A Holistic Approach to Open-Source VoIP Security

Preliminary results from the EUX2010Sec project

Lothar Fritsch, Arne-Kristian Groven,

and Lars Strand

Cancun, Mexico

March 2009

Overview

- Goal
- The EUX2010Sec project
- Structure and methodology
  - Security modeling
  - Protocol verification
  - Test lab
- Possibilities

Goal

“The overall goal of this research project is to improve both the security level and the security awareness when developing, installing and using open source VoIP/PBX/multimedia solutions.”

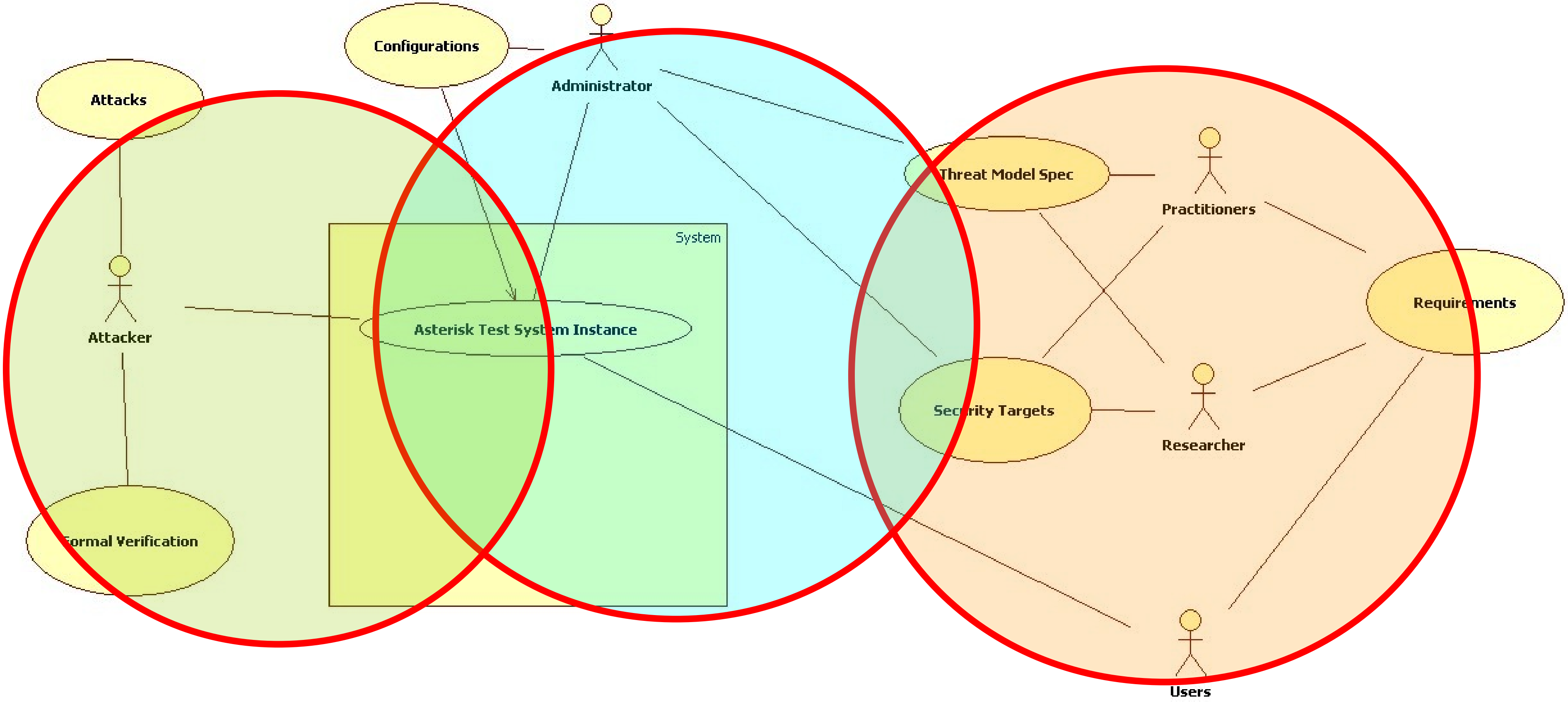
The EUX2010Sec project

- anchored in the EUX 2010 network
- Researchers from the Nordic countries.
- Open source PBX/VoIP developers, integrators and deployers, consultants, support organizations, and customers.
- EUX 2010 is to develop an integrated communication platform for voice and video communication using open source and open standards.
- The funding source is the Norwegian Research Council, and industry partners.

