security goals can be defined:
 - depending on the application environment, or
 - in a more general, technical way

Security goals depending on the application environment

Public Telecommunication Providers:

- Protect subscribers privacy
- Restrict access to administrative functions to authorized personnel
- Protect against service interruptions

Corporate / Private Networks:

- Protect corporate / individual privacy
- Ensure message authenticity
- Protect against service interruptions

Sometimes security goals
are also called *security
objectives*

All Networks:

- Prevent outside penetrations (who wants hackers?)

Security Goals technically defined

Confidentiality:

- Data transmitted or stored should only be revealed to an intended audience
- Confidentiality of entities is also referred to as *anonymity*

Data Integrity:

- It should be possible to detect any modification of data
- This requires to be able to identify the creator of some data

Accountability:

- It should be possible to identify the entity responsible for any communication event

Controlled Access:

- Only authorized entities should be able to access certain services or information

Availability:

- Services should be available and function correctly

Threats technically defined

Masquerade:

- An entity claims to be another entity

Eavesdropping:

- An entity reads information it is not intended to read

Authorization Violation:

- An entity uses a service or resources it is not intended to use

Loss or Modification of (transmitted) Information:

- Data is being altered or destroyed

Threats technically defined

Denial of Communication Acts (Repudiation):

- An entity falsely denies its' participation in a communication act

Forgery of Information:

- An entity creates new information in the name of another entity

Sabotage (Denial of Service):

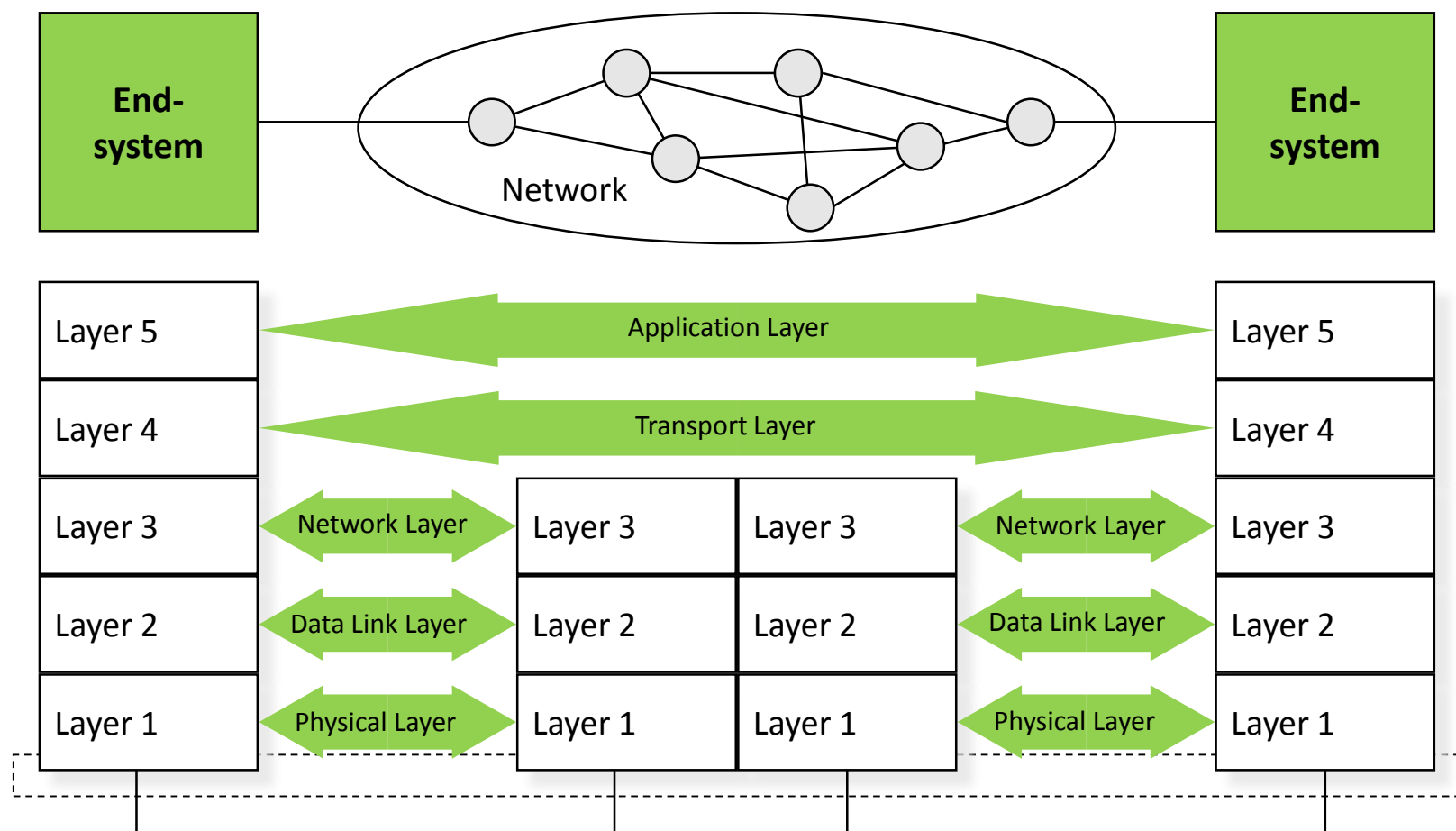
- Any action that aims to reduce the availability and / or correct functioning of services or systems

