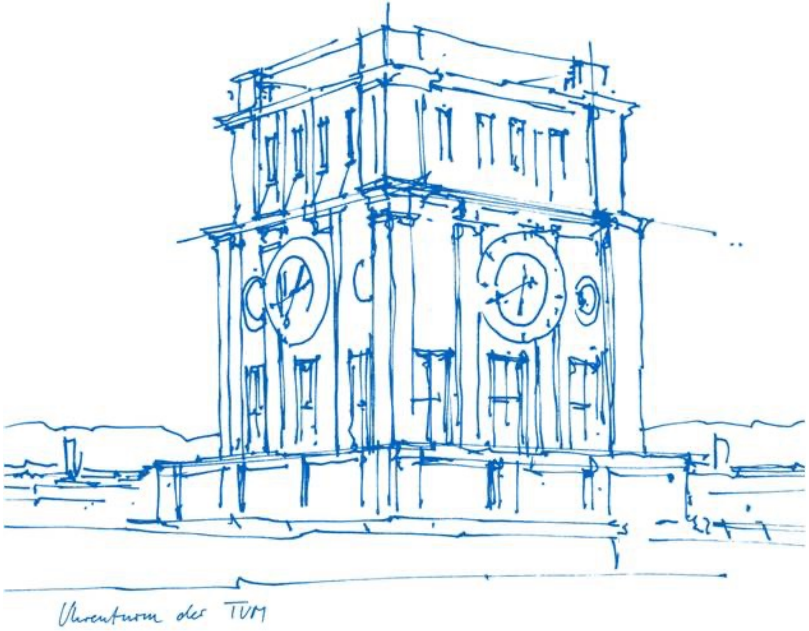
Chair of IT Security
School of Computation, Information and Technology
Technical University Munich

Seminar Cyber-Resilient Systems

Lukas Gehrke

July 9th, 2024



Introduction

Resilience is…

… the ability to be happy, successful, etc. again after something difficult or bad has happened

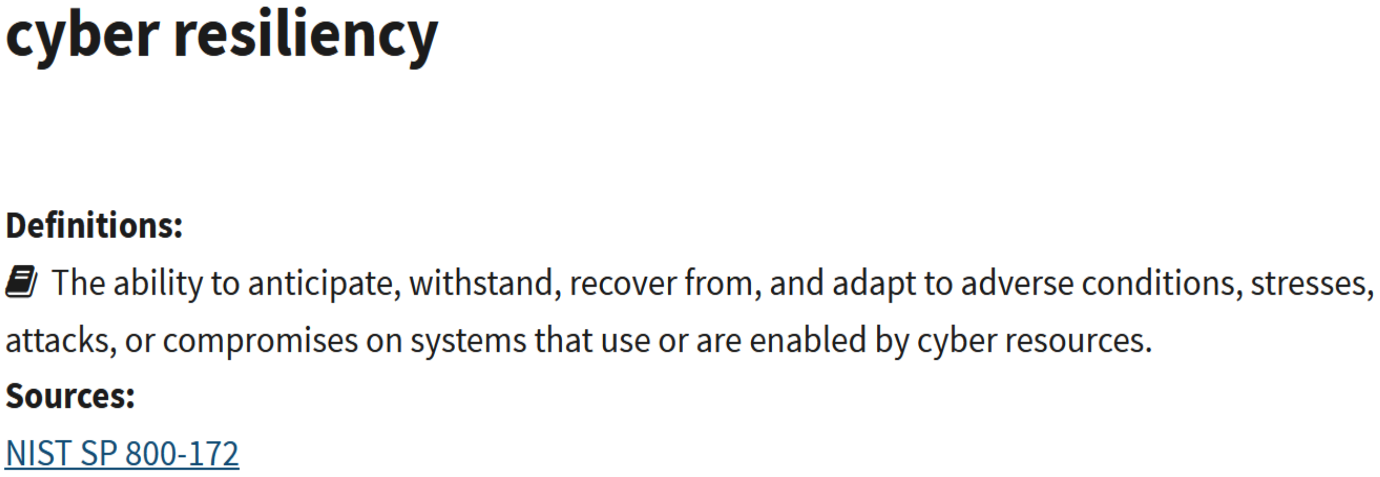
… the ability of a substance to return to its usual shape after being bent, stretched, or pressed

(Cambridge Dictionary)

What does this have to do with computers?

