EUX2010SEC - Security infrastructure for the open source Enterprise Unified Exchange (EUX2010) VoIP system – Project number 180054/S10

# Securing Open Source Communication Systems

Lars Strand, PhD fellow, Norwegian Computing Center, email: lars.strand@nr.no

## – *"Hello? Who is this?"*

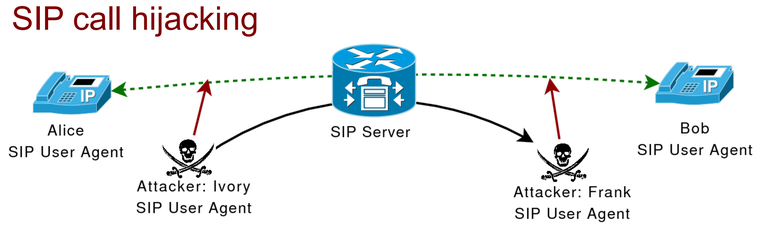
**An analysis of VoIP security threats and challenges. And proposals on how to fix them.**

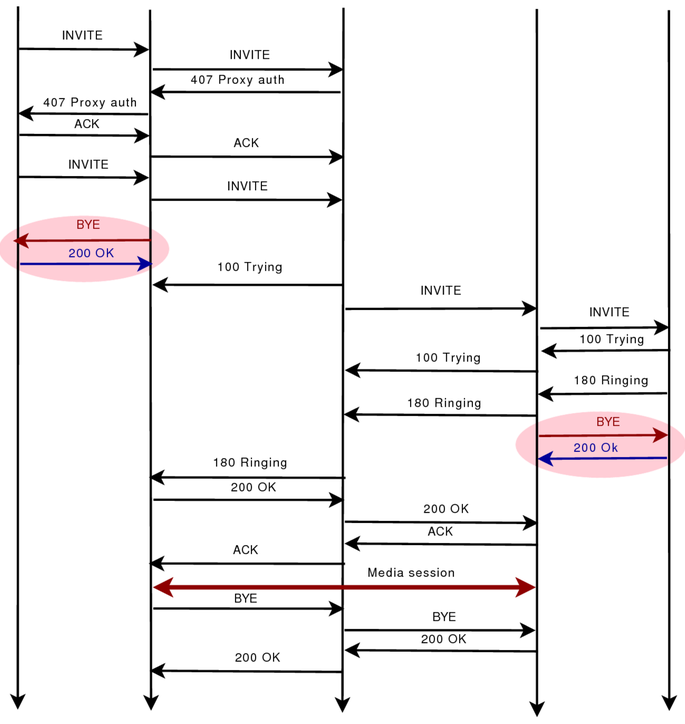
### Project goal:

*"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."*

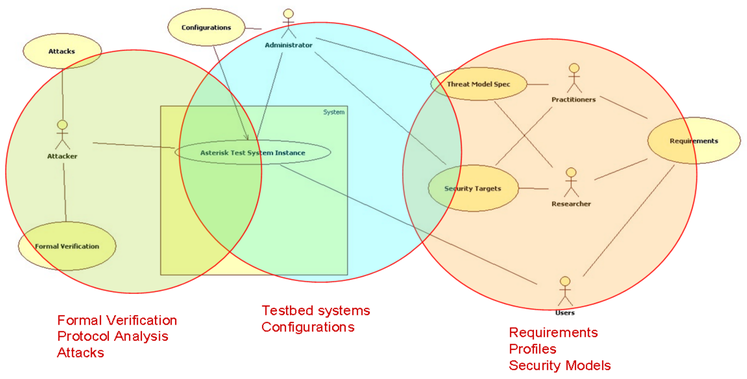
### VoIP attacks

SIP call hijacking

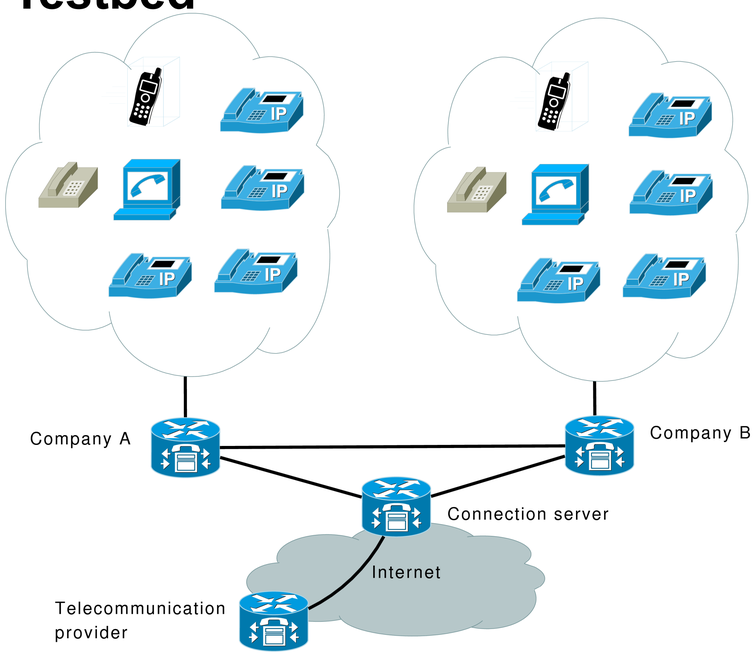



### Methodology




### Testbed

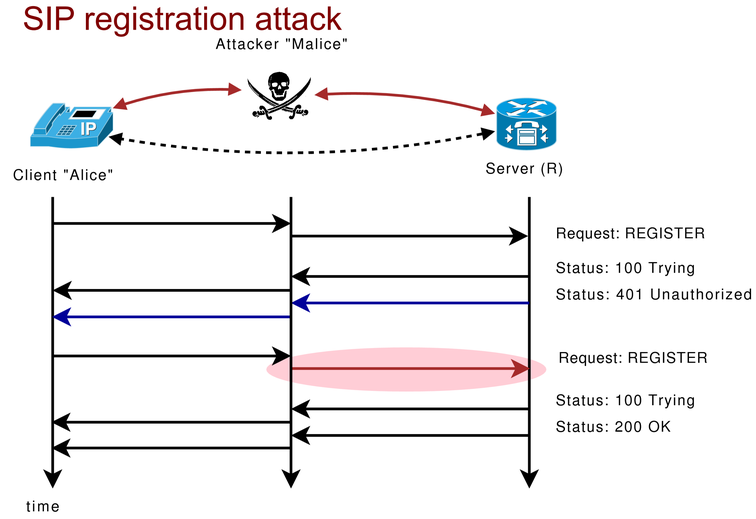


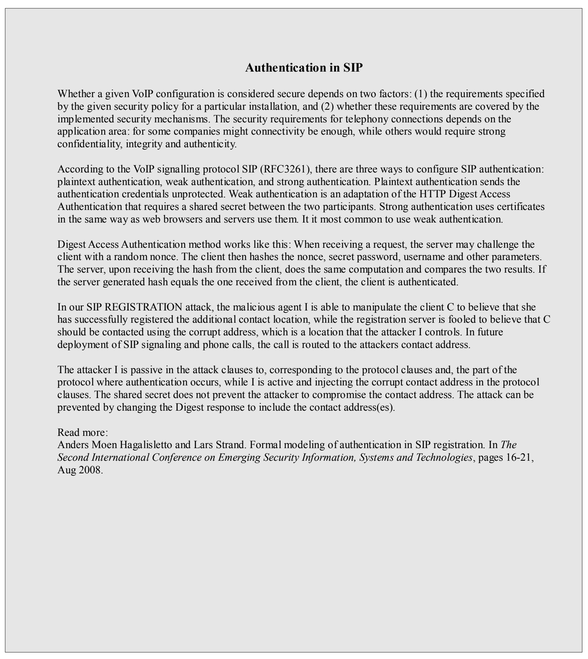

1) Gather requirements from stakeholders.
2) Formal protocol analysis – using the PROSA tool.
3) Testbed
   - Validate secure VoIP installations.
   - Automated testbed attack tool.
   - Reuse given testbed configurations to vendors and researchers.
   - Design secure VoIP installations.

### Testbed equipment

- 8 SIP hardphones
- 2 SIP softphones
- 4 analog phones (with SIP converter)
- 2 SIP wireless hardphones
- 3 Asterisk servers

### SIP registration attack



**Authentication in SIP**

Whether a given VoIP configuration is considered secure depends on two factors: (1) the requirements specified by the given security policy for a particular installation, and (2) whether these requirements are covered by the implemented security mechanisms. The security requirements for telephony connections depends on the application area: for some companies might connectivity be enough, while others would require strong confidentiality, integrity and authenticity.

According to the VoIP signalling protocol SIP (RFC3261), there are three ways to configure SIP authentication: plaintext authentication, weak authentication, and strong authentication. Plaintext authentication sends the authentication credentials unprotected. Weak authentication is an adaptation of the HTTP Digest Access Authentication that requires a shared secret between the two participants. Strong authentication uses certificates in the same way as web browsers and servers use them. It it most common to use weak authentication.

Digest Access Authentication method works like this: When receiving a request, the server may challenge the client with a random nonce. The client then hashes the nonce, secret password, username and other parameters. The server, upon receiving the hash from the client, does the same computation and compares the two results. If the server generated hash equals the one received from the client, the client is authenticated.

In our SIP REGISTRATION attack, the malicious agent I is able to manipulate the client C to believe that she has successfully registered the additional contact location, while the registration server is fooled to believe that C should be contacted using the corrupt address, which is a location that the attacker I controls. In future deployment of SIP signaling and phone calls, the call is routed to the attackers contact address.

The attacker I is passive in the attack clauses to, corresponding to the protocol clauses and, the part of the protocol where authentication occurs, while I is active and injecting the corrupt contact address in the protocol clauses. The shared secret does not prevent the attacker to compromise the contact address. The attack can be prevented by changing the Digest response to include the contact address(es).

Read more:
Anders Moen Hagalisletto and Lars Strand. Formal modeling of authentication in SIP registration. In *The Second International Conference on Emerging Security Information, Systems and Technologies*, pages 16-21, Aug 2008.

### Supervisors:

Wolfgang Leister, <wolfgang.leister@nr.no>, Chief Research Scientist, Norwegian Computing Center

Torleiv Maseng <torleiv.maseng@ffi.no>, Director of Research, Norwegian Defence Research Establishment.

Josef Noll <josef.noll@unik.no>, Professor, Unik.

### References:


- Anders Moen Hagalisletto and Lars Strand, *"Formal modeling of authentication in SIP registration"*. In The Second International Conference on Emerging Security Information, Systems and Technologies, pages 16-21, Aug 2008.
- Kuhn, Walsh, Fries, *"Security Consideration for Voice Over IP Systems"*. NIST, Jan 2005.
- Sinnreich, Johnston, "Internet Communications Using SIP". Wiley, 2nd edition 2006
- McGann, Sicker, "An Analysis of Security Threats and Tools in SIP-Based VoIP Systems", 2005
- Daniel Minoli, *"Voice over IPv6 - Architecture for Next Generation VoIP Network"*. Newnes, May 2006.


### EUX2010SEC partners:

**Read more: http://eux2010sec.nr.no/**