



University of Essex

Online

Launching into Cyber Security

Week 4 Seminar

Sammy Danso, PhD



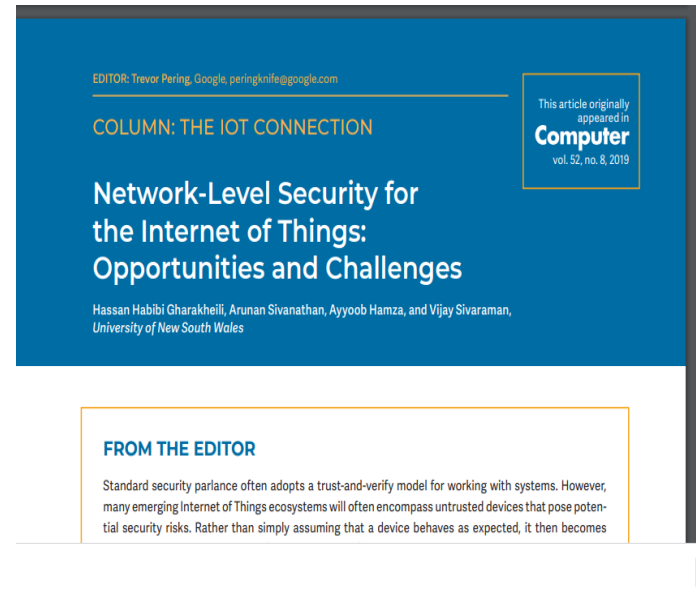
Announcement

- Collaborative discussion 1
- IEEE magazine



Announcement

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





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?



Outline

- Background to the problem
- Discuss cyber security design approaches to be employed.



Background

Scotland's Health on the Web

Putting Scotland's Health on the Web



[Home](#) [About NHS Scotland](#) [News](#) [Organisations](#) [Patients](#) [Vacancies](#) [Sites A-Z](#) [Contact Us](#)



[Home](#) > [Organisations](#)

Organisations

NHSScotland consists of 14 regional NHS Boards which are responsible for the protection and the improvement of their population's health and for the delivery of frontline healthcare services and 7 Special NHS Boards and 1 public health body who support the regional NHS Boards by providing a range of important specialist and national services.

NHS Scotland Health Boards



Background

Scotland's Health on the Web

Putting Scotland's Health on the Web



[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](#)



Background: Fife NHS Scotland health



Services

About us

Work with us

Get involved

News & updates

Mobility



Neurology



Nutrition and Dietetics



Occupational therapy



Orthotics service



Pain Management Service



Palliative care



Pharmacy



Physiotherapy



Preparing for surgery



Prosthetics service



Psychology services



Radiology (X-ray)



Rheumatology



Respiratory



Sexual health



Speech and language therapy



Spiritual care



Trauma and orthopaedics
service



Urgent Care Service



Urology



Wig Service



Wheelchair and postural
management service NHS



Winter





Background: Fife NHS Scotland health



Services

About us

Work with us

Get involved

News & updates

Radiology (X-ray)

Fife Radiology (X-ray) service comprises of five departments located across the region giving the population easy access to a variety of diagnostic imaging procedures such as CT, MRI, Ultrasound, Nuclear Medicine and DEXA scanning as well as Mammography and interventional radiology procedures.

Interventional Radiology ▶

Clinical photography ▶

Mammography and breast
ultrasound ▶

MRI Scanning ▶

PACS ▶

CT Scanning and Ultrasound
scanning ▶



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.



