Comparision of various approaches in Fault-Tolerant and Attack-Resistant system design

Filip Štěpánek, Martin Novotný

Real-world threats

Fault tolerance

Figure: Mother Nature

- “Attacks” randomly
- Safety-critical systems

Attack resistance

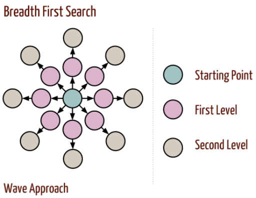
Figure: Evil computer hacker

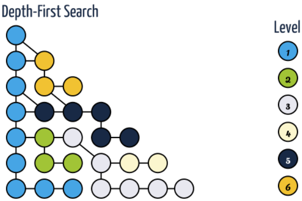
- “Attacks” with intent
- Money, banking, privacy...

Analogy?

Breadth First Search

Depth First Search





- Different approaches (e.g., levels)
  - “Nature” inserts faults from time to time
  - “Hacker” inserts faults to take advantage
- Results may be the same $\implies$ system failure

How to fight hackers and mother nature?

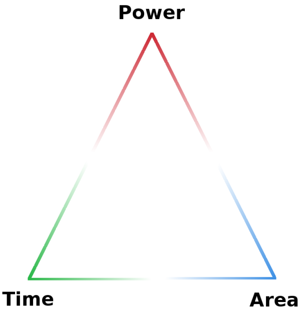
Figure: Mother Nature

Figure: Evil computer hacker

- Fault predictions and experience
- Safety standards and regulations

- Cryptography
- Countering known attacks

System design

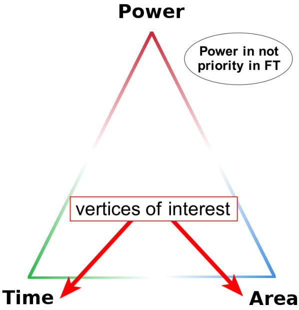


Optimizes:

- *Area*
  (e.g., minimizing the area requirements of the device)
- *Time*
  (e.g., low-latency computation)
- *Power*
  (e.g., minimizing the power consumption)

What about the Fault-tolerant and Attack-resistant systems?

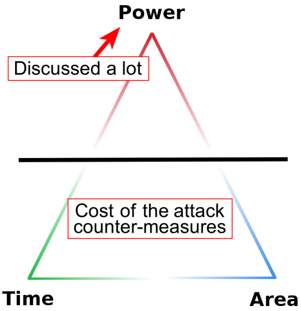
Fault-tolerant systems



Implements redundancy:

- *Area*
  $\Longrightarrow$ physical redundancy (TMR, parity checking)
- *Time*
  $\Longrightarrow$ repeating the operation
- *Power*
  $\Longrightarrow$ increasing power consumption with higher level of redundancy

Attack-resistant systems



Aims at securing the information:

- *Area, Time*
  $\Longrightarrow$ cost of the attack counter-measures
- *Power*
  $\Longrightarrow$ may reveal the processed information

Fault-tolerant and Attack-resistant systems at the same time?

Optical storage media

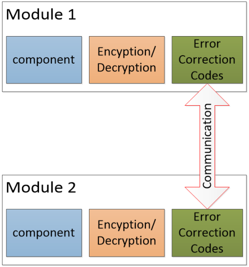
- FT properties:
  uses error-correction codes
  - Picket code
  - RS-PI code
  - RS code
- AR properties:
  protects the intellectual property (DRM)

It is not safety-critical application

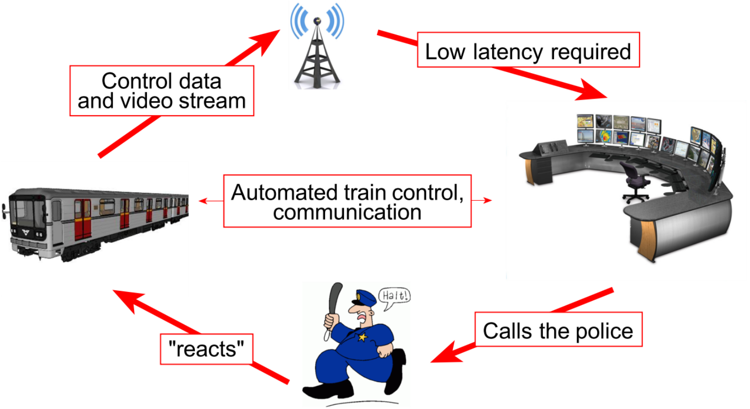
Fault-tolerant and Attack-resistant systems at the same time?

Example – Securing the communication channel

- add cryptographical scheme to the FT system
- $\Longrightarrow$ the cryptographical scheme must satisfy the FT requirements



Proposed encryption module for the Prague subway



Control data and video stream

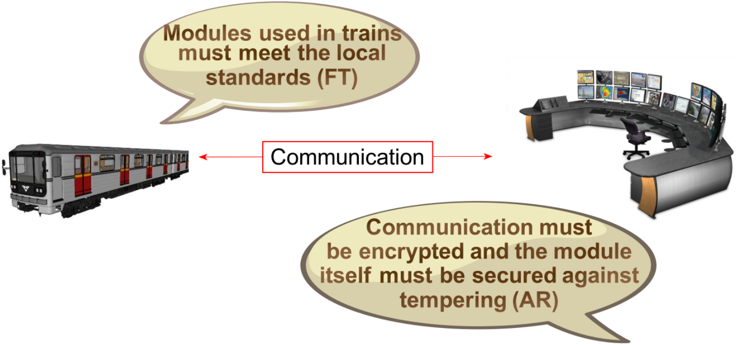
Low latency required

Automated train control, communication

Calls the police

"reacts"

Proposed encryption module for the Prague subway

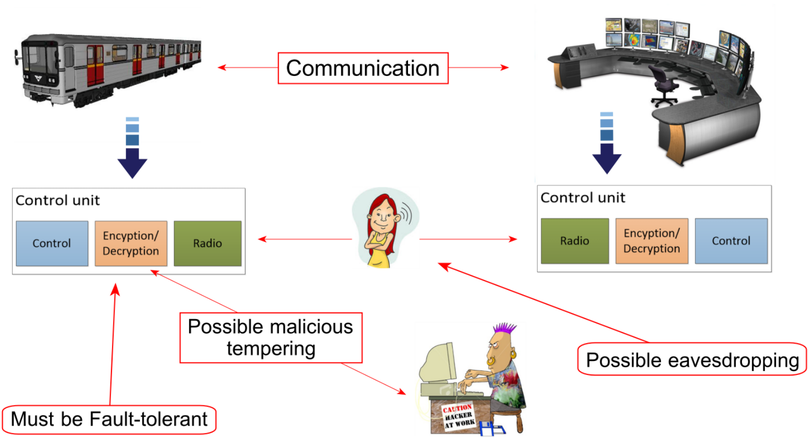


Modules used in trains must meet the local standards (FT)

Communication

Communication must be encrypted and the module itself must be secured against tempering (AR)

Proposed encryption module for the Prague subway



Communication

Control unit

Control

Encyption/ Decryption

Radio

Control unit

Radio

Encyption/ Decryption

Control

Possible malicious tempering

Possible eavesdropping

Must be Fault-tolerant

Proposed encryption module for the Prague subway

Security risks:

- Operation expectancy
- Encryption module might be "acquired"
- Masterkey management

Figure: Opencard

Fault tolerant and attack resistant systems at the same time

Our goals:

- Finding common properties of FT and AR systems
- Evaluation of FT systems using DPA (Evariste II)
- Minimizing the threat of attacks on FT systems