NTNU

Norwegian University of Science and Technology

THREAT MODELING

and STRIDE

TDT4237 2025 Per Håkon Meland

NTNU

Trump administration

US watchdog to investigate Musk 'Doge' team's access to payment systems

Treasury inspector general to launch audit as judge mulls whether access to sensitive data was unconstitutional

Robert Tait *in Washington*

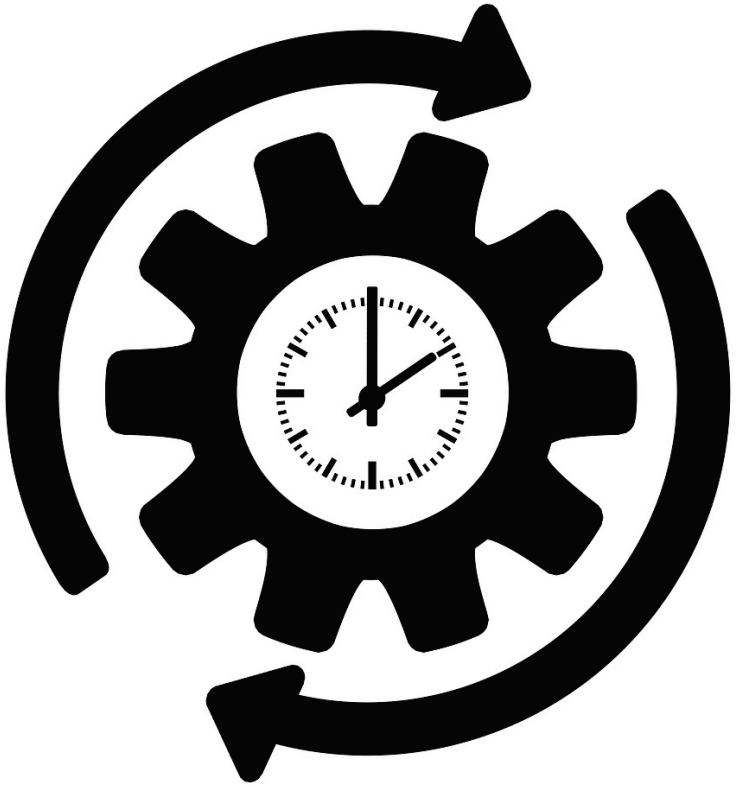
Fri 14 Feb 2025 22.03 CET

A man walks past the US treasury department in Washington. Photograph: Mandel Ngan/AFP/Getty Images

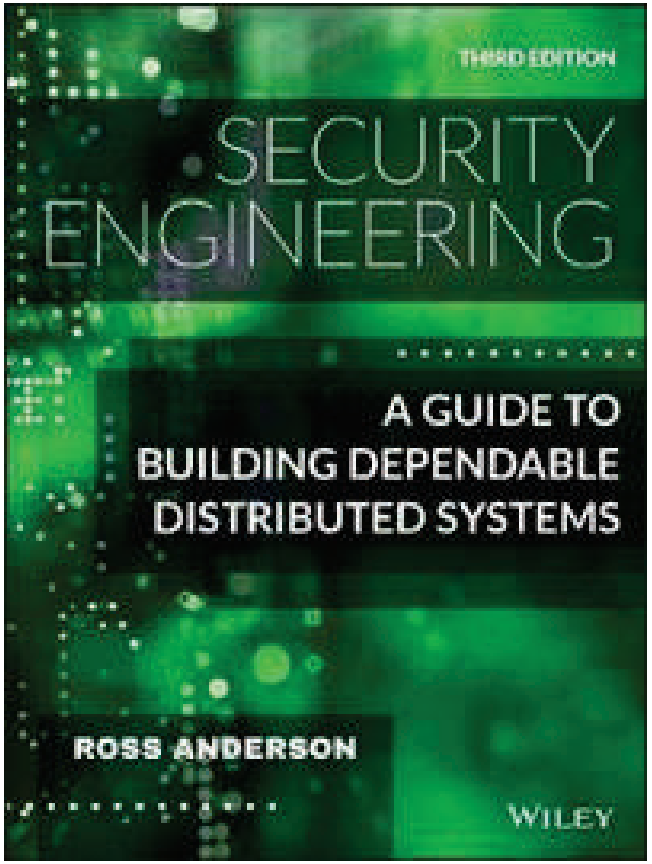
A government watchdog is to launch an inquiry into security over the US

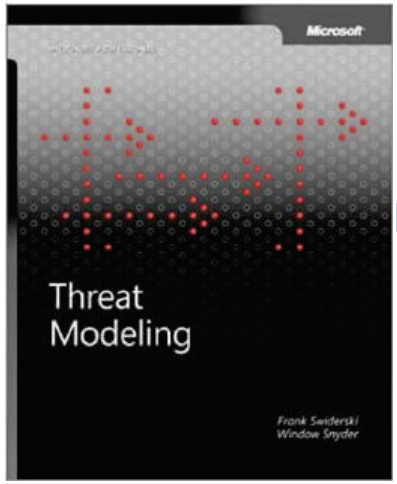
Agenda

- Introduction to threat modeling
  - What, why, when, how, who, …
  - STRIDE
- Notation examples
  - Misuse case
  - Attack tree
  - Bow-tie diagram
  - Data Flow Diagram

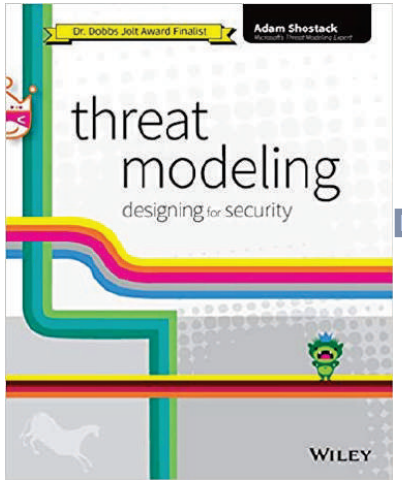


NTNU

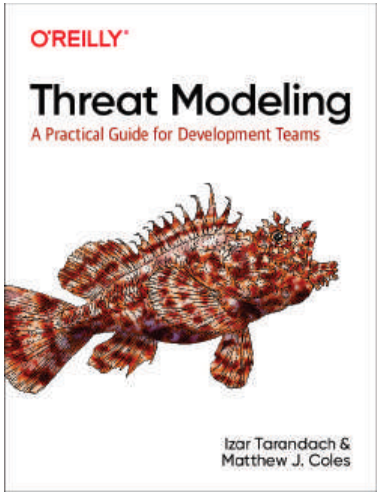




2004



2014



2020

NTNU

THREAT MODELING MANIFESTO

Values

Principles

- Patterns
- Anti-patterns

https://www.threatmodelingmanifesto.org/

NTNU

"If we had our hands tied behind our backs … and could do only one thing to improve software security … we would do threat modeling"

Michael Howard Steve Lipner

"*The Security Development Lifecycle*", Microsoft Press, 2006

What is threat modeling?

"A way of imagining the vast vulnerability landscape of a system and ways to attack it"

B. Schneier (2000): "Threat modeling and risk assessment"

"Threat modeling looks at a system from an adversary's perspective to anticipate attack goals"

Swiderski and Snyder (2004): "Threat modeling"

"… analyzing representations of a system to highlight concerns about security and privacy characteristics"

Threat modelling manifesto (2020)

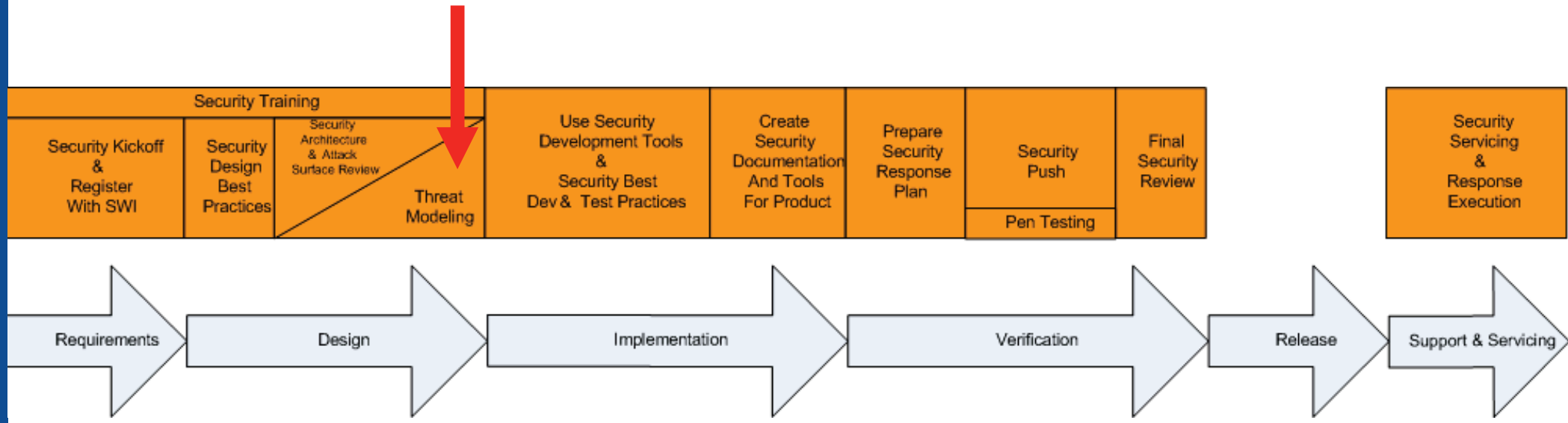
Why?

- Understand and document a system's threat environment
  - E.g. attack techniques, malicious actors, motivation, consequences
- Discover possible weaknesses as early as possible
  - E.g. missing requirements, exploitable interfaces in the design
- How to best spend your security budget
  - Mitigations and countermeasures, prioritize security requirements
- In retrospect
  - How was my system attacked?

NTNU

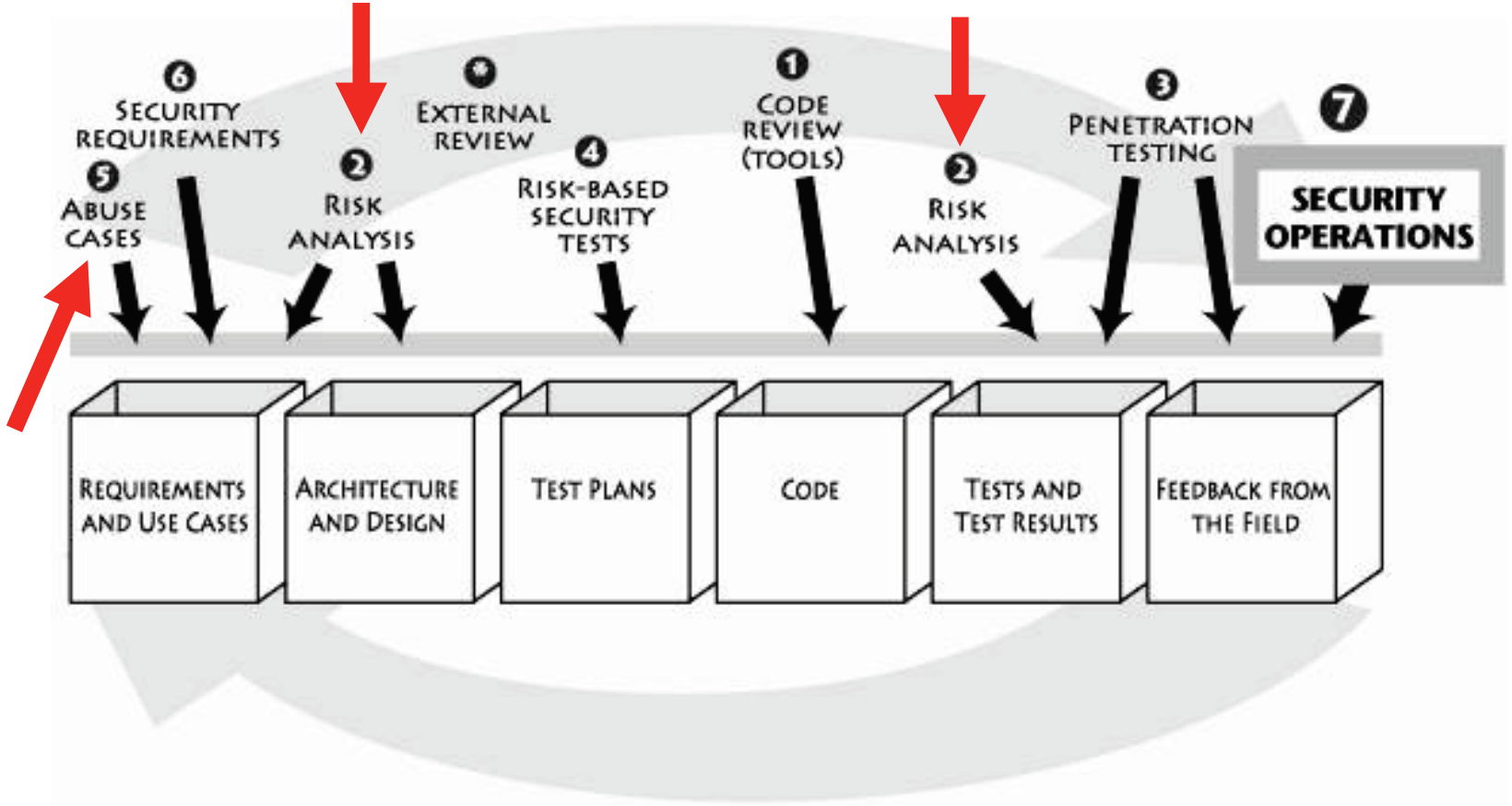
Principle: The outcomes of threat modeling are meaningful when they are of value to stakeholders

When?