Background: NHS PACS

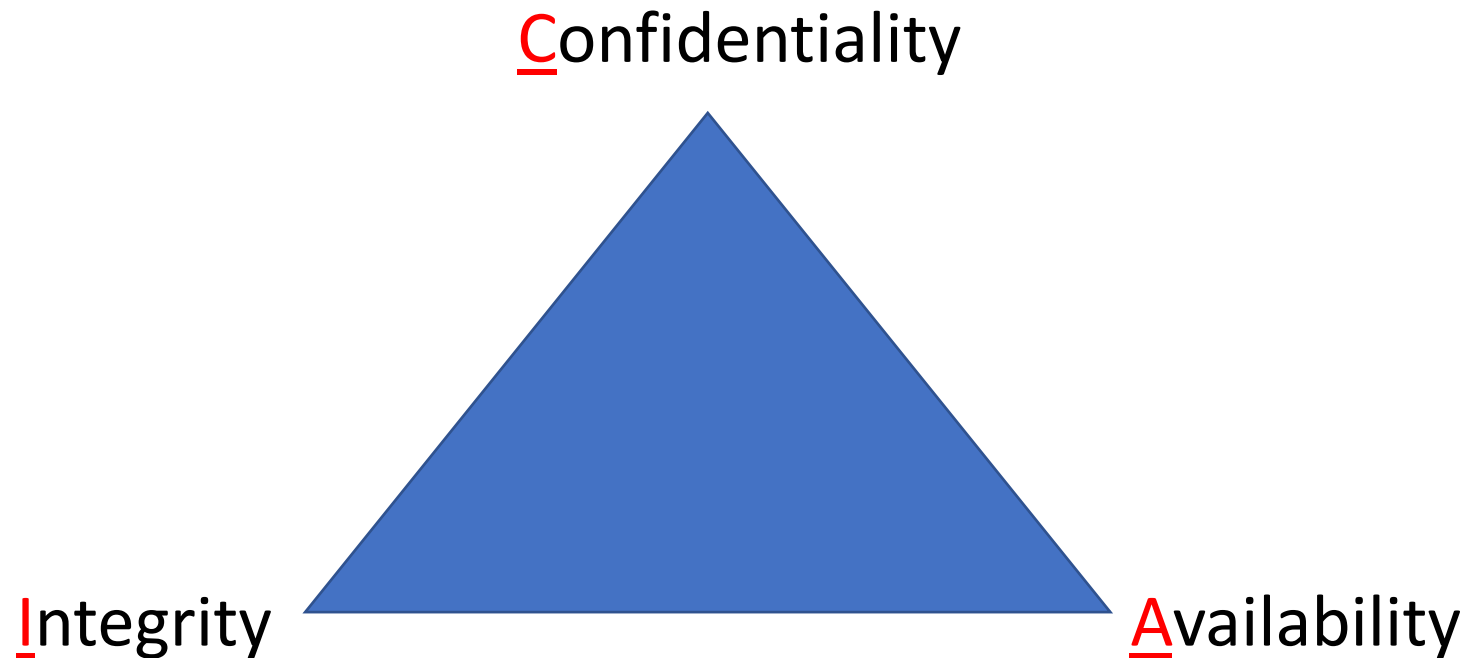
Picture Archiving Communications System (PACS)

- 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





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.

