Resilience and Security in European Communication Networks – An Industry perspective

Dr. Claus Gruber (Nokia Siemens Networks)
Dr. Serge Ferrè (Nokia)

Improving Resilience in European e-Communication Networks
ENISA Workshop on Resilience 2008
Brussels, Belgium
November 13, 2008

Greetings from Erkki Kataja

As many of you know, I am not able to participate to this Workshop, but fortunately Claus Gruber from Nokia Siemens Networks and Serge Ferré from Nokia will participate.

We have reviewed these presentations together and support fully Claus and Serge in their presentations.

I have proposed that both Claus and Serge will participate in the Round Table discussion of the last day.

I wish you all very beneficial Workshop, please enjoy it!

Importance of Resilience and Security

eCommunication networks are “Critical Infrastructures”

- More and more business processes, business collaboration and financial transactions are enabled by communication networks
- Other infrastructures (e.g. power supply, traffic, logistics) rely on resilient and secure communication networks
- Communication is central in enabling emergency and disaster reactions
- **Communication networks are "critical infrastructures“**

- **Communications networks are increasingly challenged:**
- Technically:
  Convergence towards one network infrastructure
  Ubiquitous IP-accessibility, complex interdependencies, availability of attack tools
- Exposition: Telecommunication equipment in industry plants, rural / public / residential areas
- Attractiveness: Networks as backbone of business and society, remote information source, and attackable target to attain criminal profit

Resilience and Security

Our customers' perspective

- Resilience and security are considered as **the** most important characteristic of communication systems by our customers
- Requested end-to-end availabilities between 0.999 (3 nines) and 0.99999 (5 nines)
- Reaction times in the order of 50ms to some seconds (dependent on service)
- Immense down-time costs and service level agreement penalty payments

Business operation	Industry cost range per hour downtime (US$)	Average cost per hour of downtime (US$)
Brokerage operations	5.6 to 7.3 million	6.5 million
Credit card / sales authorization	2.2 to 3.1 million	2.6 million
Pay-per-view television	67 000 to 230 000	150 000
Home shopping (TV)	87 000 to 140 000	113 000
Home catalog sales	60 000 to 120 000	90 000
Airline reservation	67 000 to 112 000	89 500
Tele-ticket sales	56 000 to 82 000	69 000
Package shipping	24 000 to 32 000	28 000
ATM fees	12 000 to 17 000	14 500

Estimation of downtime costs. Based on Contingency Planning Research and Gartner/Dataquest.

Resilience and Security
Main Threats

- Main threats for data/communication/service confidentiality, integrity, authenticity, and availability are

Resilience

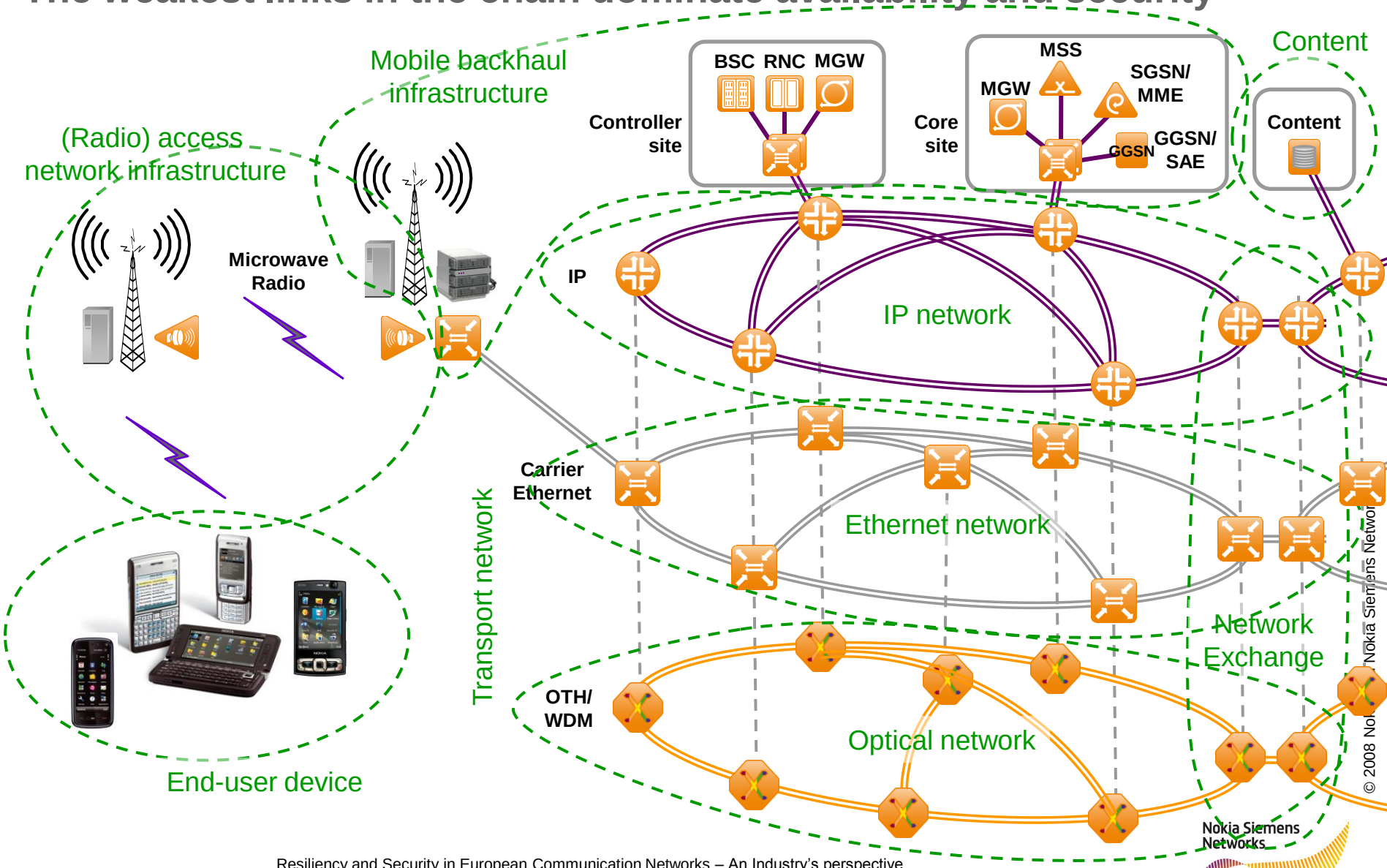
- Link and node failures
  - Excavator damages
  - Power failures
  - Misconfiguration
  - Protocol / software failures
  - Aging of elements
  - Unintentional physical damages
- Catastrophes
  - Earthquakes
  - Floods
  - Hurricanes
  - Infrastructure attacks (9/11)
- Intentional failures
  - Sabotage

