Systems Vulnerabilities – Software and Hardware Cybersecurity Concerns

Panel #2

Moderator: Andreas Aßmuth

16th April 2024

Computation World 2024 – Venice, Italy

Definition: Vulnerability

The state or condition of being weak, susceptible to attack or poorly defended.

Saltzer and Schroeder's Design Principles (1975)

- **Fail-safe defaults**

  All access is initially denied; access can only be granted with explicit permission

- **Complete mediation**

  Every access to every object must be checked.

- **Least privilege** (aka "need to know principle")

  Anyone or anything should operate using the least set of privileges necessary to complete the job.

- **Economy of mechanism**

  Keep the design as simple and minimal as possible.

- **Open design**

  Don't keep the design secret!

Saltzer and Schroeder's Design Principles (1975)

- **Fail-safe defaults**

  All access is initially denied; access can only be granted with explicit permission

- **Complete mediation**

  Every access to every object must be checked.

- **Least privilege** (aka "need to know principle")

  Anyone or anything should operate using the least set of privileges necessary to complete the job.

- **Economy of mechanism**

  Keep the design as simple and minimal as possible.

- **Open design**

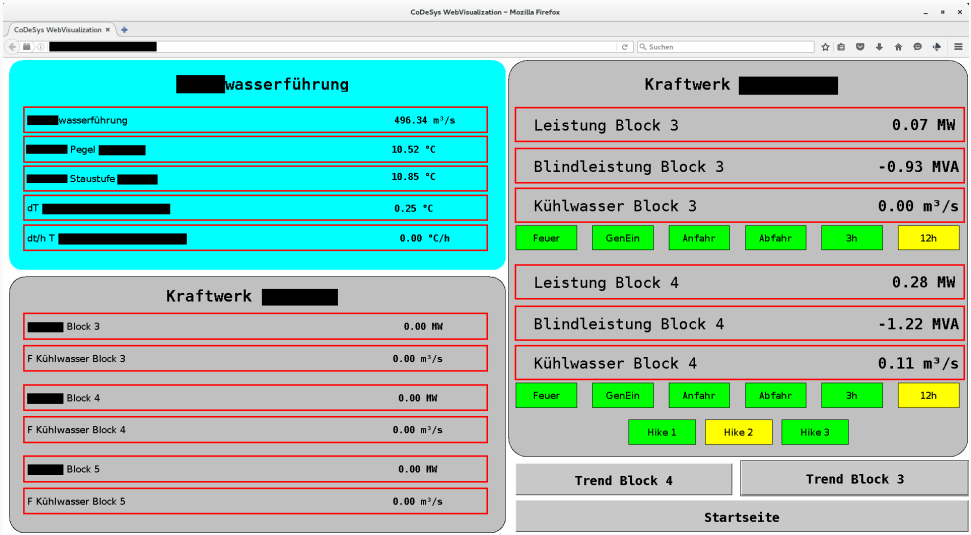
  Don't keep the design secret!

Basically, we know how to design secure systems... at least in theory...

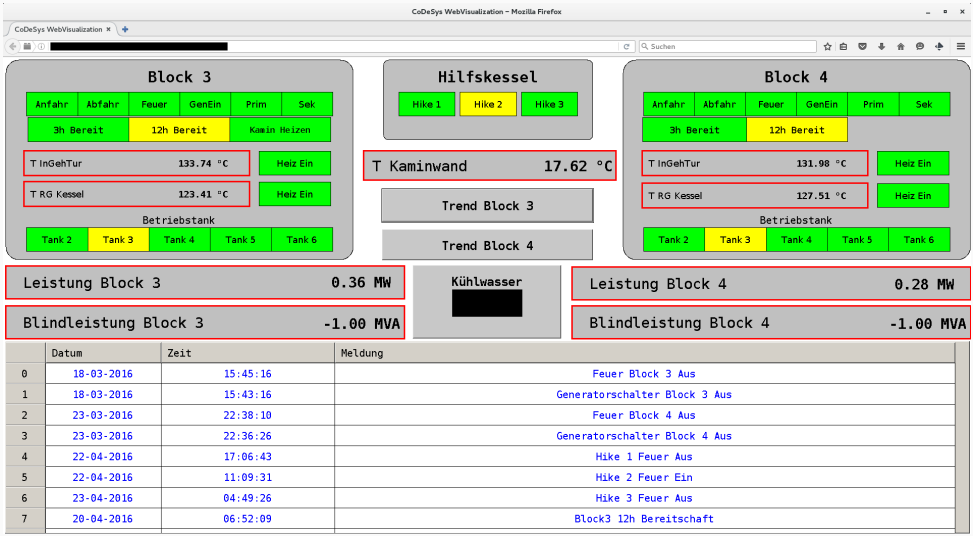
… And in Practice?!