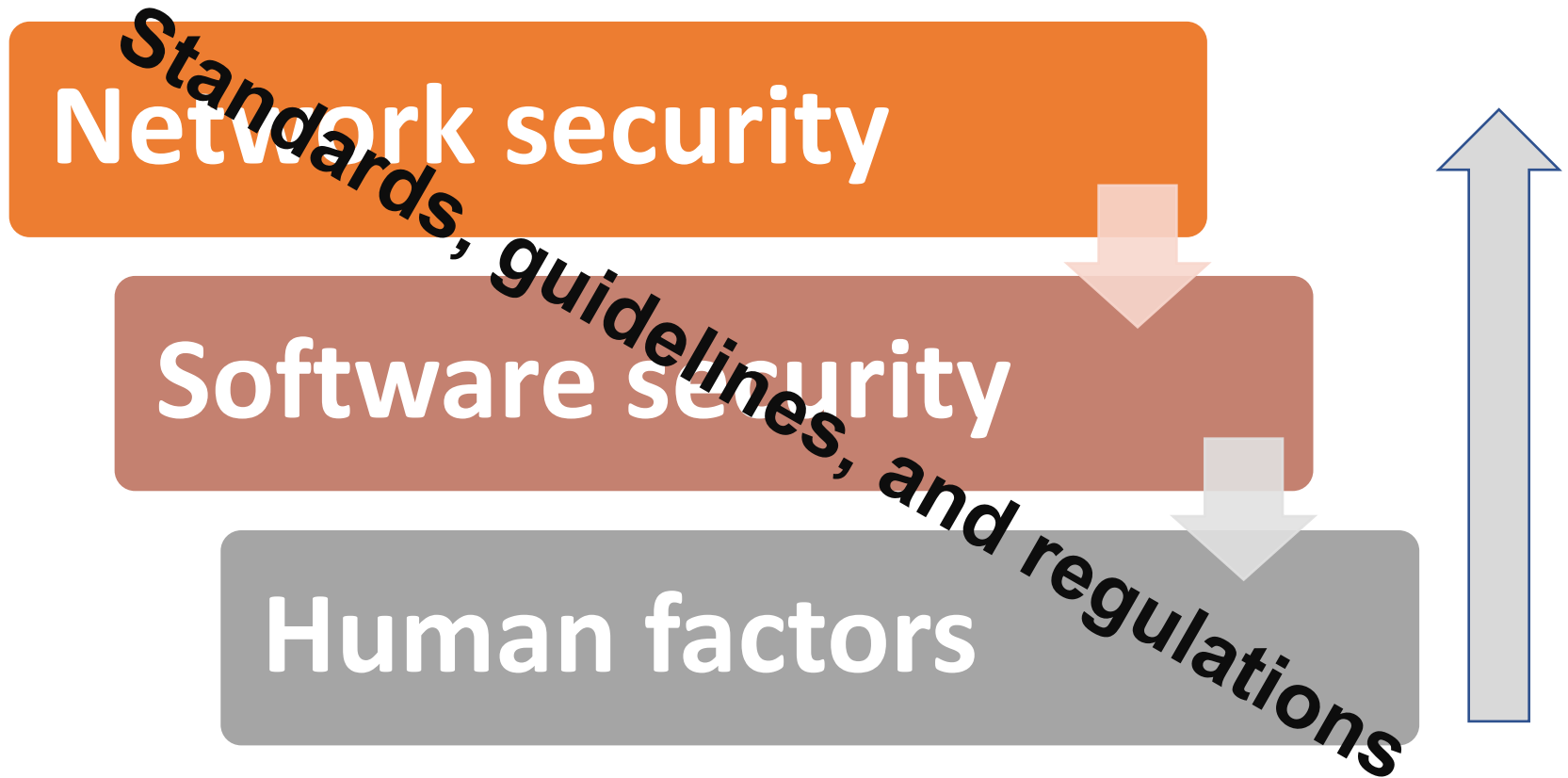


Outline

- Background to the problem
- Discuss cyber security design approaches to be employed.



