

VoIP Security Survey

Are you planning a VoIP project? Are you an industrial vendor of VoIP equipment? Does your business or organization have confidential material, or strong availability needs concerning telephony?

Then you might be interested in the EUX2010Sec security survey.

The project aims at building archetypical security profiles for real-world VoIP security needs and their corresponding implementation into a VoIP infrastructure. For this purpose, we seek users, vendors and equipment manufacturers for VoIP in all its possible applications.

As a participant in our interview-style survey, you will spend up to two hours with our experts. The interview will be a bilateral discussion of various requirements, security threats and countermeasures in VoIP as they relate to your specific application area. In return, you will receive the survey results, and possibly some feedback from our experts. Please contact the project team if you are interested in VoIP security requirements.

Islanders



Archipelagos



Fortress



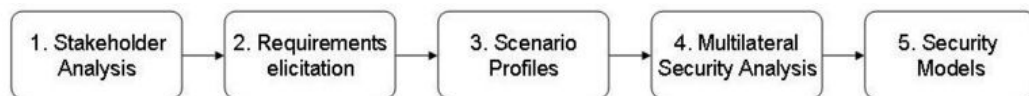
Some of EUX2010Sec's security profiles

NR  **Norsk Regnesentral**
NORWEGIAN COMPUTING CENTER

Lothar Fritsch
forsker · research scientist
DART · department of applied
research in information technology

dir. phone: (+47) 22 85 26 03
mob. phone: (+47) 968 85 758
Lothar.Fritsch@nr.no

Norsk Regnesentral · Norwegian Computing Center phone: (+47) 22 85 25 00
Gaustadalleen 23, P.O. Box 114, Blindern NO-0314 Oslo, Norway fax: (+47) 22 69 76 60
www.nr.no · nr@nr.no



Methodology

The security model activity carries out in consecutive steps. Various VoIP project partners and their customers are contacted.

- **Stakeholder Analysis:** The stakeholders will be found, and their main interests in the VoIP market be captured by means of a stakeholder. Further information is on the VoIP Stakeholder Analysis page.
- **Requirements Elicitation:** The stakeholders will be interviewed concerning their usage scenarios and requirements concerning VoIP security.
 - The interviews will collect anecdoteical accounts of problems and requirements.
 - The interviewees will be presented with scenarios and use cases to single out their typical scenarios.
- **Scenario Profiles:** From the steps above, one or more profiles for typical VoIP usage scenarios will be generated. The profiles should create the basis for further analysis, testbed creation, and verification activities. There is a first version of VoIP scenario profiles.
 - A profile is based on a use case description.
 - A profile contains a description of security, reliability, quality-of-service and scalability needs
- **Multilateral Security Analysis:** For each of the profiles, a multilateral security analysis is performed to ensure that all stakeholders' views and needs are contained. Its goal is to gather security and privacy requirements for the infrastructure in question, and to make suggestions for improvement of the requirements specification. Multilateral security analysis takes into account all stakeholder's requirements relevant to security and privacy issues.
- **Security Models:** Finally, security models will be developed for the VoIP profiles. A security model is based on security goals, and a trust model. A security model contains a description of:
 - Subjects
 - Objects
 - Rules and policies
 - Security functions

More information on the EUX2010Sec project is available as an article with IEEE (available on request from the authors):

Fritsch, Lothar; Groven, Arne-Kristian; Strand, Lars: **A holistic approach to Open-Source VoIP security: Preliminary results from the EUX2010SEC project** (Best Paper Award). The Eighth International Conference on Networks (ICN 2009), Proceedings of the The Eighth International Conference on Networks (ICN) 2009, Bestak, Robert; George, Laurent; Zaborovsky, Vladimir S., Dini, Cosmin, IEEE Computer Society, ISBN 978-0-7695-3552-4/09, pp. 275-280, March 05, 2009.