The EUX2010Sec project

- Norwegian partners
  - Norwegian Computing Center (Norsk Regnesentral)
  - Ibidium Norden
  - Redpill Linpro
  - FreeCode
  - Nimra Norge
  - Buskerud Fylkeskommune
- International partners
  - UNU-MERIT - United Nations University

EUX2010sec project structure



Formal Verification
Protocol Analysis
Attacks

Testbed systems
Configurations

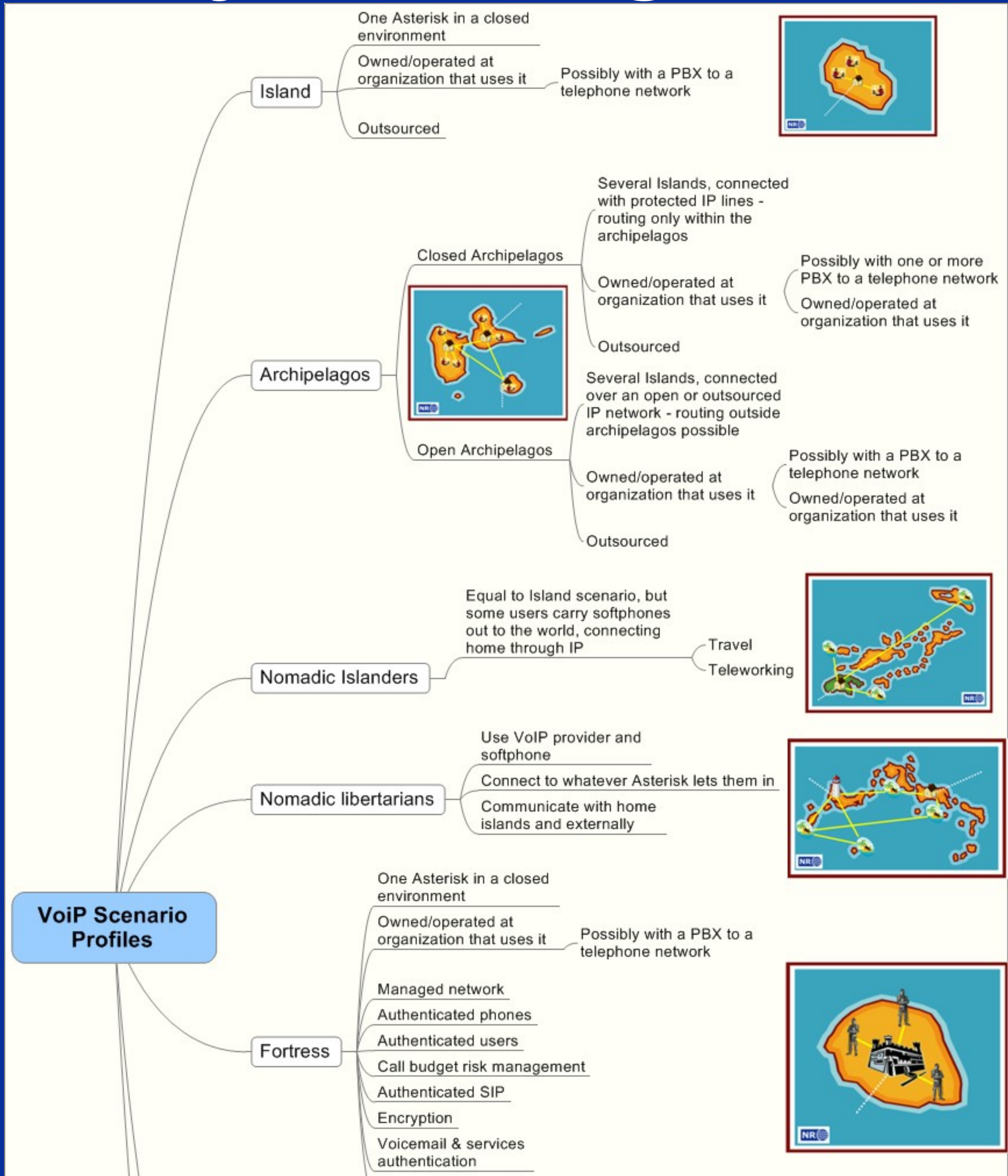
Requirements
Profiles
Security Models

Project methodology

