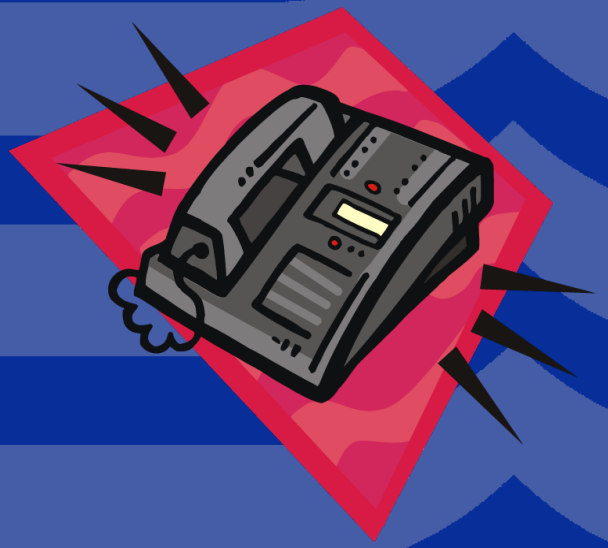
Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Do we need Security Research for VoIP products?

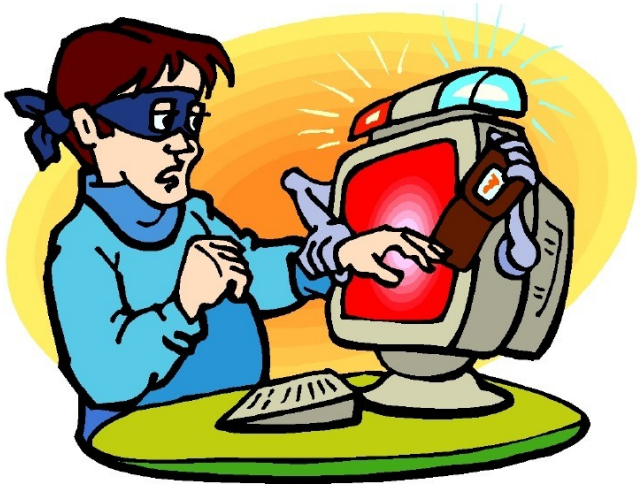
Wolfgang Leister
Chief Research Scientist
Norsk Regnesentral

October, 5th, 2006

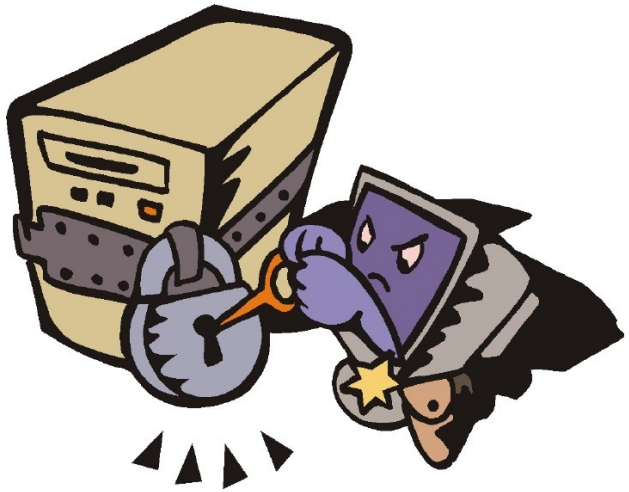


EUX VoIP Conference, Vaasa

NR work areas – ICT



- Security
  - Privacy
  - Digital forensics
  - Risk management
  - Public Key Infrastructure (PKI)
  - Digital Rights Management (DRM)
  - Mandatory Access Control



NR work areas – ICT (cont.)