Security

- Motivation:
  - Profitable use cases for organized crime
  - Software vulnerabilities/faults
  - Malicious code distribution (trojans, viruses)
  - Managed networks of manipulated devices (botnets)
  - Insider attacks and
  - Easy to use attacking toolkits
- Information gathering
  - User credentials, business information, eSpionage
- Information manipulation
- Identity spoofing
  - Misuse of service (SPAM / SPIT)
  - Unauthorized use of service (online banking)
- (Distributed) Denial of Service and blackmailing
- Theft and sabotage
  - Threatened reputation

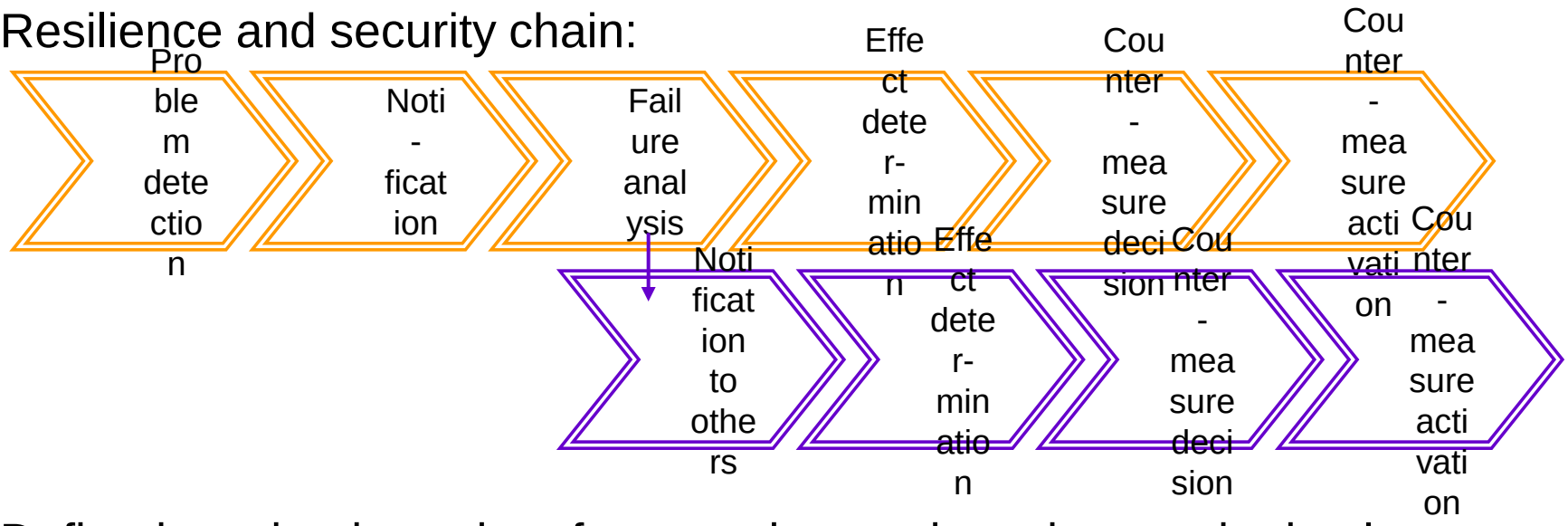
Resilience and Security

The weakest links in the chain dominate availability and security



Resilience and Security
General Approaches

- Resilience and security chain:



- Defined mechanisms, interfaces and procedures have to be in place

Analysis of the most probable threats
Analysis of effects and affected systems

Reliable/secure design of hardware and software

Assured methods to react quickly on most probable failures

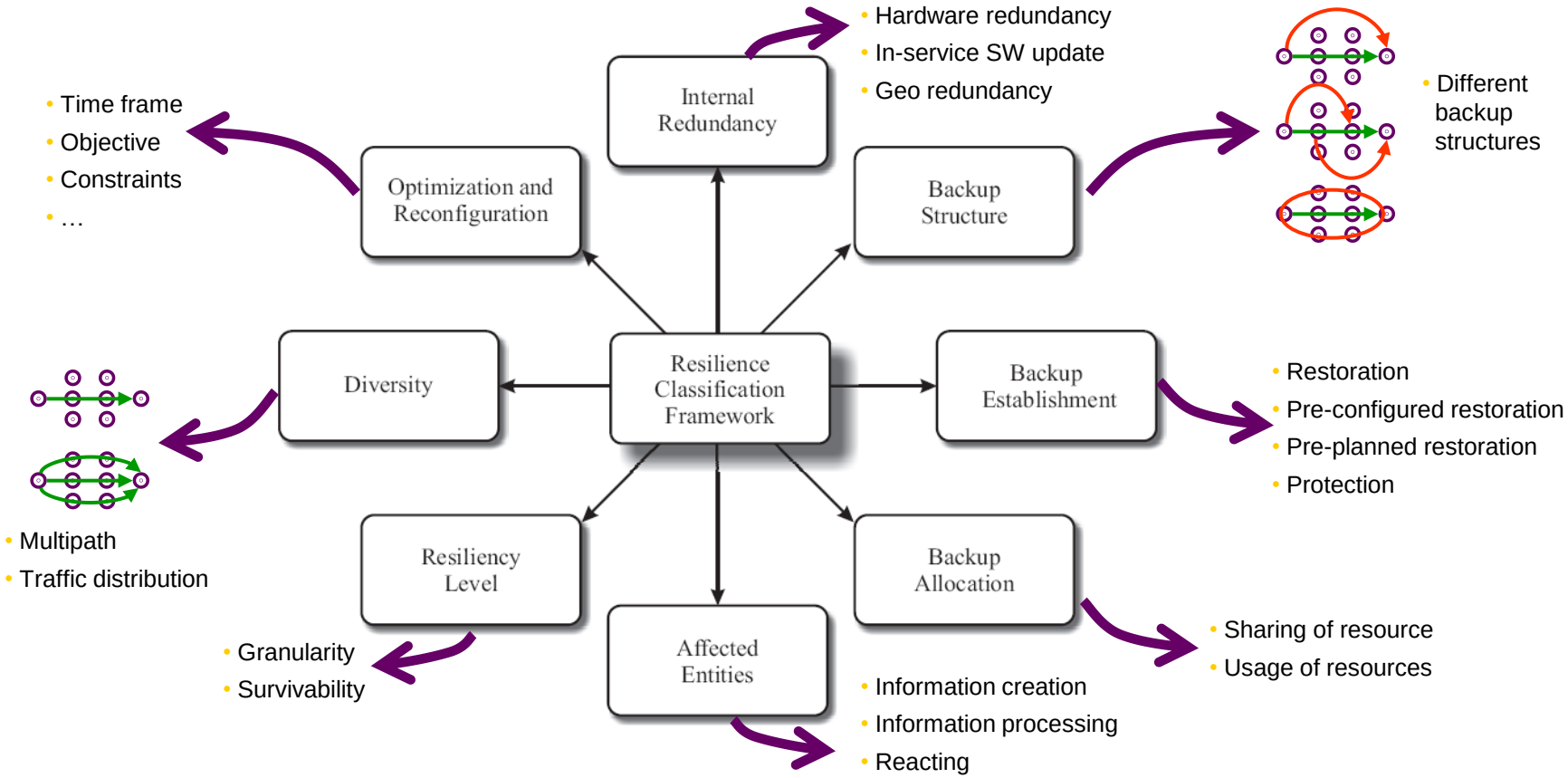
Methods and best practices to react quickly on other failure situations

Resilience in Transport Networks

Resilience Classification

Many possibilities exist to increase the end-to-end availability

- Resilience is a combination of eight main characteristics (*)
- Only a good combination enables high end-to-end availability