- Connected research in 3 areas
- Involve practitioners who provide base scenarios, and requirements profiles
- Formal modeling and verification of protocol implementations
- Testing of models and implementations in the VoIP test lab

Security modeling

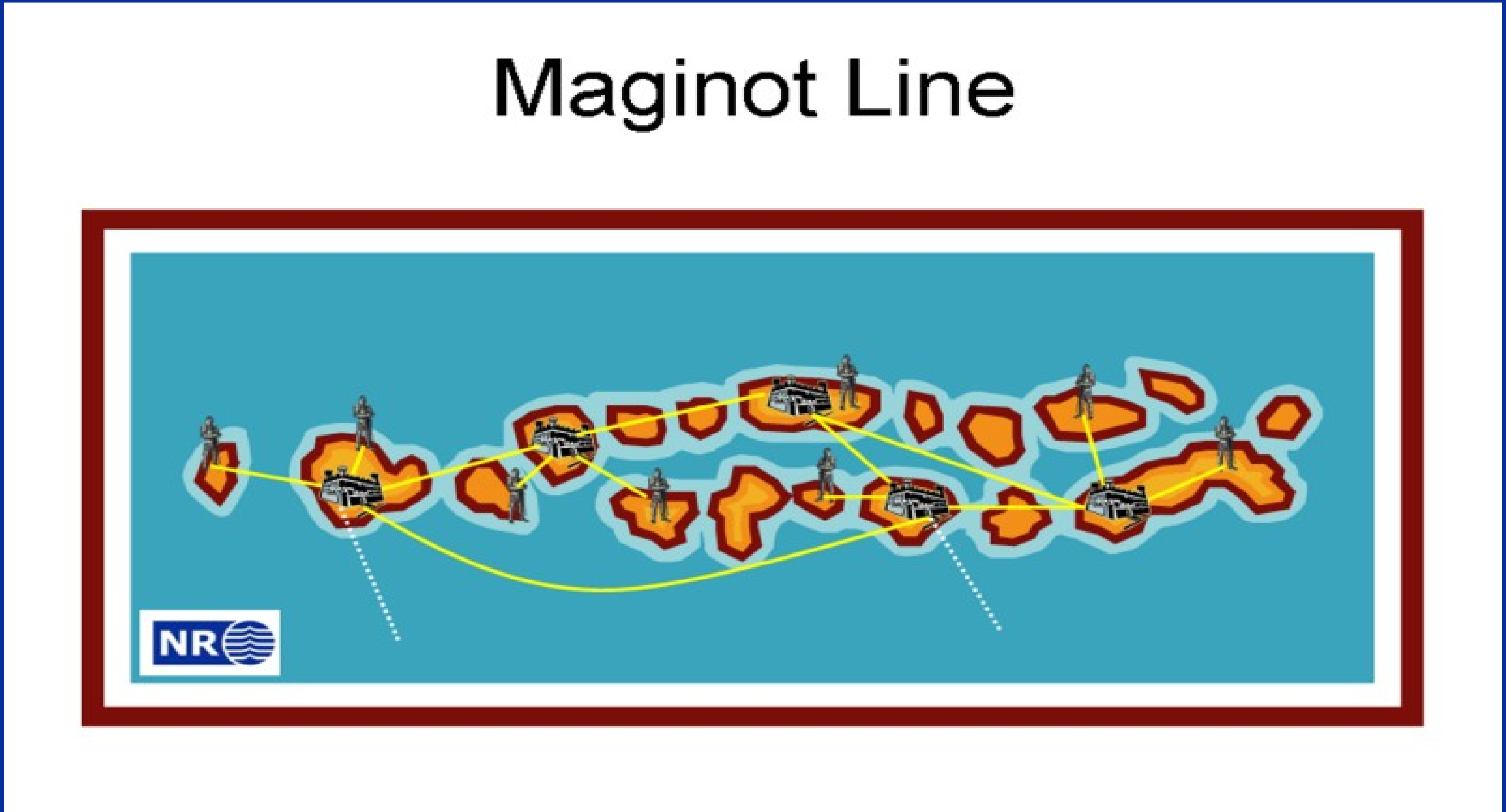
- Find stakeholders
- Create several ”requirements profiles” including:
  - threat and attack models
  - countermeasures
- Recommend secure configurations
- Verification of basic setup