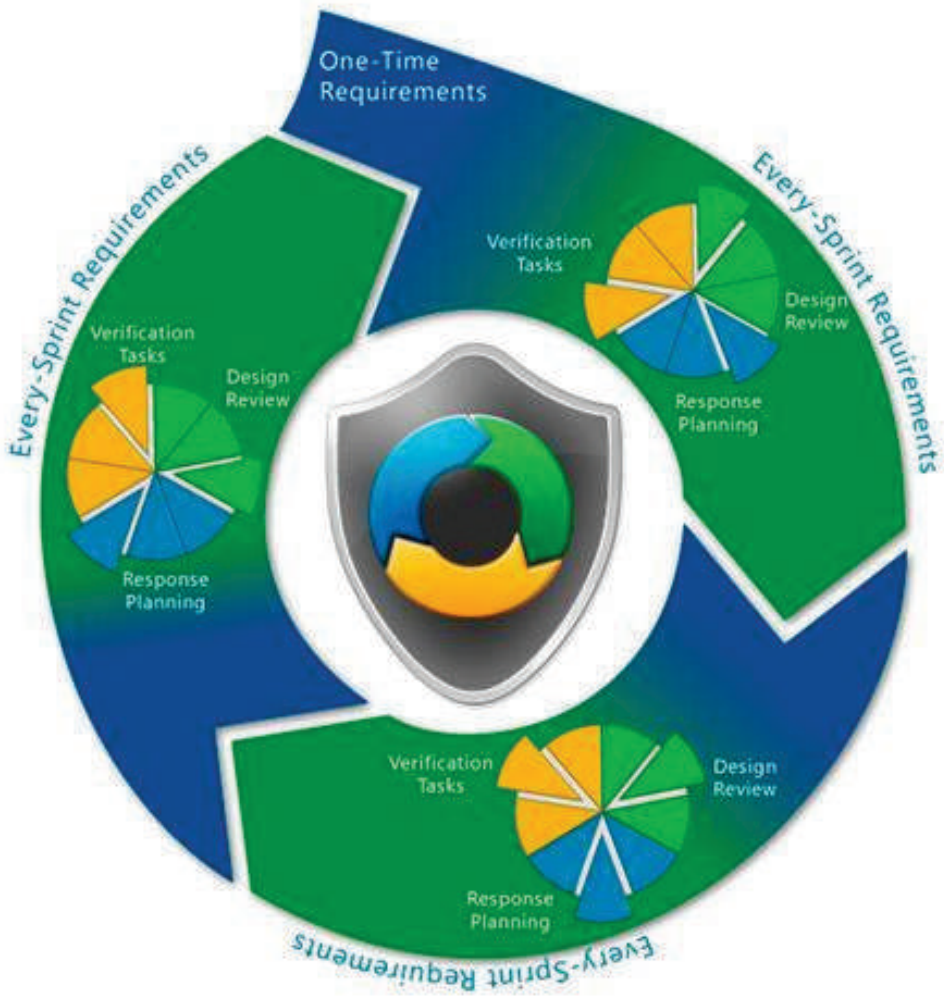
The Trustworthy Computing Security Development Lifecycle (Microsoft)
Source: http://msdn.microsoft.com/en-us/library/ms995349.aspx

Software Security Touchpoints (McGraw)



Source: http://swsec.com/resources/touchpoints/

Threat Modeling and Agile



- Project inception
  - High level threats
- Requirements planning
  - Threats with highest impact
- Sprint planning
  - Where are the threats?
- Sprint execution
  - Develop, update and complete
- Final release planning
  - Complete models

Source: Microsoft Technet (R.I.P.)

NTNU

Value: Continuous refinement over a single delivery

Principle: Early and frequent analysis

Principle: Must align with an organization's development practices

Who?

Credit: Ann de Wulf

Credit: Global Nerdy

NTNU

Value: People and collaboration over processes, methodologies, and tools

Principle: Dialog is key to establishing the common understandings that lead to value

Anti-pattern:
Hero Threat Modeller

Threat modeling does not depend on one's innate ability or unique mindset; everyone can and should do it.

Pattern: Varied Viewpoints

Assemble a diverse team with appropriate subject matter experts and cross-functional collaboration.

How?

*"there is **no single best or correct way** of performing threat modeling, it is a question of trade-offs and what we want to achieve by doing it"*

Source: A. Shostack, *"Experiences Threat Modeling at Microsoft,"* 2008.

Anti-pattern: Perfect representation

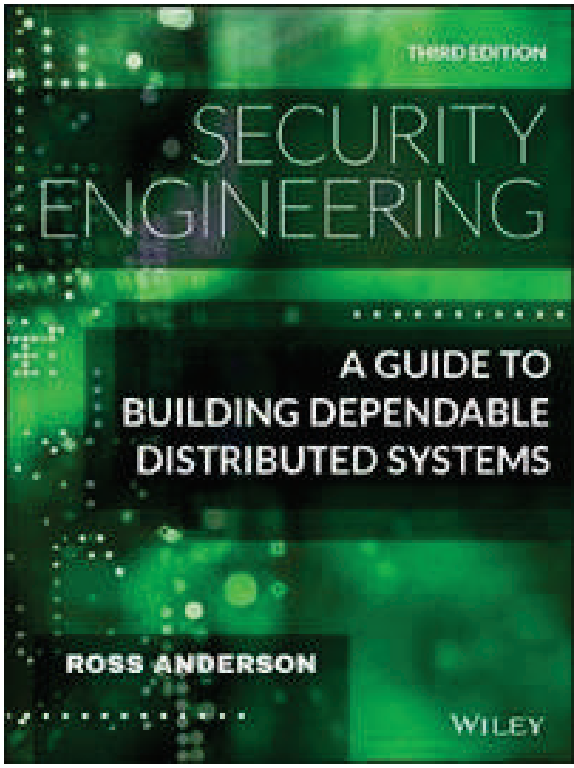
It is better to create multiple threat modeling representations because there is no single ideal view, and additional representations may illuminate different problems.

NTNU

Attacker-centric threat models

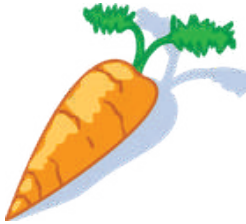
"One of the first things the security engineer needs to do when tackling a new problem is to identify the likely opponents"

"...what sort of capabilities will the adversaries have, and what motivation?"



Attributes of threat agents

Skillset



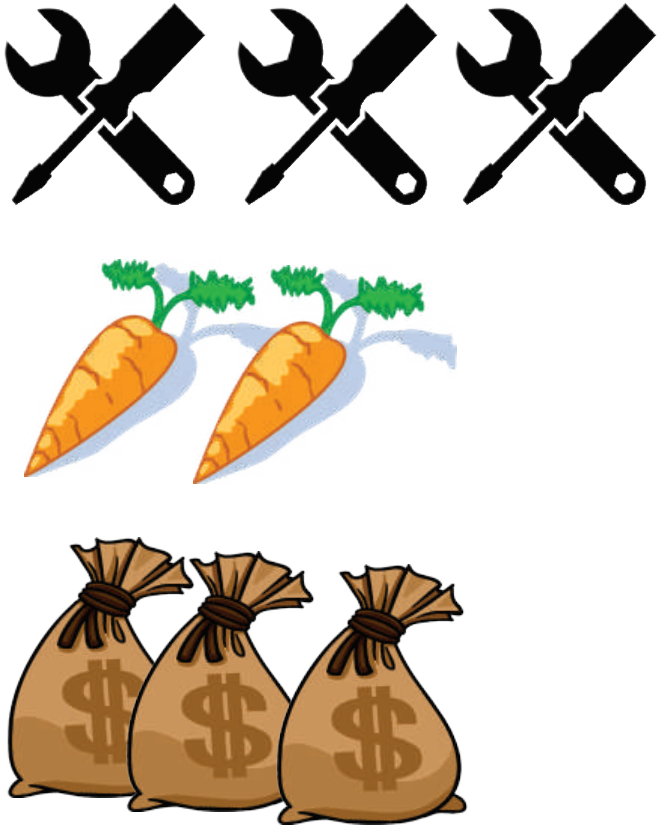
Motivation

Resources (costs)

NTNU

Threat agent: The Spooks

Threat agent: Goverment cyber warriors



NTNU

Nation State Actor

Volt Typhoon

Microsoft Security actively investigates and tracks threat actors in order to help protect customers, our platform and services from adversaries.

The actor that Microsoft tracks as Volt Typhoon is a nation-state activity group based out of China. Volt Typhoon is known to primarily target the United States and the manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors. Volt Typhoon focuses on espionage, data theft, and credential access.

Learn more

Also known as:

- VANGUARD PANDA, BRONZE SILHOUETTE

Country of origin:

China

Countries targeted:

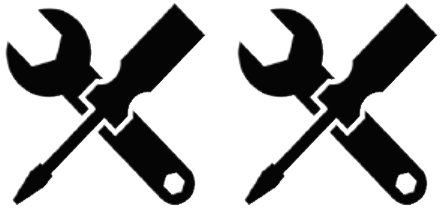
United States and Guam

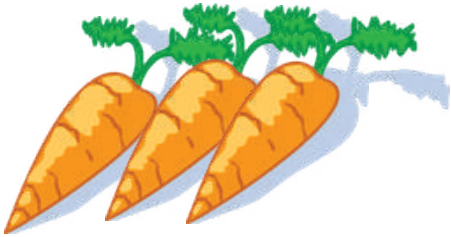
Industries targeted:

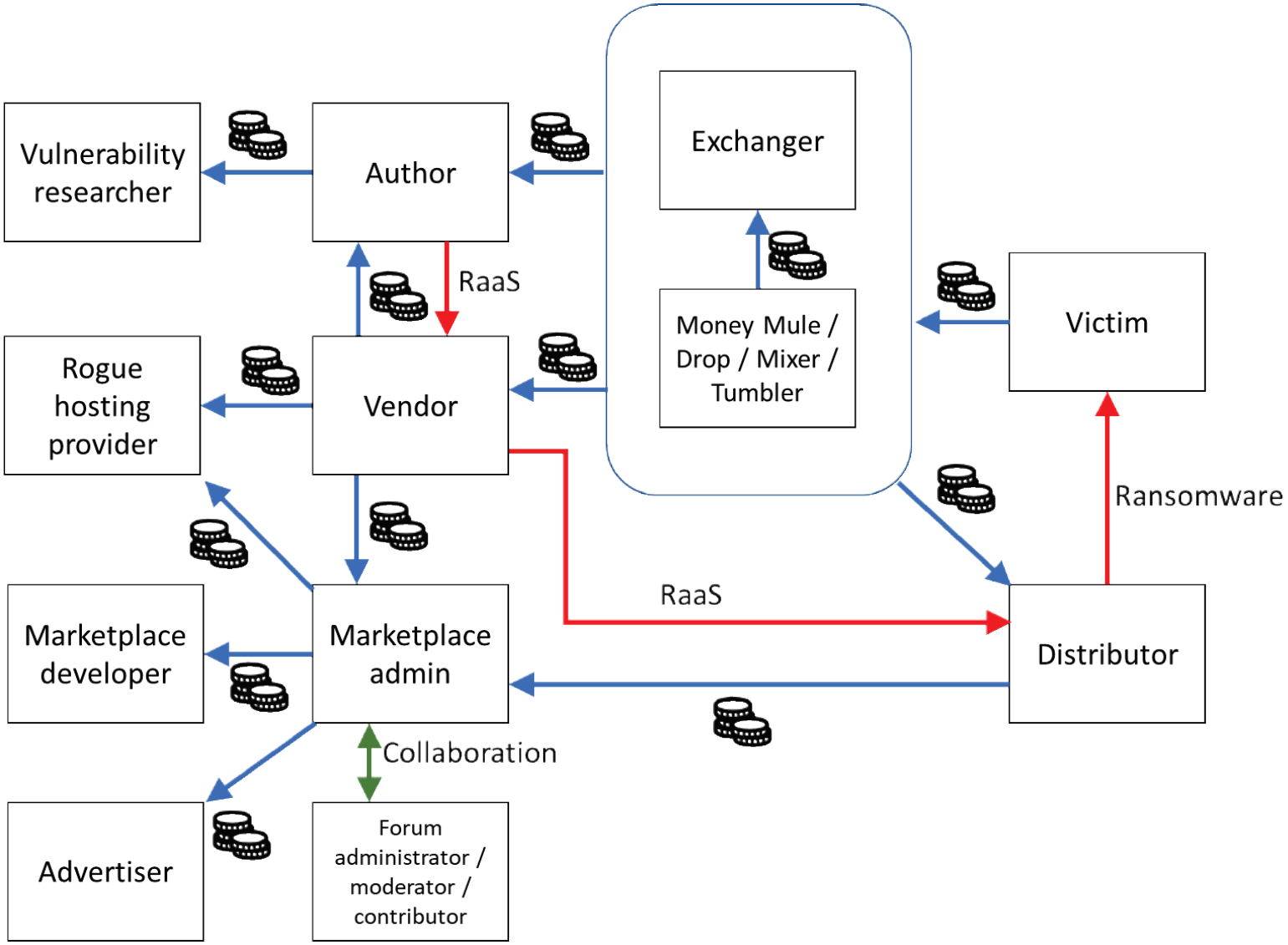
- Communications Infrastructure
- Manufacturing
- Media
- Defense
- Education
- Utilities
- Software and Technology
- Transportation
- Construction
- Government

Microsoft Security

Threat agent: The Crooks

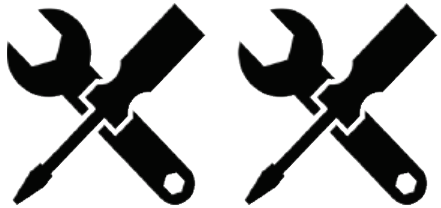






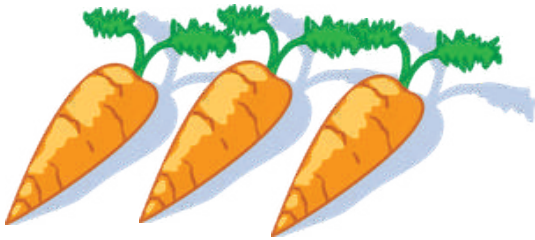
Source: Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*, *92*, 101762.

