University of Essex

Online

Launching into Cyber Security

Week 4 Seminar

Sammy Danso, PhD

University of Essex

Online

Announcement

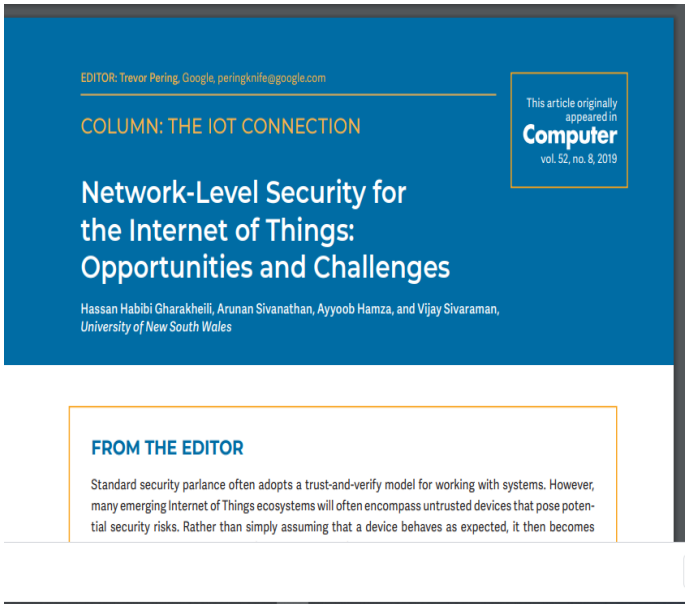
- Collaborative discussion 1
- IEEE magazine

University of Essex

Online

Announcement

https://ieeecs-media.computer.org/media/marketing/cedge_digital/ce-feb21-final.pdf



EDITOR: Trevor Pering, Google, peringknife@google.com

COLUMN: THE IOT CONNECTION

This article originally appeared in **Computer** vol. 52, no. 8, 2019

Network-Level Security for the Internet of Things: Opportunities and Challenges

Hassan Habibi Gharakheili, Arunan Sivanathan, Ayyoob Hamza, and Vijay Sivaraman, *University of New South Wales*

FROM THE EDITOR

Standard security parlance often adopts a trust-and-verify model for working with systems. However, many emerging Internet of Things ecosystems will often encompass untrusted devices that pose potential security risks. Rather than simply assuming that a device behaves as expected, it then becomes

University of Essex

Online

This week's task

- Review 3 threat modelling techniques that you have found are more commonly used in any industry of your choice.

- In deciding what techniques to apply, what considerations need to be made to professional, legal, social and ethical concerns?

University of Essex

Online

Outline

- Background to the problem

- Discuss cyber security design approaches to be employed.

University of Essex

Online

Background

University of Essex

Online

Background

Scotland's Health on the Web

Putting Scotland's Health on the Web

NHS SCOTLAND

Home | About NHS Scotland | News | Organisations | Patients | Vacancies | Sites A-Z | Contact Us

Home > Organisations > Fife

Fife

NHS Fife is working to improve health services with the involvement and support of the public and our partners in other NHS Boards, Fife Council and voluntary agencies.

Within the NHS Fife website you can find information about Fife's health services as well as details on a wide range of health topics.

Website: https://www.nhsfife.org

Coronavirus (COVID-19)

If you have concerns about Coronavirus (COVID-19) and are worried about symptoms, you must stay home and call your GP or NHS 24 (111) out of hours where you will receive help.

For the latest health information and advice please visit NHS Inform website.

Latest information on the situation in Scotland is being published by The Scottish Government.

