

VoIP Hacking

Lars Strand

PhD student

Norwegian Defence Research Establishment (FFI)

Jeløy, 15.-16. January 2009

VoIP?

- PSTN:
 - 100 year old technology, 99.999% uptime, call anyone anytime – can VoIP offer that today?
- VoIP – next big thing
 - Cheaper and added functionality.
 - Today: VoIP providers just replicate PSTN.
- VoIP loaded with security issues
 - Inherit (traditional) packet switched network security issues and introduces new ones (because of new technology).

Session Initiation Protocol

- SIP RFC 3261
- Biggest RFC IETF ever released
- SIP charter:
 - 50 SIP related RFCs
 - 23 pending SIP drafts
- Modelled after SMTP/HTTP
- Today: de facto standard in VoIP
 - other: IAX (Digium), H.323 (ITU-T), SCCP (Cisco),...
- But *"Functionality first, then security"...*

SIP

- Purpose: Set up and tear down multimedia session.
- SIP+RTP = widely used combination.
 - SIP: signalling (dial, hangup, conference call, etc.)
 - RTP: multimedia transport (voice, video, etc.)
- Transport layer (application):
 - UDP most common
 - TCP supported, but seldom used.

SIP request/response codes

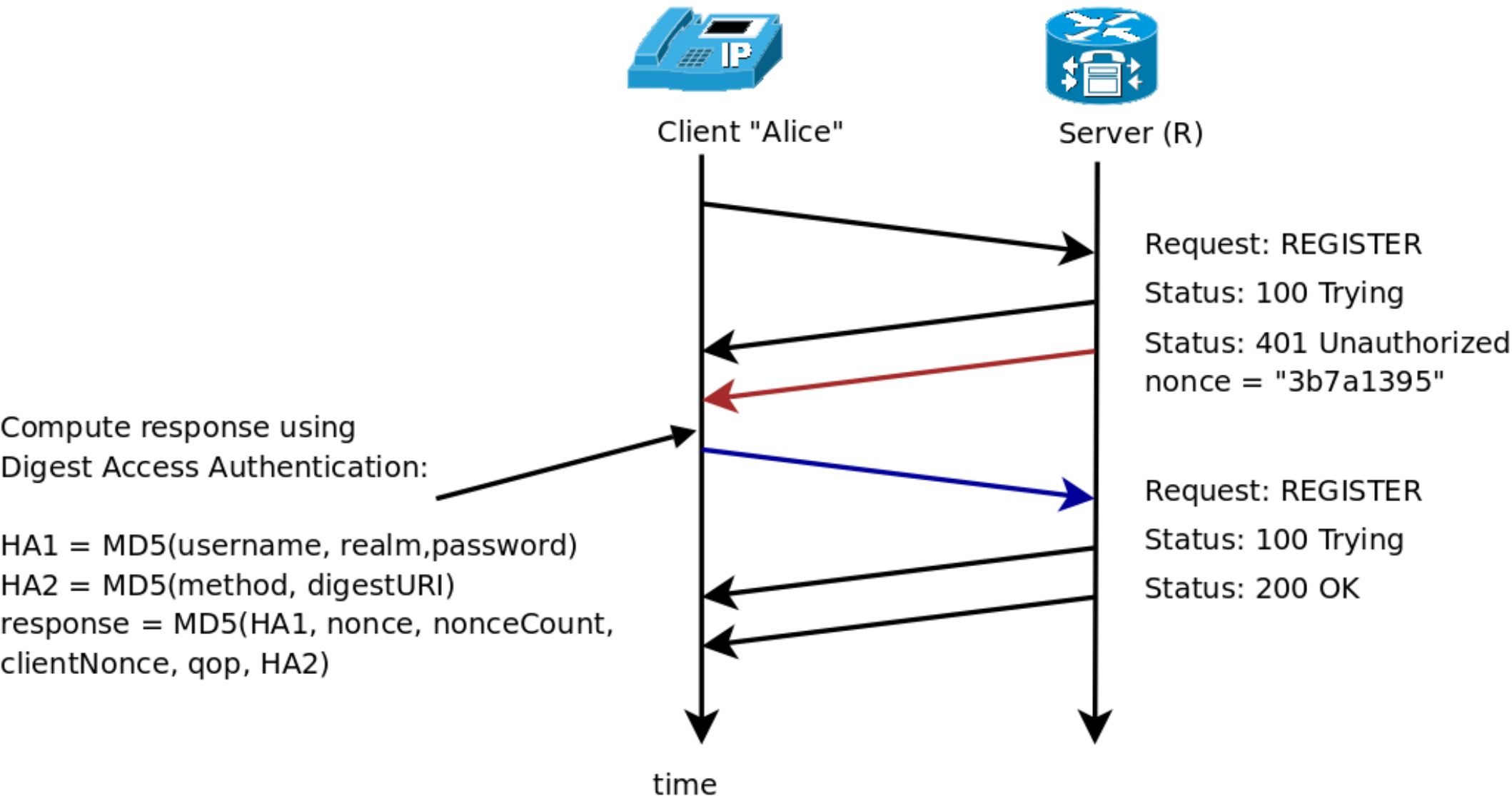
- SIP example requests
 - INVITE – calling
 - BYE – hangup
 - REGISTER – UAC (phone) register to UAS (server)
- SIP response codes
 - 100 – Trying
 - 180 – Ringing
 - 200 – OK
 - 404 – User not found