Threats and Technical Security Goals

Technical Security Goals	General Threats						
	Masquerade	Eavesdropping	Authorisation Violation	Loss or Modification of (transmitted) information	Denial of Communication acts	Forgery of Information	Sabotage (e.g. by overload)
Confidentiality	x	x	x				
Data Integrity	x		x	x		x	
Accountability	x		x		x	x	
Availability	x		x	x			x
Controlled Access	x		x			x	

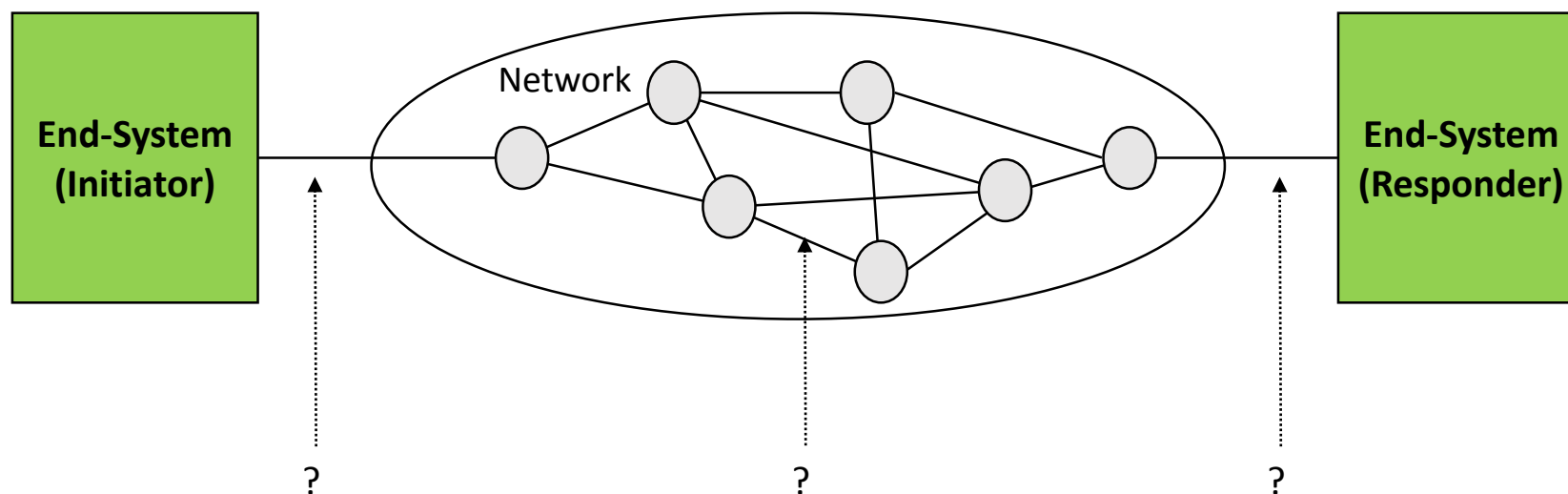
Threats are often combined in order to perform an attack!