- VoIP Scenario Profiles
  - Island
    - One Asterisk in a closed environment
    - Owned/operated at organization that uses it
      - Possibly with a PBX to a telephone network
    - Outsourced
  - Archipelagos
    - Closed Archipelagos
      - Several Islands, connected with protected IP lines - routing only within the archipelagos
      - Owned/operated at organization that uses it
        - Possibly with one or more PBX to a telephone network
        - Owned/operated at organization that uses it
      - Outsourced
    - Open Archipelagos
      - Several Islands, connected over an open or outsourced IP network - routing outside archipelagos possible
      - Owned/operated at organization that uses it
        - Possibly with a PBX to a telephone network
        - Owned/operated at organization that uses it
      - Outsourced
  - Nomadic Islanders
    - Equal to Island scenario, but some users carry softphones out to the world, connecting home through IP
      - Travel
      - Teleworking
  - Nomadic libertarians
    - Use VoIP provider and softphone
    - Connect to whatever Asterisk lets them in
    - Communicate with home islands and externally
  - Fortress
    - One Asterisk in a closed environment
    - Owned/operated at organization that uses it
      - Possibly with a PBX to a telephone network
    - Managed network
    - Authenticated phones
    - Authenticated users
    - Call budget risk management
    - Authenticated SIP
    - Encryption
    - Voicemail & services authentication

