Software Engineering

Lesson #11 - Lecture

Lesson #11 - Lecture

Your KBTU 202309 Software Engineering class information is updating …

Lesson #11 update is in progress

This will take around 2 hours to complete

Please, don’t turn off your computer

System Dependability and Security

Part #02

Part 2. System Dependability and Security

```
#include<iostream>
Using namespace std;

int main()
{
    cout << “Security engineering” << endl;

    return 0;
}
```

Part 2: Dependable systems

Agenda: Lesson #11 - Software Engineering - Lecture

Security engineering

1. Security and dependability
2. Security and organizations
3. Security requirements
4. Secure systems design
5. Security testing and assurance

Agenda: Lesson #11 - Software Engineering - Lecture

Resilience engineering

1 Cybersecurity

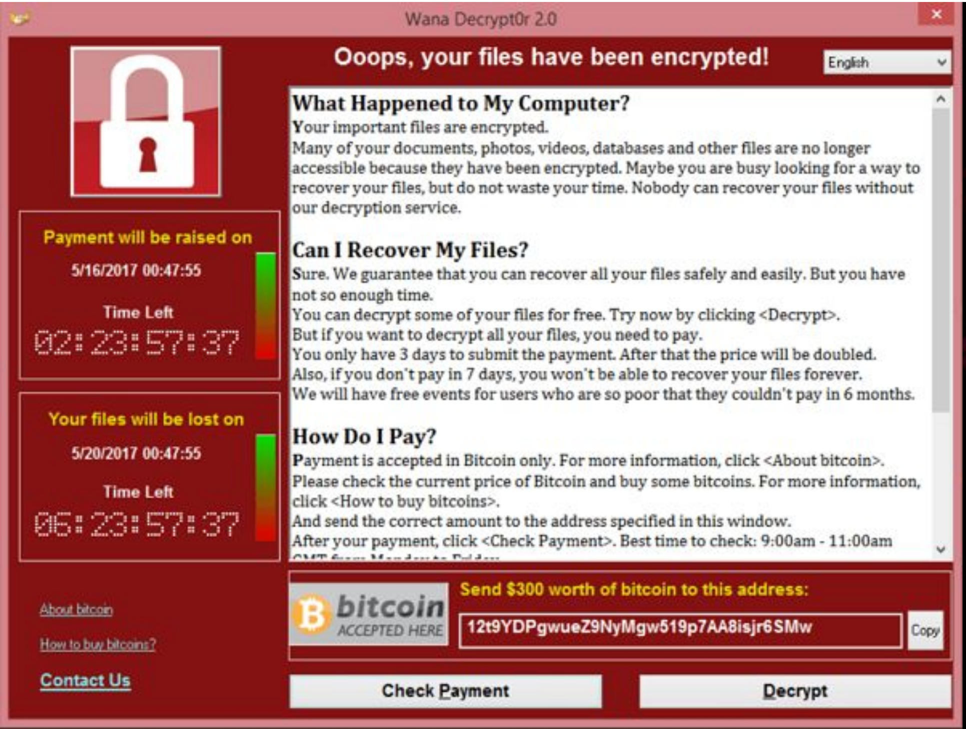
2 Socio-technical resilience

3 Resilient systems design

4 Q & A

Agenda: Lesson #11 - Software Engineering - Lecture

Security engineering



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Security engineering

Tools, techniques and methods to support the development and maintenance of systems that can resist malicious attacks that are intended to damage a computer-based system or its data

A sub-field of the broader field of computer security

Security dimensions

Confidentiality

Information in a system may be disclosed or made accessible to people or programs that are not authorized to have access to that information

CONFIDENTIAL

Security dimensions

Integrity

Information in a system may be damaged or corrupted making it unusual or unreliable