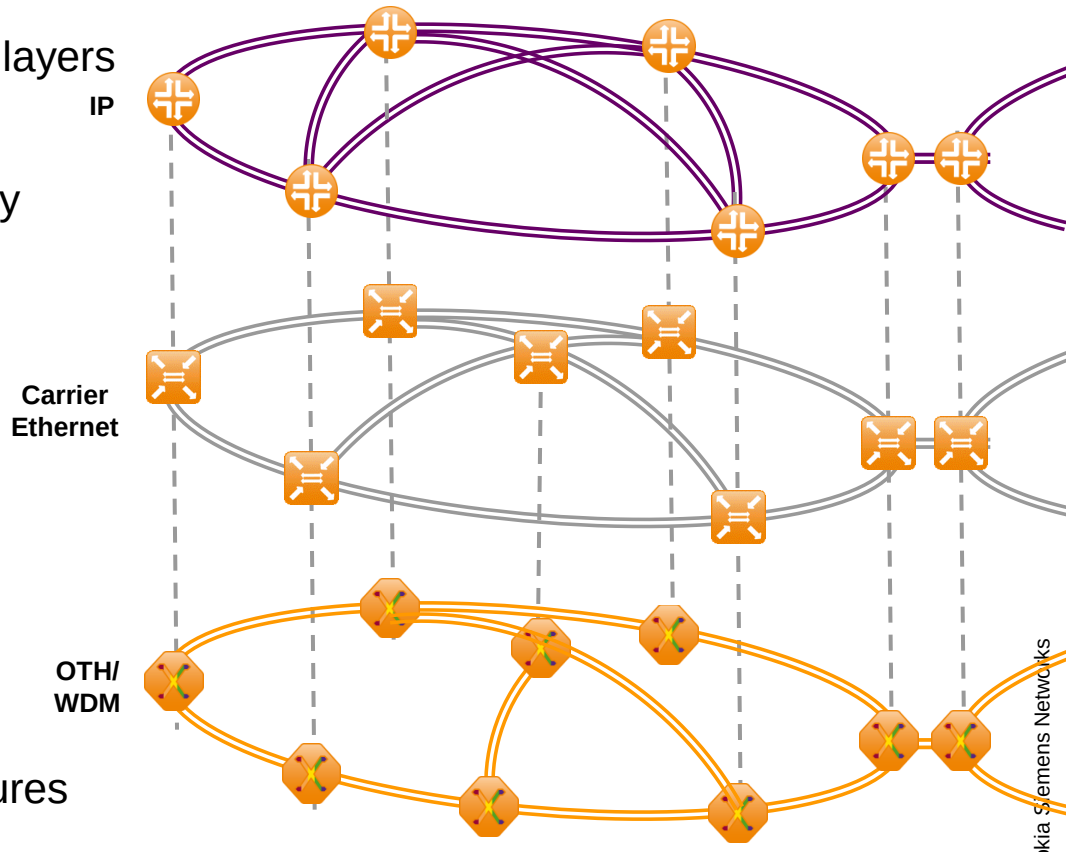


* taken from: Claus G. Gruber, “Design and Optimization of Resilient Multipath Networks”, 2006

Multilayer Resilience

Transport Network View

- Resilience mechanisms may exist on all layers
- A consideration of resilience on only one layer (e.g. IP) may be insufficient for high end-to-end availability
  - Shared risk group (SRG)
  - Reaction times
- Instead, a joint modeling and reaction is needed
  - Multilayer resilience
- Preventive and (automated) reactive mechanisms are essential
- Effects, countermeasures and coordination with other affected systems is needed
  - Interconnection of resilience mechanisms of all critical infrastructures

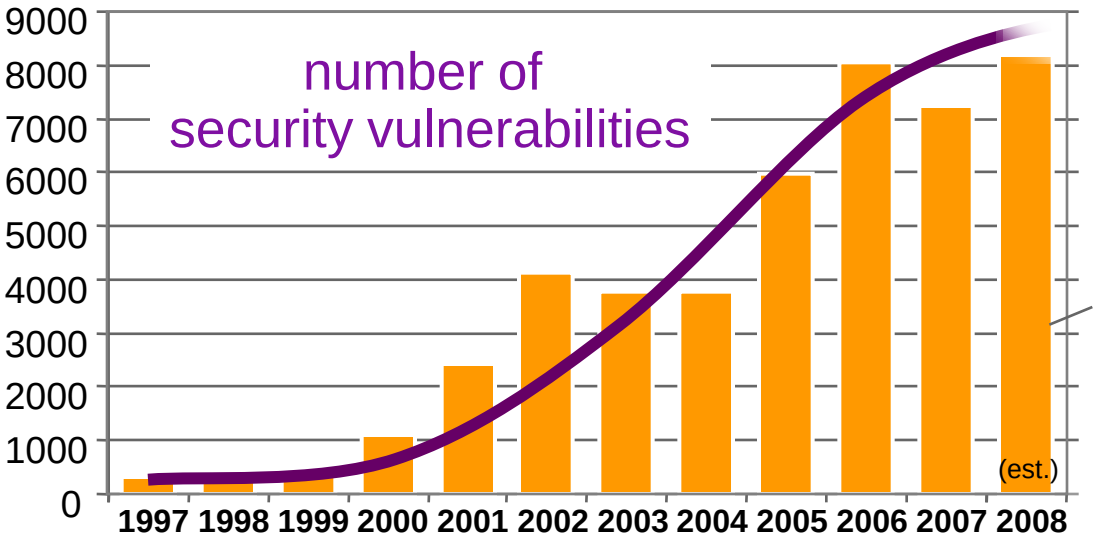


Nokia Siemens Networks assures best-in-class network resilience by assuring high component availability in combination with preventive and reactive resilience mechanisms