Threat agent: The Geeks



NTNU

Threat agent: The Terrorists



Threat agent: CEO Criminals

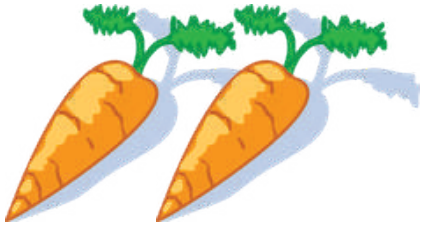
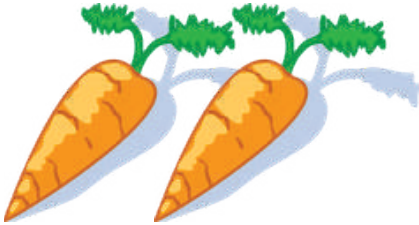


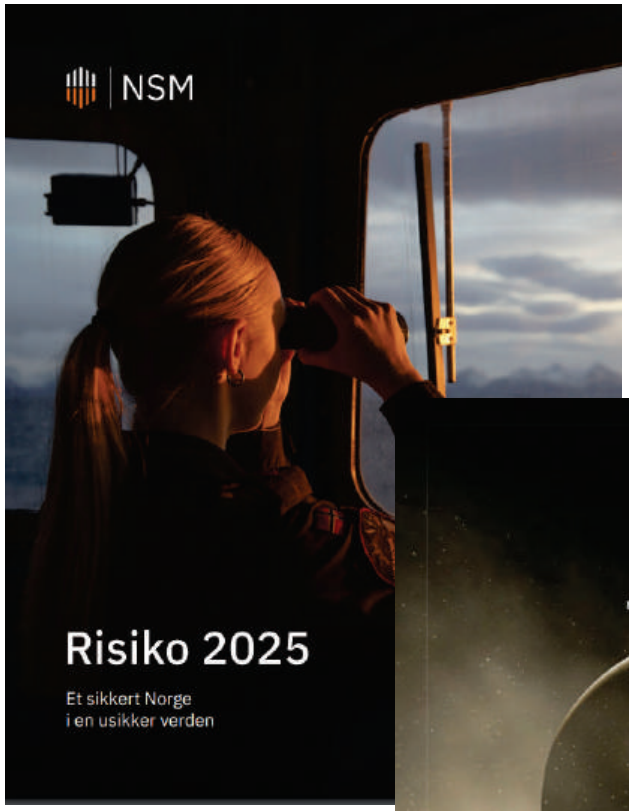
Photo from: http://andreschacin.me/Logo-competition/

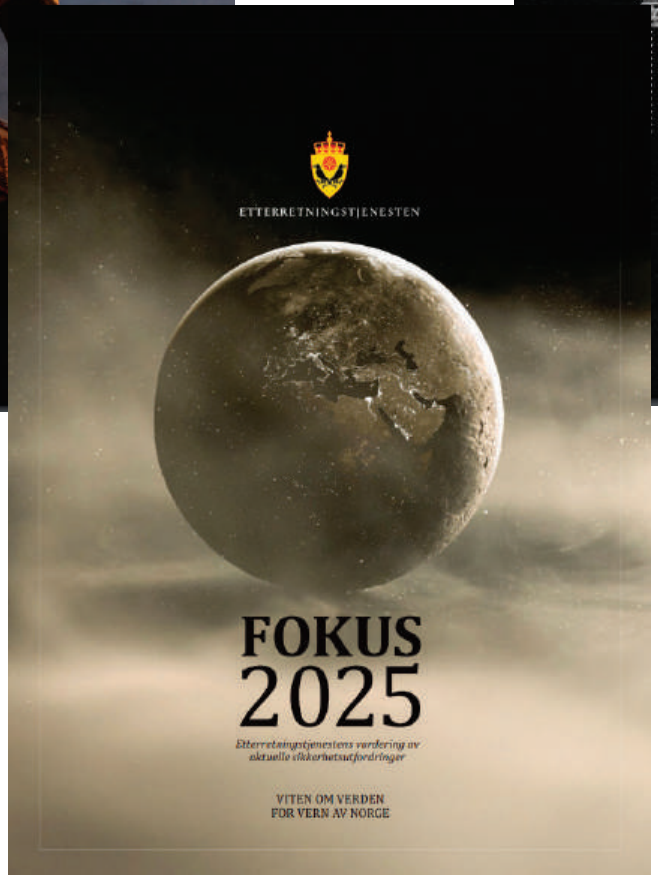
Threat agent: The Swamp



Threat agent: The Insiders

NTNU


NSM
Risiko 2025
Et sikkert Norge
i en usikker verden


ETTERRETNINGSTJENESTEN
FOKUS
2025
Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer
VITEN OM VERDEN
FOR VERN AV NORGE


PST
Nasjonal trusselvurdering
2025

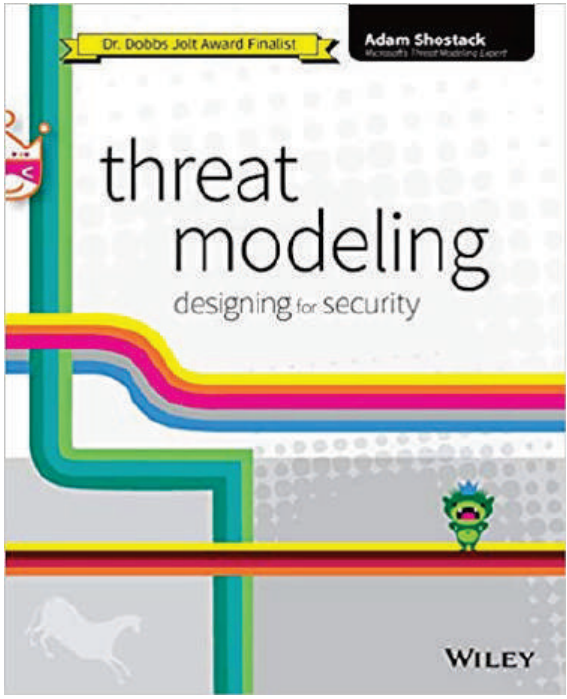

POLITIET
KRIPOS
Cyberkriminalitet 2025
Politiets årlige rapport om cyberrettet
og cyberstøttet kriminalitet

Source: Meland, P. H., Nesheim, D. A., Bernsmed, K., & Sindre, G. (2022). Assessing cyber threats for storyless systems. *Journal of Information Security and Applications*, *64*.

NTNU

Software-centric threat models

"Software-centric models are models that focus on the software being built or a system being deployed"



A typical modeling p

Pattern: Systematic Approach

Achieve thoroughness and reproducibility by applying security and privacy knowledge in a structured manner.

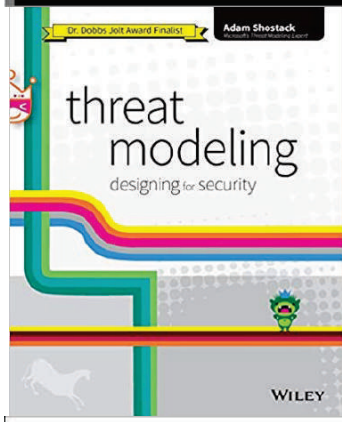
1. Identify critical assets
2. Decompose the system to be assessed
3. Identify possible points of attack
4. Identify threats
5. Categorise and prioritise the threats
6. Mitigate

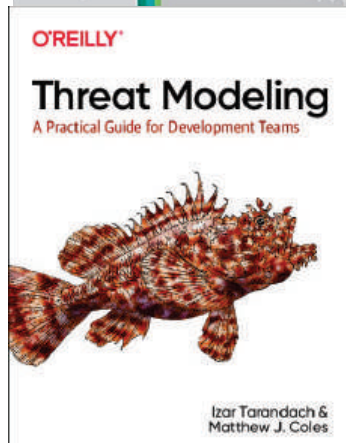
Source: Olzak, ”*A Practical Approach to Threat Modeling*”, 2006, https://adventuresinsecurity.com/blog/wp-content/uploads/2006/03/A_Practical_Approach_to_Threat_Modeling.pdf

NTNU

STRIDE

- Mnemonic for things that go wrong in security:
  - **S**poofing
  - **T**ampering
  - **R**epudiation
  - **I**nformation disclosure
  - **D**enial of Service
  - **E**levation of Privilege





NTNU

Spoofing

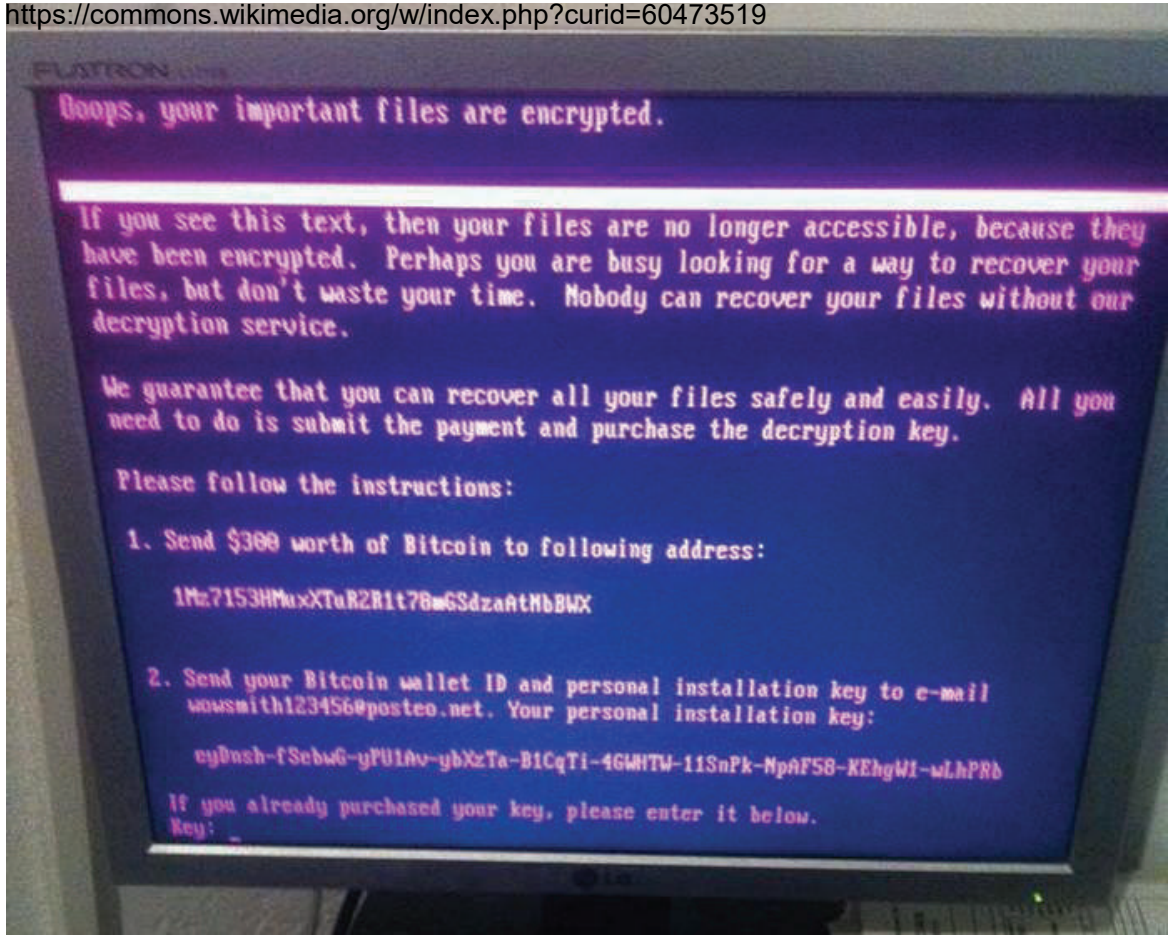
- Pretending to be something or someone you're not
- Examples:
  - Fake websites
  - Fake emails
  - CSRF
  - GPS spoofing
  - IP spoofing
  - DNS spoofing
  - Deep fake

NTNU

Tampering

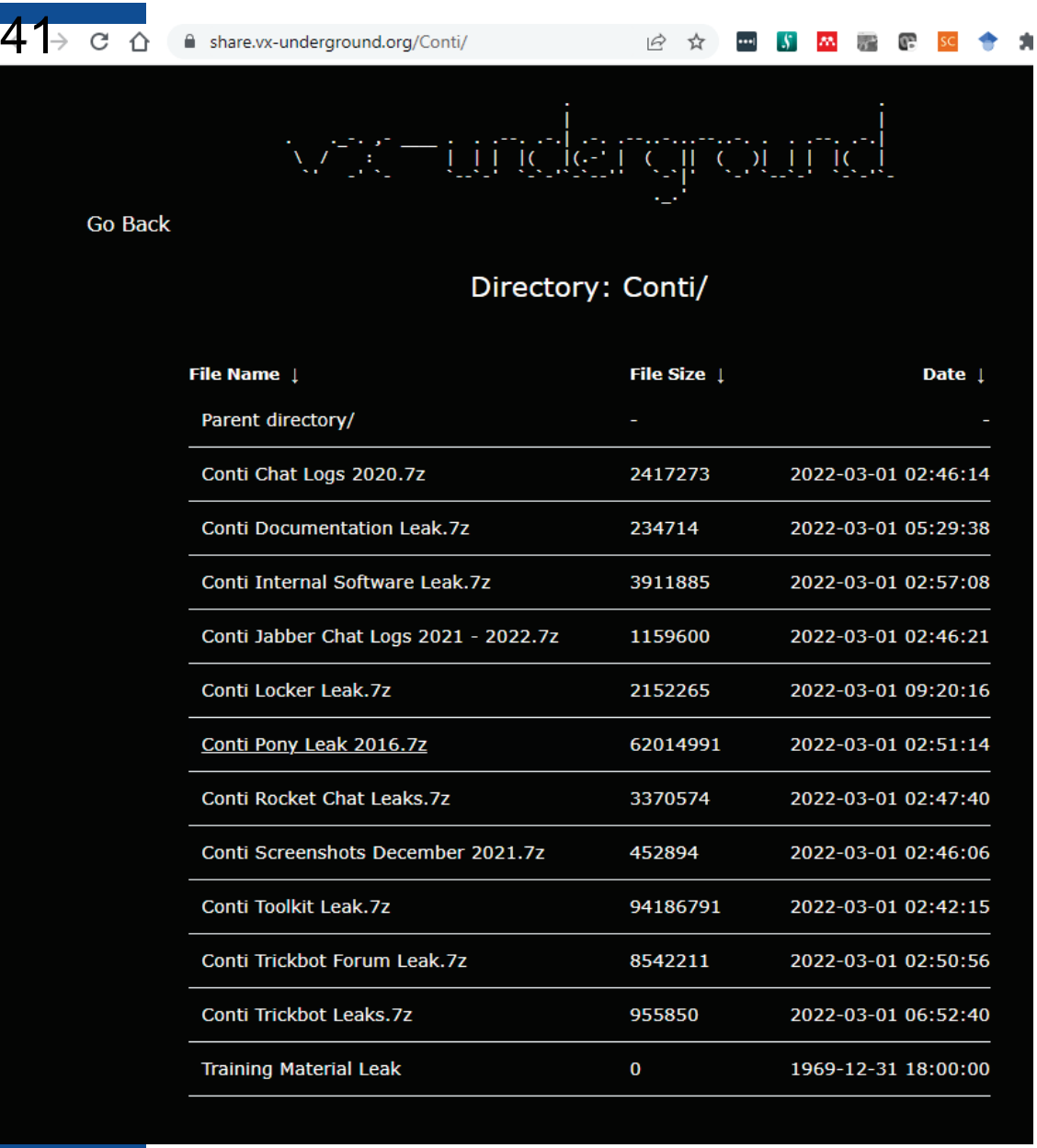
- Modifying something you're not supposed to modify
- Examples:
  - Forms
  - URLs
  - Files
  - Databases
  - Memory
  - Network data

By User:Jbuket - https://uain.press/blogs/yevgen-buket-vitannya-petru-o-vid-pyeti-dnya-konstytutsiyi/, CC BY 4.0, https://commons.wikimedia.org/w/index.php?curid=60473519



Repudiation

- Claiming you didn't do something (regardless of whether you did or not)
- Examples:
  - Claim to have not received
  - Use someone else's account
  - Attacking the logs