Availability

Access to a system or its data that is normally available may not be possible

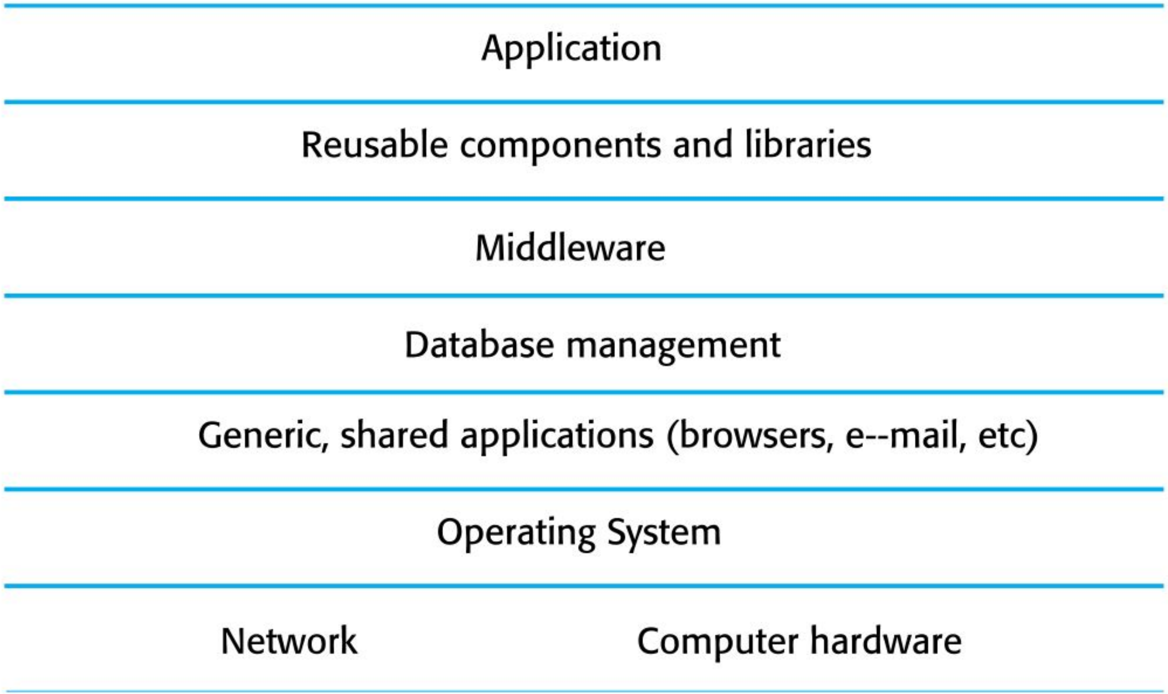
Security levels

Infrastructure security, which is concerned with maintaining the security of all systems and networks that provide an infrastructure and a set of shared services to the organization

Application security, which is concerned with the security of individual application systems or related groups of systems

Operational security, which is concerned with the secure operation and use of the organization’s systems

System layers where security may be compromised



Application

Reusable components and libraries

Middleware

Database management

Generic, shared applications (browsers, e--mail, etc)

Operating System

Network

Computer hardware

Application/infrastructure security

Application security is a software engineering problem where the system is designed to resist attacks

Infrastructure security is a systems management problem where the infrastructure is configured to resist attacks

The focus of this chapter is application security rather than infrastructure security

System security management

User and permission management

Adding and removing users from the system and setting up appropriate permissions for users

Software deployment and maintenance

Installing application software and middleware and configuring these systems so that vulnerabilities are avoided

System security management

Attack monitoring, detection and recovery

Monitoring the system for unauthorized access, design strategies for resisting attacks and develop backup and recovery strategies

data-ga-
#pricing
g-2 m-0"_da
ons Anu

Operational security

Primarily a human and social issue

Concerned with ensuring the people do not take actions that may compromise system security

- E.g. Tell others passwords, leave computers logged on

Operational security

Users sometimes take insecure actions to make it easier for them to do their jobs

There is therefore a trade-off between system security and system effectiveness

Security engineering

Security is a sociotechnical issue

https://www.youtube.com/watch?v=8bLwJy2BwKs

Security engineering

Security engineering

https://www.youtube.com/watch?v=F3smMClEodc

Agenda: Lesson #11 - Software Engineering - Lecture

Security engineering

1. **Security and dependability**
2. Security and organizations
3. Security requirements
4. Secure systems design
5. Security testing and assurance

Security

The security of a system is a system property that reflects the system’s ability to protect itself from accidental or deliberate external attack

Security is essential as most systems are networked so that external access to the system through the Internet is possible