Security in Transport Networks

Security

Threats: Number and quality of security vulnerabilities

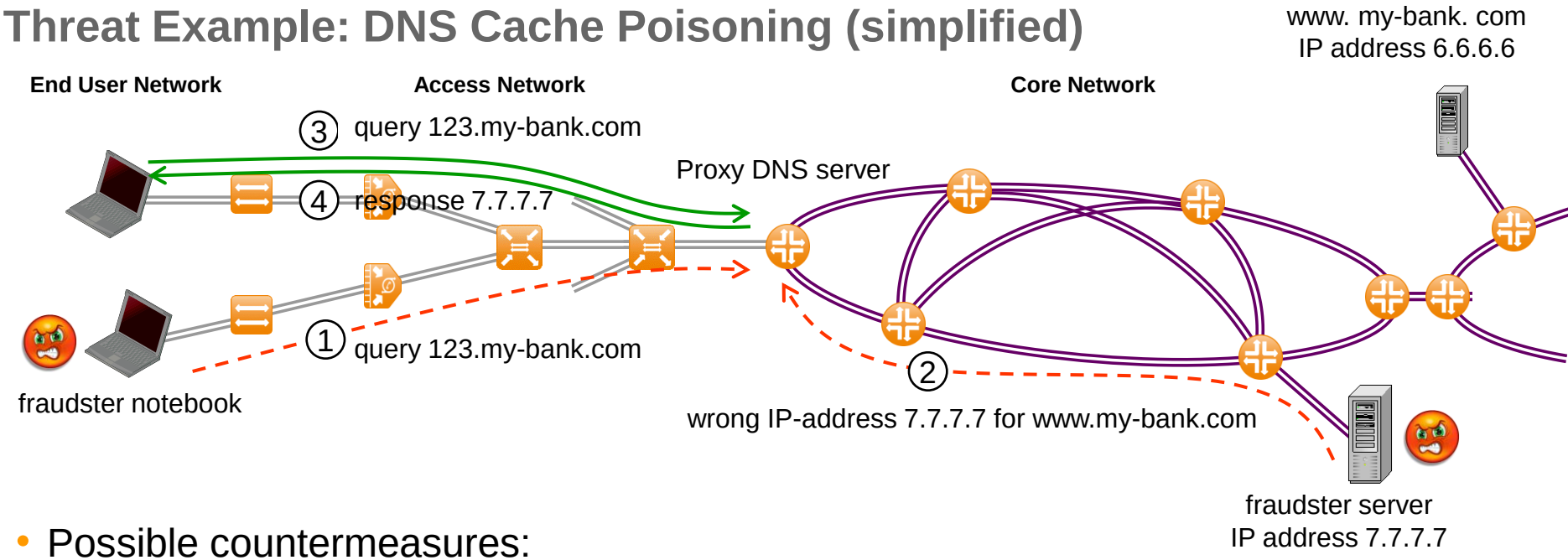


Source: CERT Coordination Center® Carnegie Mellon University

- Number of security vulnerabilities has grown over the last years
- Main trend is the change of the „nature“ / quality of the attacks
- More and more criminal background, e.g. botnets, phishing attacks, fraud, spying, blackmailing
- Some areas still with exponential growth e.g. new malicious code threats/Trojans, phishing
- Example for new quality of attacks: „Cyber-Attacks“ in Estonia, 2007
  (broad attacks on organizations critical for the national infrastructure),
  http://en.wikipedia.org/wiki/Estonian_Cyberwar

Security

Threat Example: DNS Cache Poisoning (simplified)