Architectural View of our “Object” to be protected



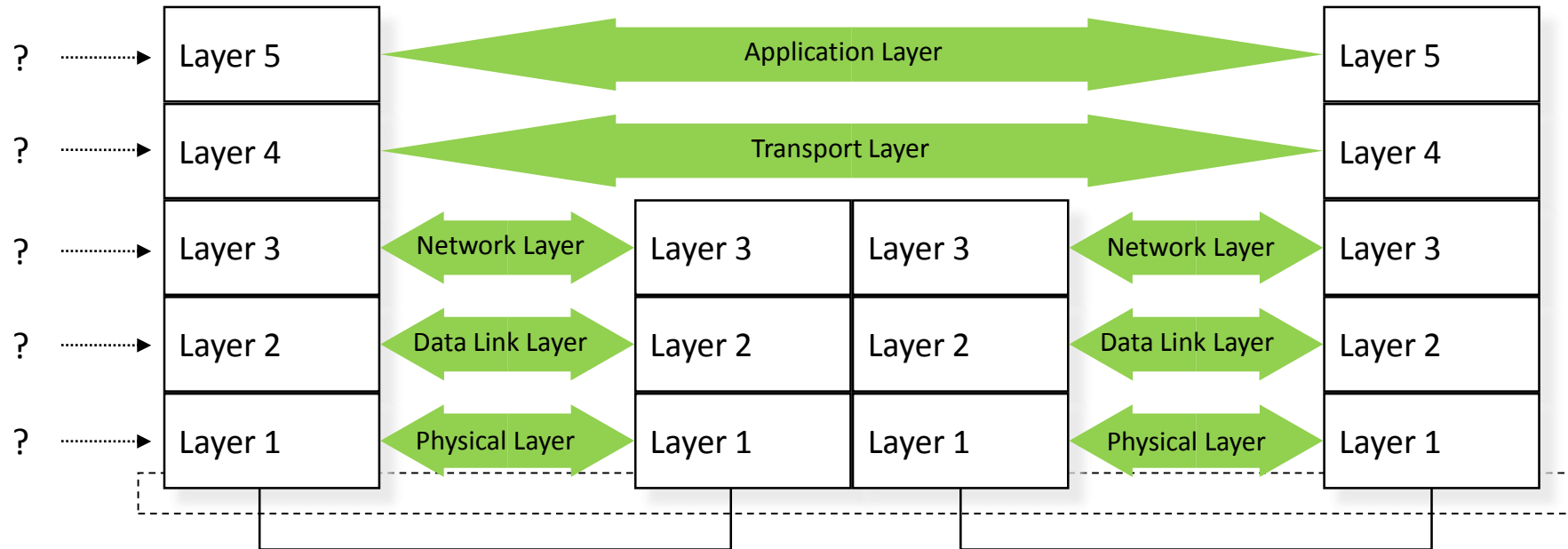
Communication in Layered Protocol Architectures

Security analysis of layered protocol architectures



Dimension 1: At which interface could an attack take place?

Security analysis of layered protocol architectures



Dimension 2: In which layer could an attack take place?

Network Security Analysis

In order to take appropriate countermeasures against threats, these have to be evaluated appropriately for a given network configuration.

Therefore, a detailed network security analysis is needed that:

- evaluates the risk potential of the general threats to the entities using a network, and
- estimates the expenditure (resources, time, etc.) needed to perform known attacks.

Attention: It is generally impossible to assess unknown attacks!

A detailed security analysis of a given network configuration / specific protocol architecture:

- might also be required in order to convince financially controlling entities in an enterprise to grant funding for security enhancements, and
- can be better structured according to more fine grained *attacks at the message level*.

Systematic threat analysis at the message level

A systematic security analysis of a layered protocol architecture has to consider the following attacking techniques:

- **Passive attacks:**
 - Eavesdropping
- **Active attacks:**
 - Delay of PDUs (Protocol Data Units)
 - Replay of PDUs
 - Deletion of PDUs
 - Modification of PDUs
 - Insertion of PDUs

Successful launch of one of the above attacks requires that:

- There are no detectable side effects to other communications (connections / connectionless transmissions)
- There are no side effects to other PDUs of the same connection / connectionless data transmission between the same entities

Security analysis of communication infrastructures

On the preceding slides, the analysis was basically concentrated on potential *attacks on the transmission of information*

Of equal importance, however, are *attacks against the systems*, that are part of or making use of a communication network:

- End systems
- Routers
- Important infrastructure servers: DNS, Email, WWW, file servers, etc.