(HTML anyone?)

SIP REGISTER

- UAC often use DHCP
- Each UAC (phone) must REGISTER at startup
- May authenticate when doing so
 - Most common method Digest Access Authentication (RFC2617)
- SIP + DAA = copied from HTTP
 - But is that a good solution?
 - What fields are protected by DAA?

DAA



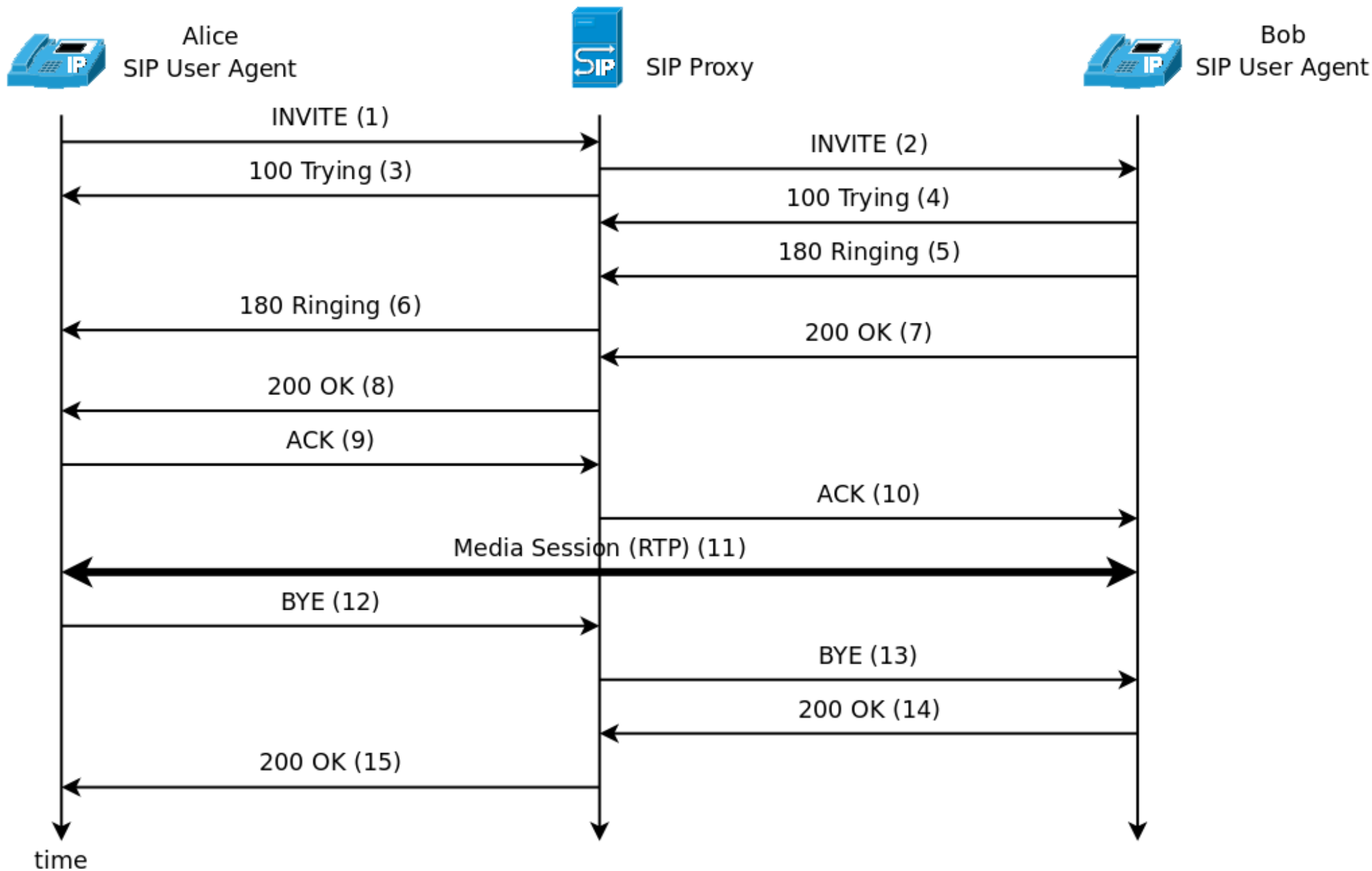
SIP and DAA

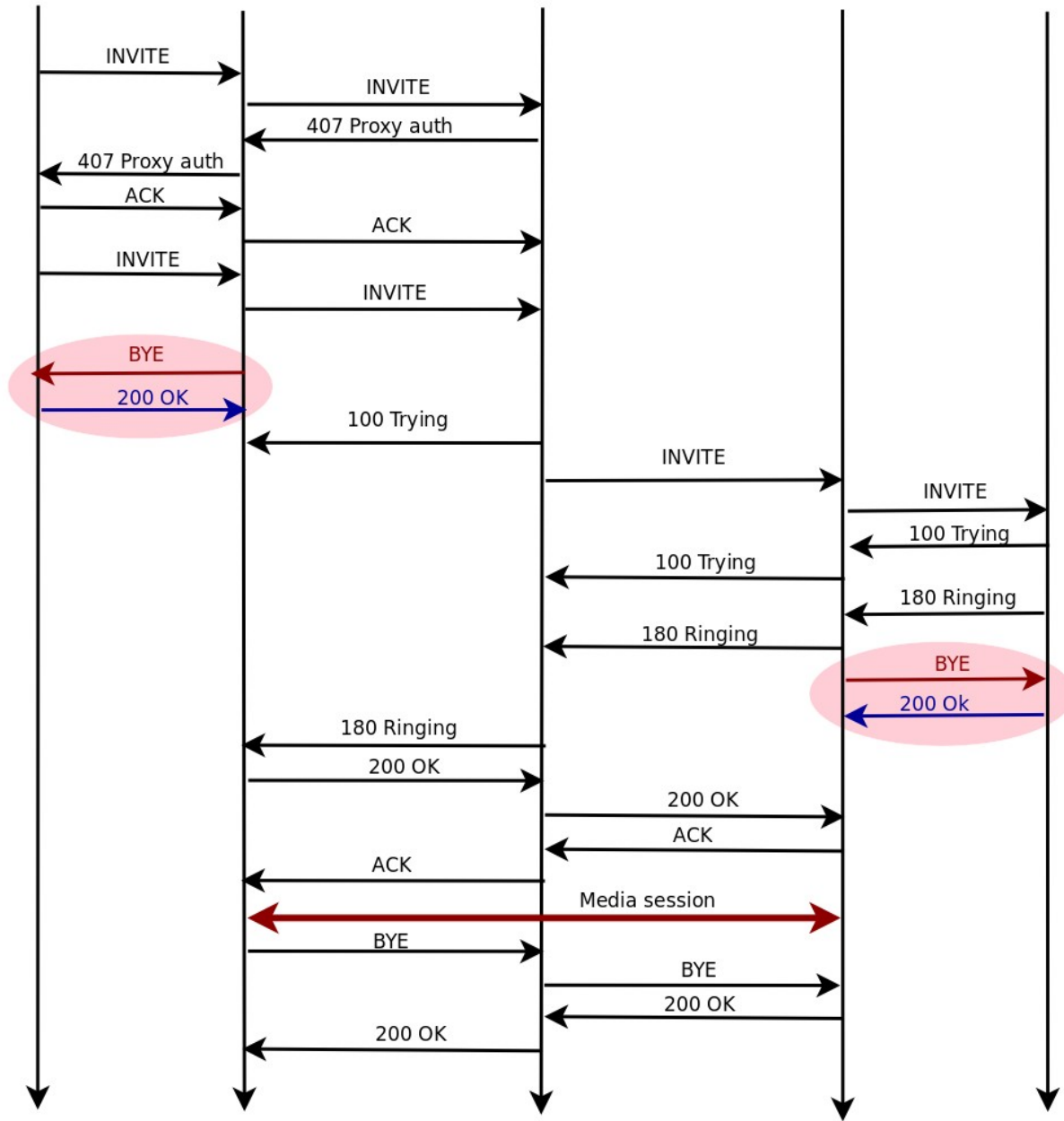
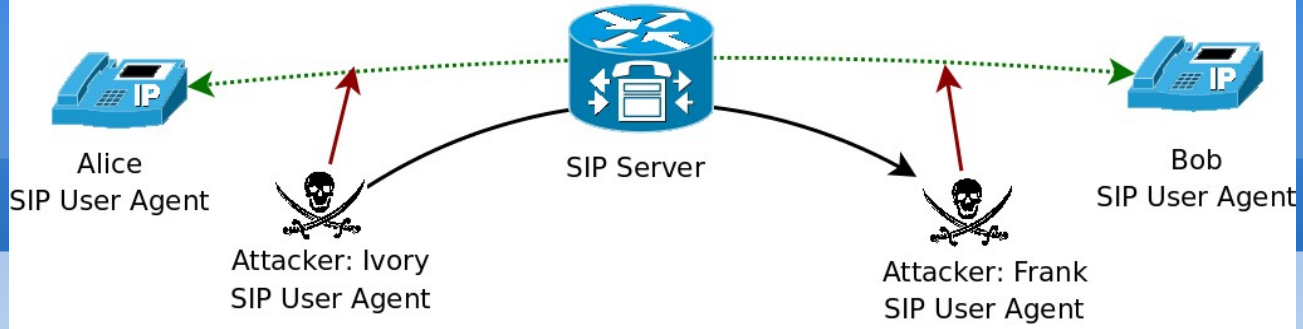
- Weakness: Contact location is not included.
- **Man-in-the-middle attack:**
 - Just eavesdrop all messages – and inject own contact location.
 - *Attacker does not even need to know the shared secret!*
- Solution: Include the Contact location in the hash as well.