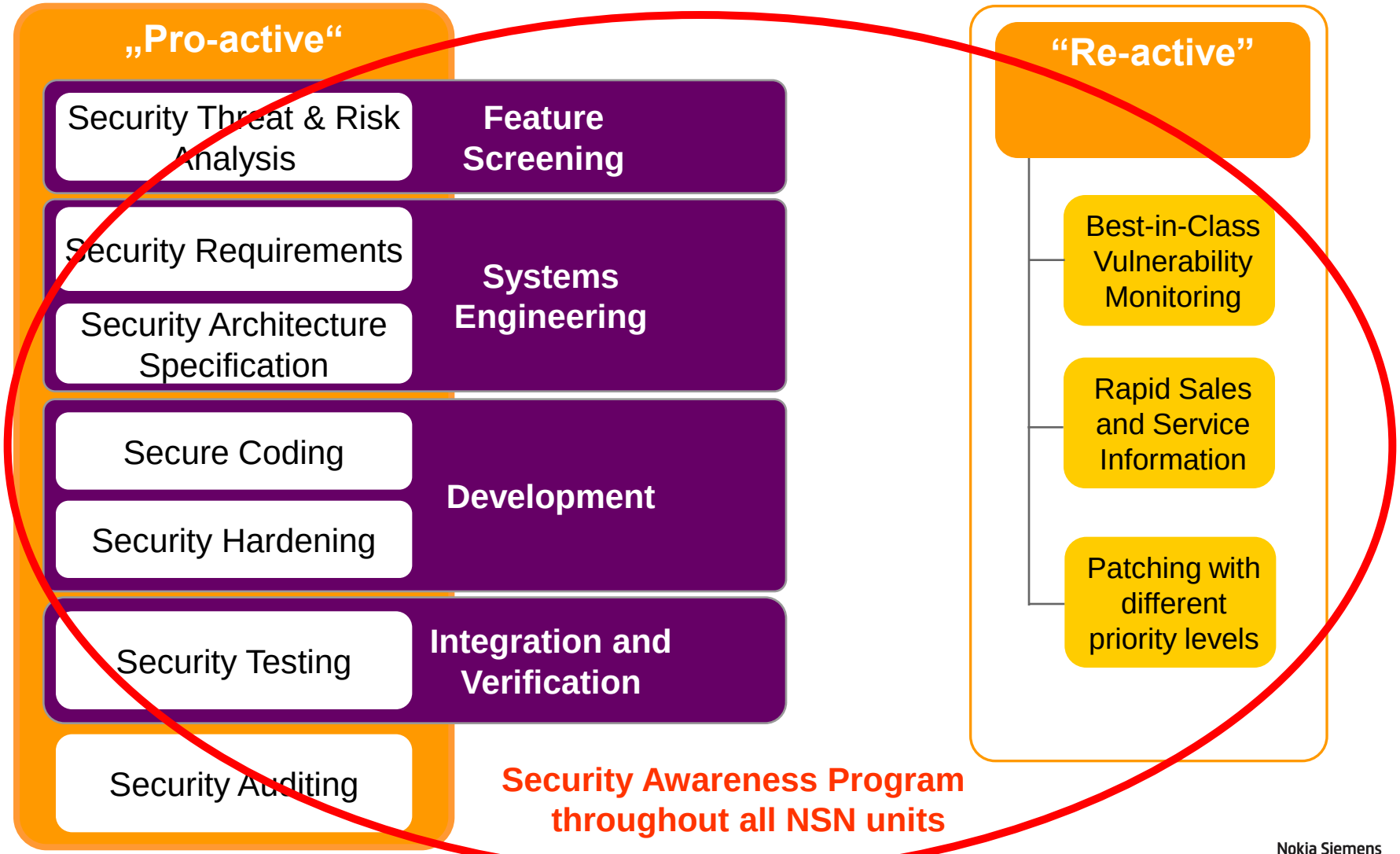


- Possible countermeasures:
  - DNS servers: randomize source port and transaction IDs in DNS requests (patch reported to be installed in most DNS servers)
    → much more difficult for fraudster to fake
  - Network: limit, check, restrict access to proxy DNS server
    → block remote fraudsters
  - Long term: implement “DNSSEC”
    → authentication and data integrity for DNS)
    (First steps towards DNSSEC already announced by US Government, proposed by RIPE)

Security
- Essential and applicable on all levels

- Product level:
  - End-user device
    - Information security
  - Communication product
    - Information and transport security (e.g. DNS-SEC)
- Configuration and management level
  - Integrity protection for devices, network components, and software
  - Standardized processes, encrypted configuration (e.g. SSH)
  - Configuration log
- Networking level
  - Monitoring (e.g. identification of denial of service attacks)
  - Reaction (e.g. automatic activation of filters)
- Process level
  - Consulting and auditing
  - Measures to increase security awareness