Latest Vacancies

Privacy & Cookies Policy

University of Essex

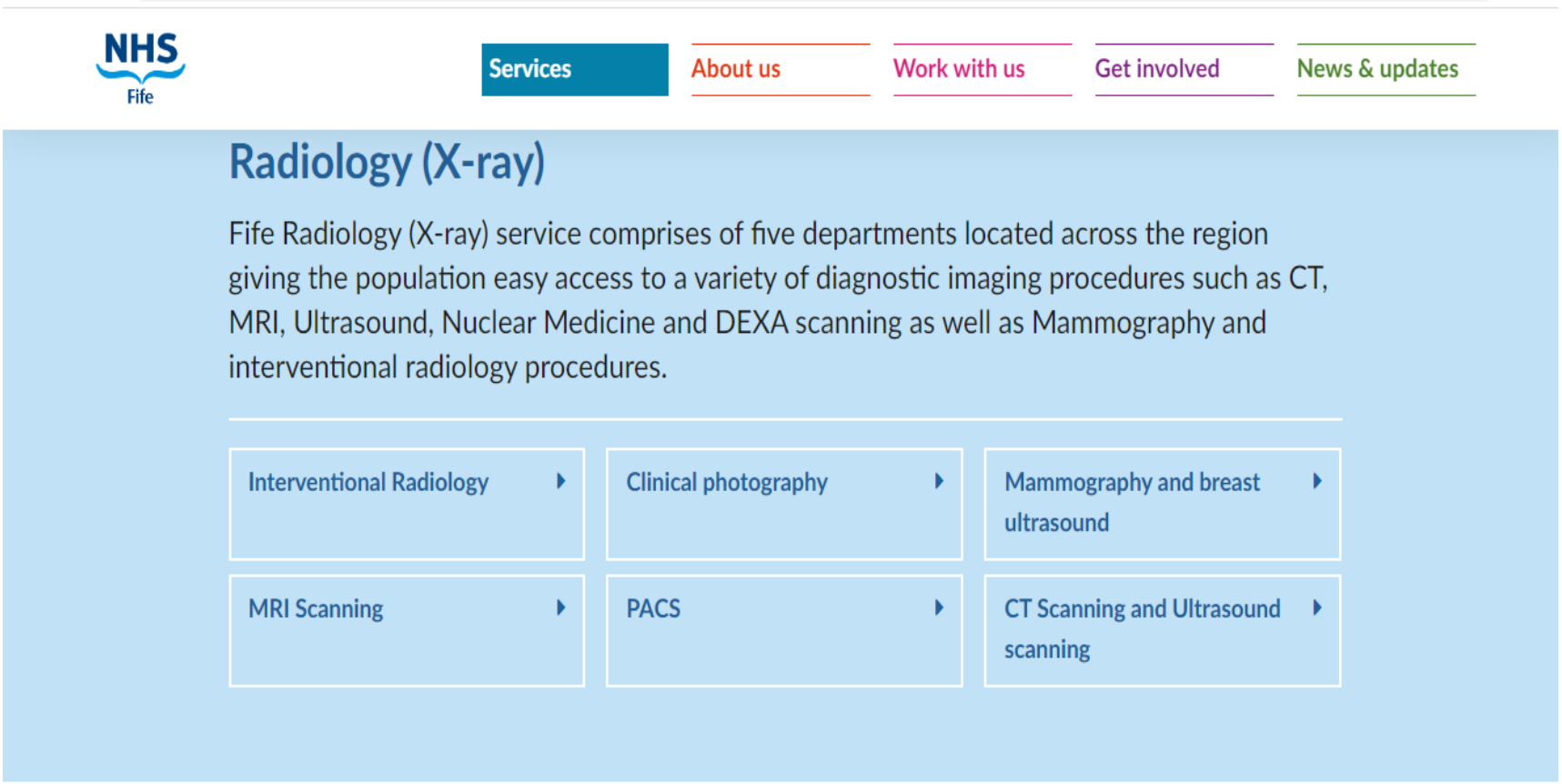
Online

Background: Fife NHS Scotland health

University of Essex

Online

Background: Fife NHS Scotland health



University of Essex

Online

Background: NHS PACS

Picture Archiving Communications System (PACS)

- Access to Radiology service is through a referral system.
- Radiology examinations are stored and reported digitally.
- Imaging is accessed by a Consultant Radiologist and compiles a report.
- Report is sent to the health professional that made the request.

University of Essex

Online

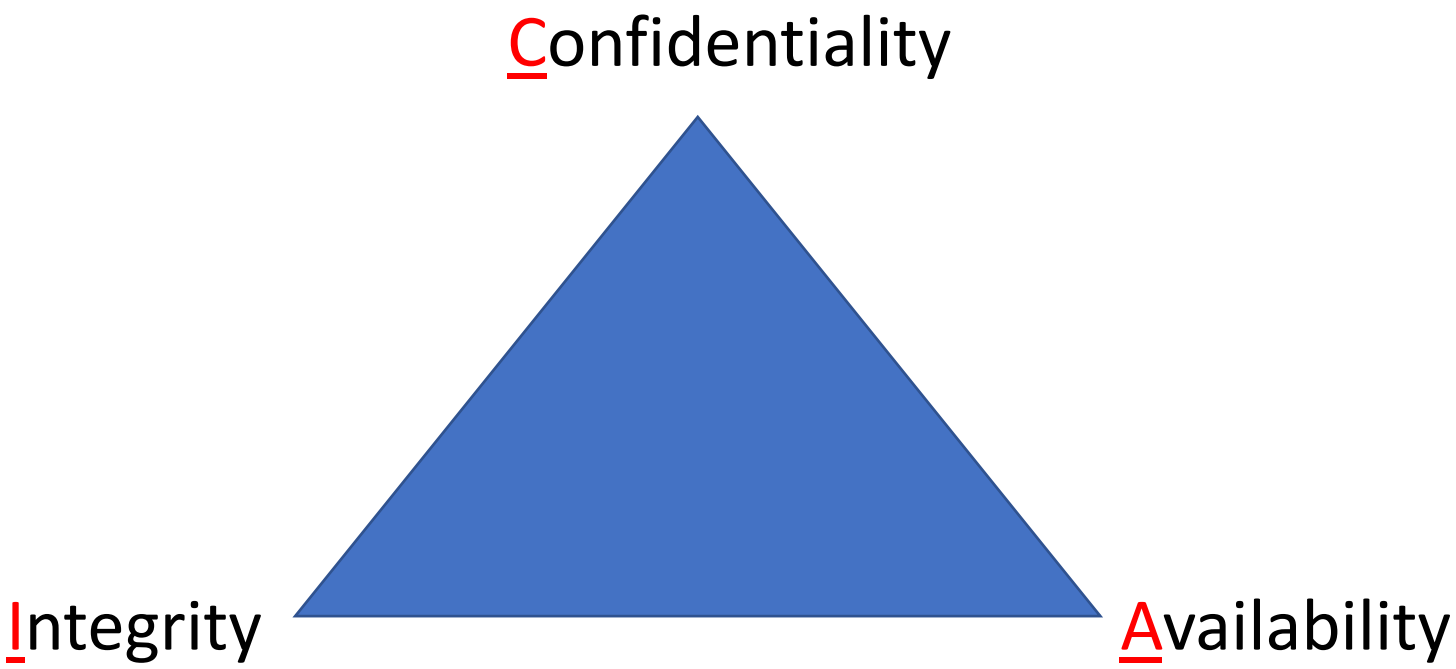
Background: NHS PACS

Picture Archiving Communications System (PACS)

- PACS is a national system – accessible across all health boards.
- Accessible by both Radiology staff and clinicians.
- You must be a doctor or be highly specialised in your clinical field to be able to read x-rays and act upon them.
- Integrates with Image Exchange Portal (IEP) for safe and secure transfer of imaging to specialised healthcare institutions around the UK.

