SIP SECURITY

Status Quo and Future Issues

23. Chaos Communication Congress: 27. - 30.12.2006, Berlin, Germany

Jan Seedorf - seedorf@informatik.uni-hamburg.de

SVS - Security in Distributed Systems

Intention of the Talk

- **Motivate SIP Security by showing key differences between SIP-based Voice-over-IP and PSTN**
- **Show important research areas of SIP Security and current approaches**
- **Give an Outlook on Security Issues in future, Peer-to-Peer based SIP networks**

(1) Signalling with SIP

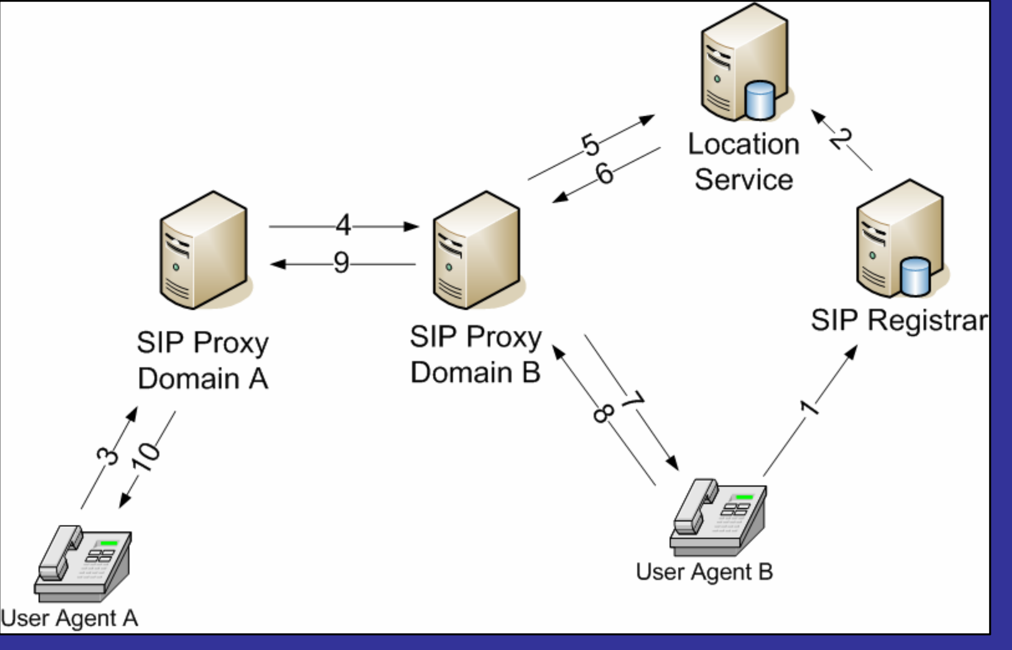
(2) Differences to PSTN

(3) Research Problems and Current Approaches

(4) Security in P2P-SIP Networks

(5) Conclusion

Introduction to SIP



What is Voice-over-IP?

real-time

The transmission of (digitised) voice over an IP-based network

Separation of signalling and media transfer

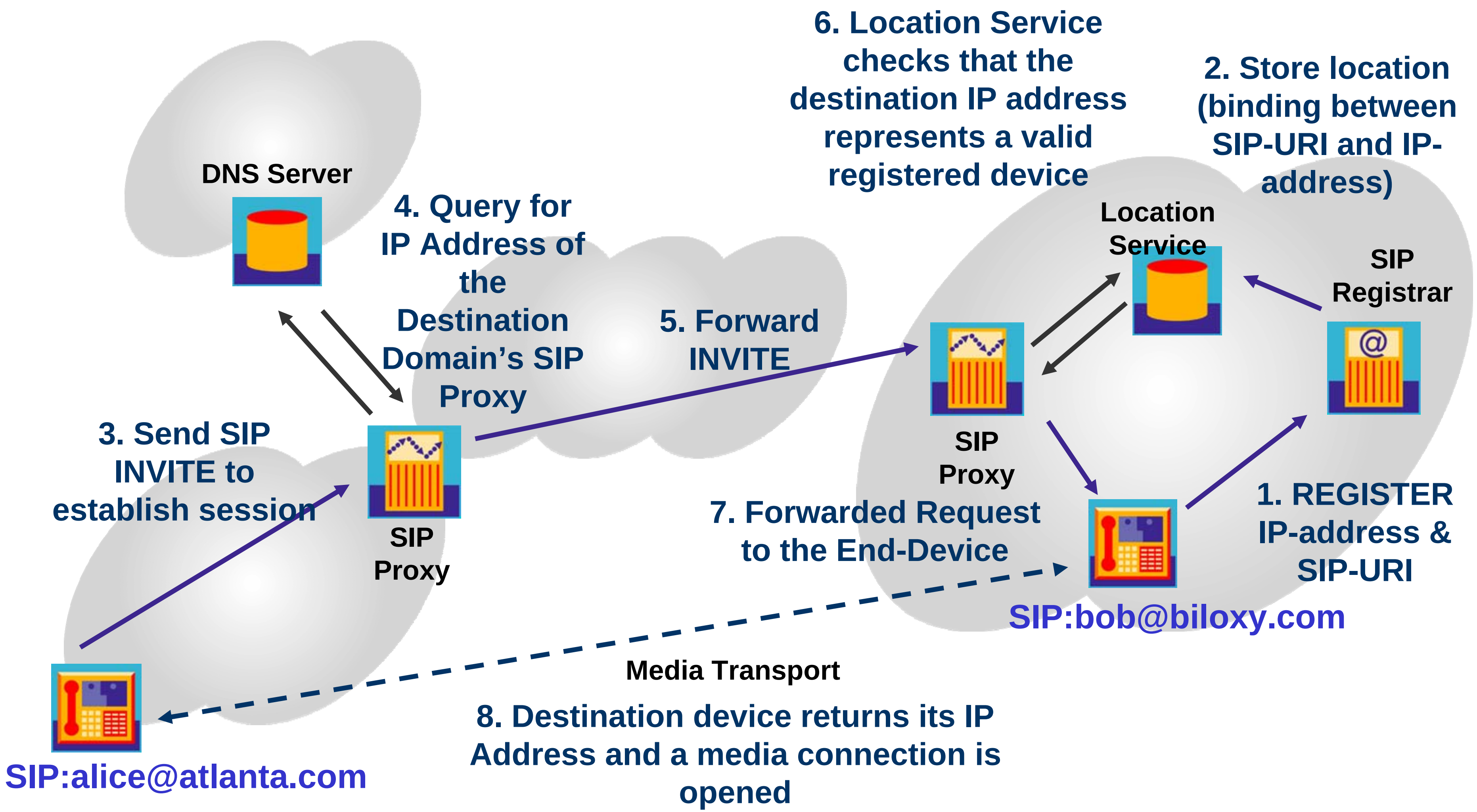
SIP: an application-layer signalling protocol for (multimedia) sessions

SIP supports

- **Mobility of users**
- **Media parameter negotiation**
- **Session Management**

Actual media transfer is (usually) based on RTP

SIP Protocol: Example of operation



Differences between SIP-based VoIP and PSTN

(PSTN)

(SIP)

Signalling

Public Switched Telephone Network

- **PSTN**
  - Signalling in a closed network (SS7)
- **SIP**
  - Signalling in an open network
  - Signalling network is highly insecure (Internet)

Terminals

- **Traditional Telephones:**
  - Simple devices
  - not much functionality
- **SIP-phones:**
  - Complex devices
  - Have their own TCP/IP stack

Mobility

- **PSTN**
  - No mobility
- **SIP**
  - Users can change their location and still use the same identity in the network
  - Only access to IP-network is required

Authentication

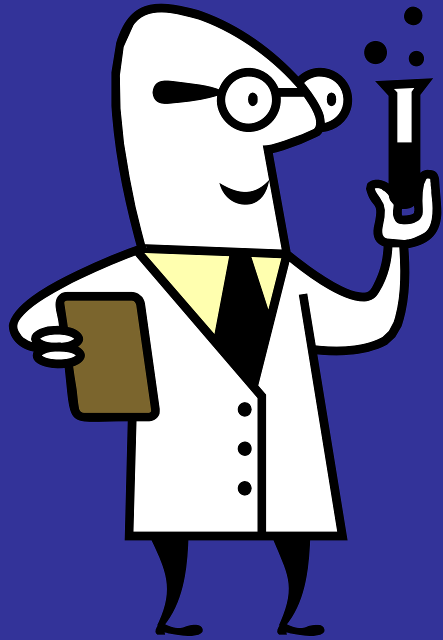
- **PSTN**
  - No authentication necessary (no mobility)
- **SIP**
  - Due to mobility on IP-layer, authentication on the application layer is necessary