Security modeling: Surveys

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



Maginot Line

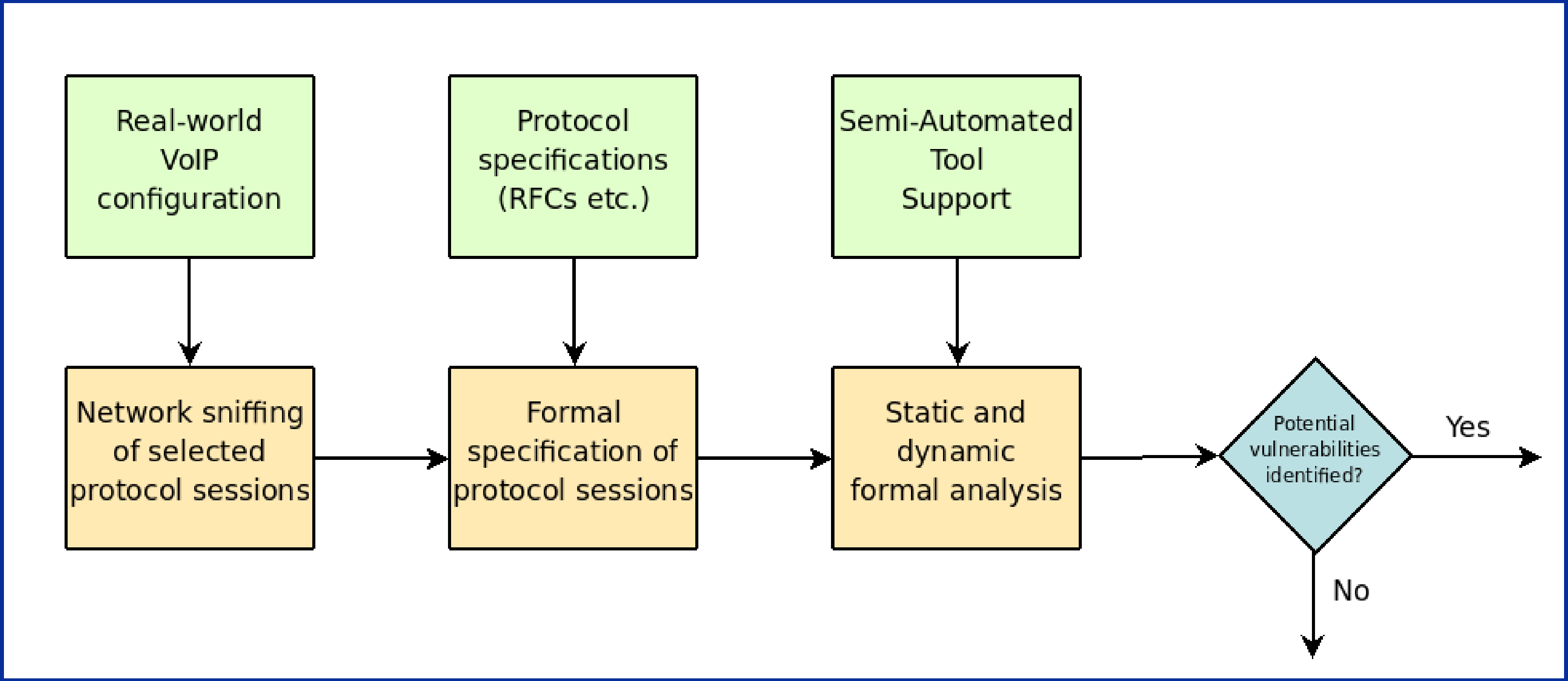
Security modeling: Surveys - prelimniary results

- Mostly re-building POTS functionality
  - Security by firewall & router
  - 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

Why formal methods?

- The *only* way to proof or verify that protocols fulfil their goals
- To find *new attacks* on protocols
- Provides an *unambiguous* specification of
  - protocol interaction and entities
  - functional and security goals
- The protocol specification can be analyzed *automatically*

Formal analysis of a VoIP system


Real-world VoIP configuration
Protocol specifications (RFCs etc.)
Semi-Automated Tool Support
Network sniffing of selected protocol sessions
Formal specification of protocol sessions
Static and dynamic formal analysis
Potential vulnerabilities identified?
Yes
No

Formal methods – preliminary results

- Analysis of the signaling protocol SIP
- Found and published attacks:
  - SIP REGISTRATION (authentication) and
  - SIP INVITE (call-setup)

Why testbed testing?

- Advantage over theoretical approach
  - VoIP tested in different scenarios
- Real life VoIP have many deciding factors for performance
  - Network congestion, network topology, protocol used, functionality used, etc.
  - Hard to do in a simulation