- Conclusion: The SIP+DAA inclusion is to simple.
- Paper published and accepted at SECURWARE2008

Attack of call-setup

- Attacker hijack phone call.
- How?
 - Man-in-the-middle
 - Attacker hang up the caller and callee but continue the call.
- First: How does a normal SIP VoIP call look like?

SIP INVITE





Attack of call setup

- Results:
 - The call will be recorded as found place between A and B, on the SIP server (and thus billed accordingly).
 - But the attacker I and F hijacked and had the call.
 - A and B will not know that their call was hijacked.
- Variation of attack:
 - One attacker, one realm
 - Two attackers, two different realms
- Paper submitted to ISPEC09

Future work

- Implement the attacks.
- Test various industry configuration
 - Correlation with security policy?
- Impact of security mechanism in VoIP
 - MAC
 - TLS/SSL or IPSec
 - Strong authentication (x509)
- VoIP DDoS attack – *very* interesting!
- SPIT
- FLOSS - how to ensure quality?

EUX2010SEC

- Project: Aug 2007 – medio 2010
- Several industry partners
 - Linpro (now Redpill Linpro)
 - Ibidium (and Nimra)
 - Freecode
- Extensive lab at NR
 - 3 high end server, several attack nodes, 16 hard-phones.
- Test various industry configurations.
 - How does security mechanism affect VoIP?
- Read more: <http://eux2010sec.nr.no>

Thank you!

Questions?