Approaches





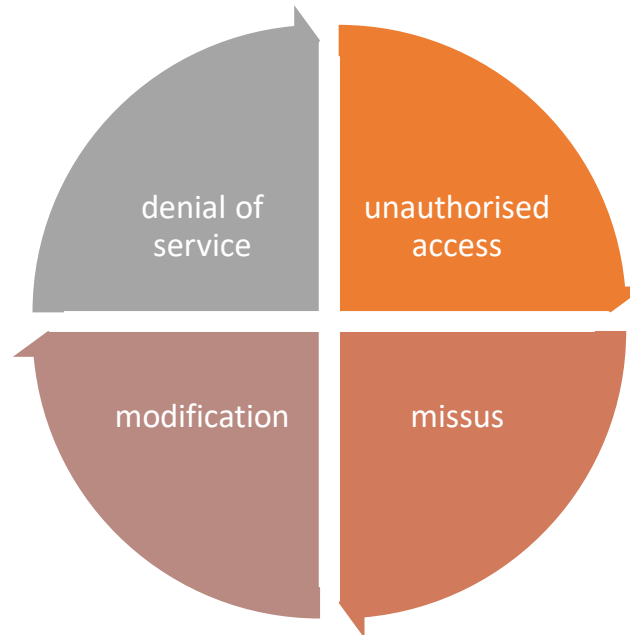
Approaches

Network security



Network security

- Network security - focuses on networked-resources

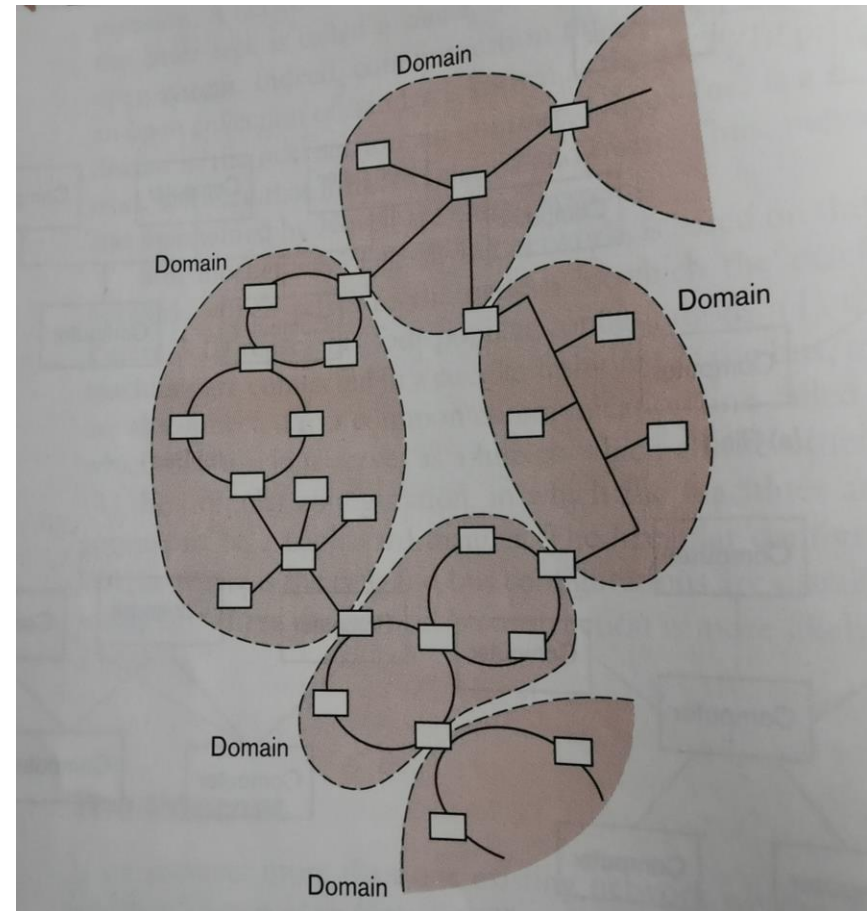


- Overall objective is to stop threats from spreading over networks



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

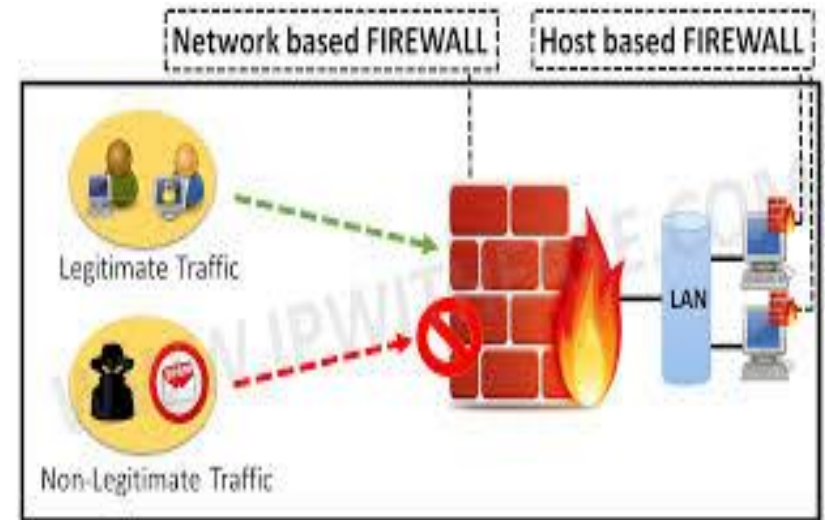




Network security

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.