Security is an essential prerequisite for availability, reliability and safety

Fundamental security

If a system is a networked system and is insecure then statements about its reliability and its safety are unreliable

These statements depend on the executing system and the developed system being the same. However, intrusion can change the executing system and/or its data

Therefore, the reliability and safety assurance is no longer valid

Security and dependability

Security and dependability

Security and reliability

If a system is attacked and the system or its data are corrupted as a consequence of that attack, then this may induce system failures that compromise the reliability of the system

Security and dependability

Security and availability

A common attack on a web-based system is a denial of service attack, where a web server is flooded with service requests from a range of different sources. The aim of this attack is to make the system unavailable

Security and dependability

Security and safety

An attack that corrupts the system or its data means that assumptions about safety may not hold. Safety checks rely on analysing the source code of safety critical software and assume the executing code is a completely accurate translation of that source code. If this is not the case, safety-related failures may be induced and the safety case made for the software is invalid.

Security and dependability

Security and resilience

Resilience is a system characteristic that reflects its ability to resist and recover from damaging events. The most probable damaging event on networked software systems is a cyberattack of some kind so most of the work now done in resilience is aimed at deterring, detecting and recovering from such attacks.

Agenda: Lesson #11 - Software Engineering - Lecture

Security engineering

1 Security and dependability

2 Security and organizations

3 Security requirements

4 Secure systems design

5 Security testing and assurance

Security is a business issue

Security is expensive and it is important that security decisions are made in a cost-effective way

- There is no point in spending more than the value of an asset to keep that asset secure

Organizations use a risk-based approach to support security decision making and should have a defined security policy based on security risk analysis

Security risk analysis is a business rather than a technical process

Organizational security policies

Security policies should set out general information access strategies that should apply across the organization

The point of security policies is to inform everyone in an organization about security so these should not be long and detailed technical documents

Organizational security policies

From a security engineering perspective, the security policy defines, in broad terms, the security goals of the organization

The security engineering process is concerned with implementing these goals

Security policies

The assets that must be protected

It is not cost-effective to apply stringent security procedures to all organizational assets. Many assets are not confidential and can be made freely available

Security policies

The level of protection that is required for different types of asset

For sensitive personal information, a high level of security is required; for other information, the consequences of loss may be minor so a lower level of security is adequate

Security policies

The responsibilities of individual users, managers and the organization

The security policy should set out what is expected of users e.g. strong passwords, log out of computers, office security, etc.

Security policies

Existing security procedures and technologies that should be maintained

For reasons of practicality and cost, it may be essential to continue to use existing approaches to security even where these have known limitations

Agenda: Lesson #11 - Software Engineering - Lecture

Security engineering

1. Security and dependability
2. Security and organizations
3. **Security requirements**
4. Secure systems design
5. Security testing and assurance

Security specification

Security specification has something in common with safety requirements specification – in both cases, your concern is to avoid something bad happening

Security specification

Four major differences

1. Safety problems are accidental – the software is not operating in a hostile environment. In security, you must assume that attackers have knowledge of system weaknesses

2. When safety failures occur, you can look for the root cause or weakness that led to the failure. When failure results from a deliberate attack, the attacker may conceal the cause of the failure

Security specification

Four major differences

3. Shutting down a system can avoid a safety-related failure. Causing a shut down may be the aim of an attack.

4. Safety-related events are not generated from an intelligent adversary. An attacker can probe defenses over time to discover weaknesses.

Types of security requirement

- Identification requirements
- Authentication requirements
- Authorisation requirements
- Immunity requirements
- Integrity requirements
- Intrusion detection requirements
- Non-repudiation requirements
- Privacy requirements
- Security auditing requirements
- System maintenance security requirements