- Multimedia multichannel
  - Video/Audio Streaming
  - Multimedia Metadata & Databases
  - Mobility
  - Games
  - Digital TV
  - Multimedia e-learning tools

Ill. Ella Okstad

Security and VoIP

- Primary Goals
  - Confidentiality
  - Integrity
  - Availability
- Secondary Goals
  - Accountability
  - Authenticity
  - Identity
  - Privacy
- Standard IEC/ISO 17799

- Two important reports:
  - BSI: VoIPSEC – Studie zur Sicherheit von Voice over Internet Protocol

Bundesamt für Sicherheit in der Informationstechnik

  - NIST: Security Considerations for Voice Over IP Systems

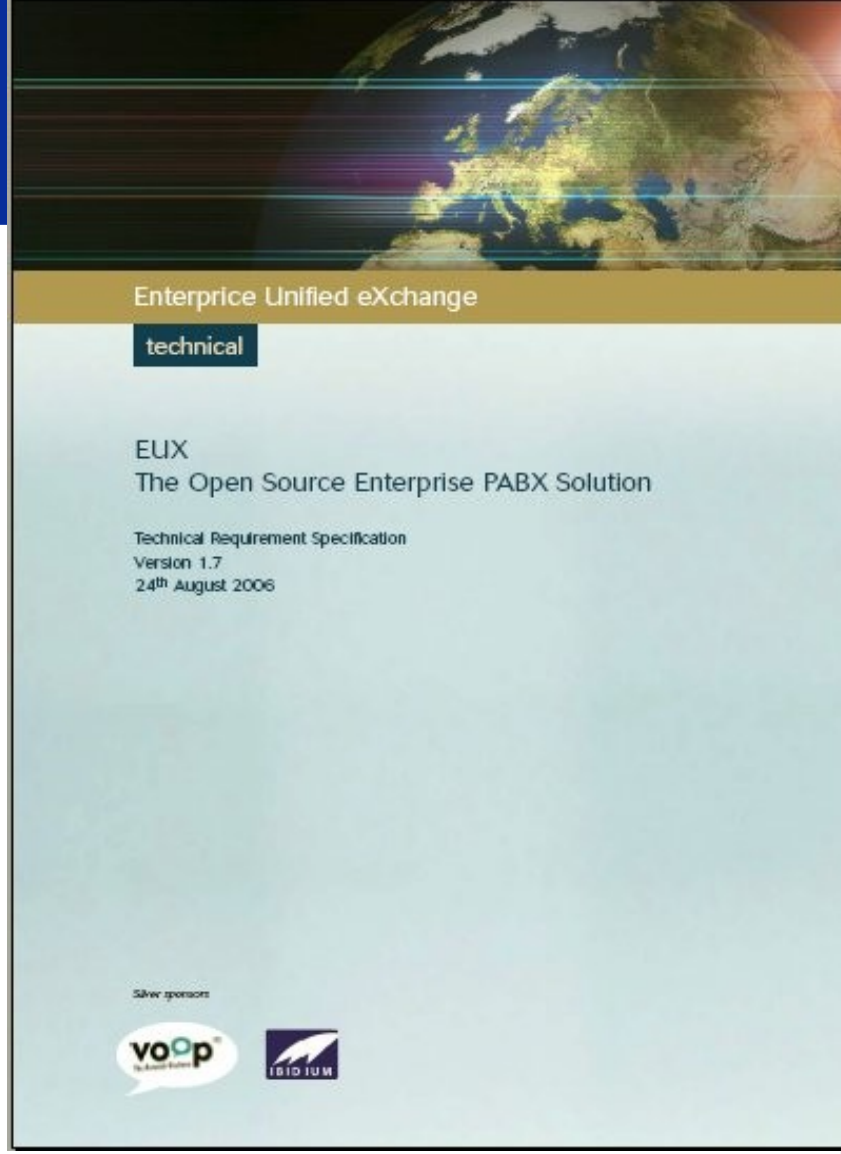
NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Security and VoIP

- Is Bob talking to who he's thinking he talks with?
- Is charging being done correctly?
- Can incoming calls be blocked selectively (avoiding spamming)?
- Can someone listen to the call?
- Can Trudy find out who Alice calls (or who is calling Alice)?
- Can Trudy detect where Alice is (location privacy)?
- Is the exchange of rich media associated to the call secure?
- Is the system available when Bob needs it?
- Can Alice make anonymous calls?

