# On the Future of Security in Future Internet

Joint ITG and Euro-NF Workshop
"Visions of Future Generation Networks" - EuroView2009,
Würzburg, July 2009

Peter Schoo

peter.schoo@sit.fraunhofer.de

Fraunhofer-Institute for Secure Information Technology (SIT)
Forschungsbereich *Netzsicherheit und Frühwarnsysteme (NES)*
Parkring 4, 85748 Garching (near Munich), Germany

Fraunhofer SIT

## Outline



Fraunhofer SIT

# What the folks say ...

*Although military security was considered when the Internet architecture was designed, the modern security issues are much broader, encompassing commercial requirements as well. Furthermore, experience has shown that it is di?cult to add security to a protocol suite unless it is built into the architecture from the beginning. (RFC 1287)*



# What the folks say ...

**CC**: Are there basic goals for the development of the Internet?

**BC**: There are so many special interests today that there must be a hundred answers to that question, depending on who you ask. My personal opinion is "the three S's": scaling, stability, security. We need the Internet to scale up to support a human population of ten billion people. We need it to be stable and reliable. We need it to be secure, both to protect privacy and freedom of information, and to minimise abuse.

1

[1] Brian E. Carpenter. University of Auckland, NZ, in Interview *A Dialogue on the Internet*, EATCS: European Assoc. f. Comp. Sci., 2008

## .. and what is basically needed for FI

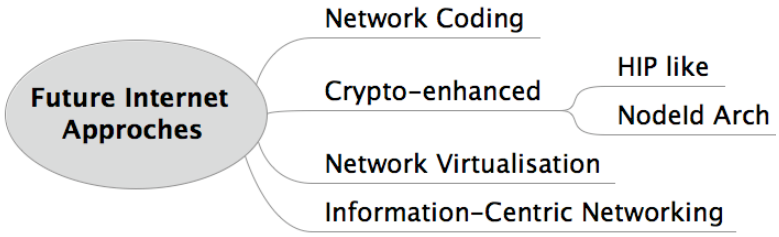
### Main Security Objectives

- Reliable authentication and authorisation
- Communication integrity, or even confidentiality
- Misuse prevention
- Ensuring availability

. . . but how to?



## Security for FI is R&D risk management




- Future Internet is . . .
  - attractive field of brand new ideas (clean slate),
  - creating opportunities to research on innovative component technologies, and
  - sometime showing viable migrations paths.
- IT Security and Privacy
  - is accepted as an important topic, however
  - too often not comprehensively considered and applied.
- Scope here:
  - Overview on instruments to be applied.
  - Architectural security principles relevant for FI R&D.

# Outline





# General Security Design Principles

- Crypto = Security / Kerkhoffs Principle
- Represent Ownership
- Build on reliable/resiliant authentication / binding
- Use detailed authorisation
- Authenticate Communication End Points
- Support communication accountability

## Architecture Design Principles Improving Security

- Hide network topology information
- Central place (for a part of the network) to express policies
- Design infrastructure services preventing misuse
- Implant into Future Internet a key infrastructure
- Minimize architectural dependability



## Protocol Security Design Principles

- Build security deep into the layers
- Include DoS mitigation
- Prefer cryptographic enhanced protocols
- Minimize protocol dependability

# Operation Aspects of Security in FI

- You can't switch off security
- Protect each communication session
- Prepare for exceptional situations
- Consider long lifetime managment



# Outline

## Established Instruments

- What it takes to make security engineering comprehensive
  - Put cryptography in practice
  - Protect data in communication
  - Software is to be secured
  - Hardware security can be deployed
  - Security is an (organisational) process
- Preference is with standard and proven security solutions
  - reduces risks and costs if new solutions aren't actually that good



## Outline

# Issues Finding Security Solutions

## Solution are typically application specific and not tranferable

- New technology → new threats
- Demand is not only technical (e.g. end point autentification)
- There is no calculus like

$$S_1 \textit{ is secure and } S_2 \textit{ is secure} \Rightarrow S_1 \oplus S_2 \textit{ is secure}$$

- Retrofitting brings sub-optimal solutions only

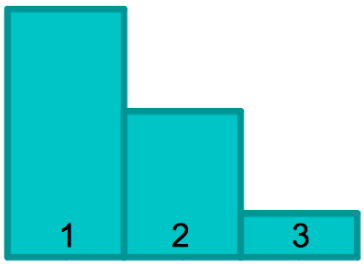
## Consequently, a strategy is required to address security in FI appropriately



# R&D Risk Minimisation Strategy re IT Security

## Minimum: early & preliminary check

better




## Strategy

1. Avoid risks where possible
   - Security principles as didactical instrument
   - Security analysis as decision support
2. Mitigate risks where technically achievable
   - Fraud and information leakage prevention, protocols secured, maintainability achievable, misuse avoidance
   - Instruments are available
3. Decide if remaining risks are bearable

# Thank you !

Questions?