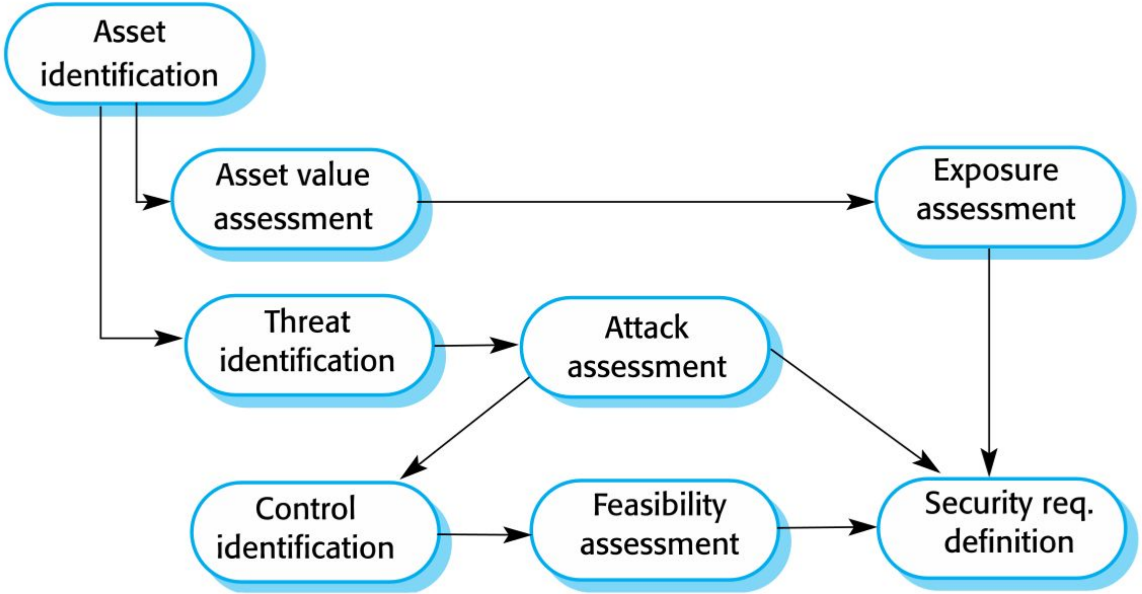
Security requirement classification

Risk avoidance requirements set out the risks that should be avoided by designing the system so that these risks simply cannot arise

Risk detection requirements define mechanisms that identify the risk if it arises and neutralise the risk before losses occur

Risk mitigation requirements set out how the system should be designed so that it can recover from and restore system assets after some loss has occurred

The preliminary risk assessment process for Security Requirements



Security engineering

1 Security and dependability

2 Security and organizations

3 Security requirements

4 **Secure systems design**

5 Security testing and assurance

Secure systems design

Security should be designed into a system – it is very difficult to make an insecure system secure after it has been designed or implemented

Architectural design

how do architectural design decisions affect the security of a system?

Good practice

what is accepted good practice when designing secure systems?

Design compromises

Adding security features to a system to enhance its security affects other attributes of the system

Performance

Additional security checks slow down a system so its response time or throughput may be affected

Design compromises

Adding security features to a system to enhance its security affects other attributes of the system

Usability

Security measures may require users to remember information or require additional interactions to complete a transaction. This makes the system less usable and can frustrate system users

Agenda: Lesson #11 - Software Engineering - Lecture

Security engineering

1 Security and dependability

2 Security and organizations

3 Security requirements

4 Secure systems design

5 Security testing and assurance

Security testing

Testing the extent to which the system can protect itself from external attacks

Security testing

Problems with security testing

Security requirements are ‘shall not’ requirements i.e. they specify what should not happen. It is not usually possible to define security requirements as simple constraints that can be checked by the system

The people attacking a system are intelligent and look for vulnerabilities. They can experiment to discover weaknesses and loopholes in the system

Security validation

Experience-based testing

The system is reviewed and analysed against the types of attack that are known to the validation team

Penetration testing

A team is established whose goal is to breach the security of the system by simulating attacks on the system

Security validation

Tool-based analysis

Various security tools such as password checkers are used to analyse the system in operation

Formal verification

The system is verified against a formal security specification

Part 2. System Dependability and Security

```
#include<iostream>
Using namespace std;

int main()
{
    cout << “Resilience engineering” << endl;

    return 0;
}
```