EUX2010 and Security

- Security must involve architecture
  - layers
  - subsystems
  - protocols
- Document focuses on functionality and technical solutions
- Term Security is mentioned seven times, only in connection with a «security analysis»
- Define EUX2010SEC project !



Security Problem Areas

- Integrity of VoIP components
- Integrity and Authenticity of voice data
- Integrity and Authenticity of signaling data
  - Identity of caller / callee
  - Time / date of call
  - Registration and localization information
  - State of terminal / state of call
- Integrity and Authenticity of rich data (multimedia)
- Confidentiality / Privacy
- Availability – QoS (Quality of Service)

Attacks to VoIP systems

- Network
  - Network/Port Scans
  - Spoofing
  - Replay
  - DoS (Denial of Service)
- Infrastructure
  - Physical access
  - Layer 2 (MAC spoofing, MAC flooding, ARP spoofing, STP, VLAN)
  - Layer 3 (IP spoofing, ICMP Redirect, IRDP spoofing, ...)
  - Layer 4 (SYN, LAND flood)
- Protocols towards PSTN
  - RTP
  - SRTP
  - H.323
  - SIP
  - MGCP / MEGACO
  - SCCP
- VoIP Middleware
- VoIP Terminals
- QoS
- Power Supply
- ...

WLAN (802.11) and VoIP

- Often used in home- and office use
- Easy installation without cable
- Security mechanisms
  - WPA / WPA2
  - MAC ACL
  - WEP (wired equivalent privacy)
- QoS / Performance problems
- WLAN can be problem for VoIP

What to do about Security?

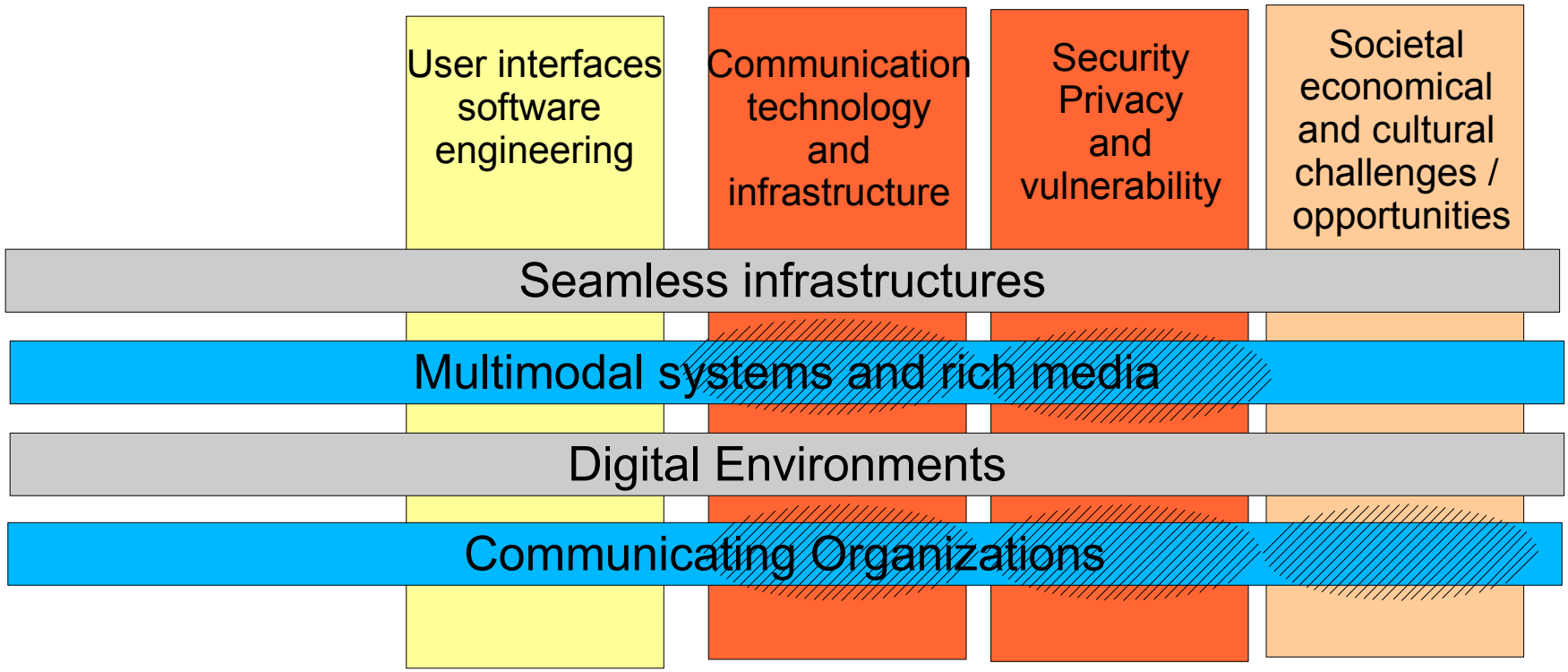
- Network design
- Power supply
- Separate data and VoIP
- Secure Network against div. attacks
- Redundancy
- QoS
- Firewalls, NAT
- Backup
- Protocols
  - Threat: Interruption / disturbance of service
  - Threat: eavesdropping, manipulation of media streams
  - Threat: manipulation of signaling and fraud