Mobility / Authentication

- A network with similar properties: GSM
  - GSM uses smartcards
  - Limited number of providers that trust each other

=> Differences between PSTN and SIP have significant consequences for security

Current Research Problems



Security in SIP Standard (RFC 3261)

- **S/MIME**
- **Digest Authentication**
- **TLS & IPSec**

=> Require a universal trust infrastructure

- **E.g. a worldwide public-key infrastructure**
- **One Root trusted by all**
- **Compatible for all users**

Current Work on SIP Security

- **Authentication**
- **Spam over Internet Telephony**
- **Lawful Interception**
- **Testing SIP Devices**

Authentication

The Problem

- SIP users are mobile, i.e. change their location
- The location cannot be used to authenticate users
- No worldwide PKI in place that can be used by all users

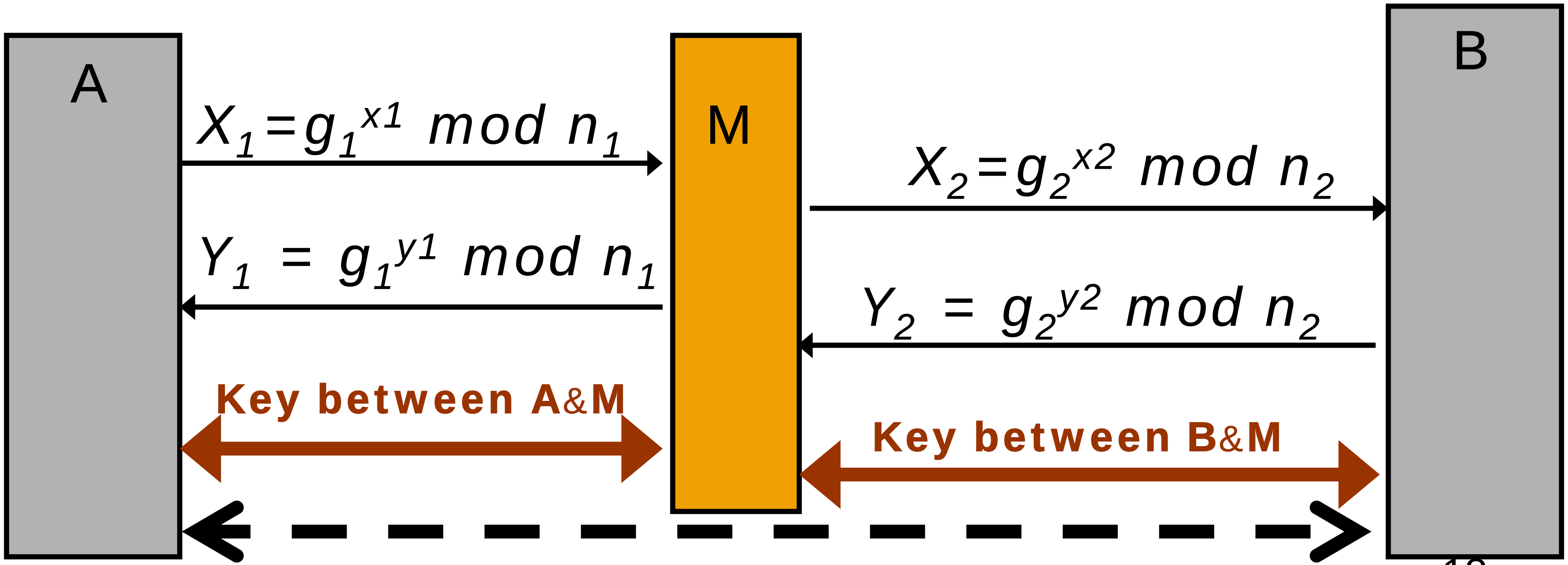
ZRTP

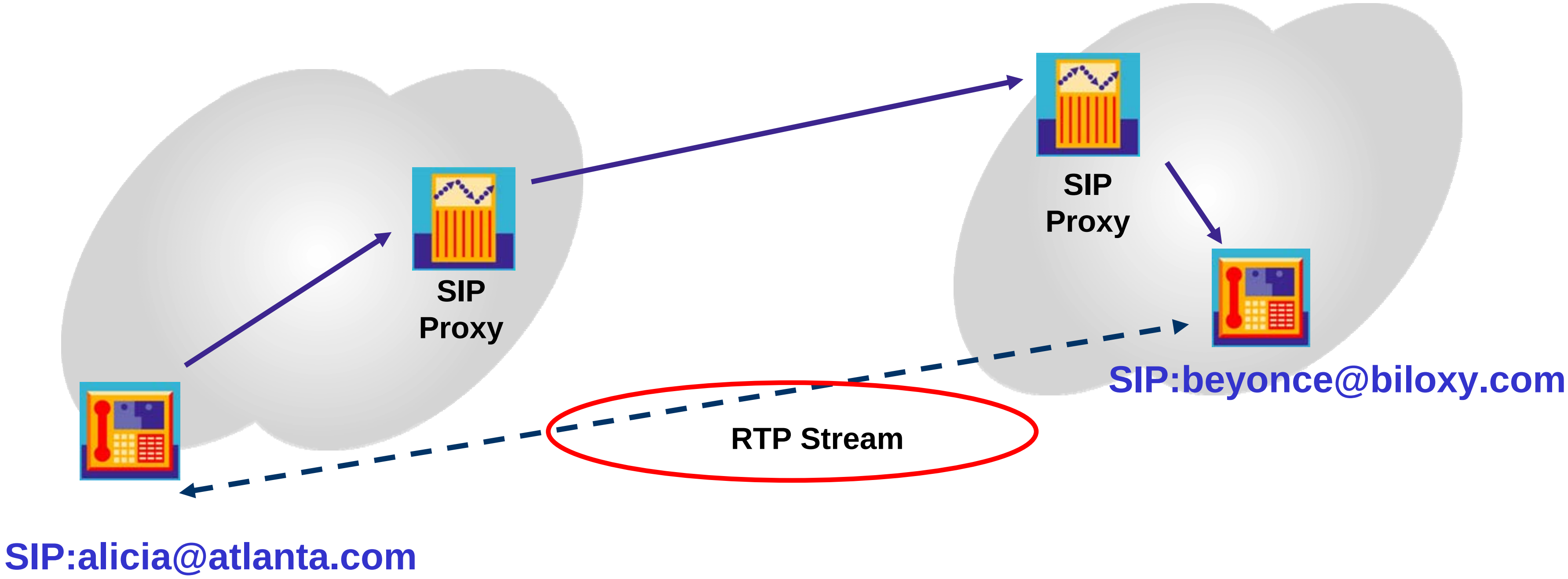
- **Developed by Phil Zimmermann (PGP)**
- **Diffie-Hellman key exchange within an RTP stream**
- **Key exchange is protected against man-in-the-middle attacks by an authentication string**
- **Authentication string is „read“ by communication partners and transmitted over RTP**

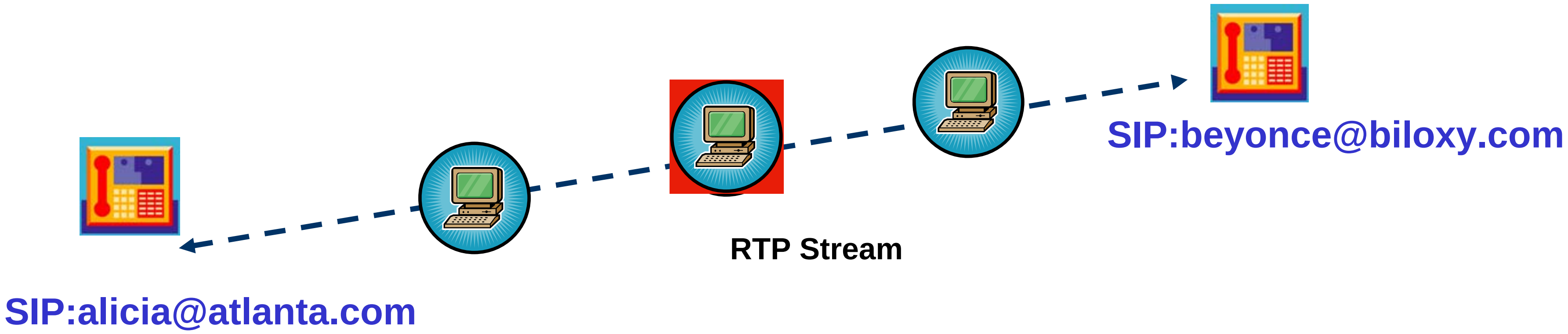
5.b) Assume Alice and Bob use the Diffie-Hellman protocol to derive a secret key. Further, assume an attacker is in the path between Alice and Bob and able to read the messages being exchanged between them.