Agenda: Lesson #11 - Software Engineering - Lecture

Resilience engineering

1 Cybersecurity

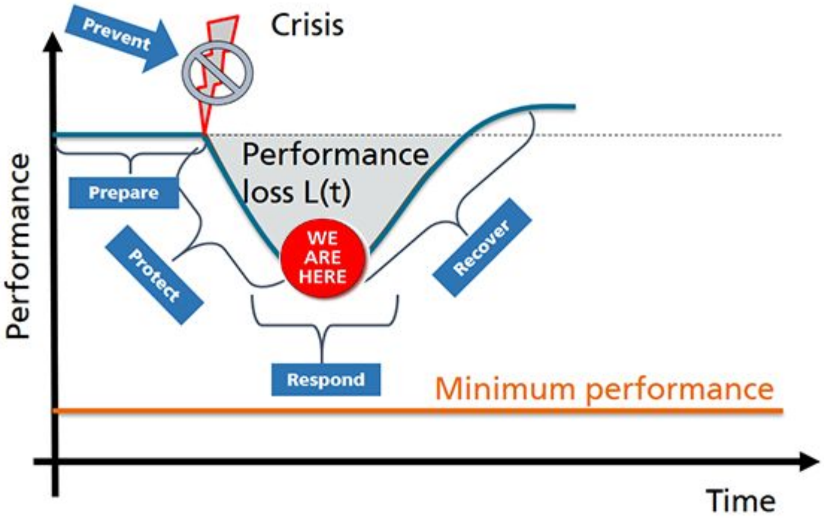
2 Socio-technical resilience

3 Resilient systems design

4 Q & A

Agenda: Lesson #11 - Software Engineering - Lecture

Resilience engineering



Resilience engineering

Resilience engineering

Infrastructure resilience

https://www.youtube.com/watch?v=z7Cwtpmj_VY

Resilience engineering

Resilience Engineering

https://www.youtube.com/watch?v=tfrneYXEgkY&t=13s

Resilience

The resilience of a system is a judgment of how well that system can maintain the continuity of its critical services in the presence of disruptive events, such as equipment failure and cyberattacks

Cyber Attacks by malicious outsiders are perhaps the most serious threat faced by networked systems but resilience is also intended to cope with system failures and other disruptive events

Essential resilience ideas

The idea that some of the services offered by a system are critical services whose failure could have serious human, social or economic effects

The idea that some events are disruptive and can affect the ability of a system to deliver its critical services

Essential resilience ideas

The idea that resilience is a judgment – there are no resilience metrics and resilience cannot be measured. The resilience of a system can only be assessed by experts, who can examine the system and its operational processes

Resilience engineering assumptions

Resilience engineering assumes that it is impossible to avoid system failures and so is concerned with limiting the costs of these failures and recovering from them

Resilience engineering assumes that good reliability engineering practices have been used to minimize the number of technical faults in a system

Resilience engineering assumptions

It therefore places more emphasis on limiting the number of system failures that arise from external events such as operator errors or cyberattacks

Resilience activities

Recognition

The system or its operators should recognise early indications of system failure

Resistance

If the symptoms of a problem or cyberattack are detected early, then resistance strategies may be used to reduce the probability that the system will fail

Resilience activities

Recovery

If a failure occurs, the recovery activity ensures that critical system services are restored quickly so that system users are not badly affected by failure