Background: Design objectives

The CIA triangle model



University of Essex

Online

Background: cyber security design principles

UK National Cyber Security Centre (2019)

1. Establish the context – determine all system components – ie have no blind spots.

2. Make compromise difficult - attacker should be able to target only parts of a system that is reachable – penetration must be difficult.

3. Make disruption difficult - resilient to DoS attacks.

4. Make compromise detection easier – have the ability to detect when attacks or suspicious activities occur.

5. Reduce the impact of compromise – when attacker succeeds in gaining access to any part of the system

Background: Cyber security design principles

UK National Cyber Security Centre (2019)

1. Establish the context – determine all system components – ie have no blind spots for PACS.

Background: cyber security design principle 1

Establish the context – determine all system components – ie have no blind spots for PACS

- Hardware
- Software
- Databases
- Networks
- People & procedures

Source: Wikipedia

Background: cyber security design principles

UK National Cyber Security Centre (2019)

2. Make compromise difficult - attacker should be able to target only parts of a system that is reachable – penetration must be difficult.

Cyber security design principles

UK National Cyber Security Centre (2019)

3. Make disruption difficult - resilient to DoS attacks.

Cyber security design principles

UK National Cyber Security Centre (2019)

4. Make compromise detection easier – have the ability to detect when attacks or suspicious activities occur.

Cyber security design principles

UK National Cyber Security Centre (2019)