Introduction

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



cyber resiliency

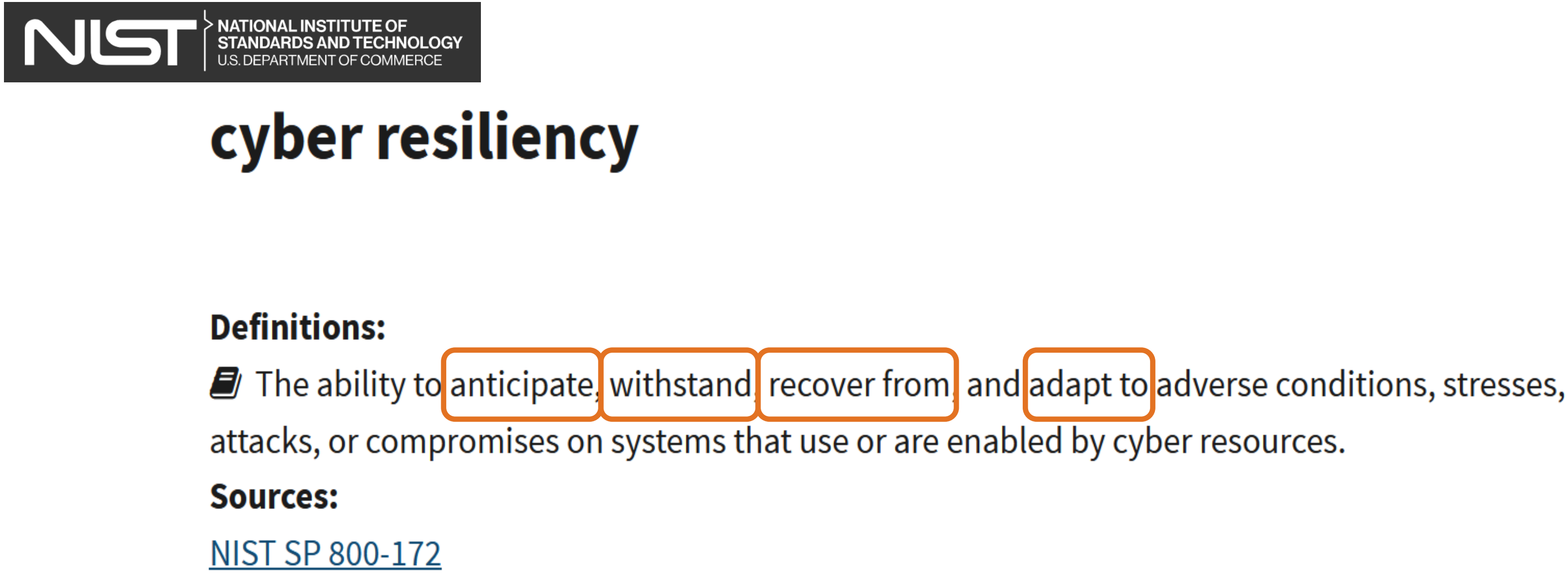
Definitions:

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Sources:

NIST SP 800-172

Introduction


NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

cyber resiliency

Definitions:

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Sources:

NIST SP 800-172

Cyber Resilience Approach

anticipate

withstand

recover

adapt

Clipart: https://www.irasutoya.com/

Cyber Resilience Approach

anticipate

withstand

recover

adapt

Fundamental Assumption: We cannot always withstand adversity.
Thus we need abilities to recover and adapt.

Clipart: https://www.irasutoya.com/

Traditional Cyber Security Approach

DIESES SYSTEM IST
SICHER
ZERTIFIKAT
5/5 STERNE

withstand

withstand

withstand

Clipart: https://www.irasutoya.com/

Research Questions

Tbd.