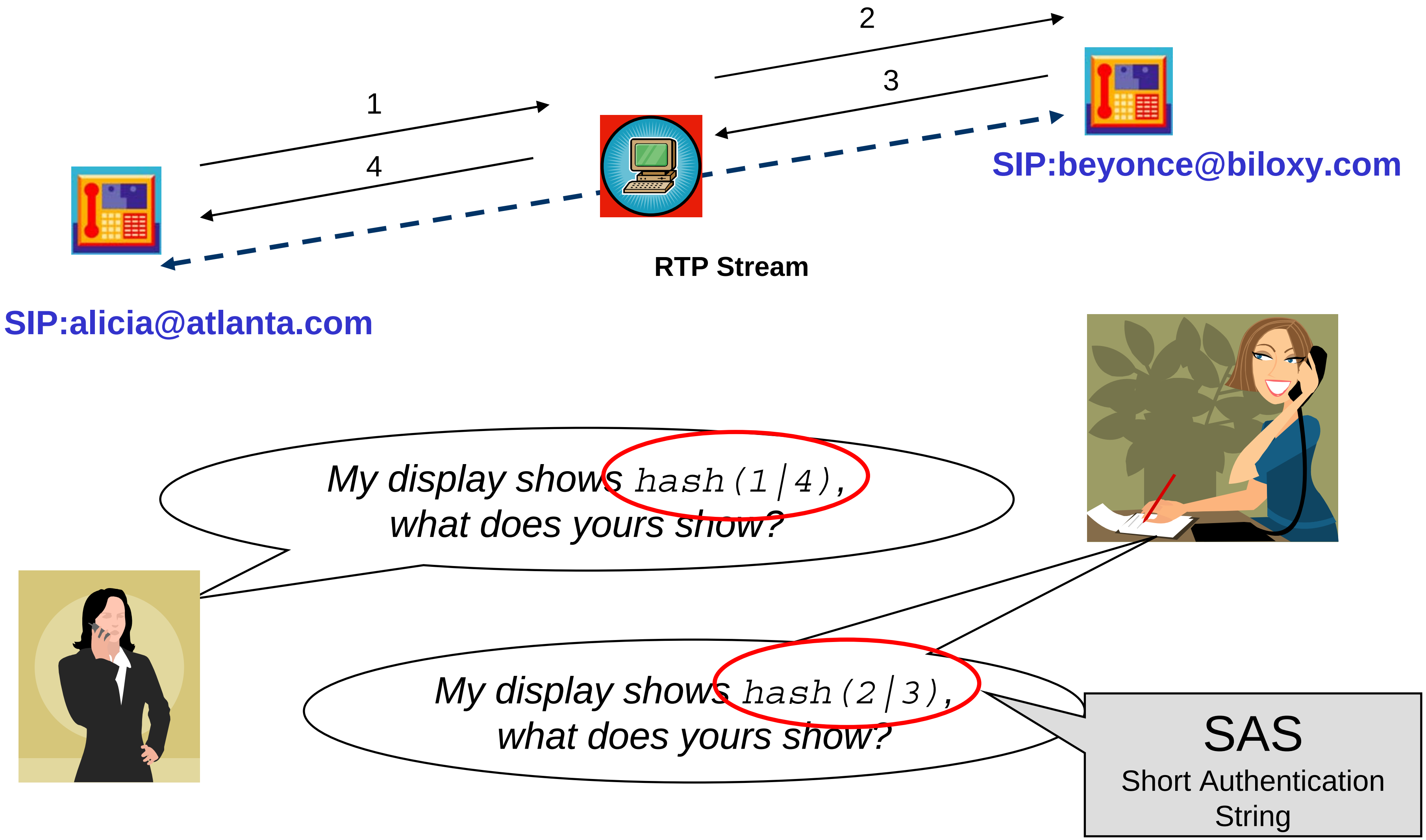
- ii. Could an attacker manage to read encrypted messages that are encrypted with a key established between Alice and Bob, when the attacker is able to read the messages and control the message flow (i.e. intercept and modify messages) between Alice and Bob?

ii: Yes. The attack is known as man-in-the-middle attack.




SIP
Proxy
SIP
Proxy
SIP:beyonce@biloxy.com
RTP Stream
SIP:alicia@atlanta.com

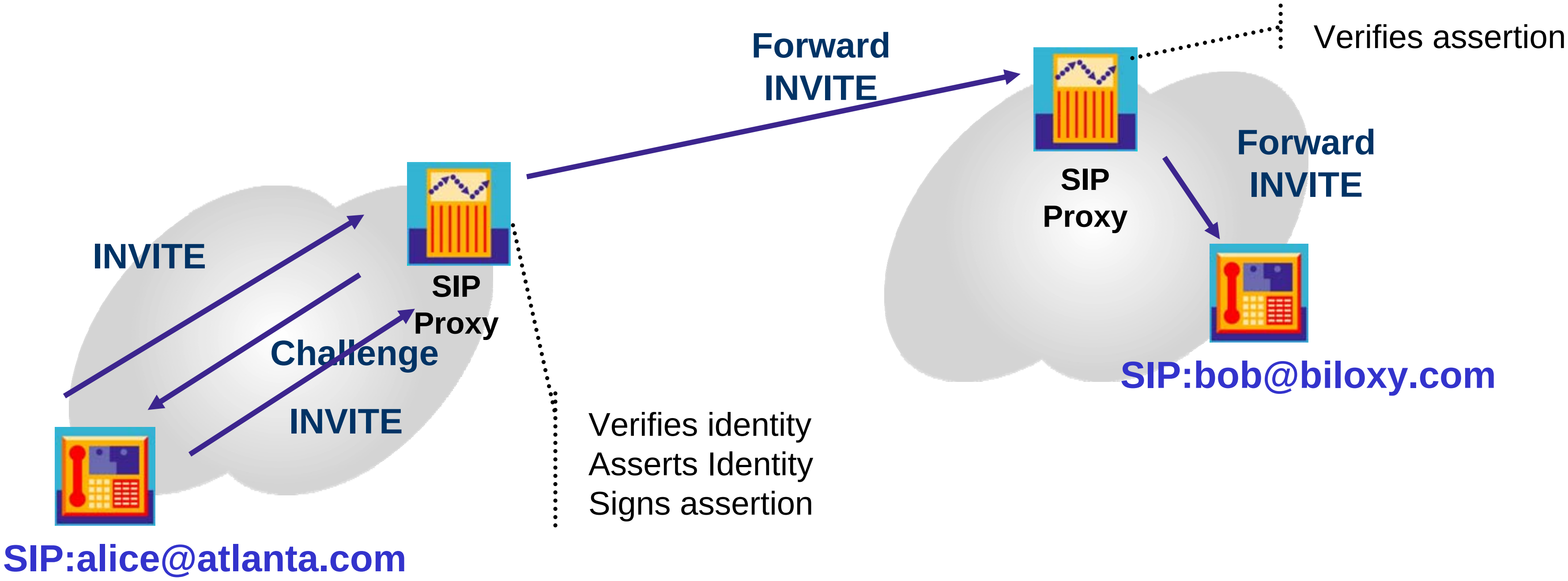

SIP:beyonce@biloxy.com
RTP Stream
SIP:alicia@atlanta.com


1
2
3
4
SIP:beyonce@biloxy.com
RTP Stream
SIP:alicia@atlanta.com
My display shows hash(1|4), what does yours show?
My display shows hash(2|3), what does yours show?
SAS
Short Authentication String