5. Reduce the impact of compromise – when attacker succeeds in gaining access to any part of the system.

University of Essex

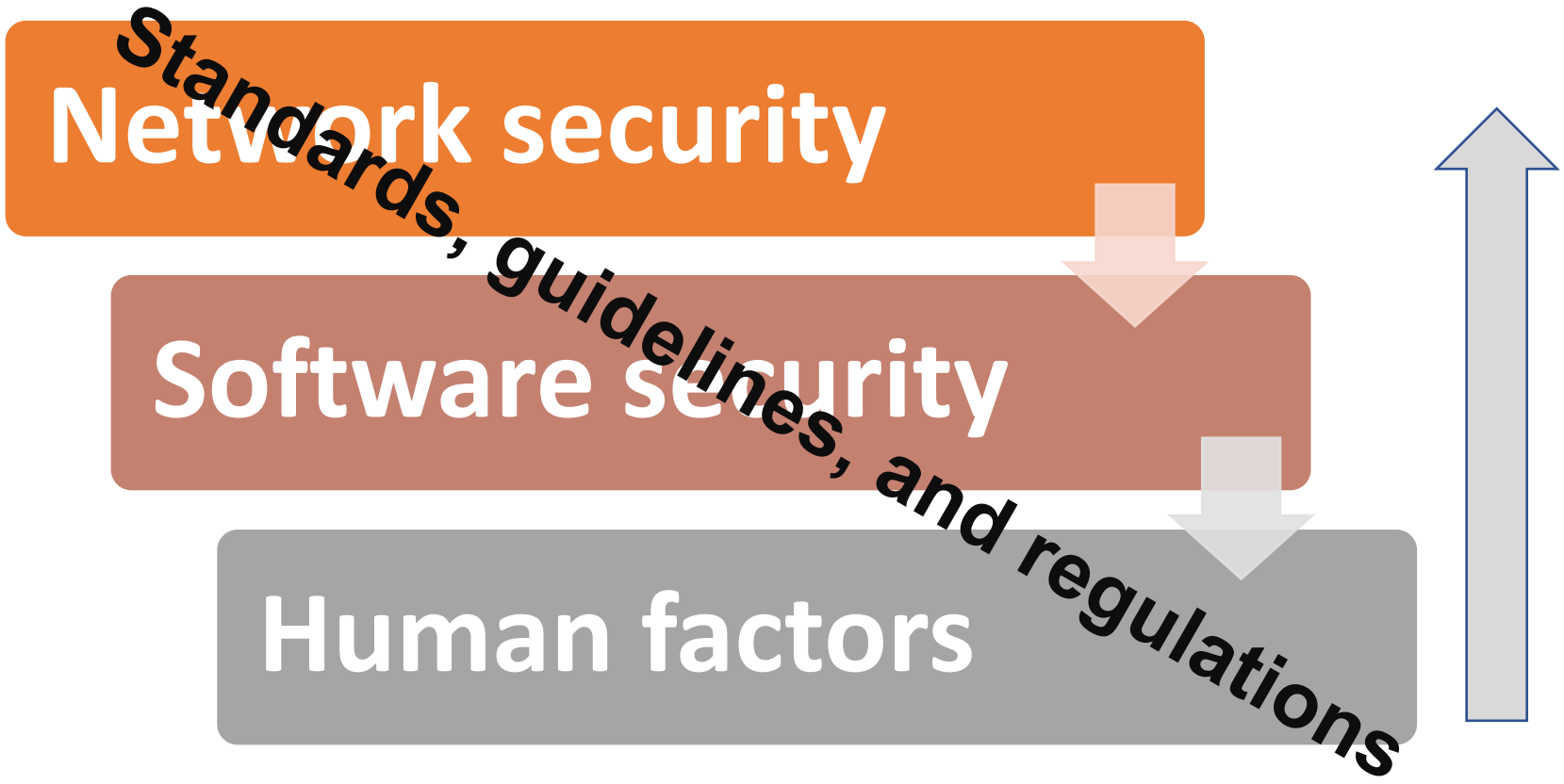
Online

Outline

- Background to the problem

- Discuss cyber security design approaches to be employed.

Approaches


Network security
Software security
Human factors
Standards, guidelines, and regulations

Approaches

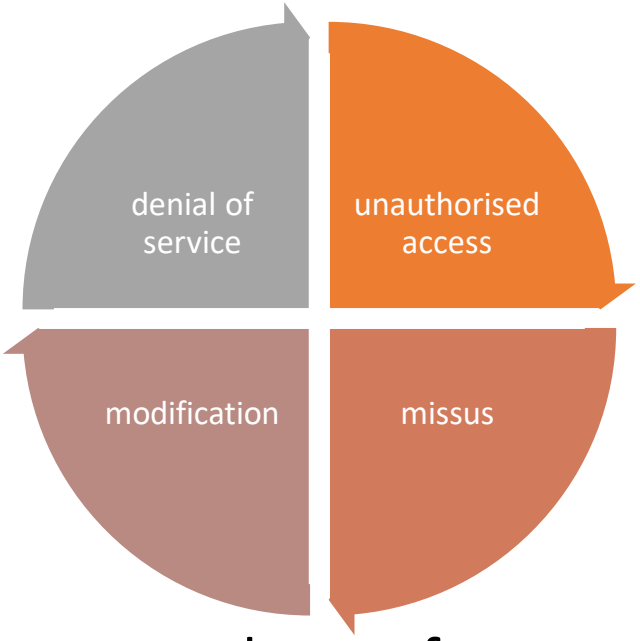
Network security

University of Essex

Online

Network security

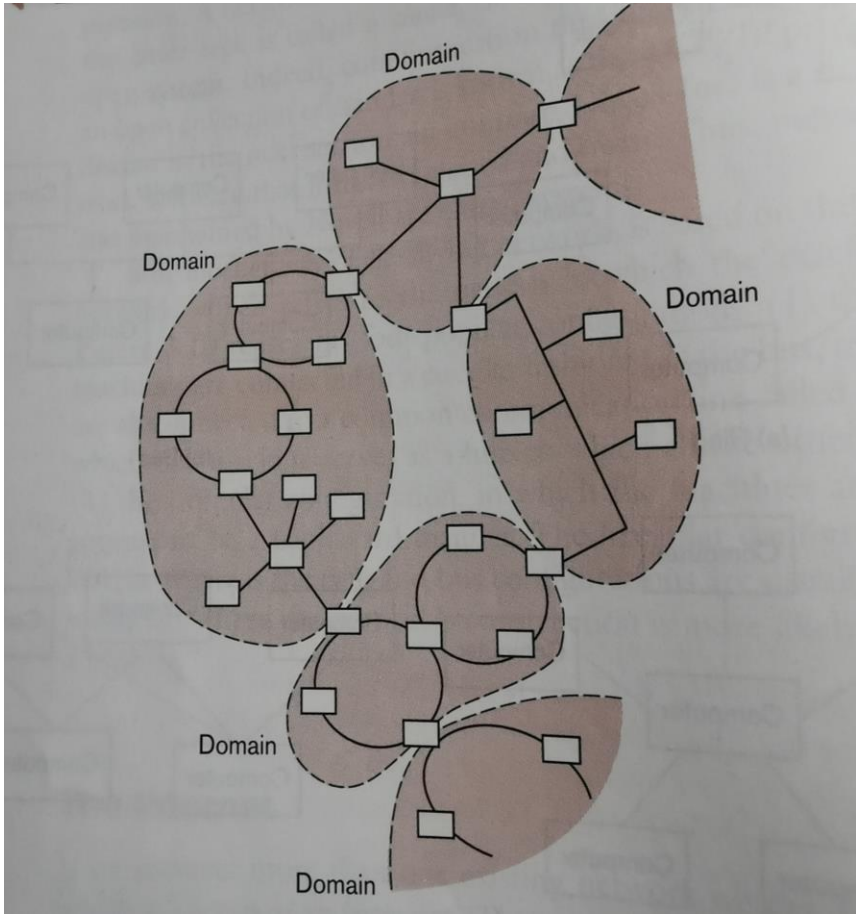
- Network security - focuses on networked-resources