We, therefore, have to extend our analysis framework:

- Dimension S.1: Which system could be attacked?
- Dimension S.2: Which component of the system is attacked (OS, protocol stack, application process, etc.)?

Security analysis of communication infrastructures

However, this introduces a new difficulty:

- An active entity (system) offers many more attacking opportunities than a passive data object (such as a PDU)
- It is, therefore, much harder to conduct a systematic analysis

Towards systematic threat analysis

One not very systematic approach is the production of *arbitrary threat lists* by any ad-hoc brainstorming method

Example: Hospital Information System

- Corruption of patient medical information
- Corruption of billing information
- Disclosure of confidential patient information
- Compromise of internal schedules
- Unavailability of confidential patient information
- ...

Drawbacks of this approach:

- Questionable completeness of identified threats
- Lack of rationale for identified threats other than experience
- Potential inconsistencies (e.g. disclosure vs. unavailability of confidential patient information in the example above)

Threat Trees: one systematic threat analysis approach

Definition: *threat tree*

- A *threat tree* is a tree with:
 - *nodes* describing threats at different levels of abstractions, and
 - *subtrees* refining the threat of the node they are rooted at,
 - where the child nodes of one node give a *complete refinement* of the threat represented by the parent node

Threat Trees: one systematic threat analysis approach

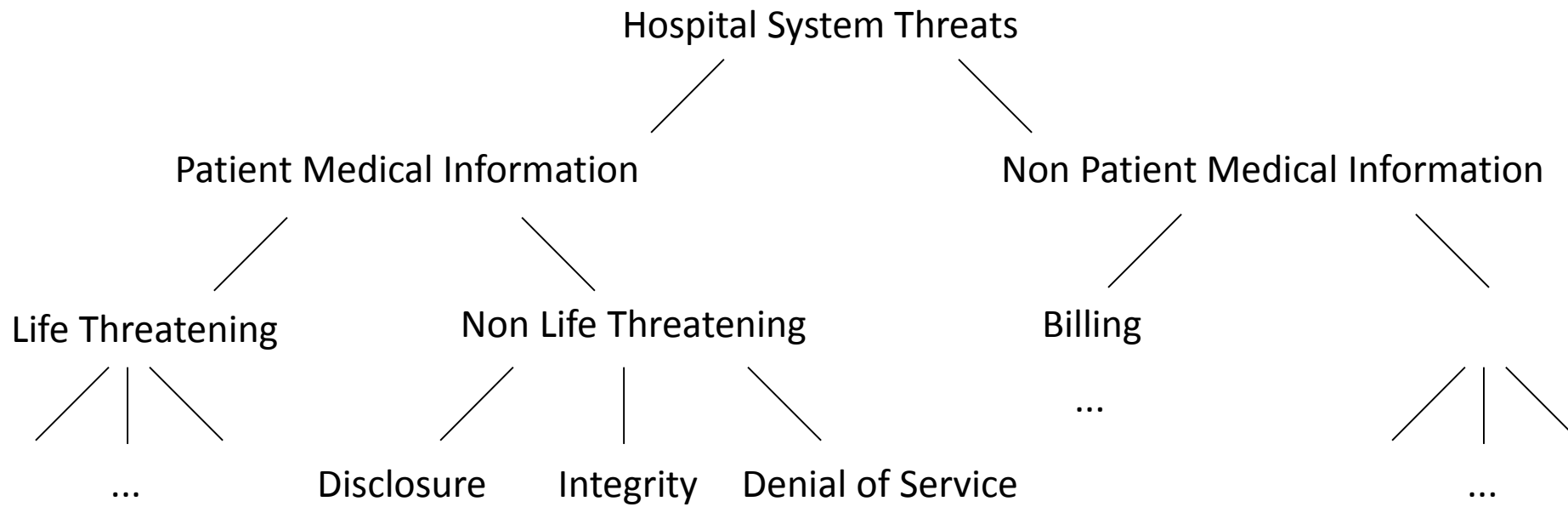
Technique for establishing threat trees:

- Start with a general abstract description of the complete set of threats that exist for a given system (e.g. “security of system X compromised”)
- Iteratively introduce detail by gradually refining the description with care
- Each introduced node may itself become the root of a subtree further describing the threat represented by the node
- Eventually, each leaf node of the tree provides a description of a threat that can be used for a (less arbitrary) threat list