Zfone
Jon Callas on his laptop
Compare with partner:
sgmf
Verified
SECURE
AES-256
Secure since:
2006/08/02 21:39
Secure
Clear

Identity Assertion

- Domains assert the identities of their SIP users
- This assertion can be digitally signed by the domain to be verified by other domains / users



RFC 3325 + *J. Peterson, C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", draft-ietf-sip-identity-06 (work in progress), October 2005.*

End-to-end authentication

- **TLS is insufficient, because**
  - **Intermediary hops may not be trustworthy**
  - **All application layer hops need keys from each other**
- **Establish end-to-end authentication directly between user agents**

V. Gurbani, F. Audet, D. Willis, "The SIPSEC Uniform Resource Identifier (URI)", internet draft (work in progress), June 2006

Spam over IP Telephony

SPIT is much more obtrusive than e-mail Spam

- **your telephone might ring in the middle of the night…**
- **E-mails get "pulled" from a server by the user; VoIP calls are "pushed" to the user**
- **Content filtering needs to be done in real-time**

Reverse Turing Tests

- **Computerized test to validate that the communication partner is human and not a machine**
- **E.g. „What is 5 minus 2?“**
- **Problems**
  - **Language**
  - **“Old people…“**
  - **Urgent Calls**

Payments at risk

- **A Micropayment System that charges for every call**

Sender authentication

- … would help to fight SPIT
  - Not in place yet
  - Would not fully solve the problem

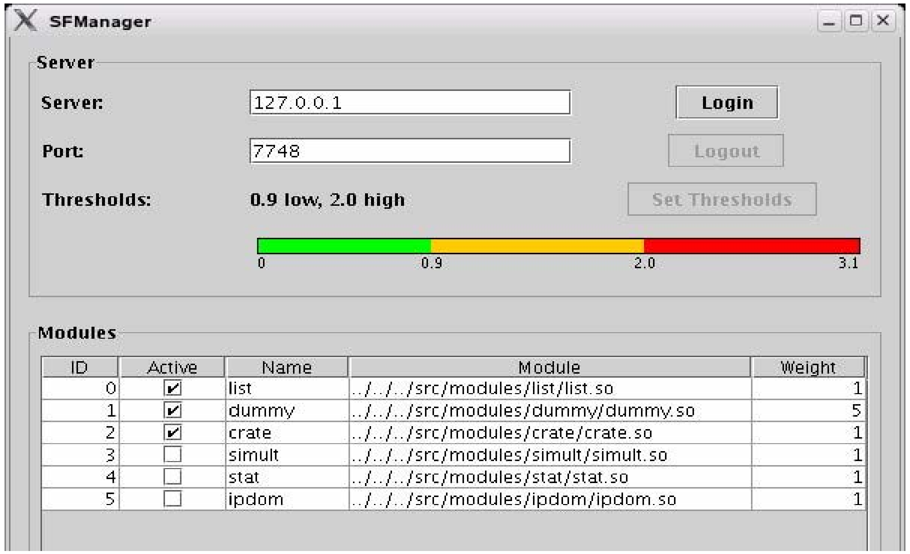
Computational puzzles

- For each Call, the initiator first has to solve a computationally complex challenge
  - Not a problem for regular call behaviour
  - Spammers would need much computation power
  - Makes spamming costly

Rosenberg, Jennings, The Session Initiation Protocol (SIP) and Spam, draft-ietf-sipping-spam-03, Oct. 2006

Example for SPIT Prevention Prototype
(NEC Europe Network Laboratories)

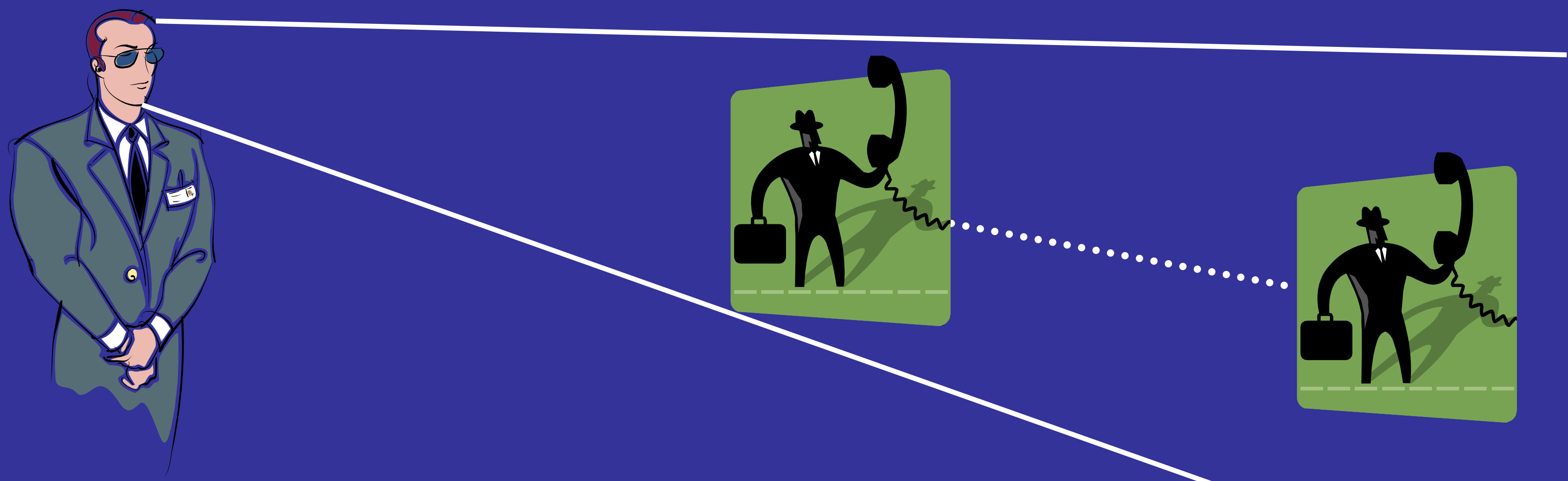
- **As a SIP Express Router (SER) module**
- **Implemented in C (autoconf, make, gcc)**
- **Modules are loaded dynamically**
- **Management applications (GUI) in Java**
  - **Load / unload / activate / deactivate modules**
  - **Adjust thresholds**
  - **Monitor call history**
  - **Monitor Turing Test**



Talk @SVS Oberseminar

- **Saverio Niccolini, NEC Europe Network Laboratories, will talk on SPIT Prevention and prototype implementation**
- **Where:**
  - **University of Hamburg**
- **When:**
  - **February 1st, 2007, 6 p.m.**
- **More info:**
  - **Google „Niccolini SVS“**

Lawful Interception

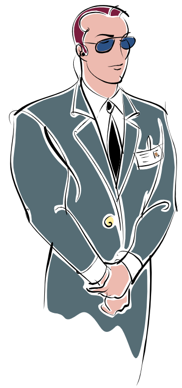


Lawful Interception

- legalised eavesdropping of communications by government agencies, e.g. when a criminal is under surveillance

Problems for Lawful Interception of VoIP

- VoIP provider and ISP can be different entities
- Signalling and payload usually take different routes
- Payload encryption in terminals