Reinstatement

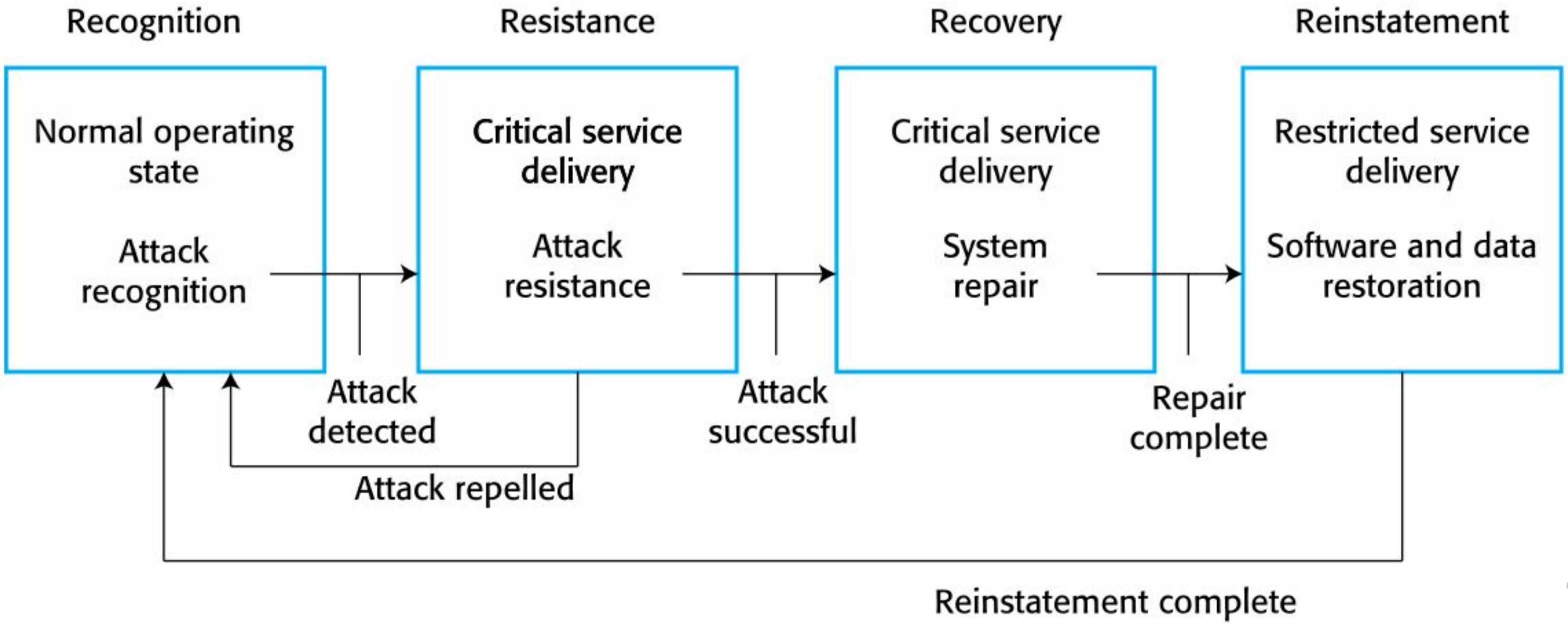
In this final activity, all of the system services are restored and normal system operation can continue

Resistance

Resistance strategies may focus on isolating critical parts of the system so that they are unaffected by problems elsewhere

Resistance includes proactive resistance where defences are included in a system to trap problems and reactive resistance where actions are taken when a problem is discovered

Resilience activities



Resilience engineering

Cyber attacks

https://www.youtube.com/watch?v=zTiOoojSqO4

Resilience engineering

System security

https://www.youtube.com/watch?v=GTxPzKfriOU

Agenda: Lesson #11 - Software Engineering - Lecture

Resilience engineering

1 **Cybersecurity**

2 Socio-technical resilience

3 Resilient systems design

4 Q & A

Cybersecurity

An introduction to cybersecurity

https://www.youtube.com/watch?v=YPxlwsxEW48

Cybersecurity

Cybercrime is the illegal use of networked systems and is one of the most serious problems facing our society

Cybersecurity

Cybersecurity is a broader topic than system security engineering

- Cybersecurity is a sociotechnical issue covering all aspects of ensuring the protection of citizens, businesses and critical infrastructures from threats that arise from their use of computers and the Internet

Cybersecurity is concerned with all of an organization's IT assets from networks through to application systems

Factors contributing to C. S. failure

- organizational ignorance of the seriousness of the problem
- poor design and lax application of security procedures
- human carelessness
- inappropriate trade-offs between usability and security

Cybersecurity

Improving cybersecurity

https://www.youtube.com/watch?v=lIKqqMJ_hYY

Agenda: Lesson #11 - Software Engineering - Lecture

Resilience engineering

1 Cybersecurity

2 Socio - technical resilience

3 Resilient systems design

4 Q & A

Socio - technical resilience

Resilience engineering is concerned with adverse external events that can lead to system failure

To design a resilient system, you have to think about sociotechnical systems design and not exclusively focus on software

Dealing with these events is often easier and more effective in the broader socio-technical system

Organizational resilience

There are four characteristics that reflect the resilience of an organization

Responsiveness
Monitoring
Anticipation
Learning

Socio-technical resilience

Organizational resilience

The ability to respond

Organizations have to be able to adapt their processes and procedures in response to risks. These risks may be anticipated risks or may be detected threats to the organization and its systems