- Overall objective is to stop threats from spreading over networks

Network security

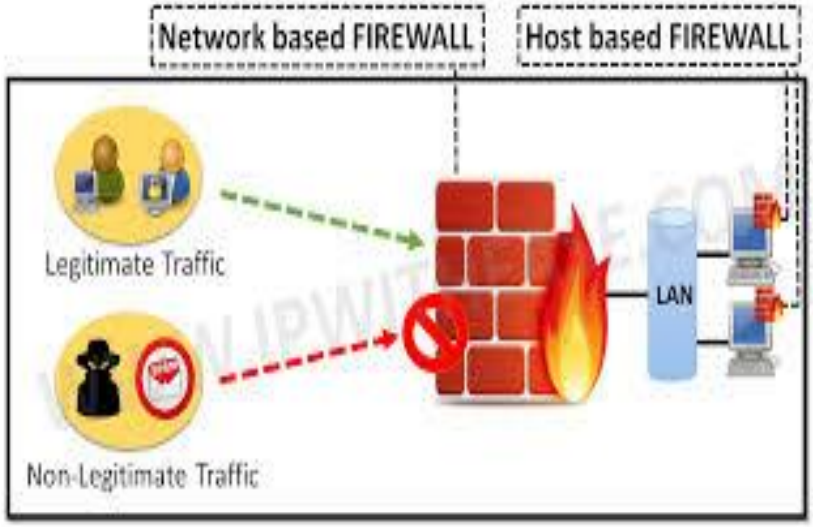
- Local Area Network
  - Domain
  - Subdomains
- Define and implement access level policies.
- Wide Area Networks
  - Connection to other health boards and UK wide.
- Different levels of firewalls



Network security

Different levels and types of firewalls

- Packet-filtering
- Circuit-level gateways
- Stateful inspection
- Software
- Hardware
- Cloud



Network security

Define and implement access level policies.

- Domain
- Subdomains
- User groups
  - Consultant Radiologists , Clinicians , Radiographers, etc
- Device / IP address level

Approaches

Software security

Software security

Security requirement:

- Identifies:
  - what needs protection, from who and for what period
- Specifies:
  - what the system must do and not do
  - why the system should behave as specified
- Avoid:
  - how problems must be solved.

Software security

Threat identification

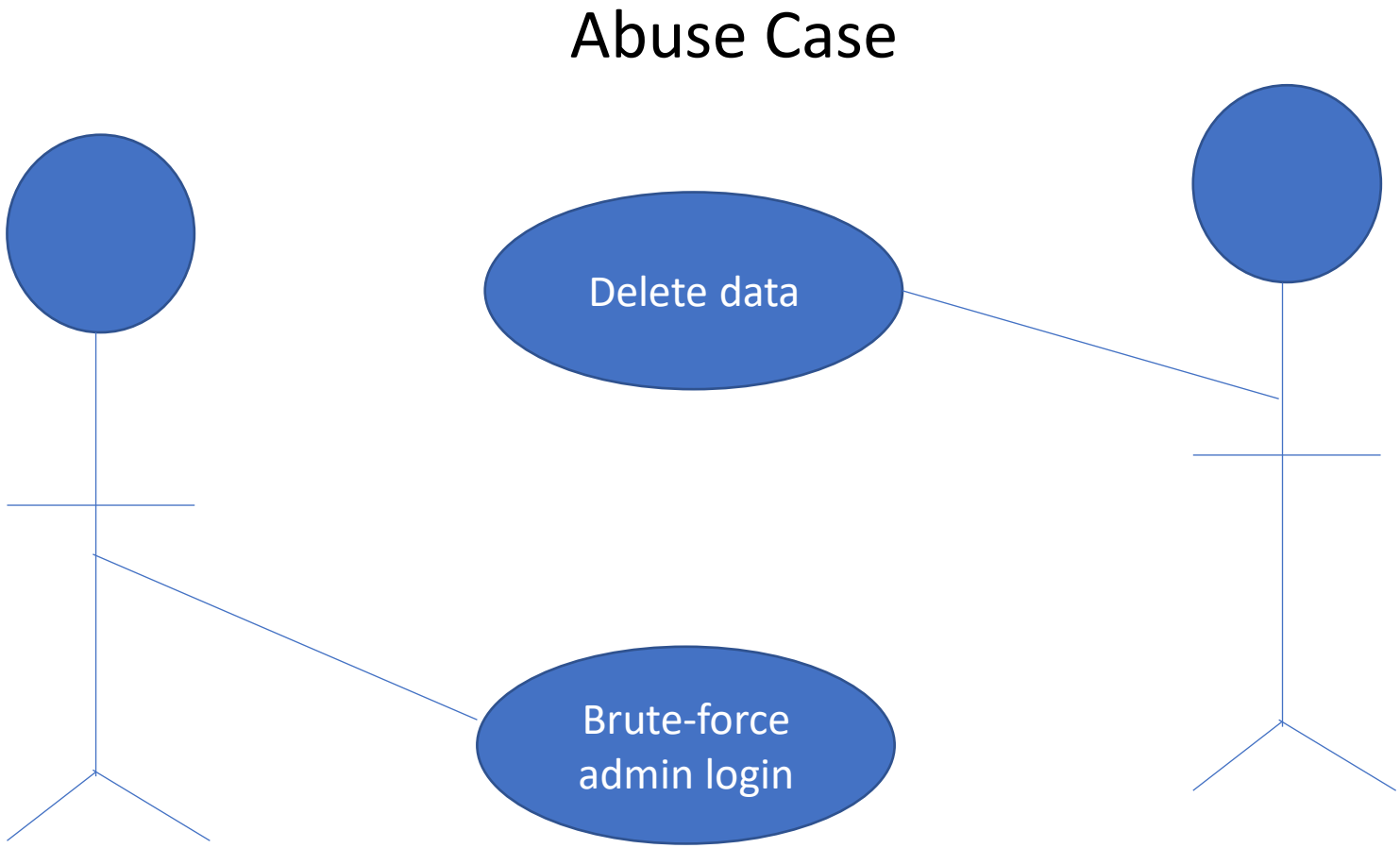
- Sometimes referred to as threat modelling
- An abstraction of the system
- Profiles of potential attackers, including their goals and methods.