Two examples following

Task Example

Topic: **Recovery** of compromised IIoT/OT devices

Questions to answer: How do state-of-the-art IIoT/OT devices work? How can they be compromised? (How can compromise be detected?) How can recovery be enforced?

Sources to start with:

- Resilient IoT standard by TCG: https://trustedcomputinggroup.org/new-tcg-guidance-simplifies-creating-cyber-resilient-devices/
- DICE standard by TCG: https://trustedcomputinggroup.org/work-groups/dice-architectures/
- „Dominance as a New Trusted Computing Primitive for the Internet of Things“ (paper, 2019)
- „The Lazarus Effect: Healing Compromised Devices in the Internet of Small Things (paper, 2020)

Task Example

Topic: **Detection** of compromise in IIoT/OT devices

Questions to answer: How do state-of-the-art IIoT/OT devices work? How can they be compromised? How can compromise be detected?

Sources to start with:

- DICE standard by TCG: https://trustedcomputinggroup.org/work-groups/dice-architectures/
- „Dominance as a New Trusted Computing Primitive for the Internet of Things“ (paper, 2019)
- „The Lazarus Effect: Healing Compromised Devices in the Internet of Small Things (paper, 2020)
- „Cyber Resilience for the Internet of Things: Implementations With Resilience Engines and Attack Classifications“ (paper 2024)
- „TeeFilter: High-Assurance Network Filtering Engine for High-End IoT and Edge Devices based on TEEs“ (paper 2024)

Further Tasks

Tbd.

- Security rather than privacy
- IoT/OT connection, also networking/cloud focus possible
- Data Science/Machine Learning topic with connection to IoT/OT possible

Seminar Learning Goals

The seminar aims at teaching you how to do an **academic literature search** and **present your results (written and spoken)**.

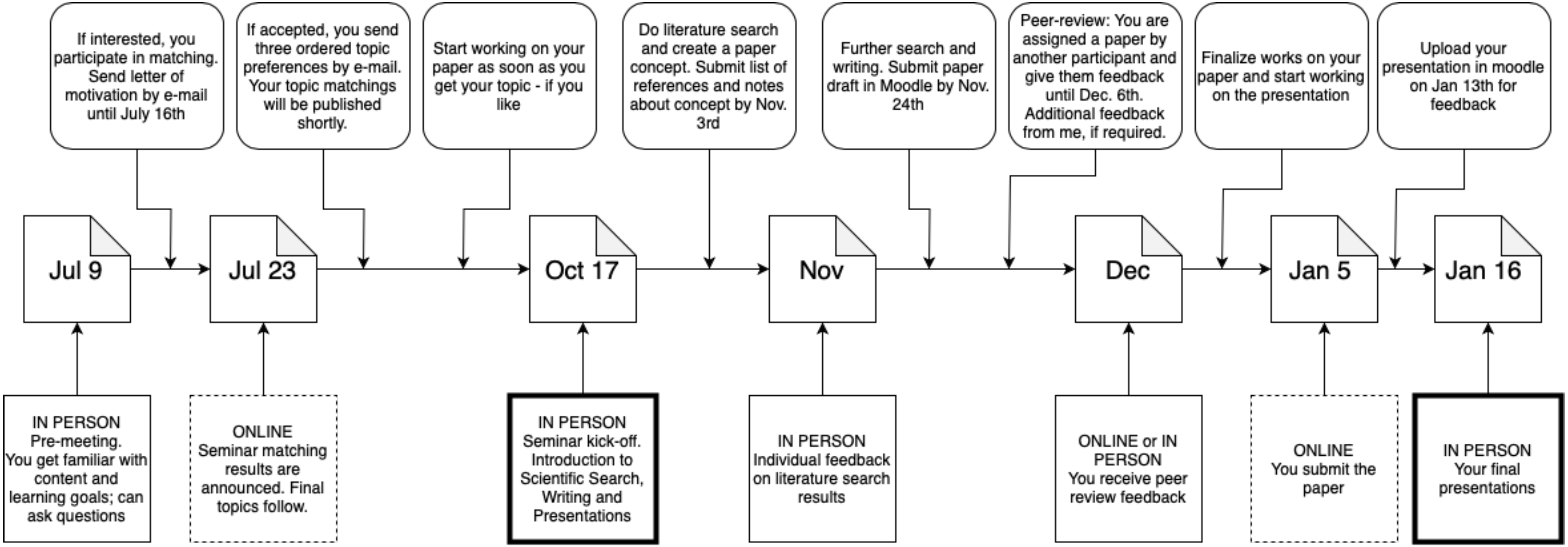
This is an excellent practice for you for…