Organizational resilience

The ability to monitor

Organizations should monitor both their internal operations and their external environment for threats before they arise

Organizational resilience

The ability to anticipate

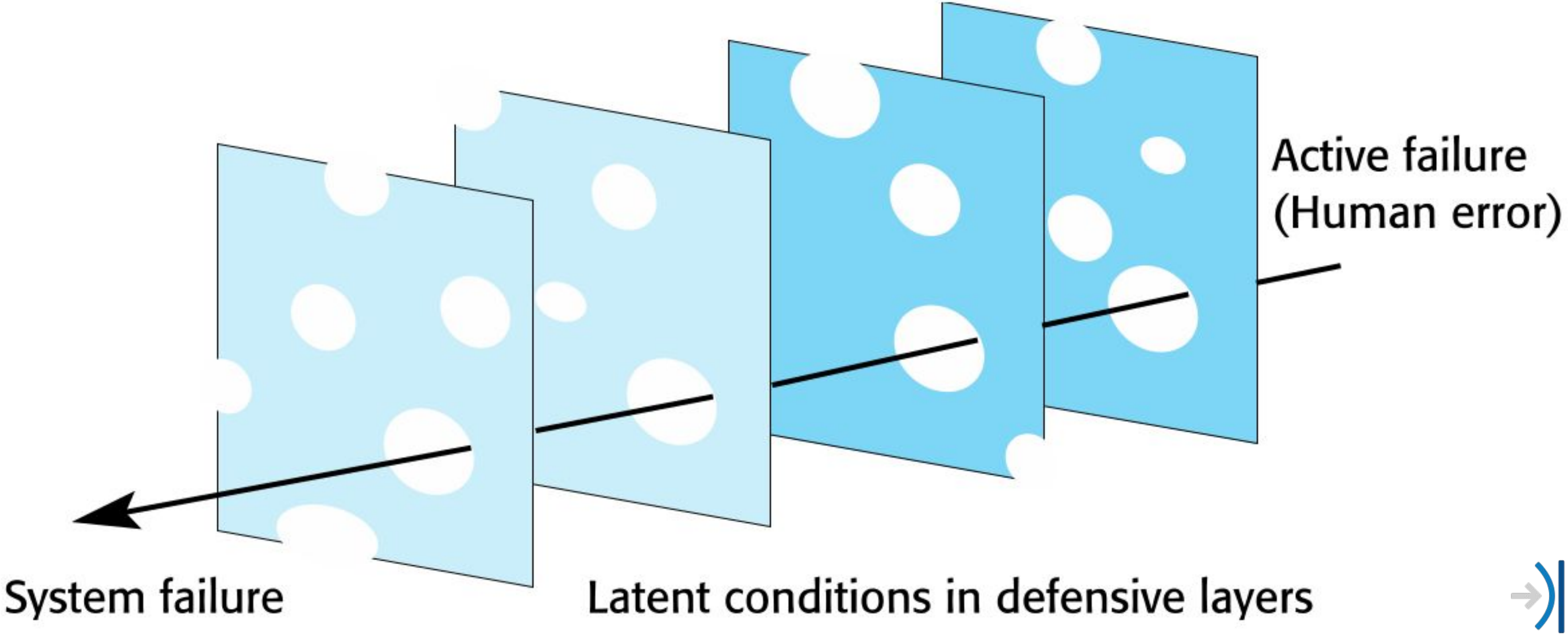
A resilient organization should not simply focus on its current operations but should anticipate possible future events and changes that may affect its operations and resilience

Organizational resilience

The ability to learn

Organizational resilience can be improved by learning from experience. It is particularly important to learn from successful responses to adverse events such as the effective resistance of a cyberattack. Learning from success allows

Reason’s Swiss Cheese Model



Swiss Cheese model

Defensive layers have vulnerabilities

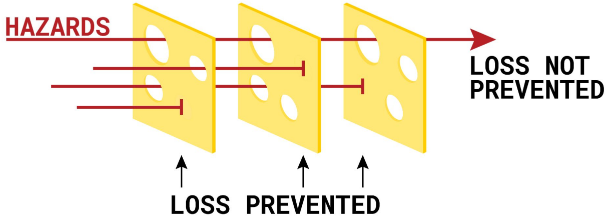
They are like slices of Swiss cheese with holes in the layer corresponding to these vulnerabilities