Software security

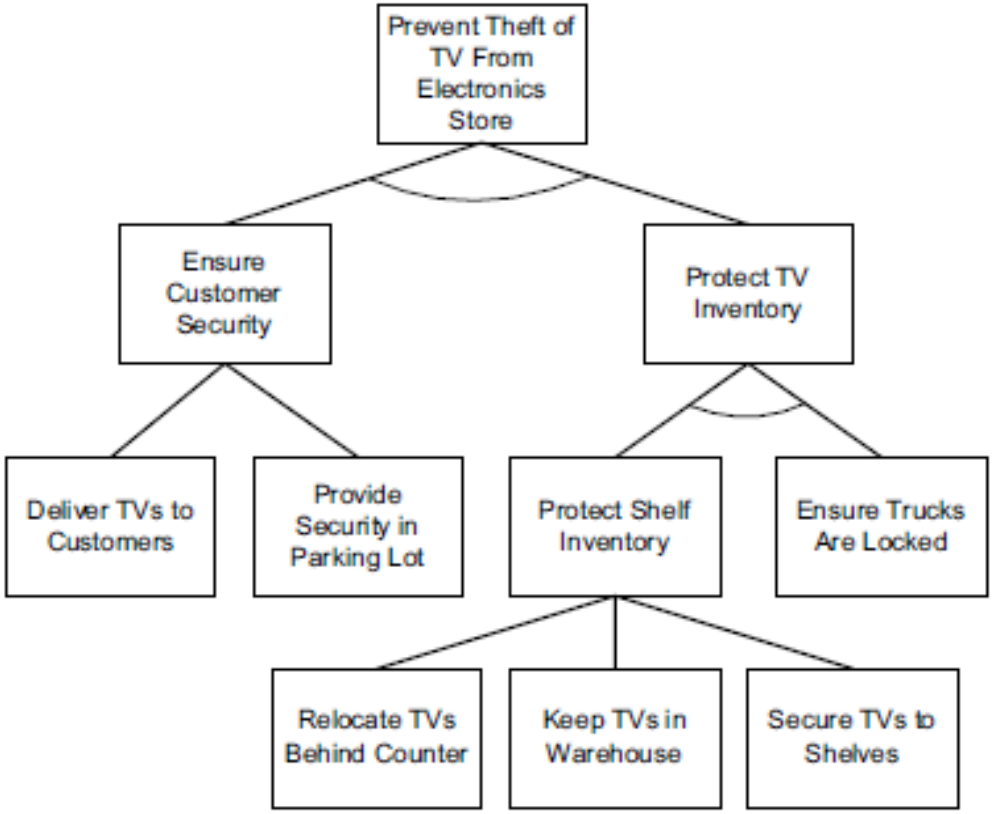
Some threat modelling techniques

- Abuse case
- STRIDE
- Attack trees
- Protection trees
- A combination of techniques