Standards are being developed

- ETSI
- 3GPP
- ATIS

Much controversy on LI for VoIP

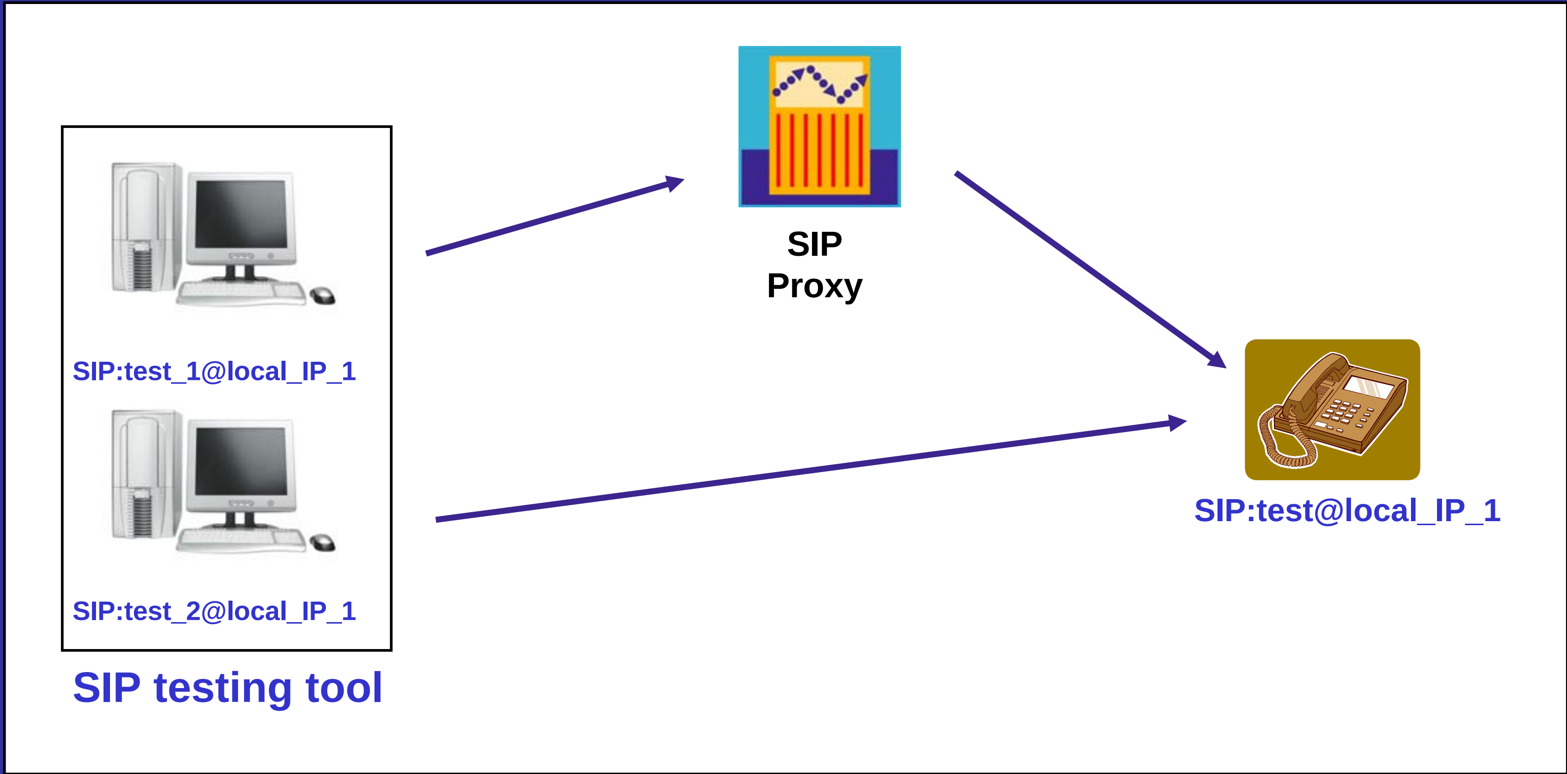
- Swiss government considers the use of trojan horses to enforce a footprint in devices
- LI imposes costs for SIP-providers that harm the development of this new technology

Much controversy on LI for VoIP (2)

"Neither the manageability of such a wiretapping regime nor whether it can be made secure against subversion seem clear. Rather it seems fairly clear that a CALEA-type regimen is likely to introduce serious vulnerabilities through its *architected security breach*."

Bellovin, Blaze, et al., "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP"

Testing SIP Devices



SIP Implementations

- **Have a TCP/IP Stack plus SIP functionality**
- **Are complex, thus susceptible to vulnerabilities**

Worms exploiting Terminal vulnerabilities spreading from phone to phone?

Approach: Testing of SIP implementations

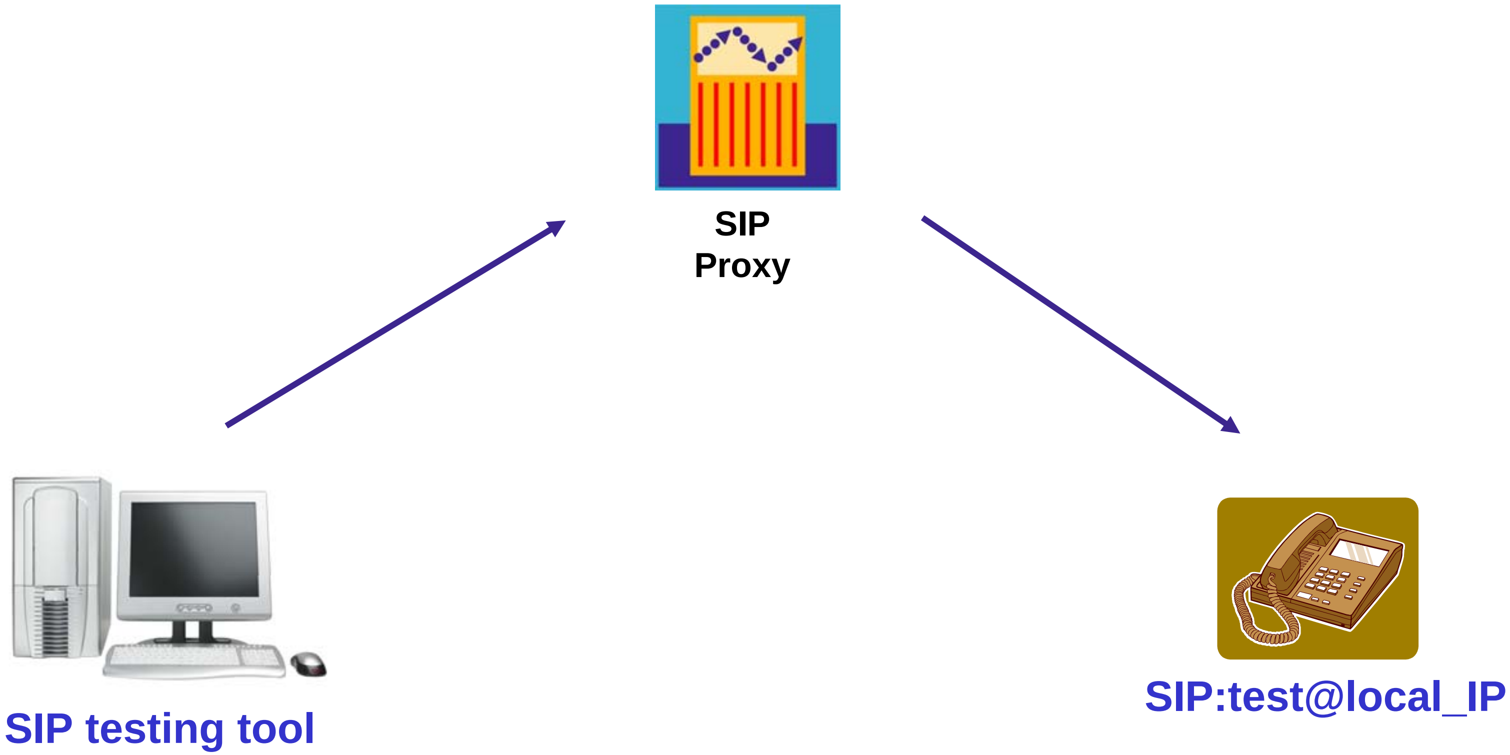
- **Many tools available as freeware**
  - SIPSAK
  - SIPp
- **Use existing SIP testing frameworks**
  - e.g. Protos Test-Suite from OULU University, Finland
- **RFC 4475:**
  - Examples of messages that can be used to “torture“ a SIP implementation