- Your thesis
- Your academic career
- Your career in the industry (structured work on paper, presentation)

To give you something to start with, the seminar includes hints on…

- Literature Search
- Scientific Writing
- Presentations (Slides and Talk)

Tentative Timeline



Jul 9

IN PERSON
Pre-meeting.
You get familiar with content and learning goals; can ask questions

If interested, you participate in matching. Send letter of motivation by e-mail until July 16th

Jul 23

ONLINE
Seminar matching results are announced. Final topics follow.

If accepted, you send three ordered topic preferences by e-mail. Your topic matchings will be published shortly.

Start working on your paper as soon as you get your topic - if you like

Oct 17

IN PERSON
Seminar kick-off. Introduction to Scientific Search, Writing and Presentations

Do literature search and create a paper concept. Submit list of references and notes about concept by Nov. 3rd

Nov

IN PERSON
Individual feedback on literature search results

Further search and writing. Submit paper draft in Moodle by Nov. 24th

Peer-review: You are assigned a paper by another participant and give them feedback until Dec. 6th. Additional feedback from me, if required.

Dec

ONLINE or IN PERSON
You receive peer review feedback

Finalize works on your paper and start working on the presentation

Jan 5

ONLINE
You submit the paper

Upload your presentation in moodle on Jan 13th for feedback

Jan 16

IN PERSON
Your final presentations

Further Organizational Matter (tentative)

Time: (tentative) Thursdays 10:00 a.m. ~ 12:00 a.m. (final presentations: 45 min x number of presenters)

Room: 01.08.033

Capacity: Eight students

Language: English

Target Group: Master’s and bachelor’s students welcome; important is that you are interested in the topic and doing Cyber Security/Resilience research.

Your presence at in-person meetings in mandatory.

Deliverable Requirements

Intermediate Version

- Draft 1: Results of literature search, ideally as table, describe your findings
- Draft 2: 80% ready paper draft with list of references for feedback, optionally also you presentation draft
- Optional, individual feedback sessions in person

Presentation

- 30 min talk and 10 to 15 min discussion
- Please use the TUM 16:9 template (PowerPoint, LaTeX)

Report

- (Exactly) Ten pages, two-column style (excluding references and appendix)
- Please use the IEEE template (https://www.ieee.org/conferences/publishing/templates.html)
- You are encouraged to use LaTeX

Requirements for Passing and Grading

Please take a look at what the terms of your degree program state about written assignments and oral presentations. („Prüfungsordnung“)

Grading will be:
50% Paper (e.g. structure, writing style, literature research results, grammar and spelling mistakes)
40% Presentation (e.g. presentation quality, usage of media, explanations, style of speaking)
10% Discussion (e.g. reaction to questions and comments of the audience)

You cannot pass the seminar if you fail one of the components Presentation or Paper.

So, you would like to participate?

For matching prioritization, send me a letter of motivation (500 words max.) where you state why you would like to participate and what interests you in cyber resilience to gehrke@sec.in.tum.de. If you have your own topic suggestion, feel free to include it.
Set as **subject: „Seminar CRS Matching“**. Deadline: July 16th, 2024, EOD

Please also briefly state your prior experience with IT security.

I am looking forward to your applications!

Thanks for your interest.

Questions?