Software security

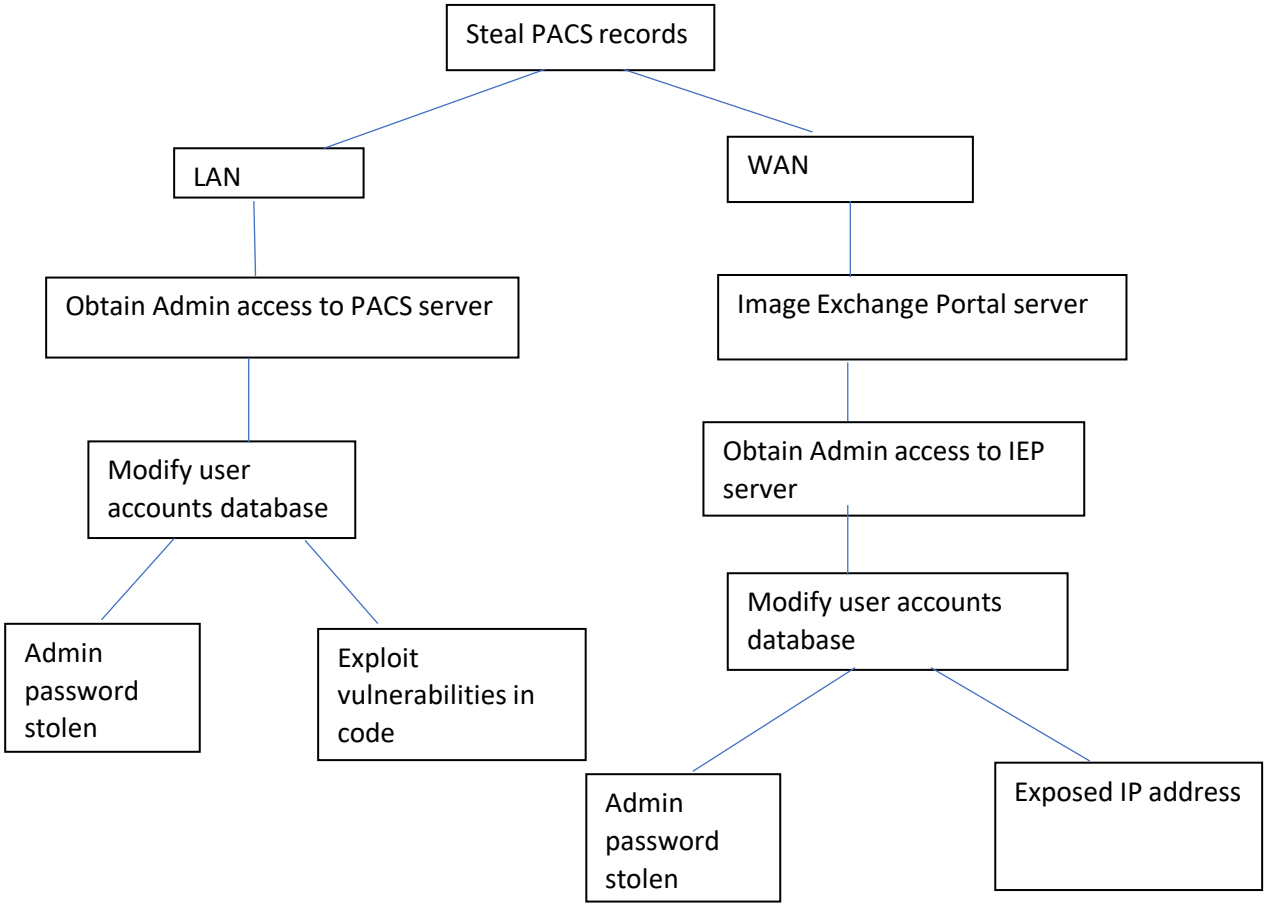


Software security



Taken from Edge et al (2007).

Software security



Software security

The STRIDE method

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

Software security

The STRIDE method

Spoofing ..

- Using fake identity to gain access.

- Threat aims at authentication

Software security

The STRIDE method

Tampering …a threat to data integrity

Software security

The STRIDE method

Repudiation .. aims at clearing activity logs to avoid auditing and tracing

Software security

The STRIDE method

Information disclosure - some possible causes include:

- Bugs in code e.g buffer overflow
- Physical access to storage areas
- External drives and USB
- Laptops

Software security

The STRIDE method

Denial of service…threat to systems availability.