… And in Practice?!

Practice: Power Plant Accessible Over The Internet



Practice: Power Plant Accessible Over The Internet



	Datum	Zeit	Meldung
0	18-03-2016	15:45:16	Feuer Block 3 Aus
1	18-03-2016	15:43:16	Generatorschalter Block 3 Aus
2	23-03-2016	22:38:10	Feuer Block 4 Aus
3	23-03-2016	22:36:26	Generatorschalter Block 4 Aus
4	22-04-2016	17:06:43	Hike 1 Feuer Aus
5	22-04-2016	11:09:31	Hike 2 Feuer Ein
6	23-04-2016	04:49:26	Hike 3 Feuer Aus
7	20-04-2016	06:52:09	Block3 12h Bereitschaft

Contributors

Moderator:

Prof. Dr. Andreas Aßmuth, Ostbayerische Technische Hochschule Amberg-Weiden, Germany

Panelists:

Lieutenant Colonel Dr. Gerhard Schwarz, Bundeswehr (German Armed Forces), Germany

Dr. Mika Helsingius, Finnish Defence Research Agency, Finland

Dr. Steve Chan, VTIRL, VT/I-PAC, USA

Moderator Position – Andreas Aßmuth

- Is “security by design” a goal or a myth?
- Same mistakes again and again... and again...
- Possible reasons: lack of knowledge, ignorance, inability, money, ...?

Moderator Position – Andreas Aßmuth

- Is “security by design” a goal or a myth?
- Same mistakes again and again… and again…
- Possible reasons: lack of knowledge, ignorance, inability, money, …?

Are we (computer scientists, engineers) architects of secure systems,
or merely artists painting over vulnerabilities?

Panelist Position – Gerhard Schwarz

Threats own more than the one “technical dimension”!

- Threads cannot be reduced to only hardware or software security. Therefore, the scope of security awareness has to be larger. It has to be as large as the concerned “operational environment” (OE).
- The OE spans infrastructure, systems and assets, people and knowledge, processes. Even time, e.g., resources for recovery or disaster management. Furthermore in a multi domain perspective.
- Best practice proved to be continuous assessment of threads versus vulnerabilities as well as improvement to the whole OE.
- Multi domain approach challenges the situational awareness towards information sharing and aggregation.

BUNDESWEHR

Panelist Position – Mika Helsingius

- **Warfare, Man-in-the-Loop, Cyberattack**

  AI usage in warfare is difficult to predict. In spite of talks about ethics, there will be autonomous weapons. Attitude towards Ai varies around the world. It is difficult to imagine the level of AI systems at the end of this decade. AGI might be much closer than we have thought just two years ago.

- **Warfare**

  Probably AI will be used first in some very specific places. AI could be used in operational planning, then it is up to the officers to make the final decision. Experiments with games like starcraft etc. have shown that AI can propose very alien but creative and efficient options on how to proceed. AI could help to handle large amounts of situational awareness data. Some actors could use it to combine kinetic, information and cyber operations.

- **Man-in-the-Loop**

  Man in the loop has been hot topic in autonomous systems. There has been a desire to keep man in OODA-decision loop (observe, orient, decide, act), but it might not be realistic. All kind of drones (air, sea, ground) are coming increasingly important, but near the enemy lines electronic warfare is a problem. We will see more full autonomic behavior this year. Earlier simulations with ground systems and airplanes have shown that keeping man in the loop comes with heavy price. Some kind of kill switch might be more realistic solution in the end.

- **Cyberattack**

  Former representative from Finnish F-Secure said this month that the defender has still the advantage. They had used some levels of AI already for 19 years, but malicious actors are just learning. They have seen only 3 malware exploiting LLM:s (for mutations etc.). This might change some day. Modern societies use more and more highly interconnected systems. In the future they might be more under the risk from state level opponents, one must also pay attention to cascading effects. Quantum technology is also developing fast, encryption is under risk and the combination of quantum and AI could lead into some new and interesting developments.

Panelist Position: Cyber Defense of AI Computing Frameworks – Steve Chan

The cyber defense of AI computing frameworks and mitigation against the tampering of ML models is among the latest defender challenges.

The recent compromise of Ray AI framework production clusters illuminates the very real possibilities related to the tampering with and the corrupting of ML models at the training and/or fine-tuning phases. This could have devastating downstream consequences, as this paradigm is on par with hidden defects/failures.

As AI-based cyber attacks rise, the need for enhanced AI-centric defenses also increases so as to better address the increasing cycles of adaptation of AI-based attacks.

Thank you very much for attention!