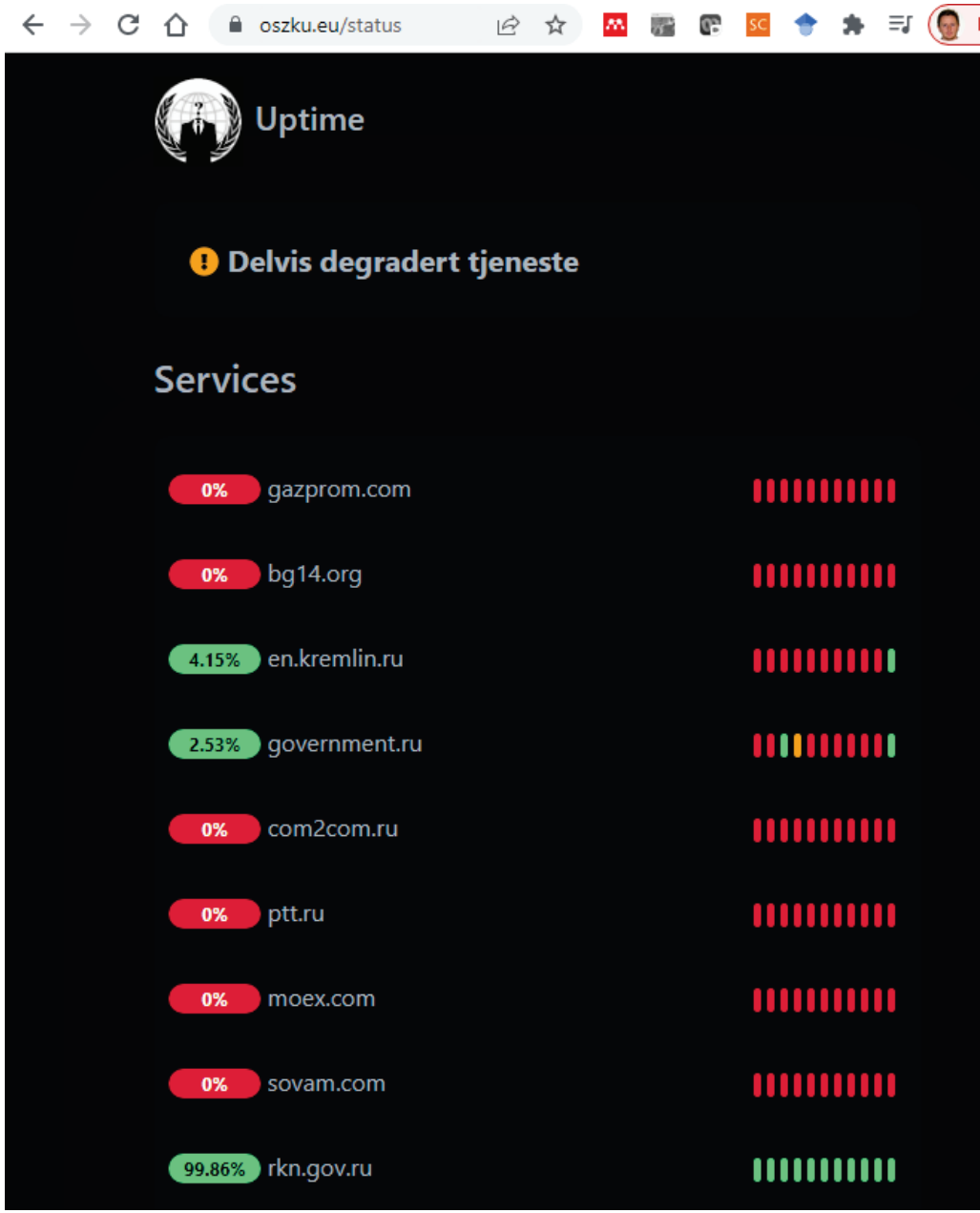


Information disclosure

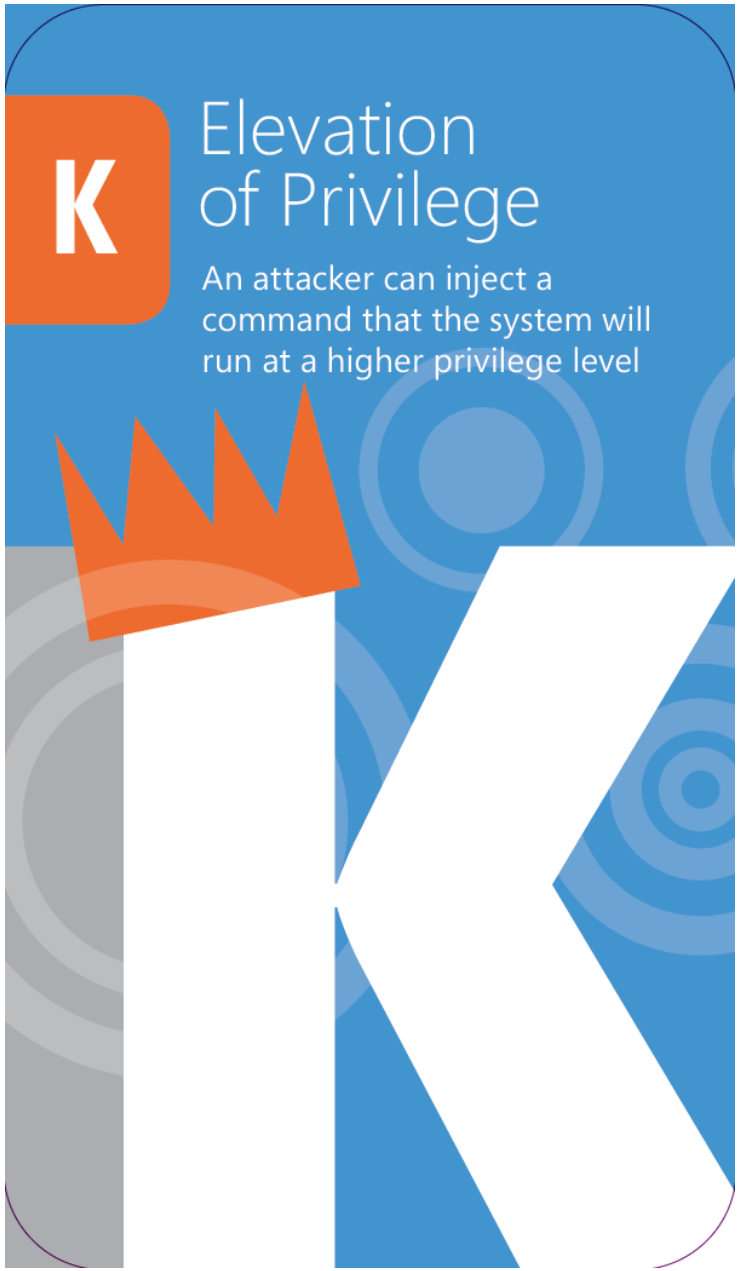
- Exposing information to people who are not authorized to see it
- Examples:
  - Steal file or database contents
  - Eavesdrop network data
  - System/API information

Denial of Service

- Attacks designed to prevent a system from providing service
- Examples:
  - Network flooding
  - Crashing software
  - Making systems slow
  - Filling storage



NTNU

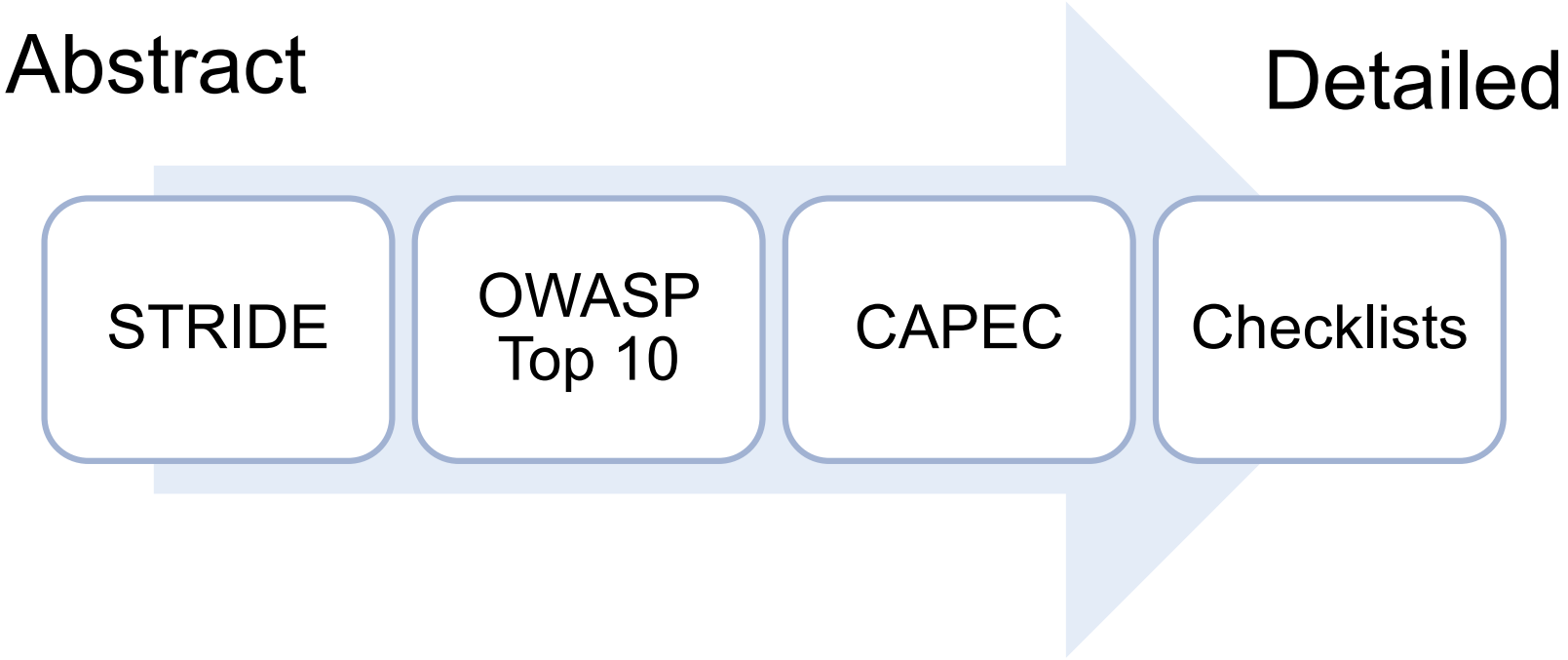


https://shostack.org/games/elevation-of-privilege

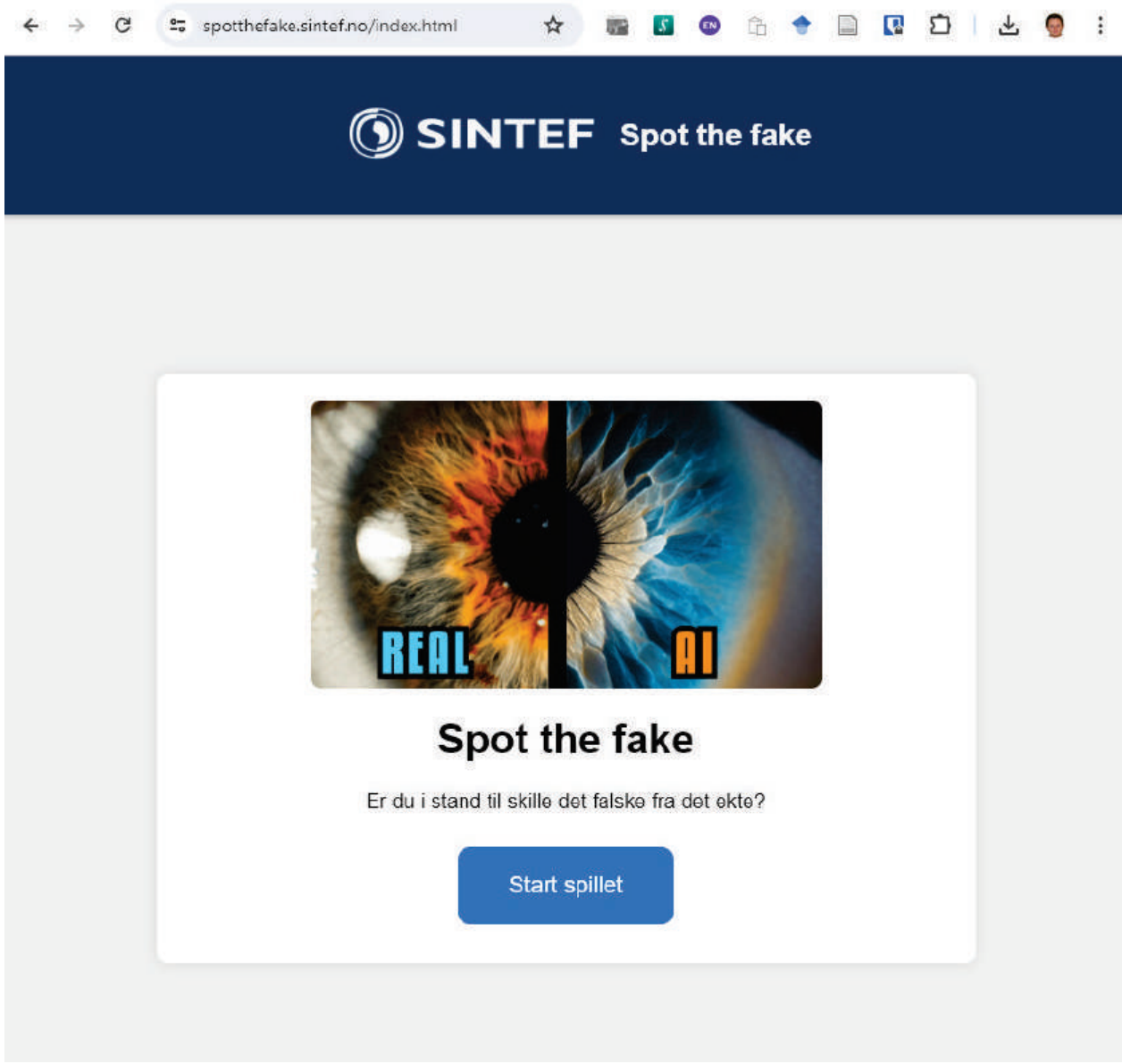
Elevation of Privilege

- A program or user is technically able to do things that they're not supposed to do
- Examples:
  - XSS
  - Buffer overflow
  - Injection attacks
  - Modify access control
  - Social engineering