How to test SIP Implementations

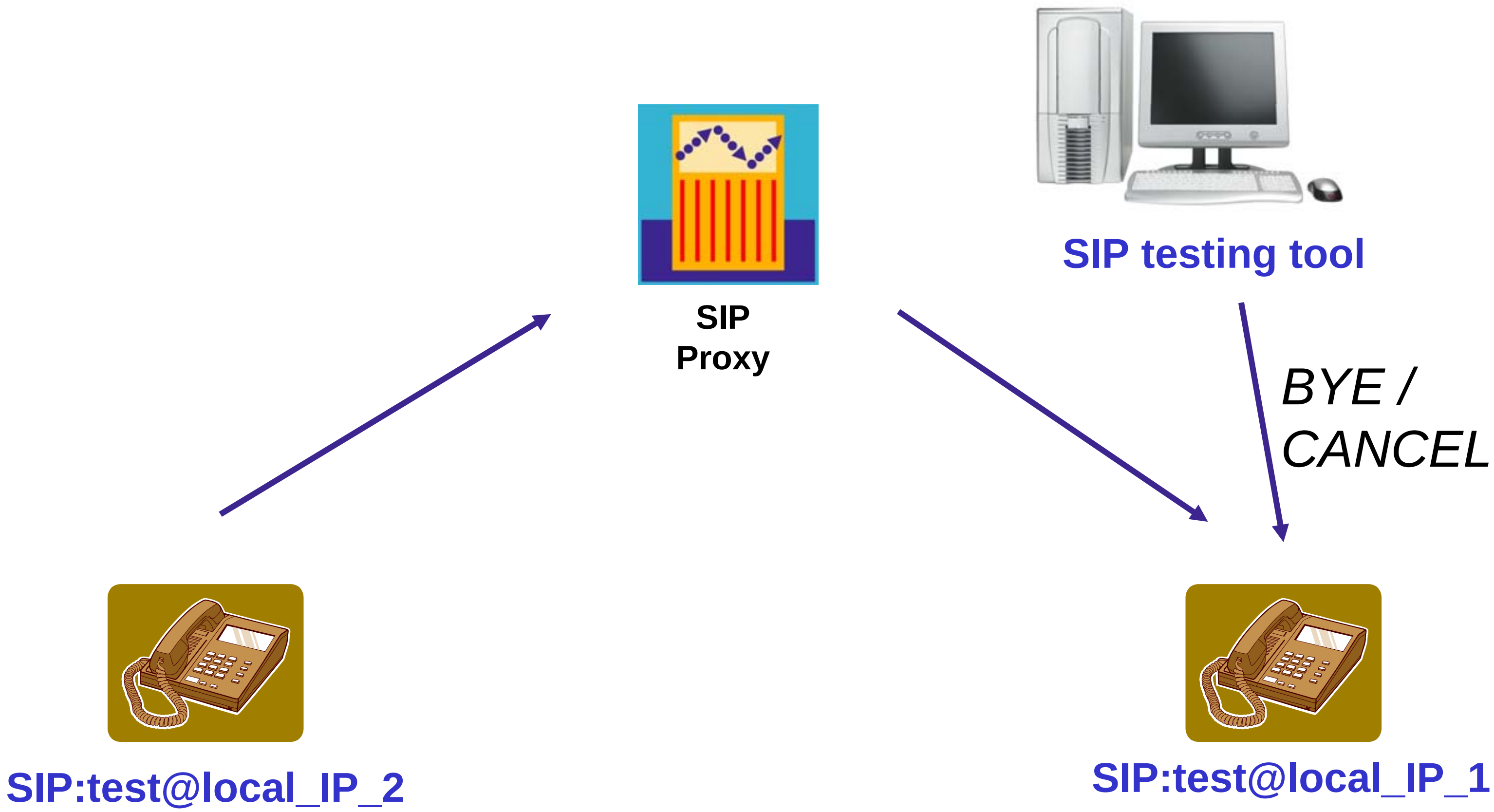
- Think of a test scenario
- Write a script using existing tools
- Execute test and log result

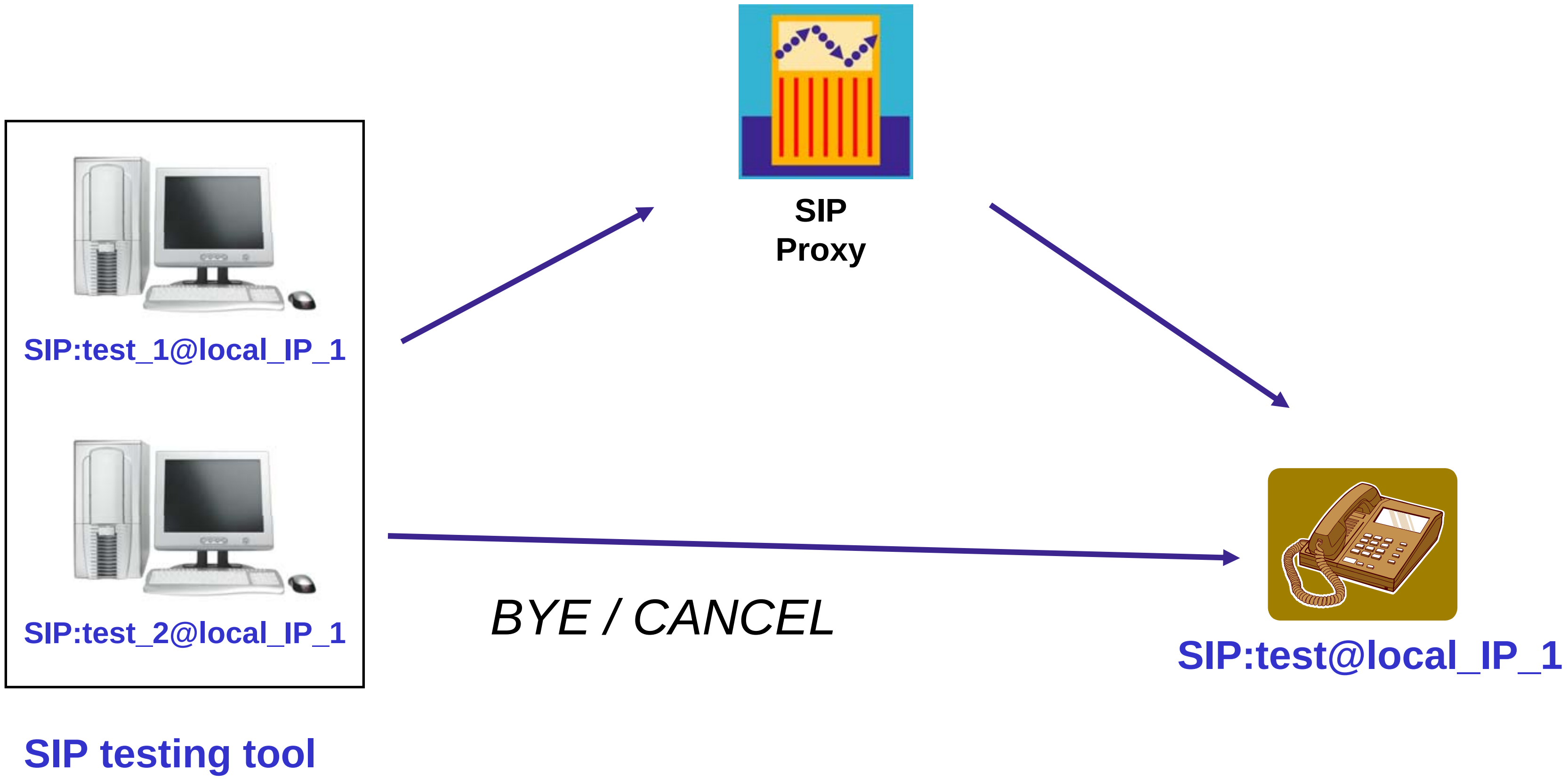
What we have done...