NR Norsk Regnesentral
 www.nr.no


Security Requirements and Security Modeling for VoIP Systems

Lothar Fritsch
 24-Jun-2008, Oslo

EUX2010Sec project
<http://eux2010sec.nr.no>



NR Norsk Regnesentral
 www.nr.no



NR Norsk Regnesentral
 www.nr.no

Designing Security

- ▶ Security can be reached in many ways
 - Removal of threats & vulnerabilities
 - Protection of the infrastructure
 - Insurance
 - 24/7 maintenance and supervision
- ▶ In Computer Research, there is a distinction between safety (reliability) of a system, and information security.
 - Power failure, broken cable, flood, unreliable staff, scalability issues
 - Hacking, billing fraud, data protection & privacy issues, SPAM & SPIT

Information security

- ▶ Information security looks at four properties of information in systems:
 - **integrity**: information is not modified
 - **confidentiality**: secret information stays secret
 - **accountability**: actions are authorized, or can be accounted for
 - **availability**: the information is available when necessary and can be accessed.

4

Security in a context

- ▶ Information security needs a context, e.g.
 - who is allowed to access data
 - what should never happen to data
- ▶ This is called a **security model**. It contains:
 - **security goals**
 - **attacker descriptions**
 - **threat models**
 - **trust models**

5

Security in changing contexts

- ▶ However, if some of the context changes, information security can be in trouble:
 - System upgrades / progress of infrastructure
 - combination of security measures with distinct security models or conflicting goals
 - system ageing / progress of threats
- ▶ Hence, good security concepts have extensive documentation on "secure operation" including security models, context, lifespan, and audit suggestions.
- ▶ Frequent auditing is an essential part of information security management, e.g. ISO 27000 or BS7799.

6

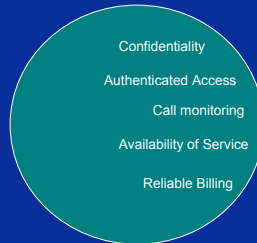
Finding Security Requirements

- ▶ To design a security model, we start with the functional requirements of a system, derived from a use case
 - Asterisk / VoIP telephony:
 - Make phone calls
 - Availability
 - No unauthorized outside calls
 - No unauthorized call diversion, monitoring, eavesdropping or denial-of-service
 - Scalable
- ▶ BUT: There might be conflicting views...