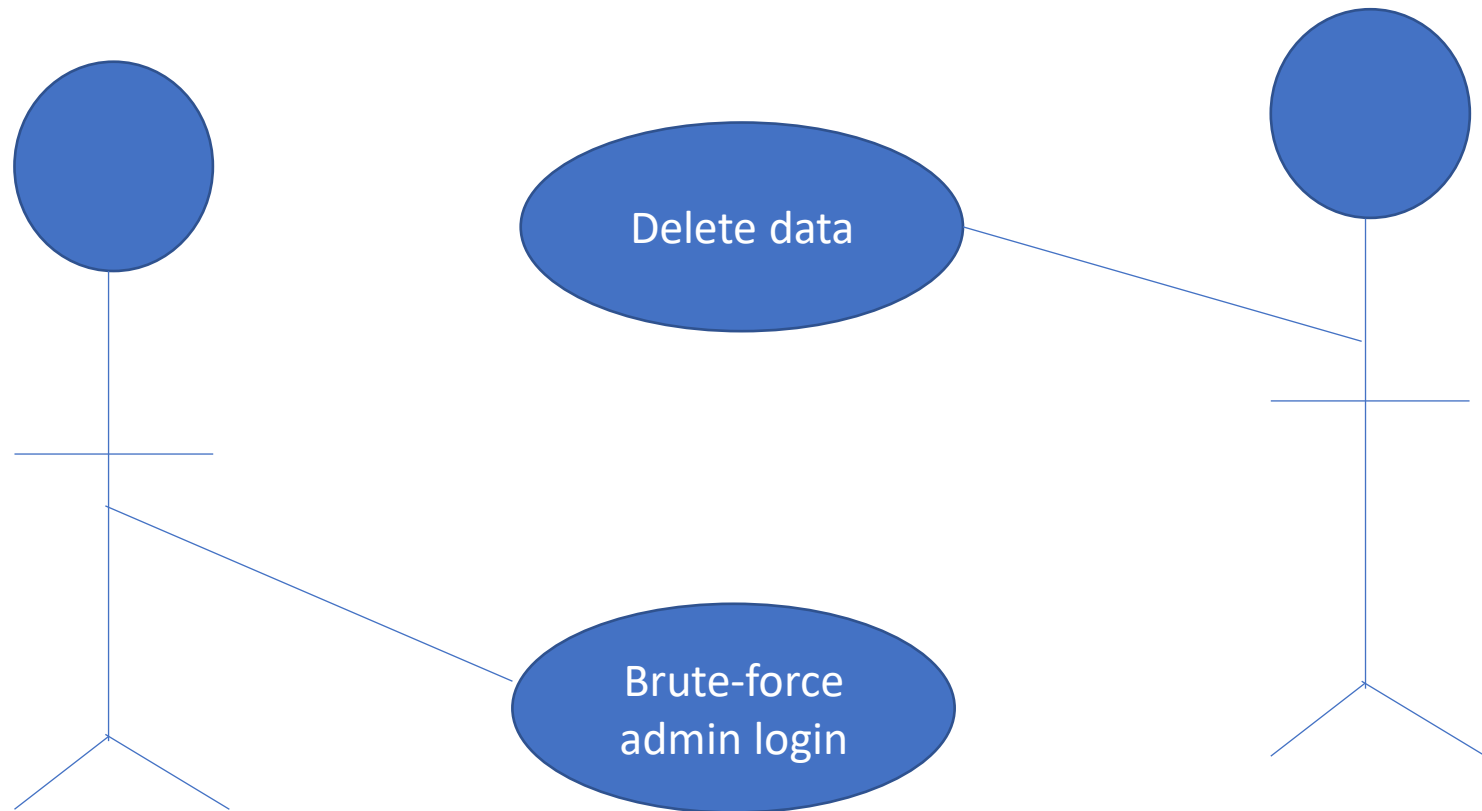
Software security

Some threat modelling techniques

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

Software security

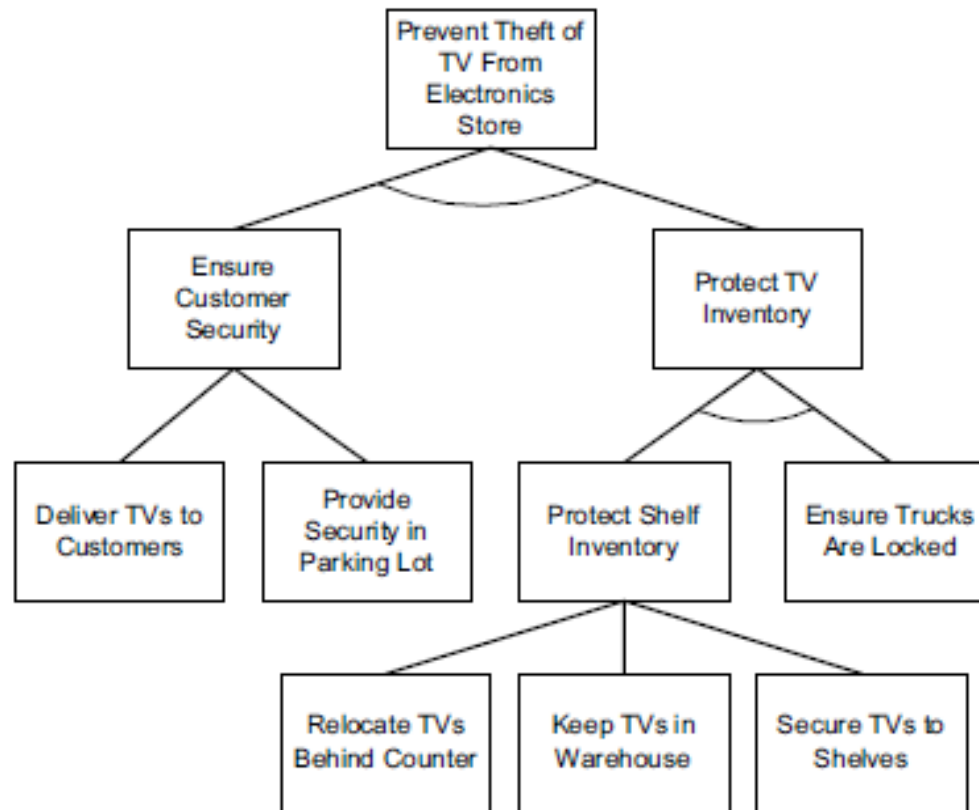
Abuse Case



Cyber criminal

Malicious staff

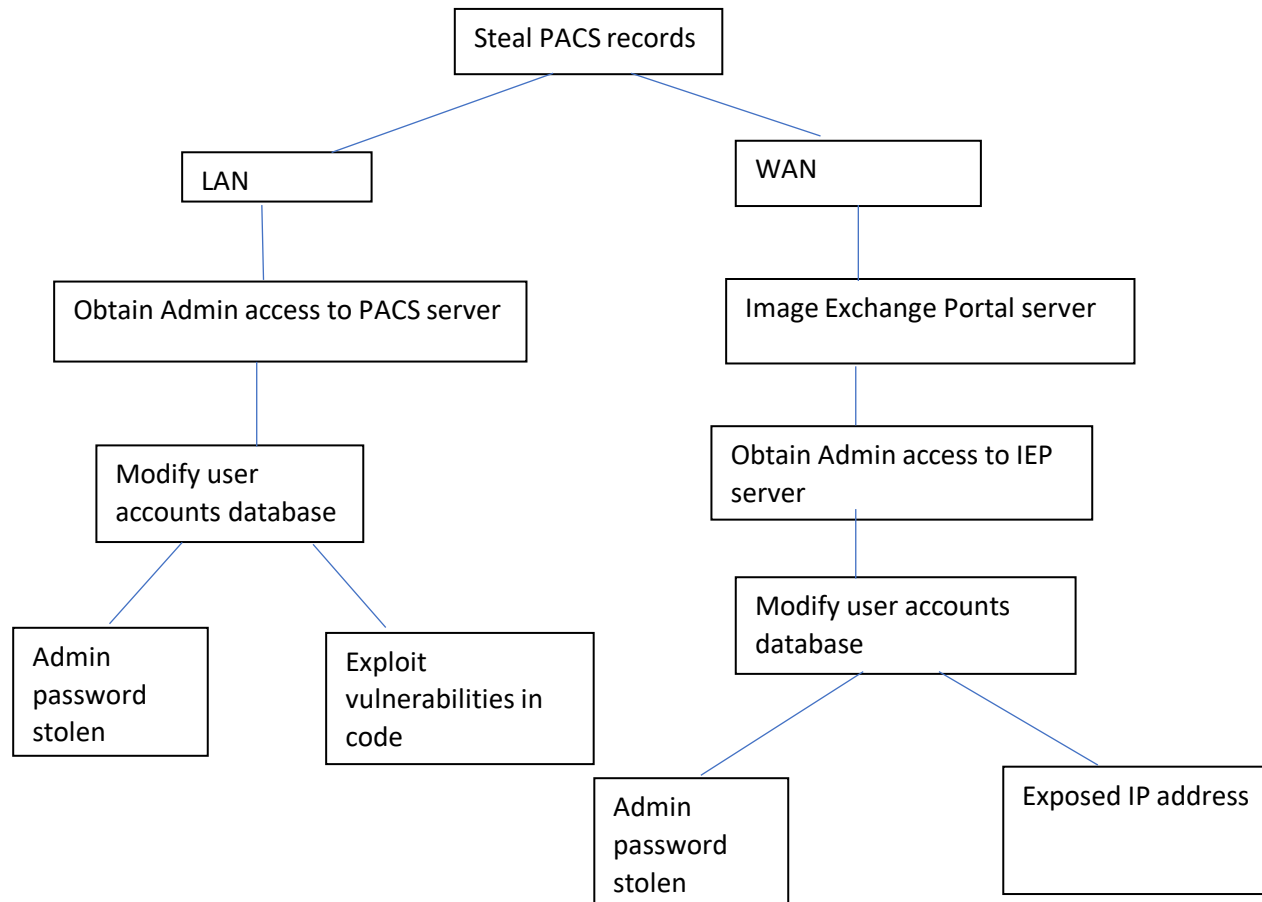
Software security



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

Iampering ...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

IMPACT				
	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		LIKELIHOOD		



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.



Additional resource

Special thanks to Doug Leece.