Nokia Siemens Network's Security Processes in Product Development

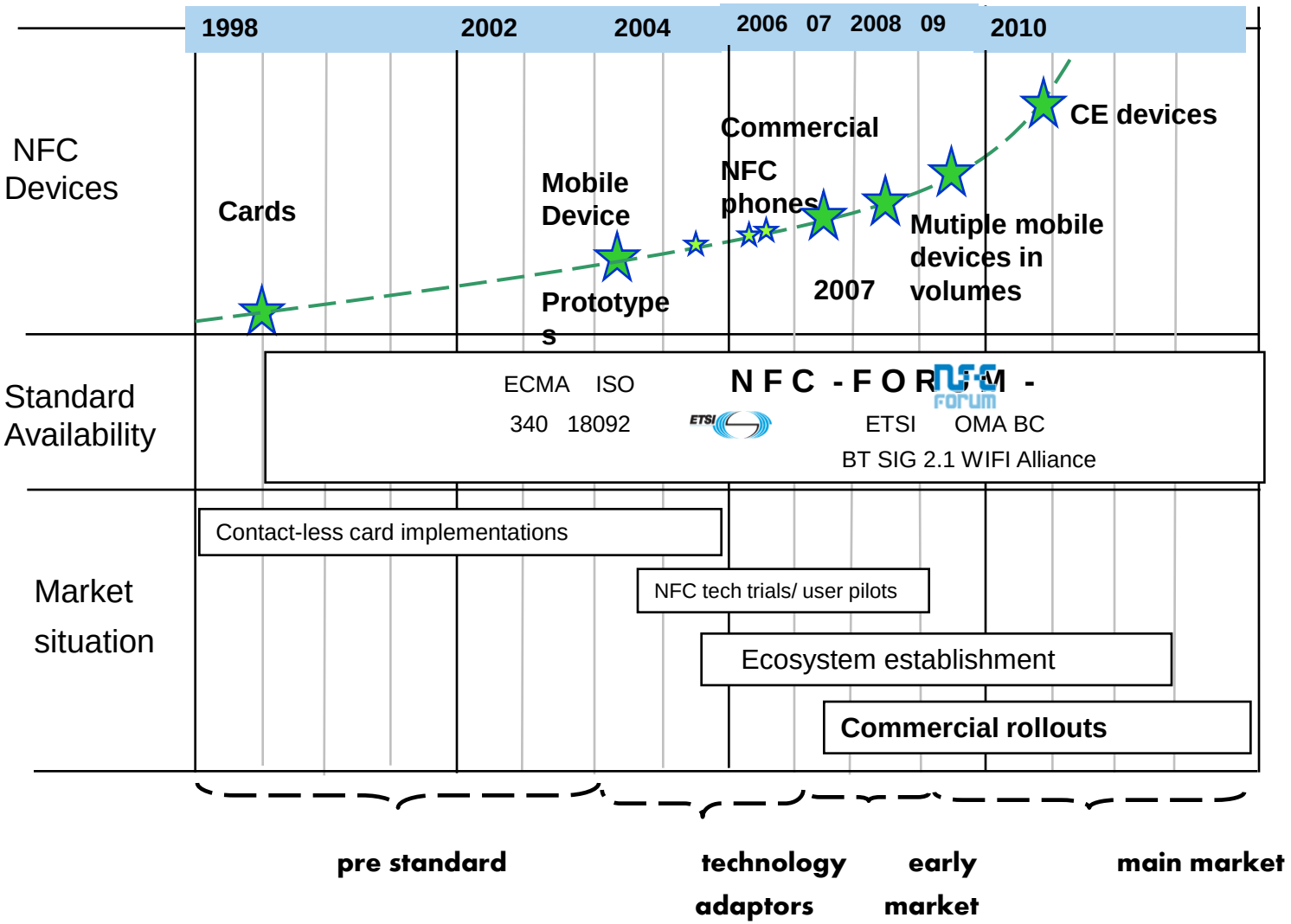


Near Field Communication

What is Near Field Communication (NFC)

- NFC is a short-range wireless communication technology - enables the exchange of data over a few centimeters
- Share media and contacts simply by touching your mobiles together
- Leave your wallet at home and pay for goods and travel tickets using your Nokia mobile

NFC evolution

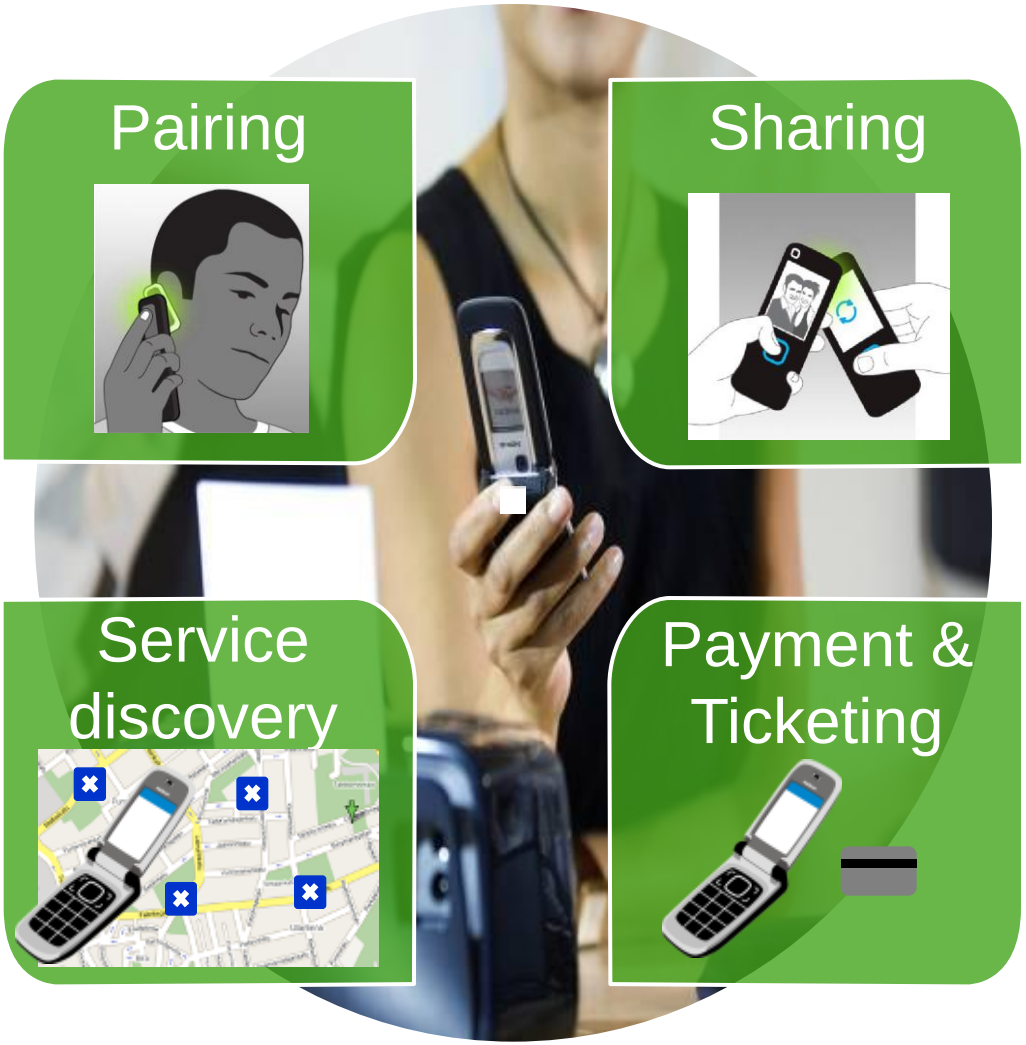


NFC Key Use Cases

Pair and connect easily with other devices (speakers, headsets…)