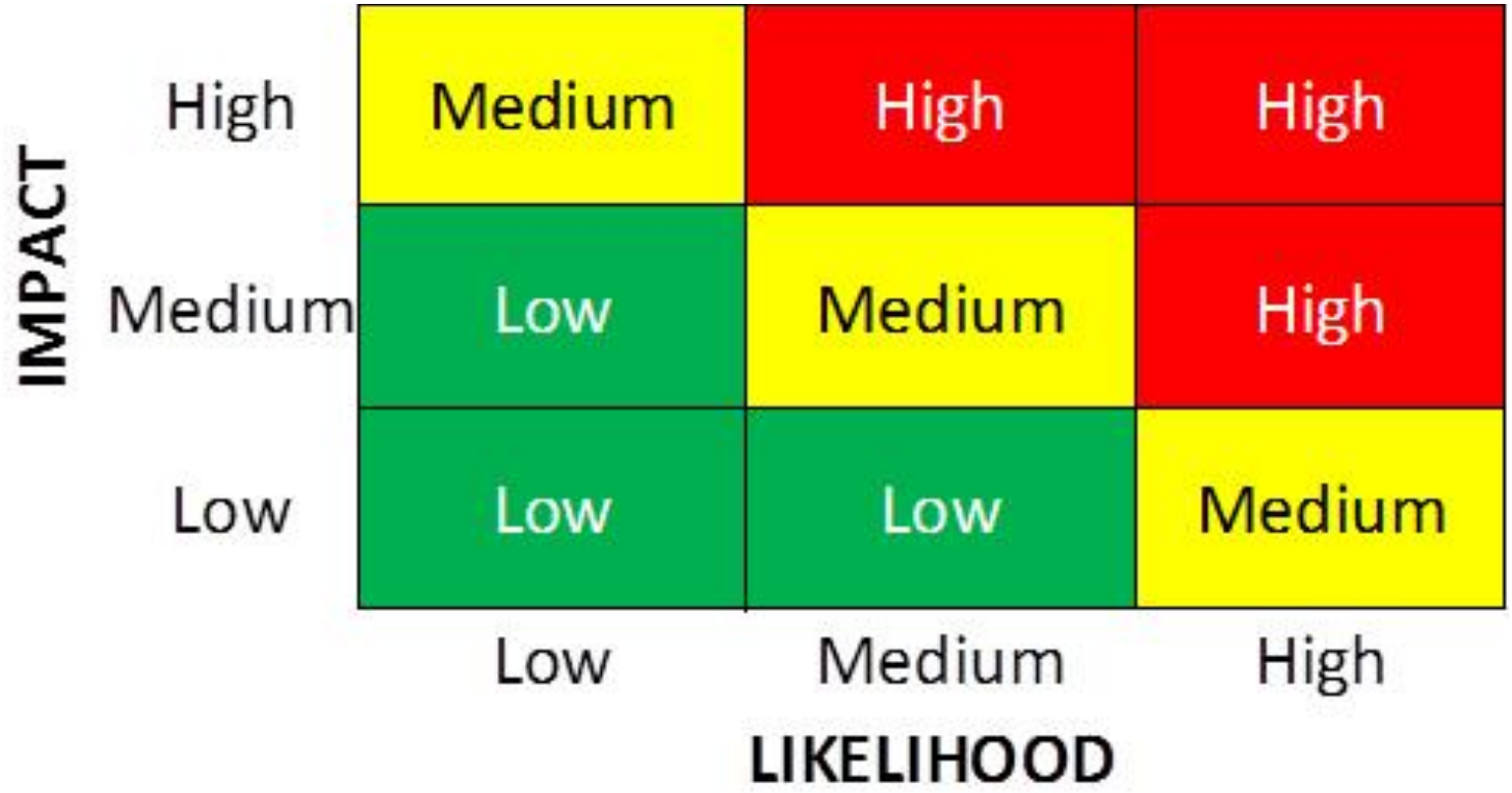
Software security

The STRIDE method

Elevation of privilege.. threat aiming at authorisation

Software security

Threat Assessment



Summary

- Applying some design principles (e.g UK National Cyber Security Centre (2019) is a useful approach as it provides a framework to security design of a system.

- Combining Network and Software approaches to security design offers the best design solution, BUT may not be optimal.

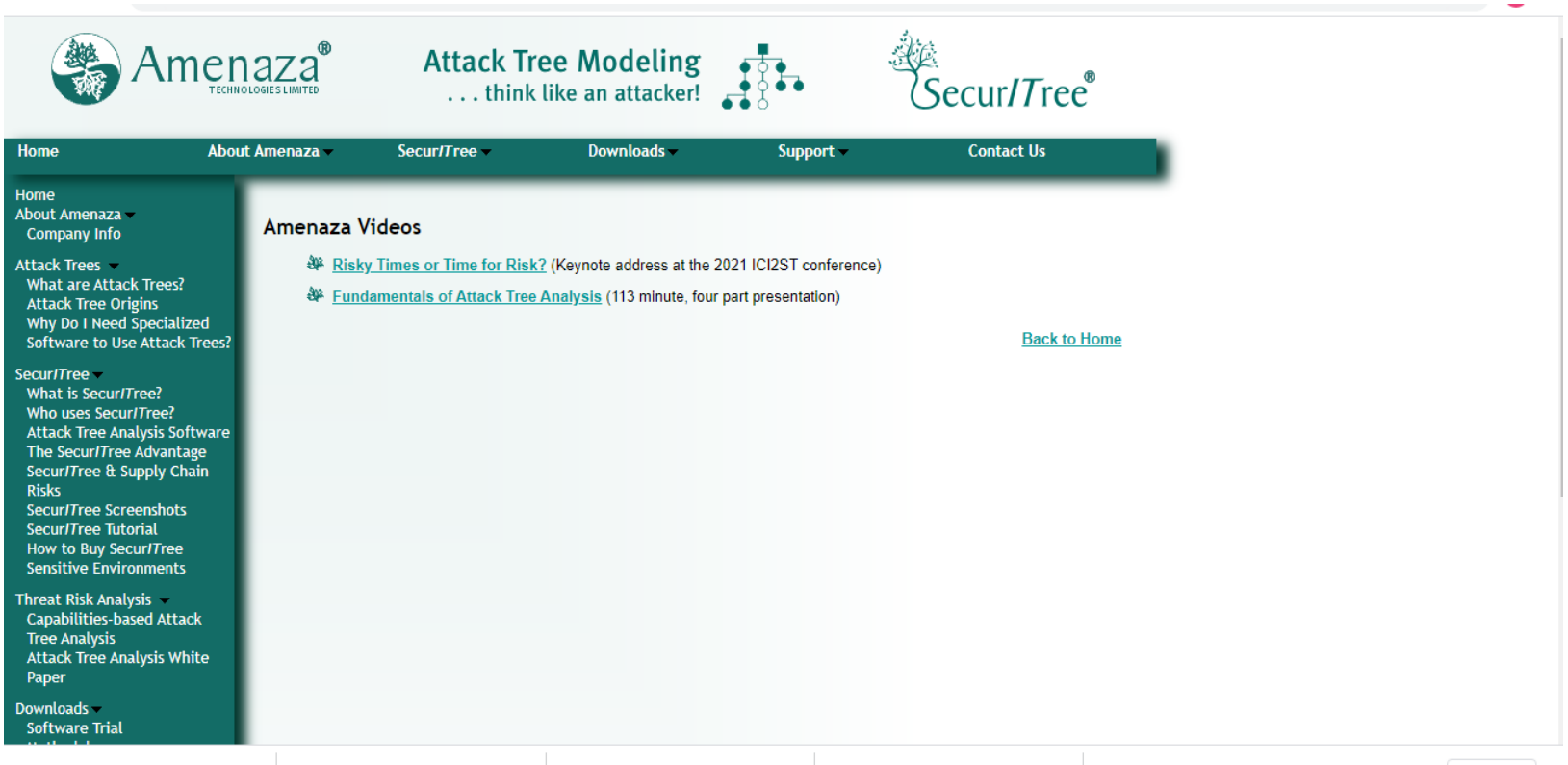
- The human factors may still exist even after employing technological solutions.

University of Essex

Online

Additional resource

Special thanks to Doug Leece.



https://www.amenaza.com/videos.php

Exercise

- Try your hands on:
- Protection tress
- Abuse cases