EUX2010SEC - Goals

- **Development of a security framework for EUX2010.** The security framework will address requirements for security, privacy, billing, regulatory conformance, etc.
- **Development of tools for evaluating the security for VoIP / PABX solutions and installations.** Security is tailored to each PABX installation; therefore a set of comprehensible and generic rules, policies, and tools will be given to the installation consultants. Scenarios for installation.
- **Multimedia / enriched media and security.** Other data types than pure voice data are used (files, chat, fax, images, films, multimedia, etc.) – convergence of VoIP and multimedia.
- **Contributions to improve confidence in secure open source products in VoIP market segments.** The reputation of open source products in the market is often questionable. By providing an (publicly) open and provable security framework for VoIP the position of open source products will be strengthened.

VERDIKT-program call

- From the program call;
  - One row should preferably match more than one column:



EUX2010SEC – Project Setup

- Research Partners – get funding for research from NFR, perform research for the consortium, one international research partner is very positive!
- Industry partners – participate with their use of resources or with €€
- Public sector – can participate and be end user of product – use of resources does not count
- Non-Norwegian companies can participate
- One Industry partner is applicant / contract partner to NFR
- Project Manager appointed by consortium

EUX2010SEC – Project Setup

- Research Partners:
  - Norsk Regnesentral
  - UNU-MERIT (NL)
- Budget:
  - NFR funds ca. 30% of total budget, if project is funded
  - 70% must be funded by partners, in effort or in €€
  - Effort calculation: each employee with hourly rate of 1.6 ‰ of nominal fee per year.
  - NFR pays to contract partner in advance 3 times a year. Contract partner is responsible for accounting. Contract partner pays research partners.
  - Duration: 3 years

EUX2010SEC Project Setup

- Example:
- 3 years, budget per year 5 mill NOK
- Research: 1.5 mill NOK (NR: 1.15, UNU: 0.35)
- Industry: 3.4 mill NOK
  - Company 1: 1400 hrs / 800 NOK = 1120 kNOK
  - Company 2: 900 hrs / 600 NOK = 540 kNOK
  - Company ...: ... hrs / ... NOK = ... kNOK
- Other funding: 100000 NOK