Comparison 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

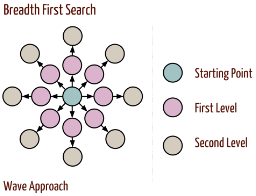
Figure: Evil computer hacker

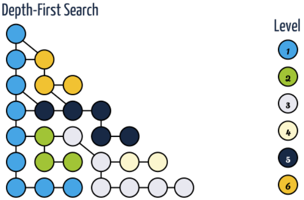
- “Attacks” with intent
- Money, banking, privacy...

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?

Fault tolerance

Figure: Mother Nature

- Fault predictions and experience
- Safety standards and regulations

Attack resistance

Figure: Evil computer hacker

- Cryptography
- Countering known attacks

Fault tolerant and attack resistant systems at the same time

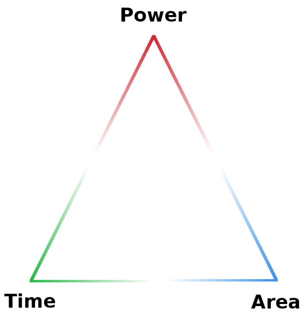
Our goals:

- Finding common properties of FT and AR systems
- Minimizing the threat of attacks on FT systems

Problem:

- Is it possible?
- Do the FT properties compromise the security of the system?

System design

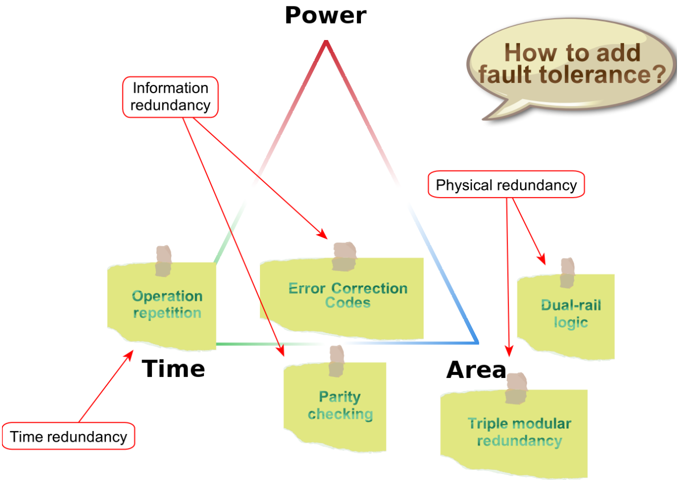


Optimizes:

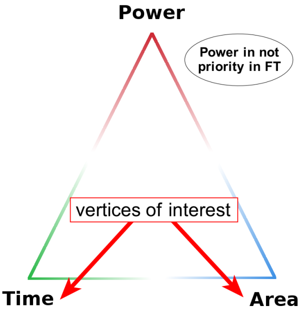
- *Area*
  (e.g., minimizing the area requirements of the device)
- *Time*
  (e.g., low-latency computation)
- *Power*
  (e.g., minimizing the power consumption)

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

Fault-tolerant systems



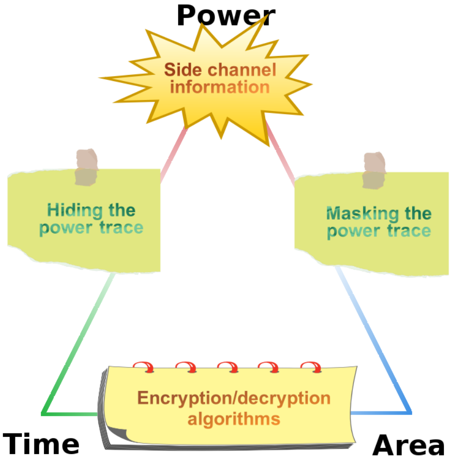
Fault-tolerant systems



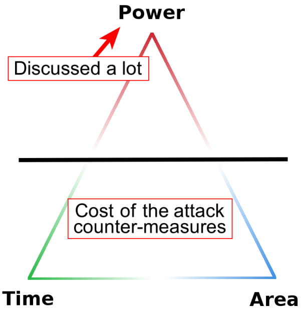
Implements redundancy:

- *Area*
  ⟹ physical redundancy
- *Time*
  ⟹ repeating the operation
- *Power*
  ⟹ power consumption may increase with higher level of redundancy

Attack-resistant systems



Attack-resistant systems



Aims at securing the information:

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

Other properties

Fault tolerance

- High level of observability
- FT systems are designed for long operation periods
- Fault models/predictions operate "above the data"
- Difficult to measure

Attack resistance

- Observability features might be used to the attacker advantage
- Operates until feasible attack is introduced
- Cryptography includes confusion & diffusion features
- Cost of the attack $\Longrightarrow$ security of the system

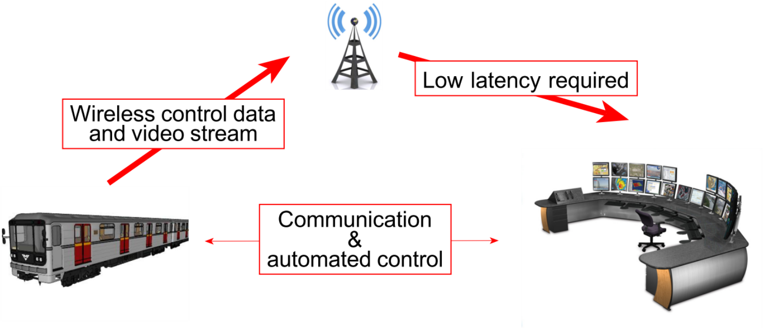
Fault-tolerant and Attack-resistant systems at the same time?

Example – 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

Proposed encryption module for the Prague subway

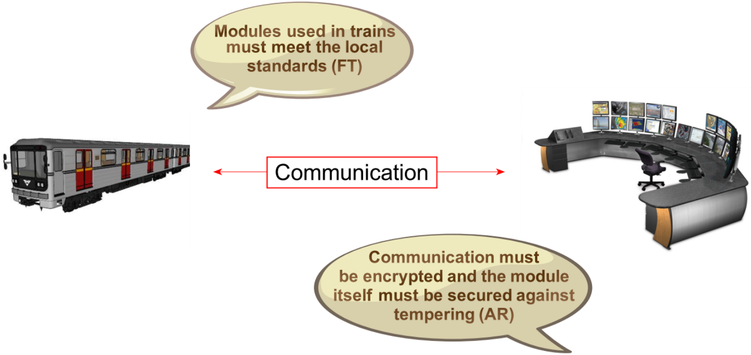


Wireless control data and video stream

Low latency required

Communication & automated control

Proposed encryption module for the Prague subway

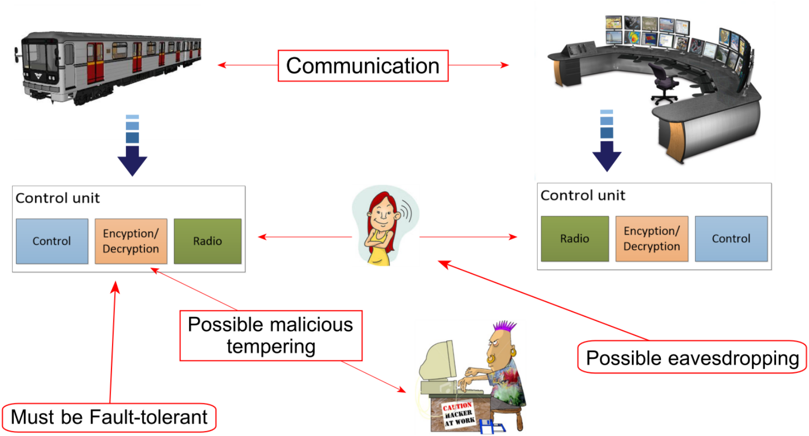


Modules used in trains must meet the local standards (FT)

Communication

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

Proposed encryption module for the Prague subway



Proposed encryption module for the Prague subway

Can the module be stolen?
Operation expectency
!
Masterkey management

Summary

- Basic idea of fault tolerant and attack resistant systems
- Difficulties of implementing both shown by an example

...do you think that the fault tolerance can compromise the attack resistance?