The main idea of this technique is to postpone the creation of (arbitrary) threat lists as much as possible

Example:

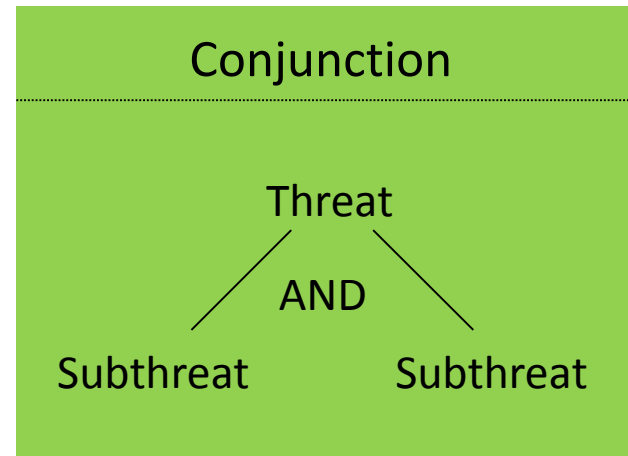
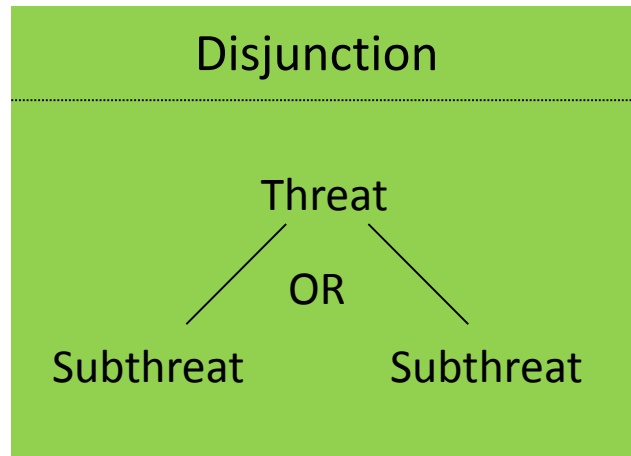
A hospital information system threat tree



It is important that at each level of refinement the child nodes of a node maintain *demonstrable completeness* so that one can be confident that nothing has been missed

Inferring composed threat in threat trees

The child nodes of one node can actually be in different relations to their parent node with the two most common relations being:

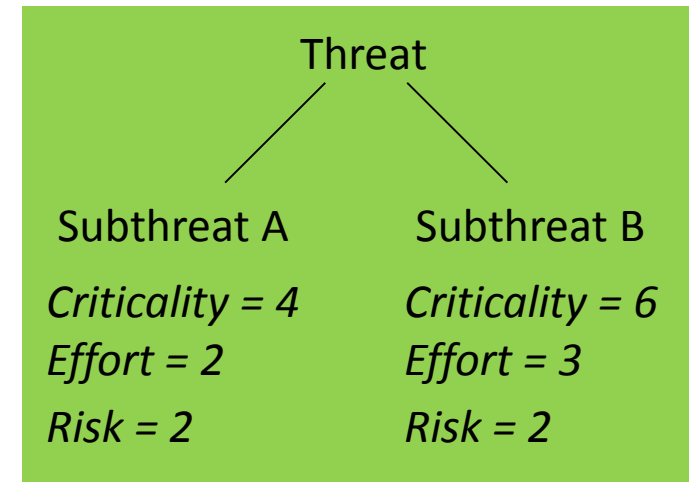
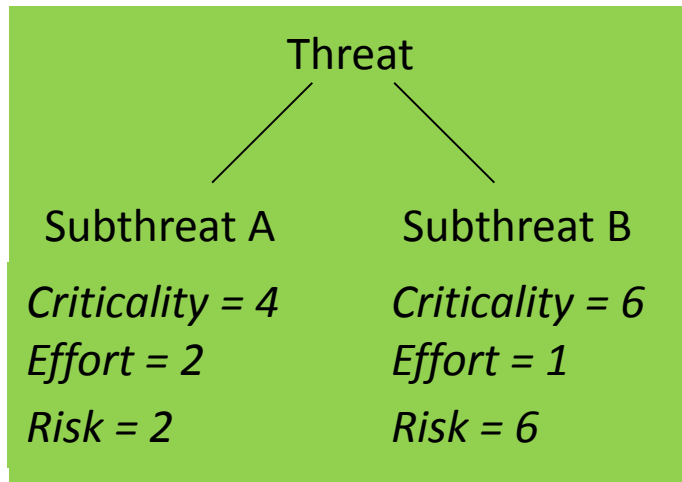