Threat details



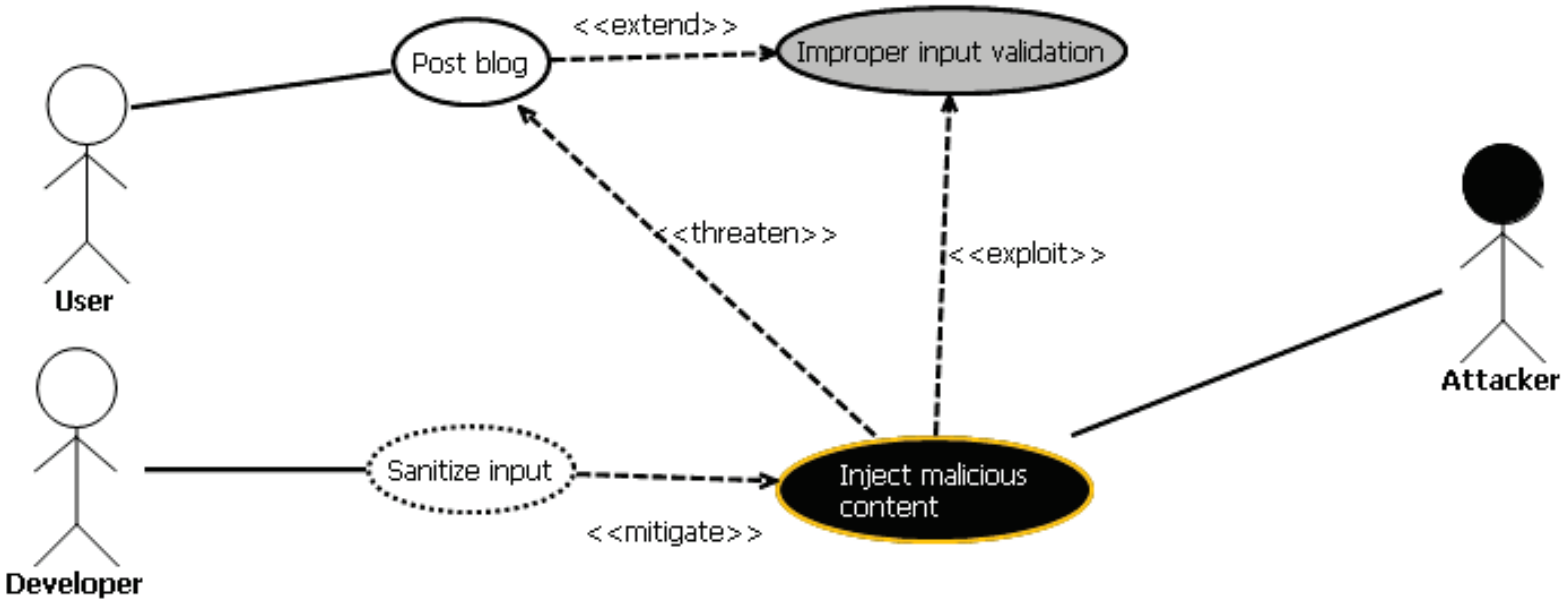
Test yourself!



Notations crash course

Misuse cases

- Extends UML use cases
- High level negative scenarios
- Easy to grasp by different stakeholders



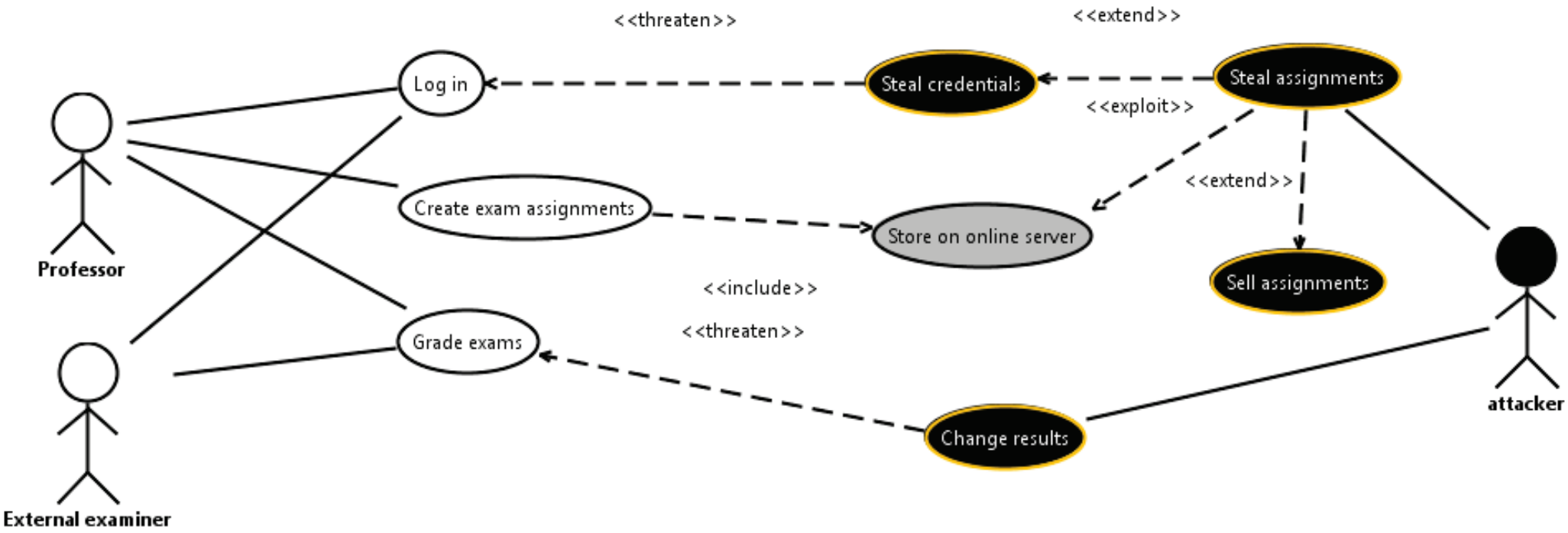
Source: Sindre and Opdahl (2001). "Capturing Security Requirements through Misuse Cases"

NTNU

Example: Threats to digital exams

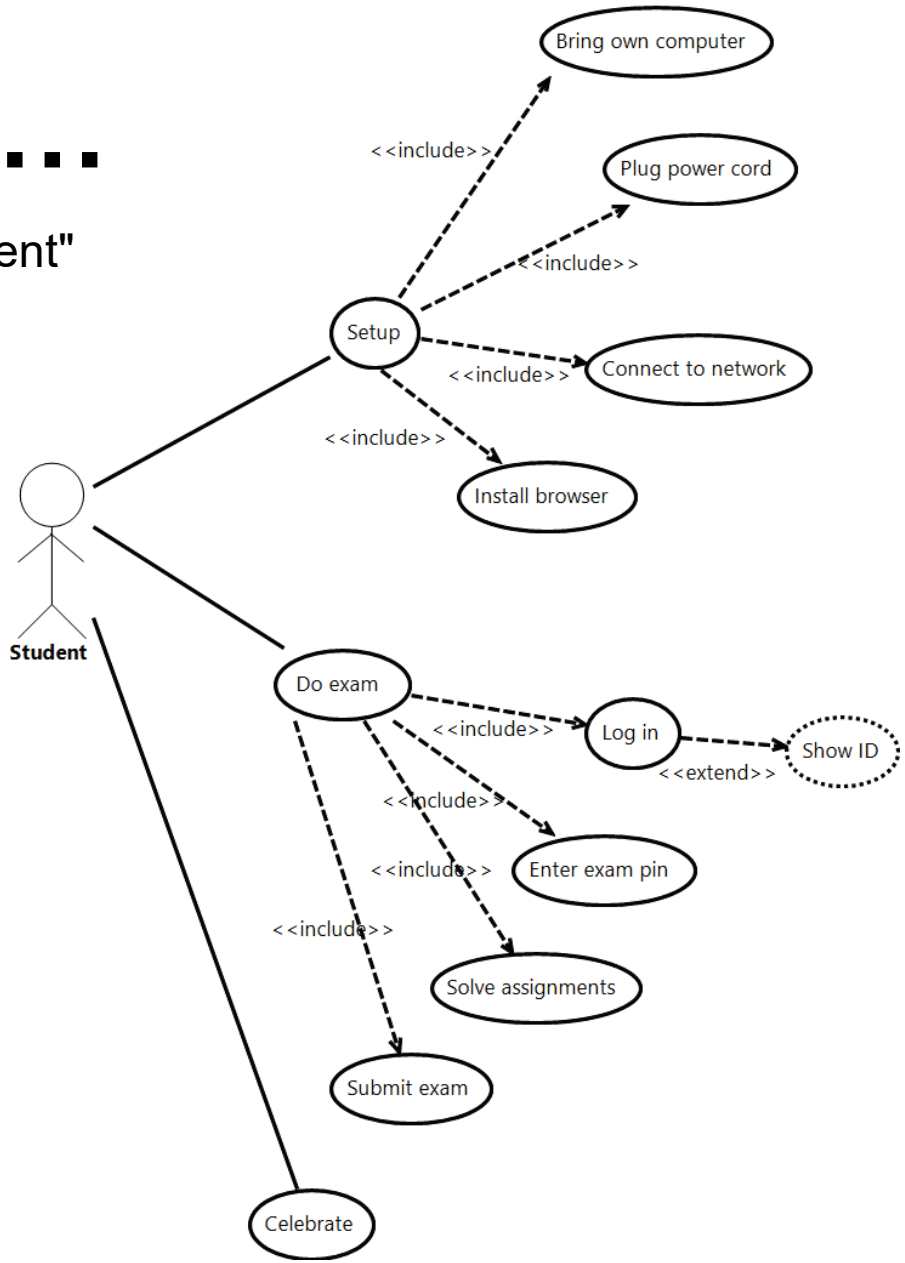
Image: Jönköping University

- **Exams are created, solved and graded online**
- **Personal computers**
- **Confined room**
- **Actors:**
  - **Professor**
  - **Student(s)**
  - **(Software developer, administrator)**


<<threaten>>
<<extend>>
Log in
Steal credentials
Steal assignments
<<exploit>>
Professor
Create exam assignments
Store on online server
<<extend>>
Sell assignments
<<include>>
<<threaten>>
Grade exams
attacker
Change results
External examiner

Consider…

What could a "bad student" do during the exam?



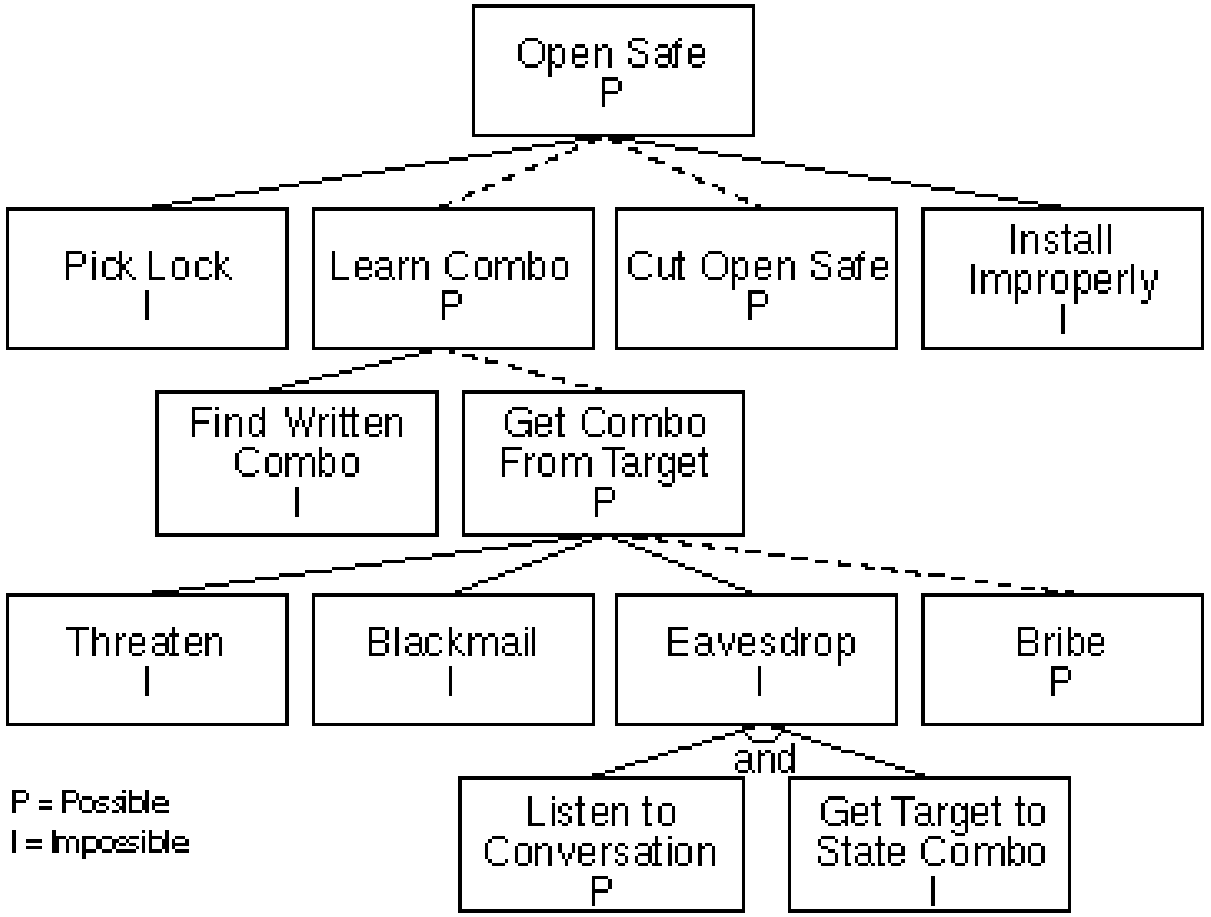
Attack trees

- Possible ways of achieving an attack goal
- Tree structure with AND/OR nodes
- Easy to grasp by different stakeholders
- More technical than misuse cases