Initiate applications by touching a tag

Get information by touching smart posters



Share between two devices

Your phone is your credit card and or Transit/Travel card

Nokia experience, extract from published projects

• Rabo, Roda JC,	Netherlands	**Payment**
• Oulu	Finland	City services
• Mobilkom	Austria	**Transport** and **payment**
• Helsinki airport	Finland	Business solution
• Amsterdam, JCB	Netherlands	**Payment**
• Frankfurt, RMV	Germany	**Transport**, consumer services
• Nedap	Netherlands	Healthcare business solution
• Manchester City Football	UK	Stadium
• Biffa	UK	Asset management
• London, O2, TFL, Visa	UK	**Payment**, **transport** and services
• BBVA	Spain	**Payment**
• SBI	India	**Payment**
• Beijing, Xiamen, Guangzhou	China	**Payment** and **transport**
• Chunghwa	Taiwan	**Payment** and **transport**
• KL, May Bank	Malaysia	**Payment**, **transport** and SD
• Atlanta, Chase, NXP	USA	**Payment**, **ticketing**, consumer services
• 7 Eleven, PeopleBank	USA	**Payment**
• Philadelphia, Bank of America	USA	**Payment**
• New York, Citibank	USA	**Payment**, **ticketing**, SD
• HSBC	USA	**Payment**
• Wells Fargo	USA	**Payment**
• Washington, US Bank	USA	**Payment** and more…….

Learning´s from NFC projects

Market acceptance

- More than 80% of consumers like the NFC payment and ticketing concept
- Payment and Transit applications are the No. 1 motivation factor for purchasing NFC devices with 86% rate

Acceptance

- Transit system have contactless infrastructure and large user base
- Contact-less acceptance POS availability is key
- Payment and Transport transactions will merge

Service offering and customer care process

- Transport and Banking applications must be Multi Operator
- Easy of use in care, both issuing and replacement is key.
- Value added offerings are must, payment alone does not pull it off

Nokia is the NFC market leader

- 2004, Nokia together with Philips and Sony announced the founding of **NFC Forum**.
- Nokia and Giesecke & Devrient formed a JV, **Venyon,** to provide services over-the-air to the NFC ecosystem
- Nokia invested in **ViVOtech**, the market leader in Contactless Payment readers & infrastructure
- Nokia invested in **Inside Contactless,** the market leading chip manufacturer in contactless payment
- **Nokia 6131 NFC** world's first phone with NFC integrated technology shipping since 05/2007
- An extensive participation in **NFC trials and commercial projects in Europe, North America and Asia**

Today, more than 160 NFC Forum Member companies

NFC Joint Venture

Contactless Payment Leader

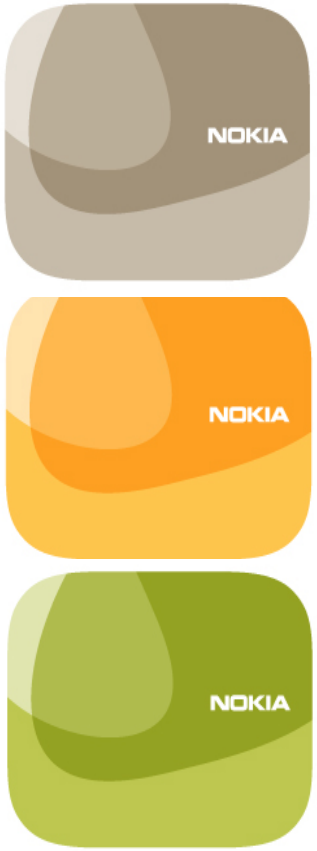
Leading Chip Manufacturer for Contactless Payment

Nokia 6131 NFC- World's first fully integrated NFC phone

Nokia executed a large number of NFC trials

Nokia Already shipped 3 NFC devices

Now taking the next step: Introducing the Nokia 6212



The best ever user experience

3G NFC enabled phone for Easy Pairing & Sharing, Service Discovery, Payment and Ticketing with integrated secure chip

NOKIA

Conclusion

- Resiliency and security are of utmost importance for our society
- Telecommunications networks are part of "critical infrastructures“
- Resilience and security measures have to be taken at all levels
- Cooperation of software vendors, hardware vendors, providers, and regulators is needed
- Many and sufficient concepts and solutions exist today, the challenge is cost!
- Interdependency to other infrastructures have to be taken into account
  - Leverage the possibilities of a reliable communication network

Nokia and Nokia Siemens Networks provide the full range of resilience and security services by providing own systems and integrating best-in class OEM / 3rd party products

Resiliency and Security in European Communication Networks – An Industry's perspective

Dr. Claus Gruber (Nokia Siemens Networks)
Dr. Serge Ferrè (Nokia)

Improving Resilience in European e-Communication Networks
ENISA Workshop on Resilience 2008
Brussels, Belgium
12-13 November 2008