The screenshot shows the Amenaza Technologies Limited website. The header includes the Amenaza logo, the tagline 'Attack Tree Modeling ... think like an attacker!', and the SecurITree logo. A navigation bar contains links for Home, About Amenaza, SecurITree, Downloads, Support, and Contact Us. A sidebar on the left lists various topics under 'Home', 'Attack Trees', 'SecurITree', 'Threat Risk Analysis', and 'Downloads'. The main content area is titled 'Amenaza Videos' and lists two videos: 'Risky Times or Time for Risk?' and 'Fundamentals of Attack Tree Analysis'. A 'Back to Home' link is also present.

Amenaza TECHNOLOGIES LIMITED

Attack Tree Modeling
... think like an attacker!

SecurITree

Home | About Amenaza | SecurITree | Downloads | Support | Contact Us

Home
About Amenaza
Company Info
Attack Trees
What are Attack Trees?
Attack Tree Origins
Why Do I Need Specialized Software to Use Attack Trees?
SecurITree
What is SecurITree?
Who uses SecurITree?
Attack Tree Analysis Software
The SecurITree Advantage
SecurITree & Supply Chain Risks
SecurITree Screenshots
SecurITree Tutorial
How to Buy SecurITree
Sensitive Environments
Threat Risk Analysis
Capabilities-based Attack Tree Analysis
Attack Tree Analysis White Paper
Downloads
Software Trial

Amenaza Videos

- [Risky Times or Time for Risk?](#) (Keynote address at the 2021 ICI2ST conference)
- [Fundamentals of Attack Tree Analysis](#) (113 minute, four part presentation)

[Back to Home](#)

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



Exercise

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