Credit: World of Warcraft

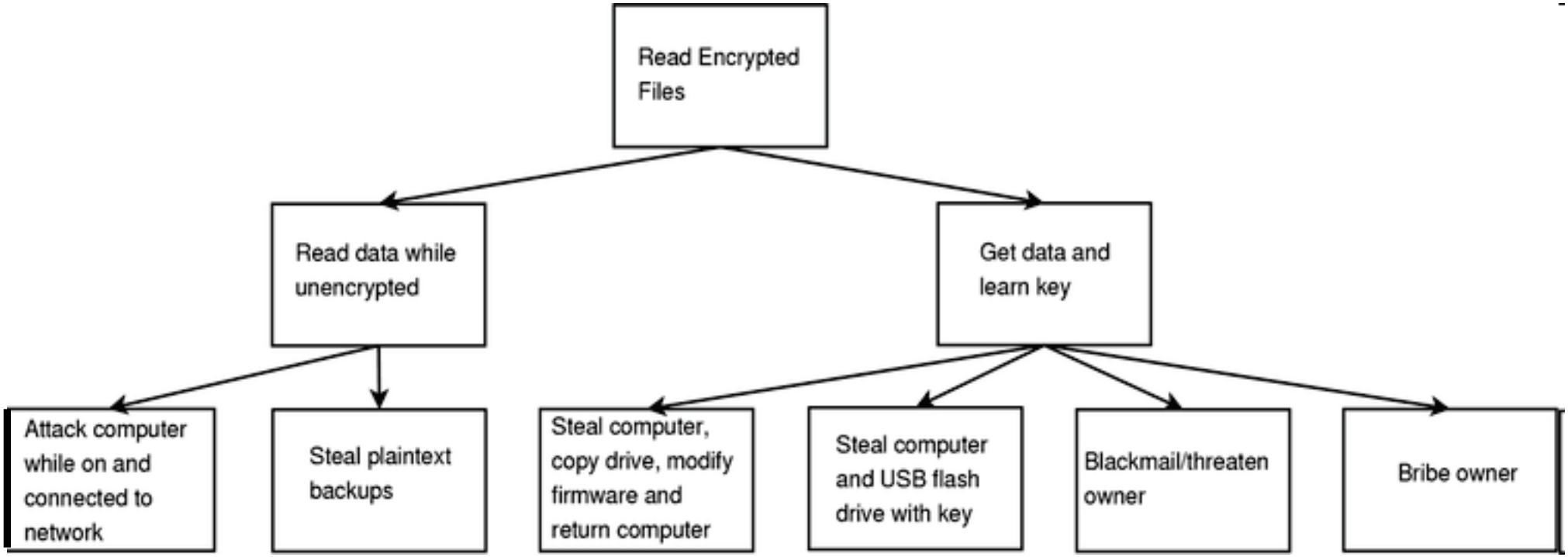
Source: Bruce Schneier: "Attack Trees", Dr. Dobb's Journal December 1999

Attack tree - example



Attack tree source: http://www.schneier.com/paper-attacktrees-ddj-ft.html

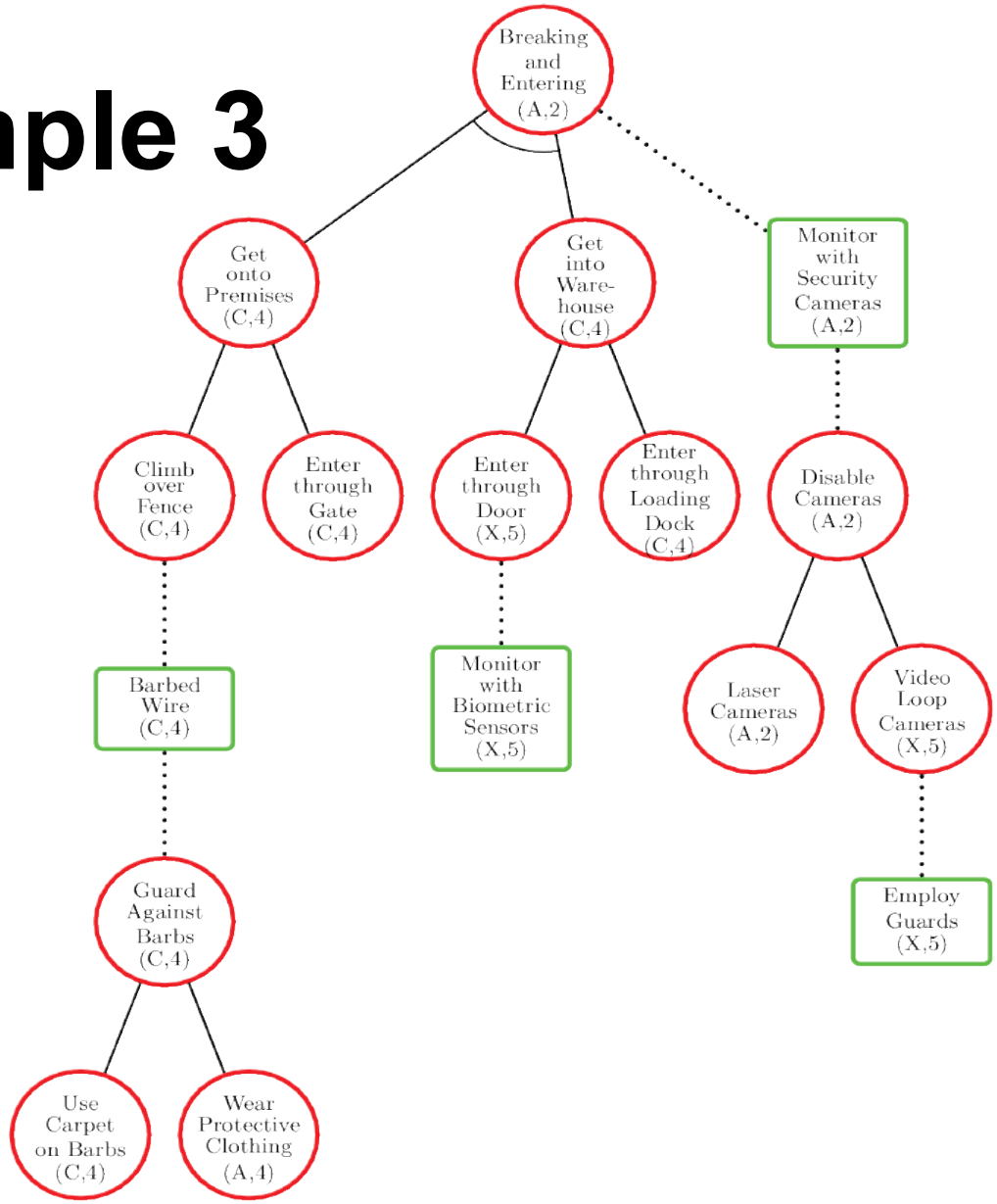
Attack tree – example 2



Source: http://www.linuxjournal.com/article/7743

Attack tree – example 3

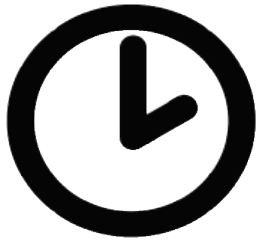
(Attack-Defense Tree)

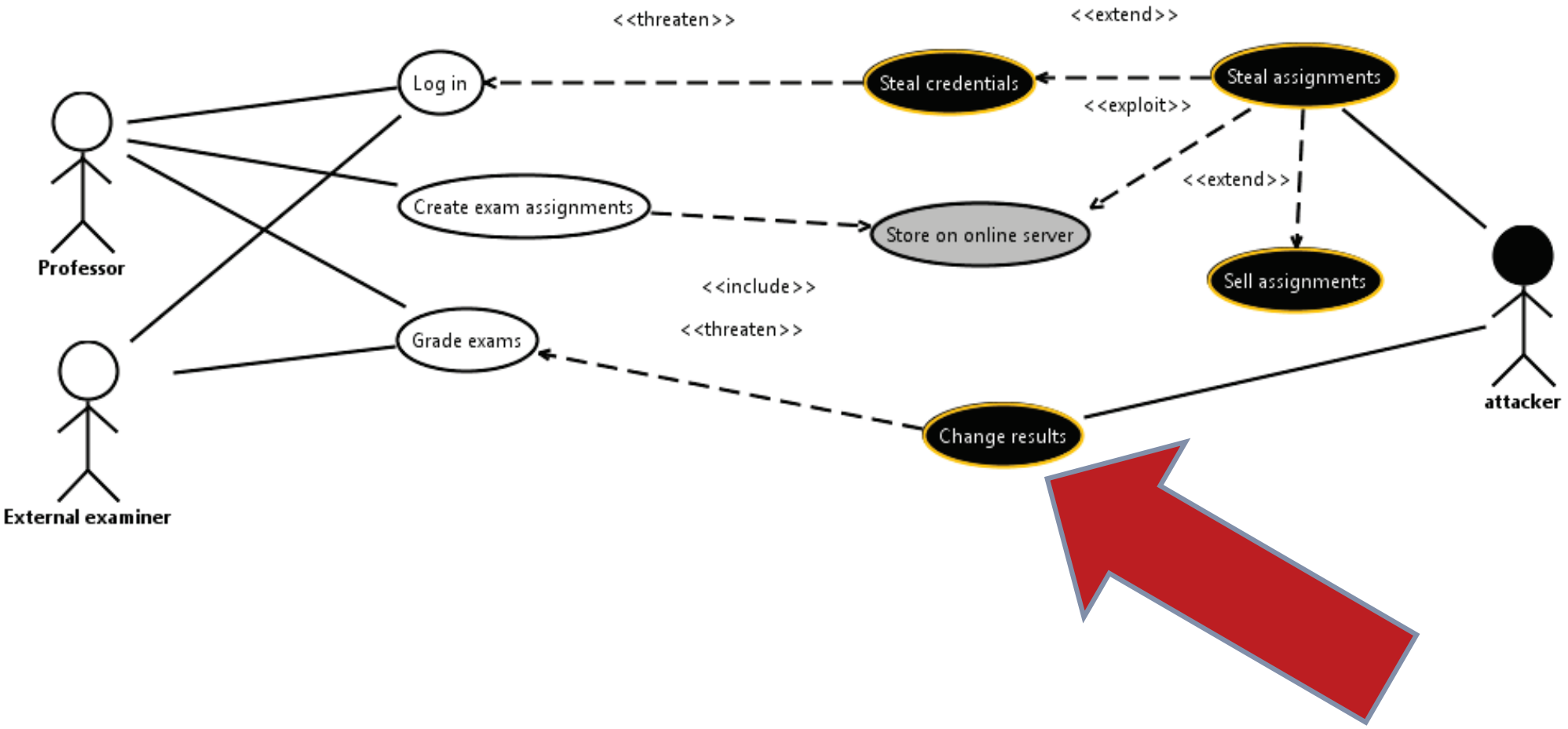


Source: Alessandra Bagnato, Barbara Kordy, Per Håkon Meland, Patrick Schweitzer. *Attribute Decoration of Attack-Defense Trees.* International Journal of Secure Software Engineering, volume 3(2), pages 1-35. IGI Global, 2012.

Attack tree attributes examples

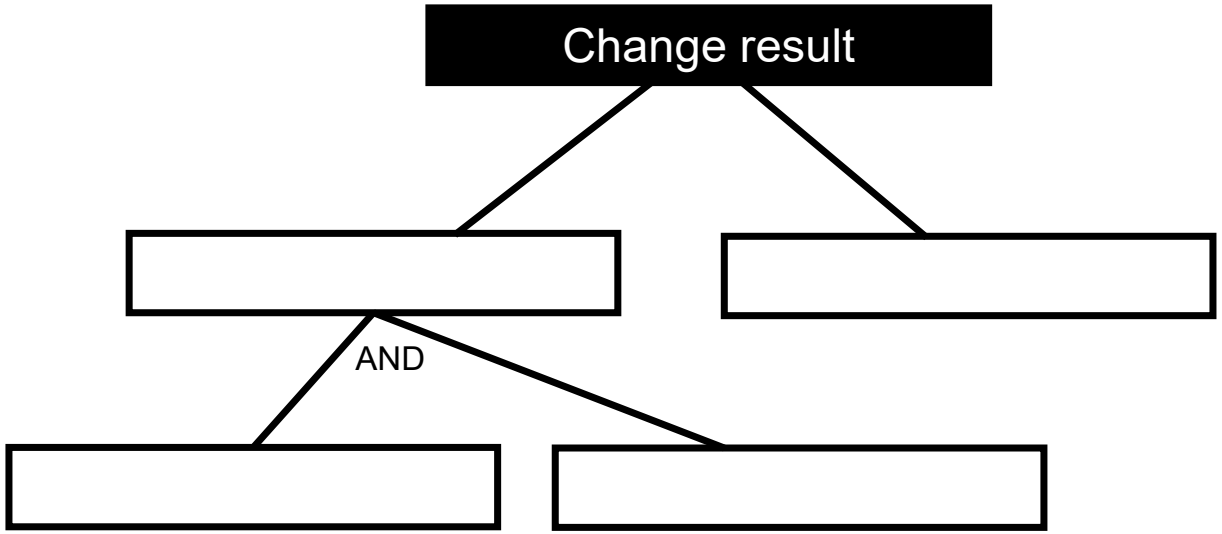
- Cost
- Detectability
- Difficulty
- Impact
- Penalty
- Profit
- Probability
- Special skill
- Time




<<threaten>>
<<extend>>
Log in
Steal credentials
Steal assignments
<<exploit>>
Create exam assignments
Store on online server
<<extend>>
Sell assignments
Professor
<<include>>
<<threaten>>
Grade exams
attacker
Change results
External examiner

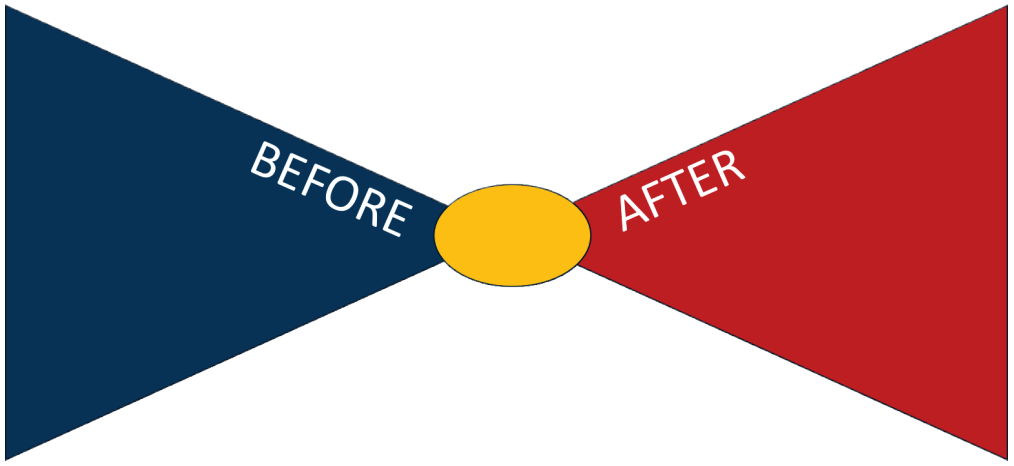
Let's try…

Suggest attack tree nodes (sub goals) on how an attacker might change the result of an exam