Testbed goals

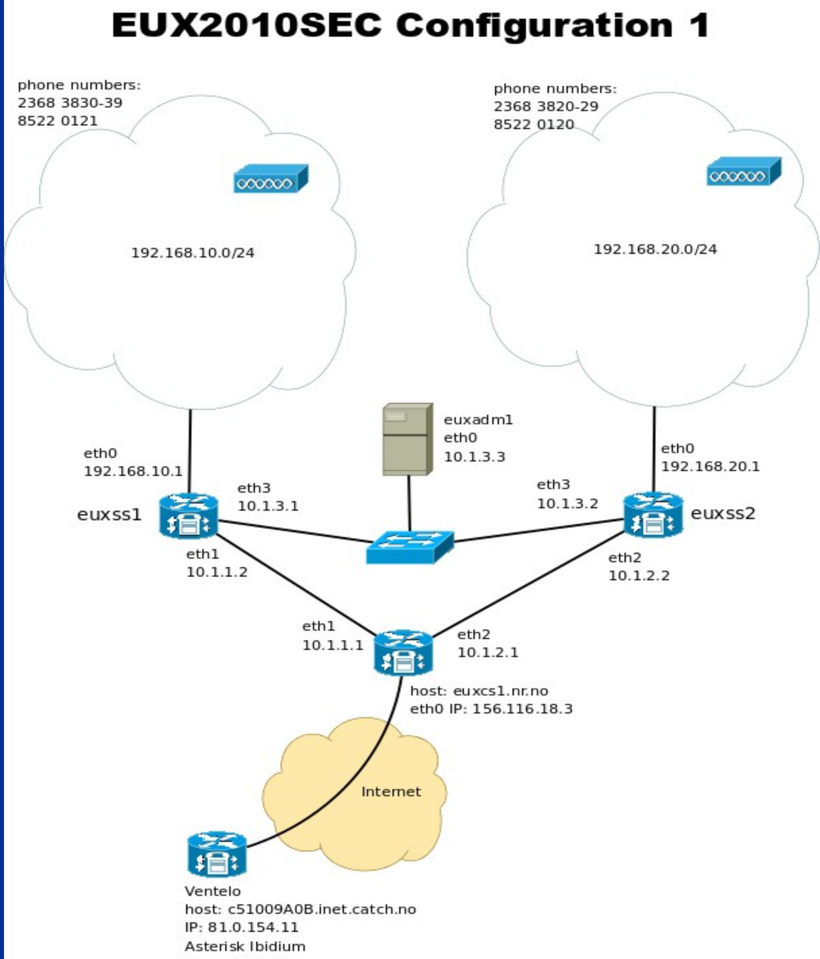
1. Validate a given VoIP configuration against the security requirements given by the stakeholders
2. Create automated VoIP testbed attack tools
3. Reuse a given testbed configuration to third party vendors or researchers
4. Create VoIP configurations that are arguable more secure, based on our findings from the above three goals

Testbed

- Equipment
  - Three high-end servers
  - Two attack nodes
  - Two management nodes
  - 16 Hardphones, 8 different models
  - Two switchboards (on two laptops)
- Software
  - Linux
  - Asterisk and OpenSER
  - MRTG, Munin, Nagios, Subversion, ++

Testbed – preliminary results

- VoIP preliminary testing to learn the protocols
- Network dumps used as input for formal analysis.
- Replicated two of our stakeholders VoIP setups



References

- Anders Moen Hagalisletto, Lars Strand, Wolfgang Leister and Arne-Kristian Groven. Analysing Protocol Implementations. Accepted for publication in The 5th Information Security Practice and Experience Conference (ISPEC 2009), Apr 2009.
- Lothar Frisch, Arne-Kristian Groven, Lars Strand, A holistic approach to Open-Source VoIP security: Preliminary results from the EUX2010SEC project. Accepted for publication in ICN 2009. *The Eighth International Conference on Networks*, Mar 2009.
- Anders Moen Hagalisletto and Lars Strand. Formal modeling of authentication in SIP registration. *Emerging Security Information, Systems and Technologies*, 2008. SECURWARE '08. Second International Conference on, pages 16-21, Aug 2008.
- Presentations
- Strand, Lars: FLOSS Quality and Maturity Models, presentation VERDIKT at VERDIKT programme conference 2008, 29-30 October 2008, Bergen, Norway.
- Strand, Lars: Authentication in SIP, poster presentation at VERDIKT programme conference 2008, 29-30 October 2008, Bergen, Norway.
- Fritsch, Lothar: Interdisciplinary Requirements for VoIP Security Design, EUX2010SEC internal workshop on 17-Apr-2008, Oslo, Norway
- Strand, Lars: Securing Open Source Communications Systems, poster presentation at VERDIKT programme conference 2007, 29-30 October 2007, Hell, Norway

The future of OSS-based VoIP…?

Securing Open Source Communication Systems
And proposals on how to fix them.
VoIP attacks
EUX2010SEC
LAB
Lars Strand