- Written a simple test tool
- Uses netcat and python
- Implements RFC 4475 (torture test messages) and some other tests


SIP
Proxy
SIP testing tool
SIP:test@local_IP

Testing SIP Implementations




SIP
Proxy
SIP:test_1@local_IP_1
SIP:test_2@local_IP_1
BYE / CANCEL
SIP:test@local_IP_1
SIP testing tool

Test Cases

- **Implementation of RFC 4475** (May 2006)
  - Torture test messages
  - 13 valid messages, 19 invalid messages
- **Denial of Service Tests on Session**
  - Send BYE or CANCEL message to phone under test while a session is being established
- **Denial of Service Tests on Phone**
  - Invite Message with different Tag and CallId
  - 1000 and 10000 Invite Messages
- **Buffer Overflow Search**
  - Inserting a long string in different headers

SISU Test Tool

```
SISU - (S)end S(i)p Me(s)sage Men(u) by Mieke and Stephan


<1> normal Invite-Message
<2> Torture Test Message - Based on - Rfc: 4475 - Network Working Group, 2006
<3> DosTest
<4> CancelMenu
<5> ByeMenu
<6> BufferTests
<7> Send a File (The File must be stored in the tmp folder)
<0> Quit


Sisu bezeichnet eine angeblich nur den Finnen eigene Eigenschaft. Das Wort ist daher auch kaum übersetzbar, bedeutet aber sov
iel wie Kraft, Ausdauer oder Beharrlichkeit, besonders in anscheinend aussichtslosen Situationen.
```

SISU Test Tool

Applications Places System

voip@ubuntu: ~/Desktop/Gruppe 1/montag

File Edit View Terminal Tabs Help

```
Invalid Messages Menu

Based on - Rfc: 4475 - Network Working Group, 2006

4311176@10.10.10.111:5060

<1> 1 : Invite Message
<2> 2 : Invite Message
<3> 3 : Invite Message
<4> 4 : Register Message
<5> 5 : Options Message
<6> 6 : Invite Message
<7> 7 : Invite Message
<8> 8 : Invite Message
<9> 9 : Invite Message
<10> 10 : Options Message
<11> 11 : Invite Message
<12> 12 : Invite Message
<13> 13 : Register Message
<14> 14 : Options Message
<15> 15 : Options Message
<16> 16 : Options Message
<17> 17 : Options Message
<18> 18 : Unknown Message
<19> 19 : Invite Message

<0> TortureMenu
```


hat ein Problem festgestellt und muss beendet
werden.
Falls Sie Ihre Arbeit noch nicht gespeichert hatten, können Daten möglicherweise verloren gegangen sein.
Dieses Problem bitte auch an Microsoft berichten.
Ein Problembericht, den Sie uns senden können, wurde erstellt. Wir werden diesen Bericht vertraulich und anonym bearbeiten.
Um zu sehen, welche Daten Ihr Bericht enthält, klicken Sie hier.
Problembericht senden
Nicht senden


Fehler: Netzwerk-Zeitüberschreitung
Der Server unter 10.10.10.14 braucht zu lange, um eine Antwort zu senden.
Die Website könnte vorübergehend nicht erreichbar sein, versuchen Sie es bitte später nochmals.
Wenn Sie auch keine andere Website aufrufen können, überprüfen Sie bitte die Netzwerk-/Internetverbindung.
Wenn Ihr Computer oder Netzwerk von einer Firewall oder einem Proxy geschützt wird, stellen Sie bitte sicher, dass Firefox auf das Internet zugreifen darf.
Nochmals versuchen

Valid Invite Message #7 (RFC 4475)

- **Phone 1:** *Rings*
- **Phone 3:** *Crash*
- **Phone 2 and 4:** *No Reaction*

Denial of Service Test (10000 messages)

- **Phone 1 and 4:** *No Reaction*
- **Phone 2 and 3:** *Stressed*

BYE and CANCEL Tests

- **Phone 1-4:** *Accurate behaviour*
- **Successful tearing down of sessions on other implementations**

Other Problems...

Anonymity in SIP communications

- Any intermediary can see who called whom
- RTP streams can be eavesdropped easily
- Possible Solution: Use a B2BUA as an pseudonimity-service

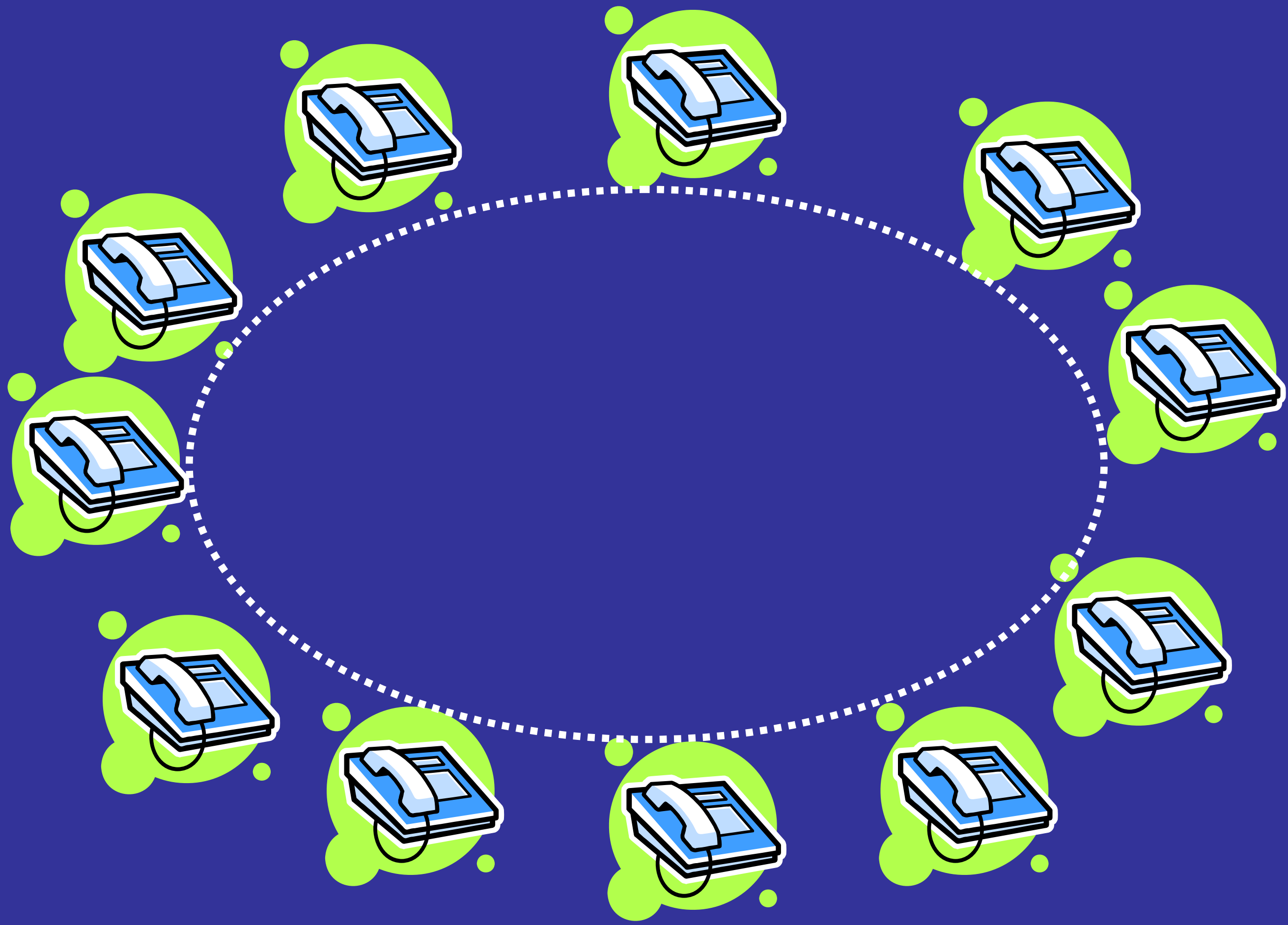
Emergency Calls

- How to prioritize emergency calls in a network with no quality of service (IP-networks)?
- See further „Emergency Context Resolution with Internet Technologies (ecrit)" *(http://www.ietf.org/html.charters/ecrit-charter.html)*

Usability

- How shall users cope with certificates or other credentials in SIP-Phones? (does not work with https-webpages)

Future Security Issues: P2P-SIP



What is P2P-SIP?