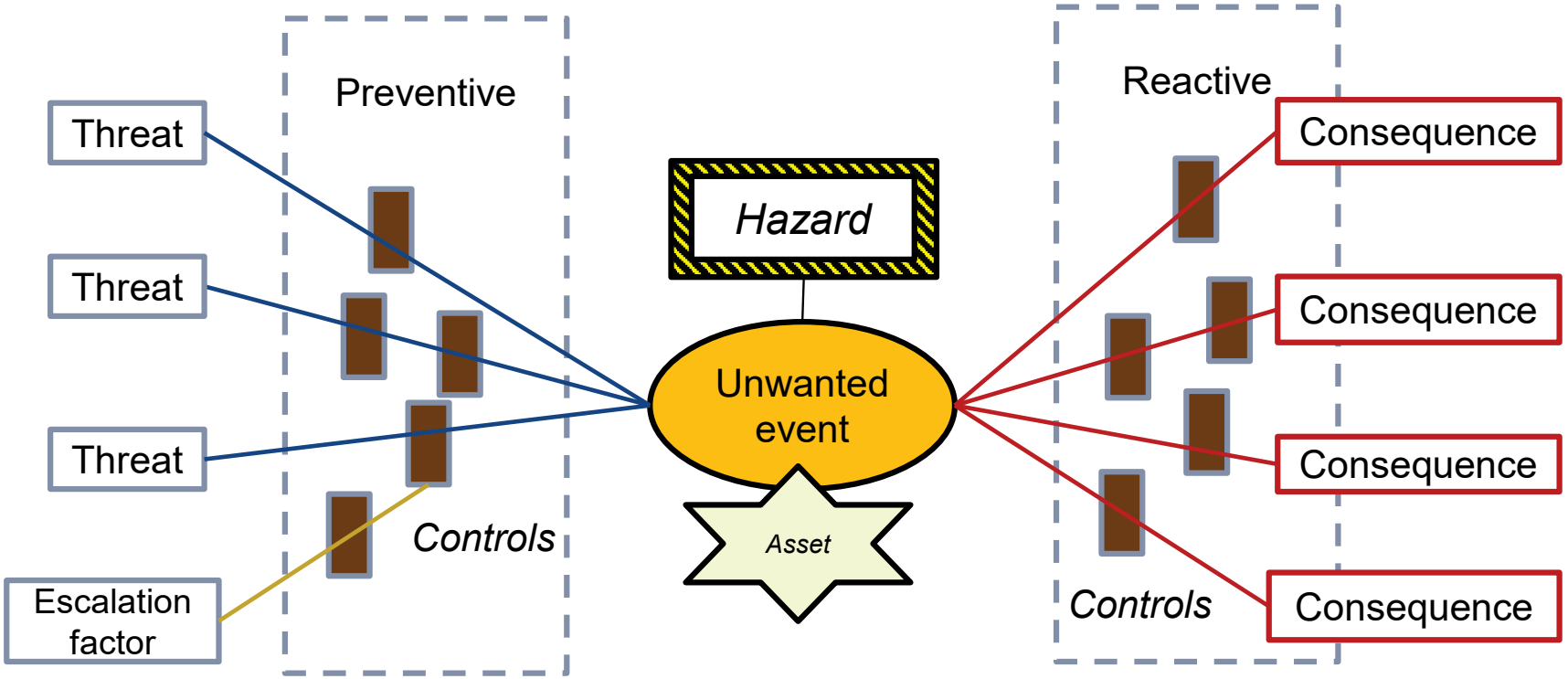


Bow-tie diagram

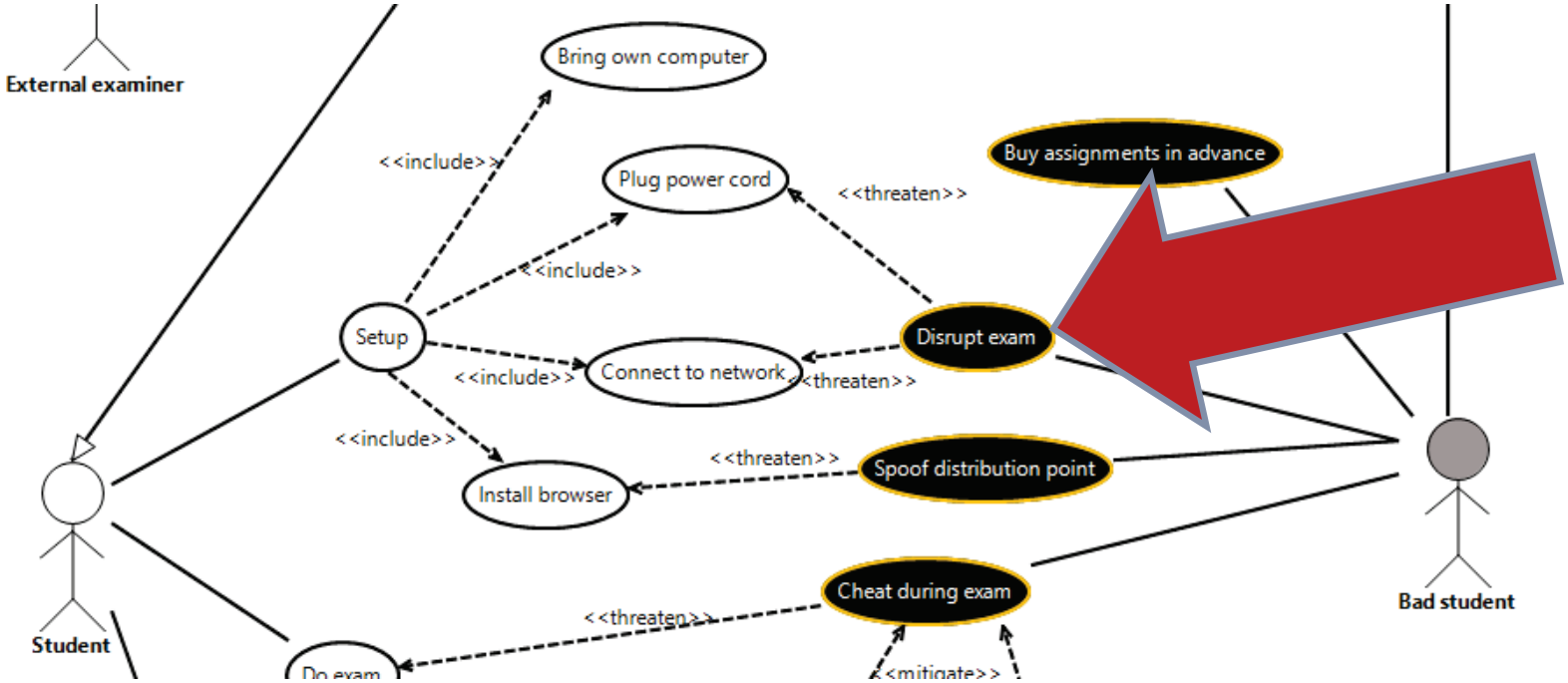
- Model a single unwanted event at a time
- Different causes/threats to unwanted events
- Different consequences once the event has happened
- Preventive/reactive controls
- Tradition from safety

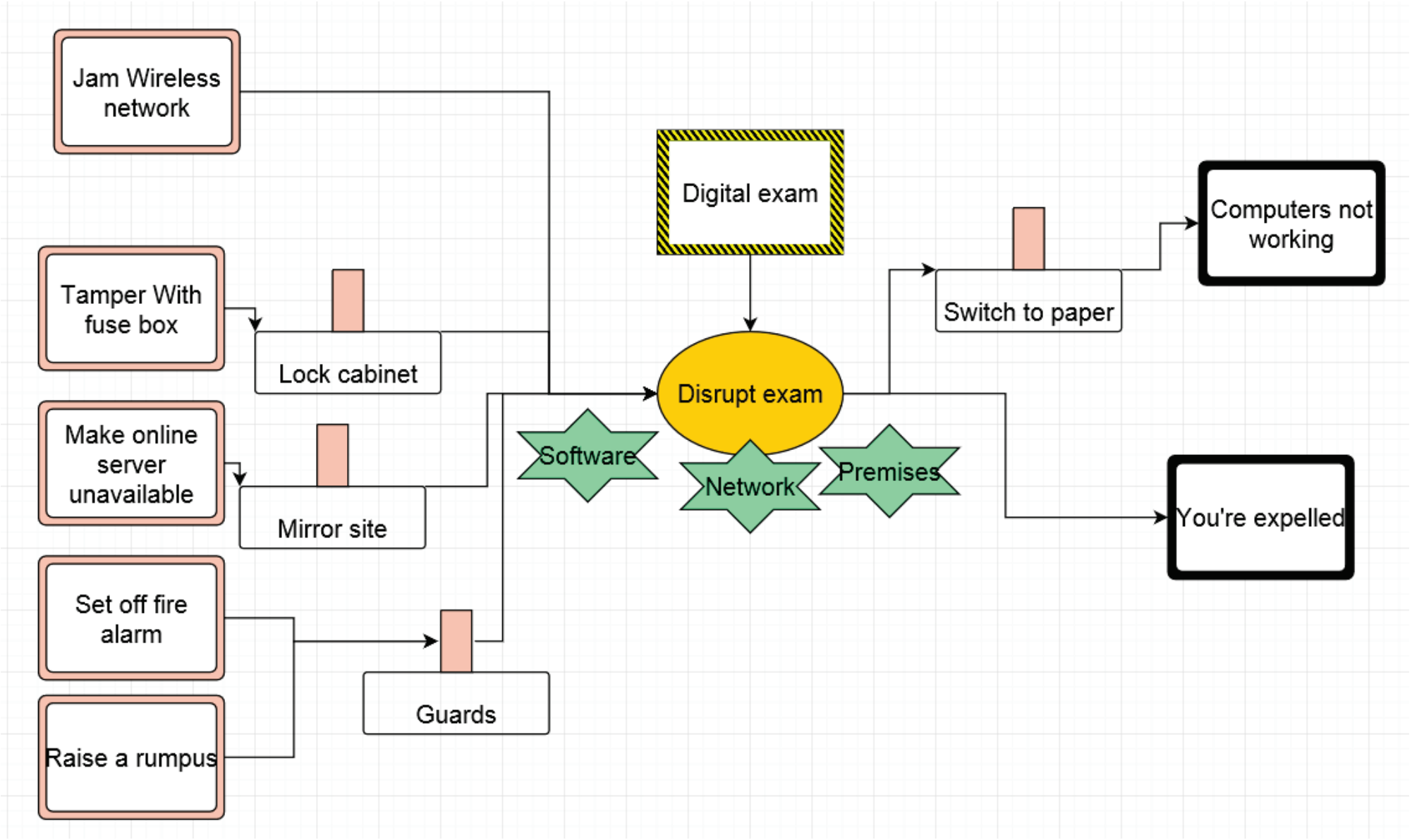


Bow-tie notation

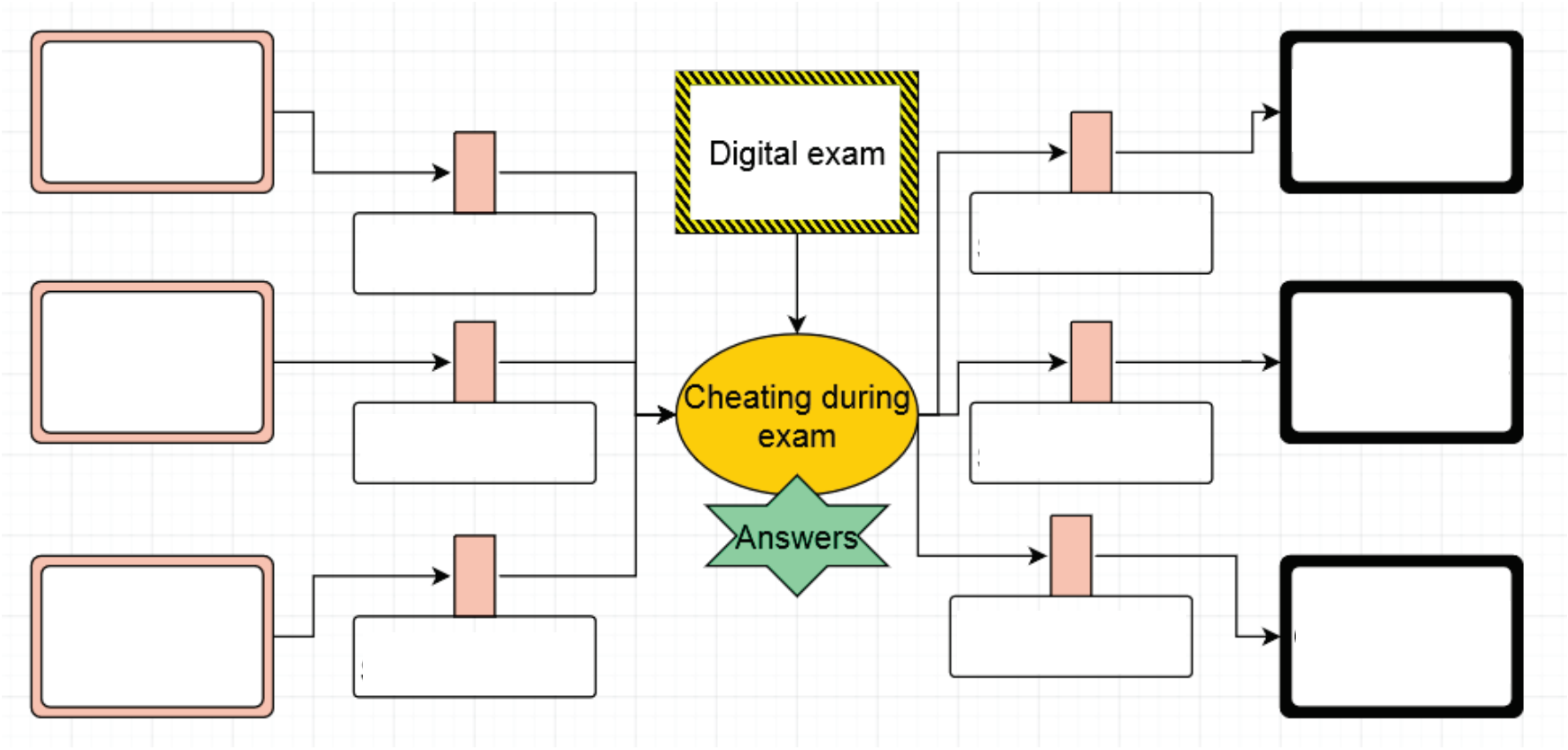


Let's drill down another misuse case



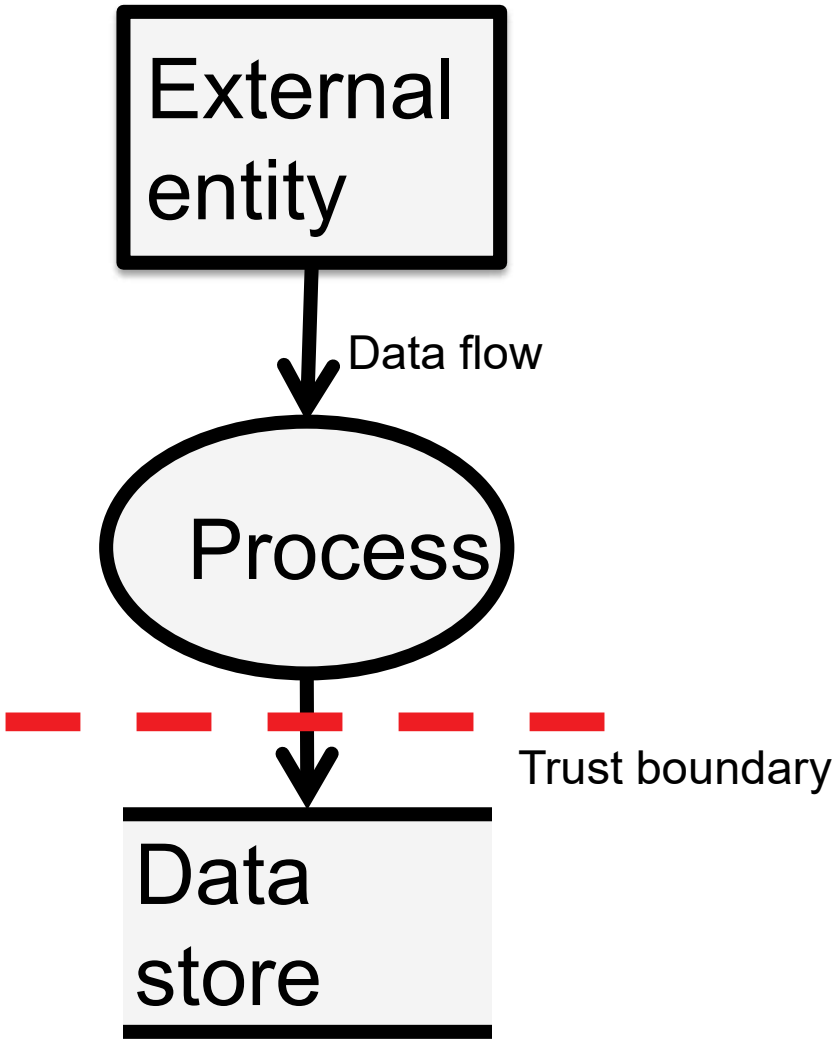

Jam Wireless network
Digital exam
Computers not working
Tamper With fuse box
Lock cabinet
Switch to paper
Disrupt exam
Make online server unavailable
Mirror site
Software
Network
Premises
You're expelled
Set off fire alarm
Guards
Raise a rumpus