These relations can be used to infer composed threat:

- Augment nodes with effort estimations (e.g. easy, moderate, high)
- Infer effort of an OR-related composed threat as the lowest effort value of its child nodes (the attacker will most likely take the easy way...)
- For AND-related composed threats, the highest effort is inferred

Supporting systems engineering with threat trees

When augmented with appropriate attributes (e.g. estimated criticality and attacker effort for individual threats), threat trees can help to gain insight where to spend resources to decrease the overall system's vulnerability:



- The second threat tree re-evaluates risk after some protective measure has been taken to increase the attackers effort for sub-threat B
- In the above example, risk is assessed with the following formula:
 - $\text{Risk} = \text{Criticality} / \text{Effort}$

A high level systems engineering process

Specify system architecture:

- Identify components and interrelations

Identify threats, vulnerabilities and attack techniques:

- The threat tree technique provides help for this step

Estimate component risks by adding attributes to the threat tree:

- However, removing subjectivity from initial assessments is often impossible and other attributes than criticality and effort (e.g. risk of detection) might have to be considered as well

Prioritize vulnerabilities:

- Taking into account the components' importance

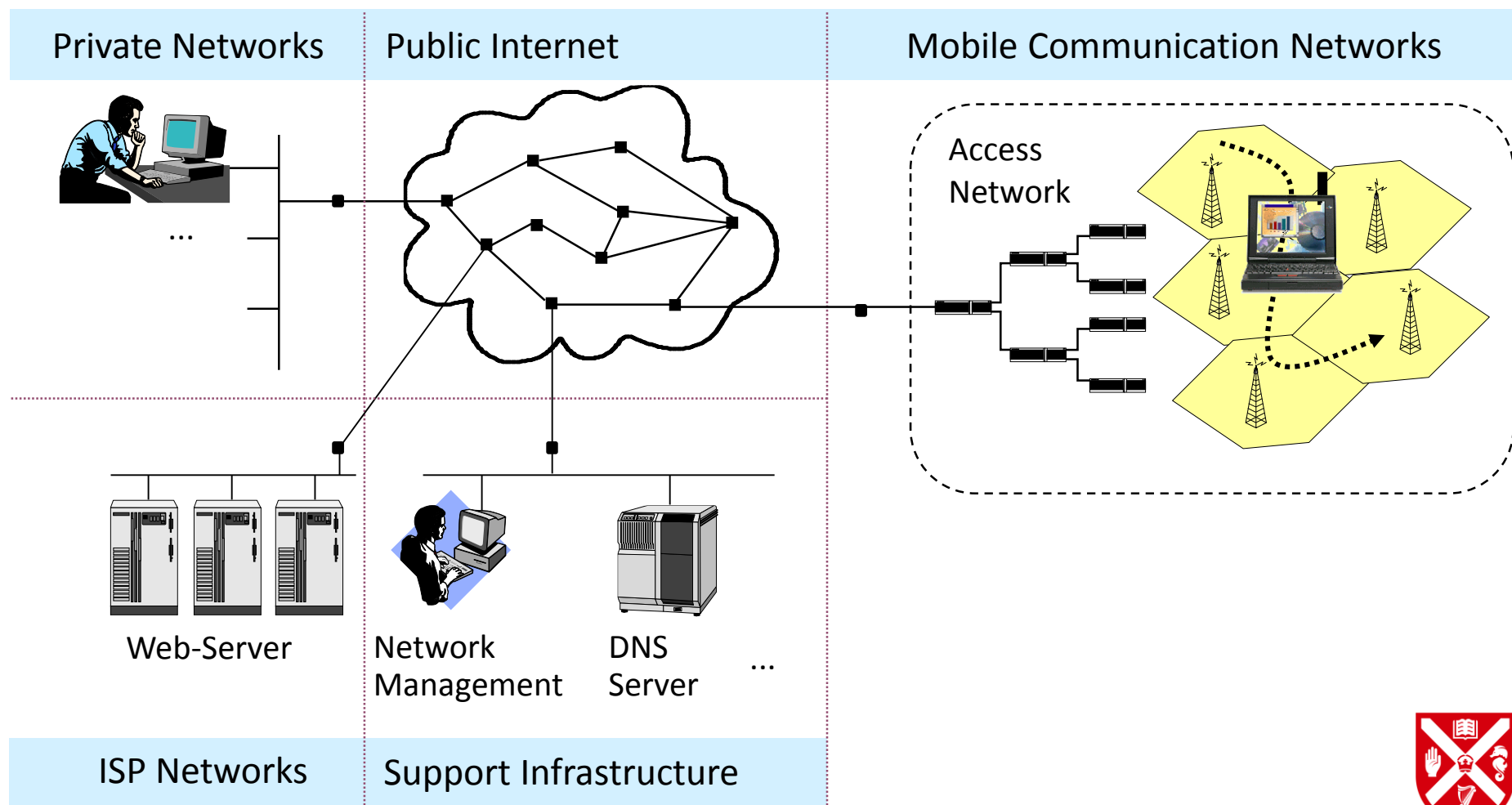
Identify and install safeguards:

- Apply protection techniques to counter high priority vulnerabilities

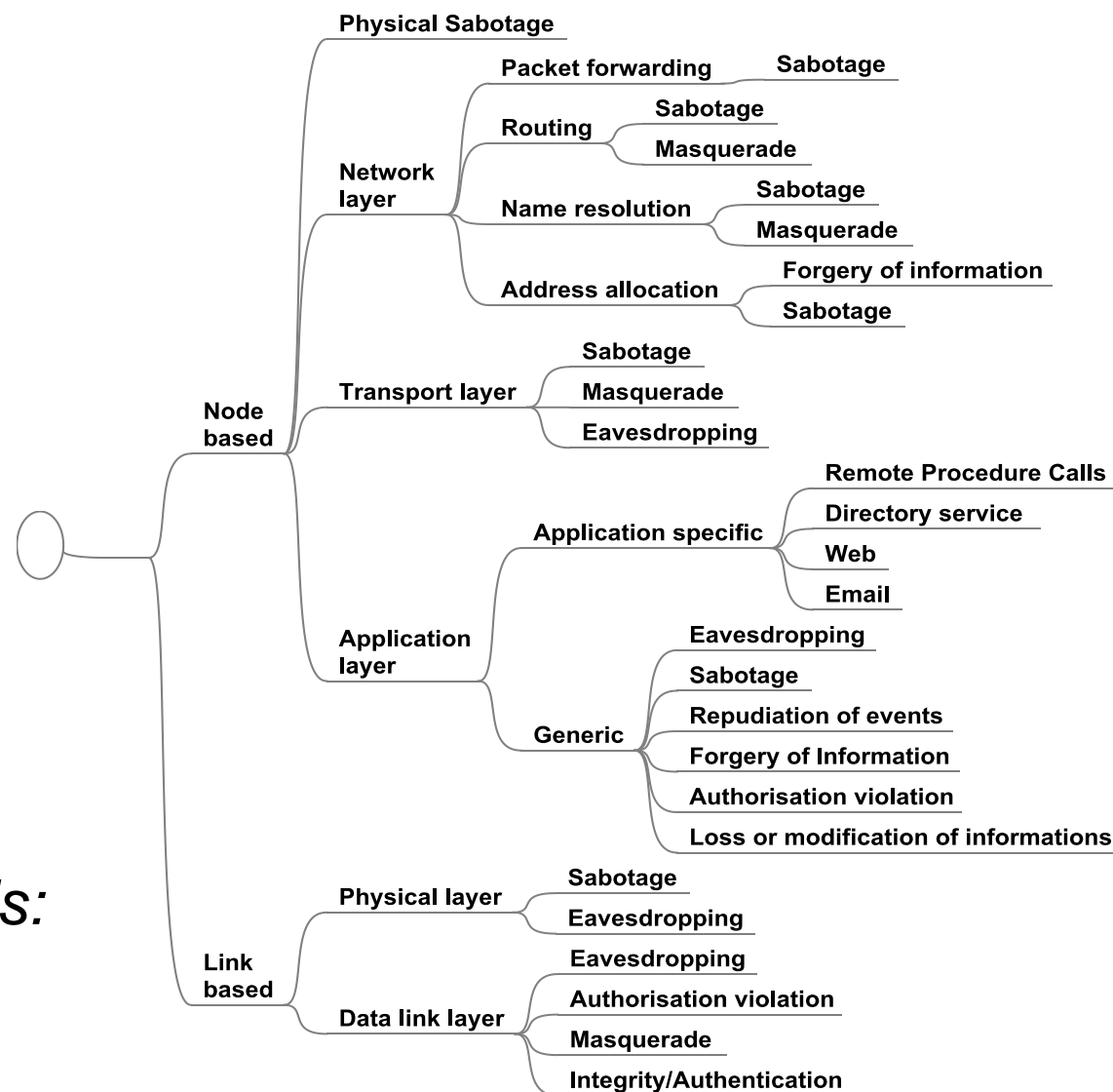
Perform potential iterations of this process