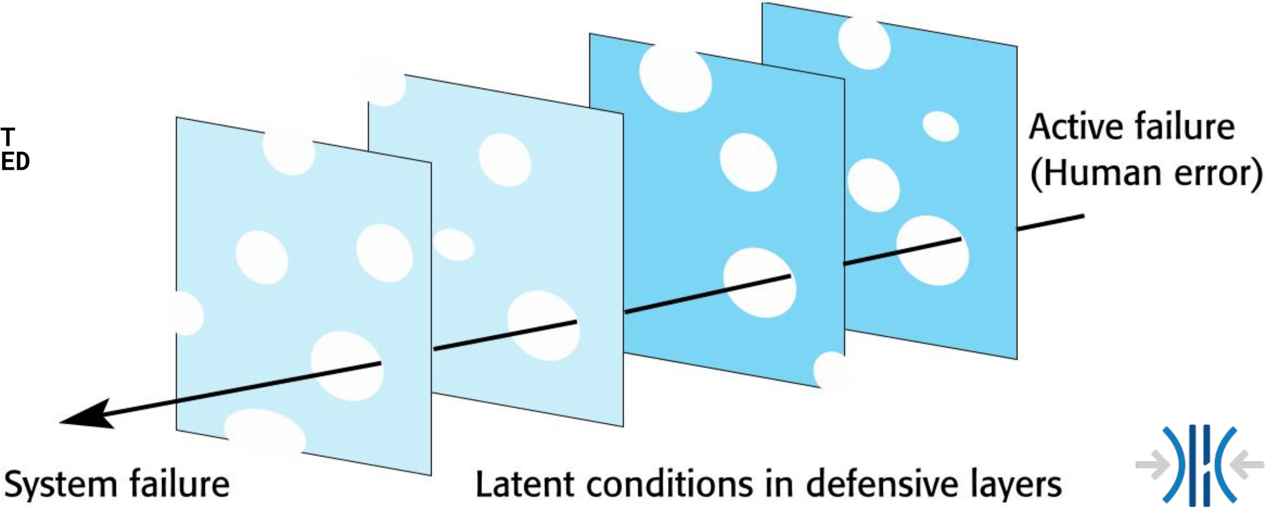
Vulnerabilities are dynamic

The ‘holes’ are not always in the same place and the size of the holes may vary depending on the operating conditions

Swiss Cheese model

System failures occur when the holes line up and all of the defenses fail





Socio-technical resilience

Security is a sociotechnical issue

https://www.youtube.com/watch?v=8bLwJy2BwKs

Agenda: Lesson #11 - Software Engineering - Lecture

Resilience engineering

1 Cybersecurity

2 Socio-technical resilience

3 Resilient systems design

4 Q & A

Resilient systems design

Identifying critical services and assets

Critical services and assets are those elements of the system that allow a system to fulfill its primary purpose. For example, the critical services in a system that handles ambulance dispatch are those concerned with taking calls and dispatching ambulances

Resilient systems design

Designing system components that support problem recognition, resistance, recovery and reinstatement

For example, in an ambulance dispatch system, a watchdog timer may be included to detect if the system is not responding to events

Survivable systems analysis

System understanding

For an existing or proposed system, review the goals of the system (sometimes called the mission objectives), the system requirements and the system architecture

Critical service identification

The services that must always be maintained & components that are required to maintain these services are identified

Survivable systems analysis

Attack simulation

Scenarios or use cases for possible attacks are identified along with the system components that would be affected by these attacks

Survivable systems analysis

Survivability analysis

Components that are both essential and compromisable by an attack are identified and survivability strategies based on resistance, recognition and recovery are identified

Resilience engineering

Resilience Engineering 2

https://www.youtube.com/watch?v=YacGeQOotMo

Agenda: Lesson #11 - Software Engineering - Lecture

Resilience engineering

1 Cybersecurity

2 Socio-technical resilience

3 Resilient systems design

4 **Q & A**

Agenda: Lesson #11 - Software Engineering - Lecture

Q & A