Let's try…

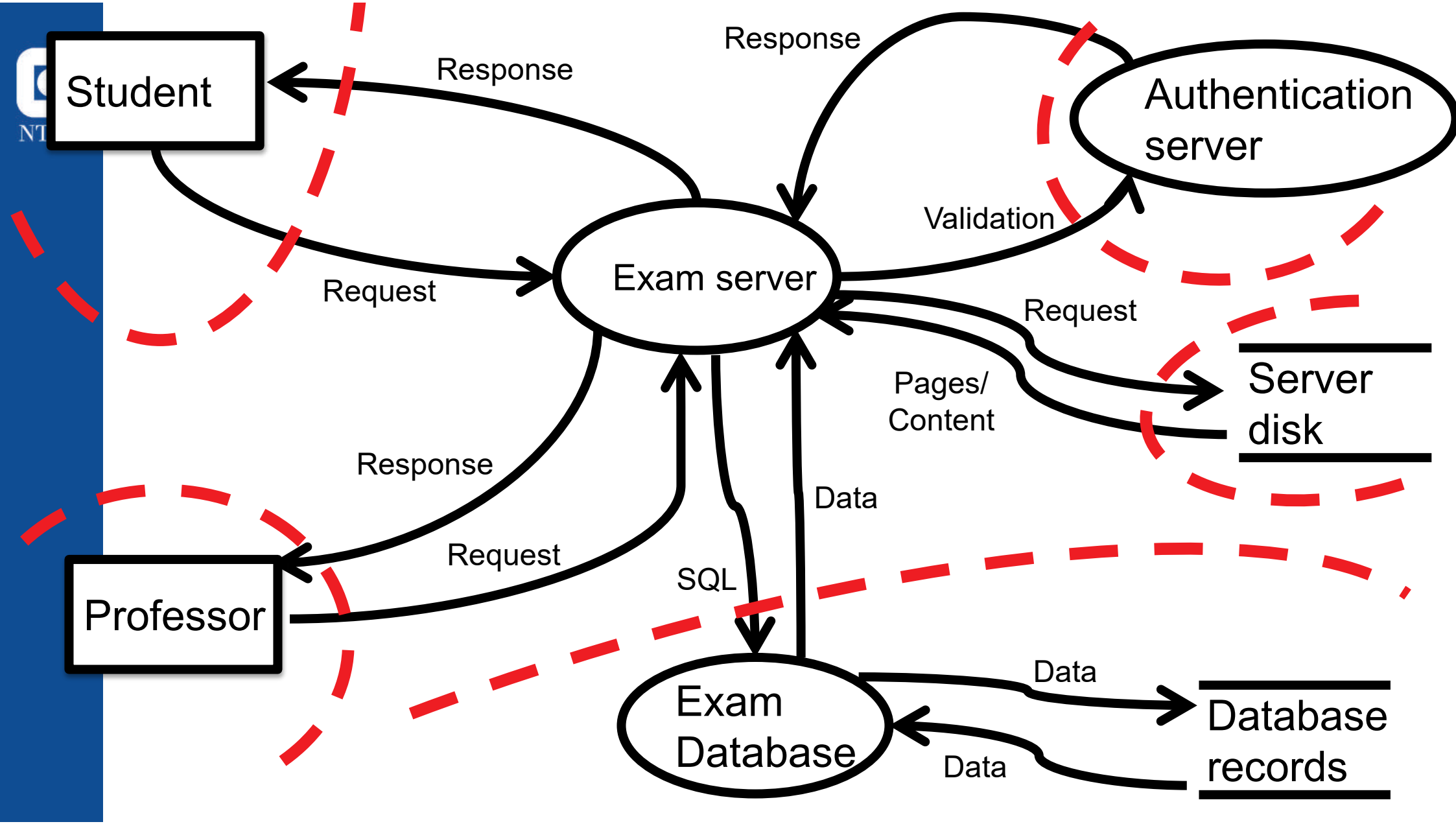


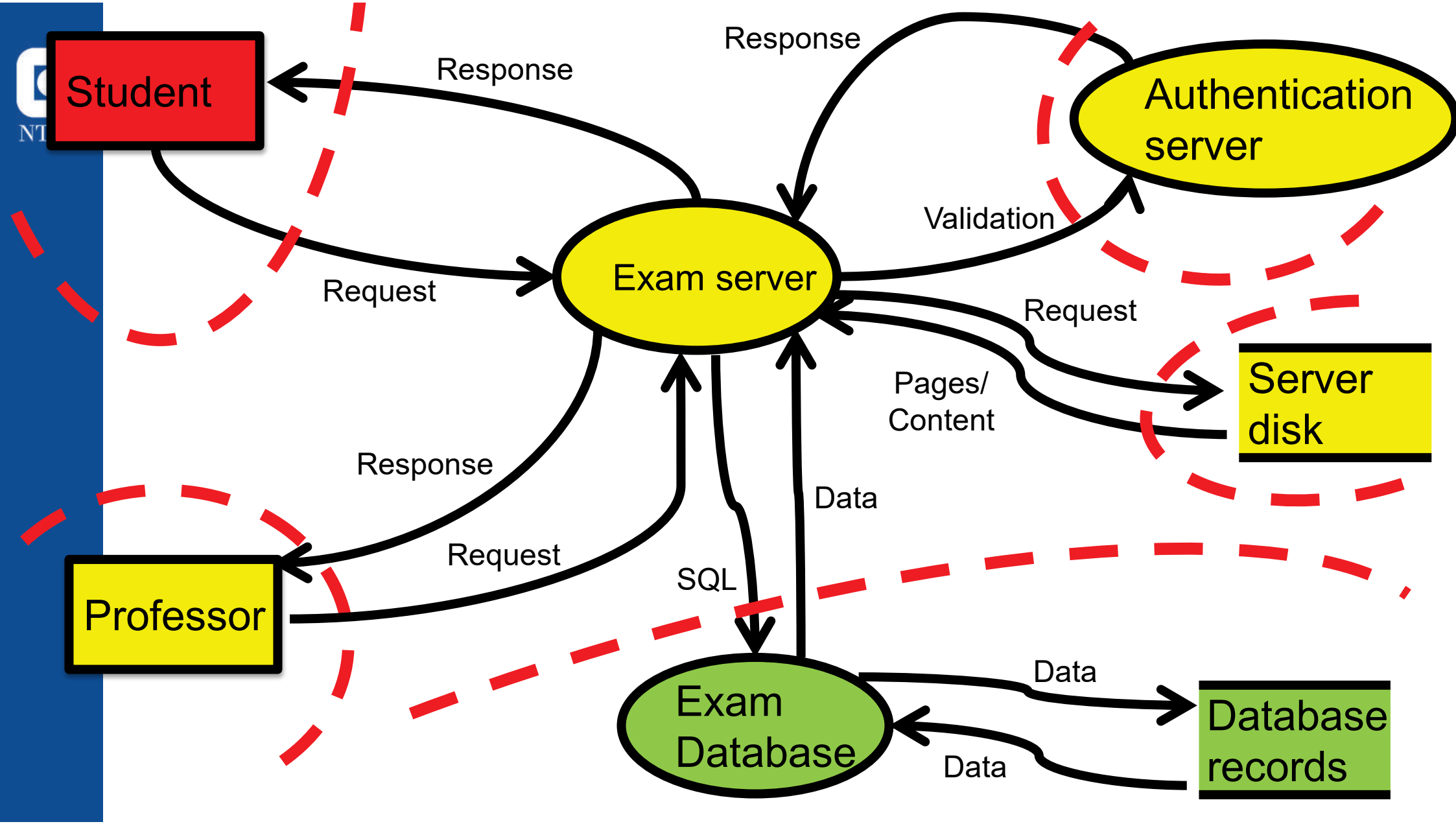
Data Flow Diagram

- Understand the system
- Data flow between subsystems
- Find attack surface and critical components
- Trust/Privilege boundaries



Source: Swidersky, Snyder "Threat modeling", Microsoft Press 2004


Student
Response
Response
Authentication server
Validation
Exam server
Request
Request
Pages/ Content
Server disk
Response
Request
Data
Professor
SQL
Exam Database
Data
Data
Database records

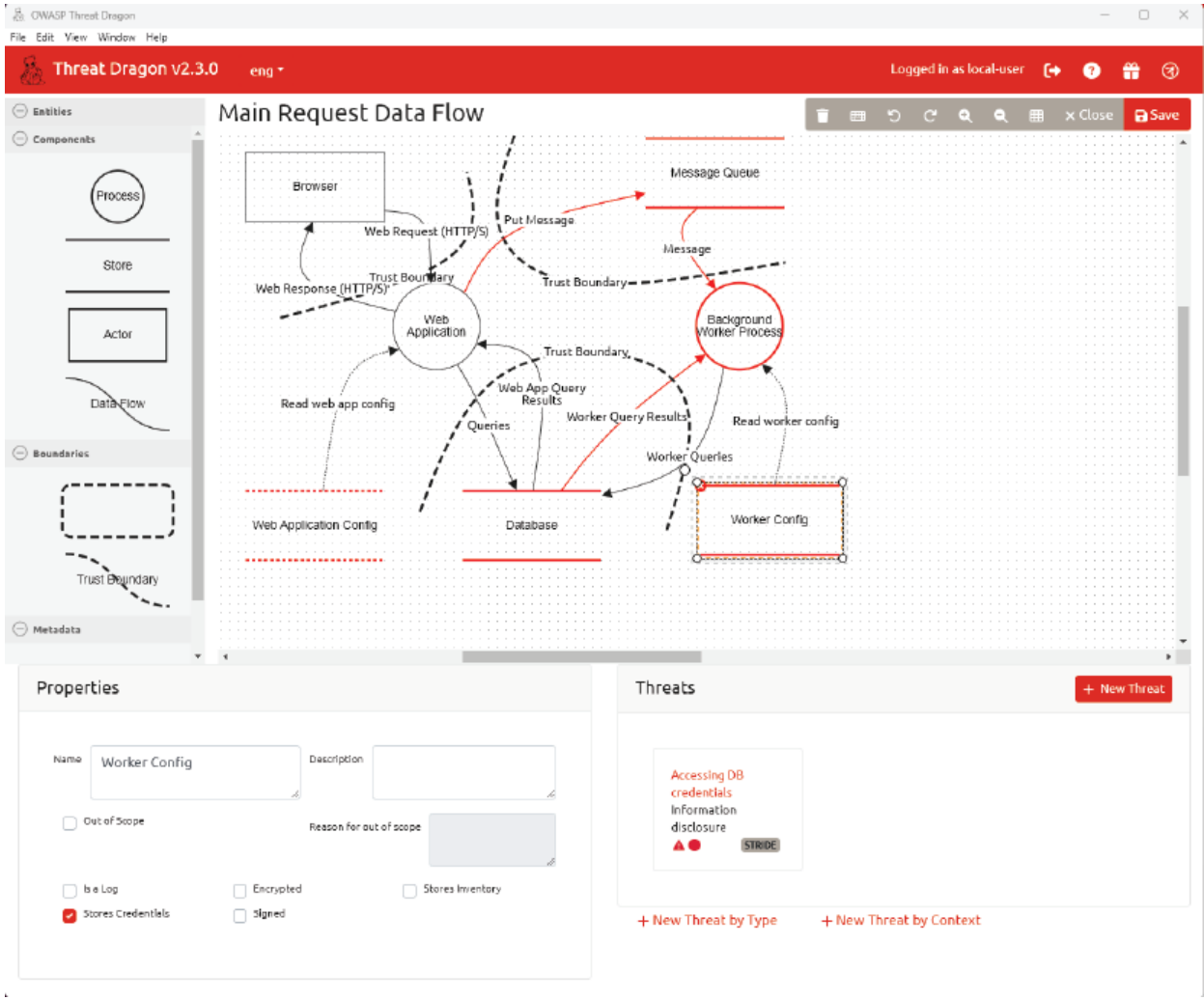

Student
Response
Response
Authentication server
Validation
Exam server
Request
Request
Server disk
Pages/ Content
Response
Request
Professor
SQL
Data
Exam Database
Data
Data
Database records

Applying STRIDE

	S	T	R	I	D	E
Student	x		x			x
Professor	x					
Exam server		x			x	x
Exam database				x	x	
Authentication server					x	
Server disk		x		x	x	
Database records		x		x		

OWASP Threat Dragon

- Exercise 3
- Web, Windows, MacOS, Linux
- Supports STRIDE
- https://owasp.org/www-project-threat-dragon/



Threat modeling essentials

- What are you building?
- What can go wrong?
- What should you do about those things that can go wrong?
- Did you do a decent job of analysis?

Threat modeling manifesto (2020)

Next time

Risk Management during development

- Risk management frameworks
- Security requirements
- CVSS
- Security Economics
- Security engineering book
  - Chapter 8.6: The economics of security and dependability
  - Chapter 27.2: Risk management
  - Chapter 27.4: Prioritising protection goals