- Re-assess risks of the modified system and decide if more iterations are required

A high level model for Internet-based IT infrastructure



A high level threat tree for Internet-based IT infrastructure



Resource for threat analysis:

<https://attack.mitre.org/>

Countering attacks: Three principle classes of action

Prevention:

- All measures taken in order to avoid that an attacker succeeds in realizing a threat
- Examples:
 - Cryptographic measures: encryption, computation of modification detection codes, running authentication protocols, etc.
 - Firewall techniques: packet filtering, service proxying, etc.
- Preventive measures are by definition taken *before an attack takes place*

Detection:

- All measures taken to recognize an attack *during or after it occurred*
- Examples:
 - Recording and analysis of audit trails
 - On-the-fly traffic monitoring

Reaction:

- All measures taken in order to react to *ongoing or past attacks*

Safeguards against information security threats (1)

Physical Security:

- Locks or other physical access control
- Tamper-proofing of sensitive equipment
- Environmental controls

Personnel Security:

- Identification of position sensitivity
- Employee screening processes
- Security training and awareness

Administrative Security:

- Controlling import of foreign software
- Procedures for investigating security breaches
- Reviewing audit trails
- Reviewing accountability controls

Safeguards against information security threats (2)

Emanations Security:

- Radio Frequency and other electromagnetic emanations controls
- Referred to as *TEMPEST protection*

Media Security:

- Safeguarding storage of information
- Controlling, marking, reproduction and destruction of sensitive information
- Ensuring that media containing sensitive information are destroyed securely
- Scanning media for viruses

Lifecycle Controls:

- Trusted system design, implementation, evaluation and endorsement
- Programming standards and controls
- Documentation controls

Safeguards against information security threats (3)

Computer / System Security:

- Protection of information while stored / processed in a system
- Protection of the computing devices / systems themselves

Communications Security:

- Protection of information during transport from one system to another
- Protection of the communication infrastructure itself

Security Services - Overview

Authentication

- The most fundamental security service, which ensures that an entity has, in fact, the identity that it claims to have

Integrity

- It ensures that data created by specific entities may not be modified without detection

Confidentiality

- The most popular security service, ensuring the secrecy of protected data

Access Control

- Controls that each identity accesses only those services and information it is entitled to

Non-Repudiation

- Protects against the possibility for entities participating in a communication exchange to later falsely deny that the exchange occurred

Security supporting mechanisms

General mechanisms:

- *Key management*: All aspects of the lifecycle of cryptographic keys
- *Random number generation*: Generation of cryptographically secure random numbers
- *Event detection / security audit trail*: Detection and recording of events that might be used in order to detect attacks or conditions that might be exploited by attacks
- *Intrusion detection*: Analysis of recorded security data in order to detect successful intrusions or attacks
- *Notarization*: Registration of data by a trusted third party that can confirm certain properties (content, creator, creation time) of the data later on

Communication specific mechanisms:

- *Traffic padding & cover traffic*: Creation of bogus traffic in order to prevent traffic flow analysis
- *Routing control*: Influencing the routing of PDUs in a network

Summary

- ❑ Threats and Security Goals
- ❑ Threat Analysis
 - ❑ message level (layered protocol architecture)
 - ❑ communication infrastructure
- ❑ Threat Trees
- ❑ System Security Engineering
- ❑ Security Services

Questions?

Next Session: Friday, 18 January 2019

Introduction to Network Security – Part 2