Security Requirements I: Vendor



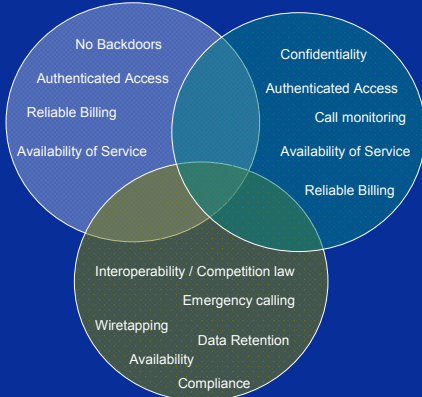
Security Requirements II: User



Security Requirements III: Government

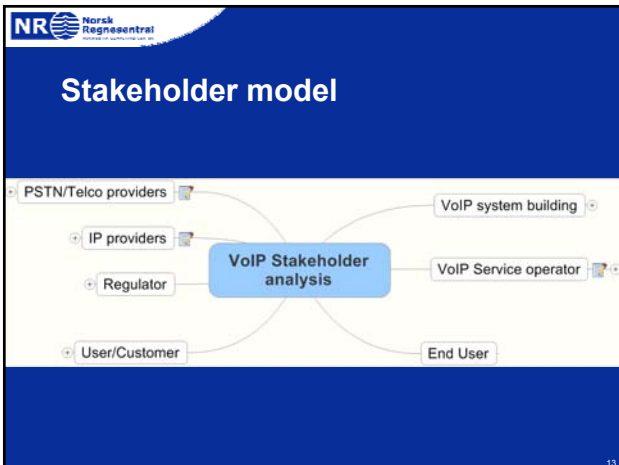


Possible conflicts

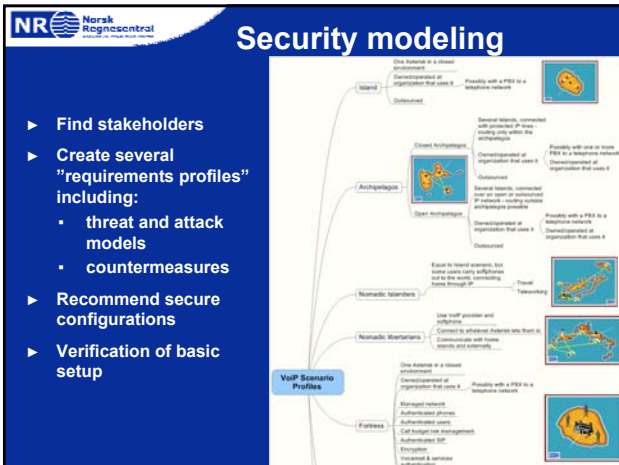


Approach

- ▶ Prepare different "requirements profiles"
- ▶ Perform stakeholder analysis
- ▶ Make security model
- ▶ Make security specification and documentation
- ▶ Implement VoIP system



-
- Profiling VoIP use through the security lens**
- ▶ Create several "requirements profiles" including:
 - threat and attack models
 - countermeasures
 - ▶ Recommend secure configurations
 - ▶ Formal verification of basic setup



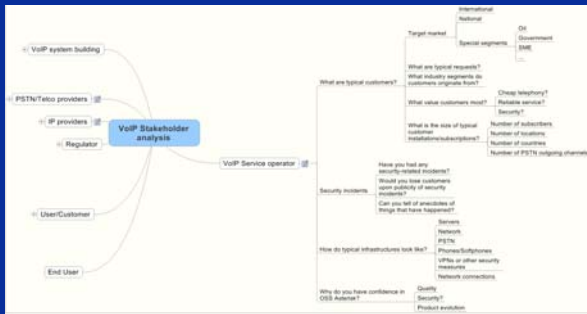
Security modeling: Surveys

- ▶ Effort to "de-geek" security talk by using graphical metaphors on stakeholder interviews

Maginot Line



Stakeholder Interviews



Security modeling: Surveys - preliminary results

- ▶ Mostly re-building traditional telephony functionality
 - Security by firewall & router (dedicated lines)
 - No certificates
 - MAC authenticated phones → no softphones!
- ▶ Greatest concerns: Money loss, unavailability
- ▶ Unaware of IP based threats such as hijacking, man-in-the-middle, confidentiality issues
- ▶ No security engineering in many cases

Security modeling: Surveys - preliminary results (II)

- ▶ Configuration complexity issue
 - Too many configuration files
 - dial plans and other rules can be a source of error
 - tool support appreciated
- ▶ Redundancy of service providers might not be available on the Norwegian market
- ▶ Patch levels and mesh-ups of various layers of Open-Source components might not live up to the latest versions.
- ▶ Active avoidance of innovations (e.g. SoftPhones) due to security challenges.

Your Collaboration in EUX2010Sec

- ▶ Stakeholder analysis with customers
- ▶ Requirements elicitation
- ▶ Security & threat modelling
- ▶ Documentation
- ▶ Audit preparation

Please ask questions, and discuss!

Project overview

Fritsch, Lothar; Groven, Arne-Kristian; Strand, Lars:

A holistic approach to Open-Source VoIP security: Preliminary results from the EUX2010SEC project

The Eighth International Conference on Networks (ICN 2009), Proceedings of the The Eighth International Conference on Networks (ICN) 2009, Bestak, Robert; George, Laurent; Zaborovsky, Vladimir S., Dini, Cosmin, IEEE Computer Society, ISBN 978-0-7695-3552-4/09, pp. 275-280, March 05, 2009.

Best-Paper-Awarded Conference Article on ICN2009