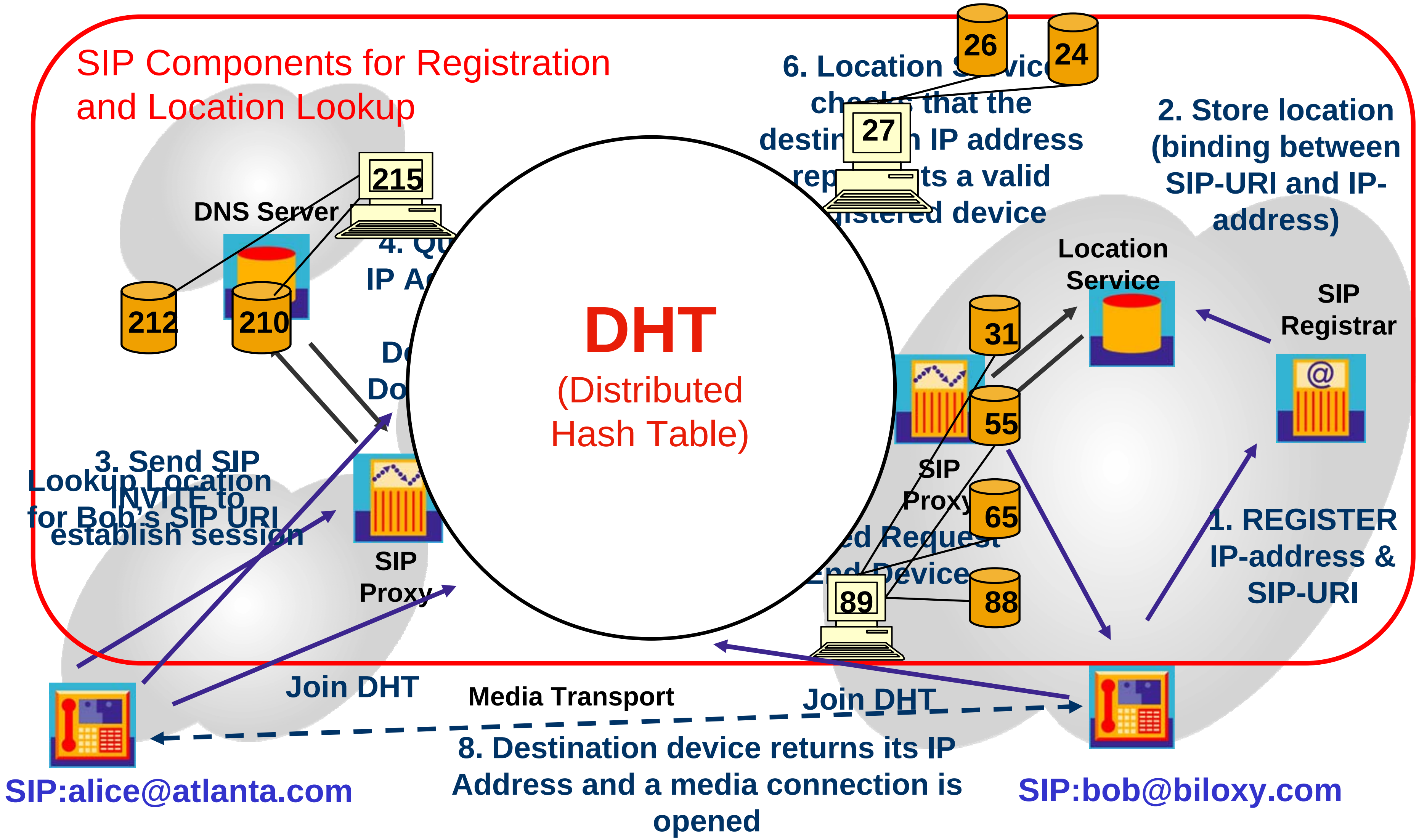
- Using a peer-to-peer network as a substrate for SIP user registration and location lookup

Not P2P SIP:

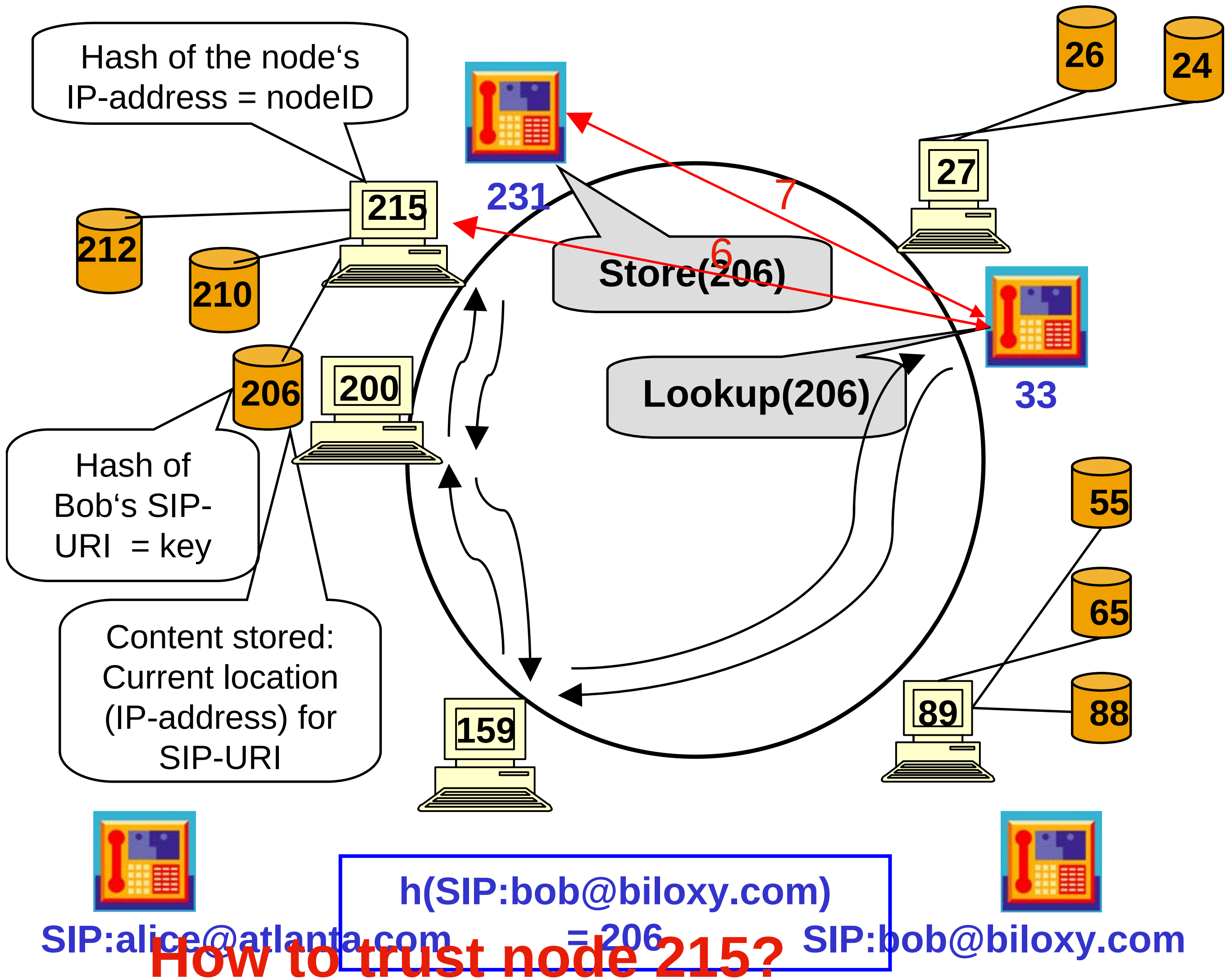
- SIPShare
- Skype

Benefits

- Cost reduction
- Ability to deploy without modifying controlled infrastructure (DNS)
- Robustness against failure
- Scalability



SIP Components for Registration and Location Lookup
DNS Server
215
212
210
DHT
(Distributed Hash Table)
6. Location Service checks that the destination IP address represents a valid registered device
26
24
27
2. Store location (binding between SIP-URI and IP-address)
Location Service
SIP Registrar
31
55
SIP Proxy
65
88
89
1. REGISTER IP-address & SIP-URI
3. Send SIP INVITE to establish session
Lookup Location for Bob's SIP URI
SIP Proxy
Join DHT
Media Transport
Join DHT
8. Destination device returns its IP Address and a media connection is opened
SIP:alice@atlanta.com
SIP:bob@biloxy.com



How to trust node 215?

Distributed Hash Table (DHT) offers:
Store(key)
Lookup(key)

(1) Bob's node joins the DHT

(2) Alice's node joins the DHT

(3) Bob registers his URI with the DHT

(4) Alice wants to call Bob

(5) DHT delivers the node (+IP-address) responsible for Bob's URI to Alice (node 215)

(6) Alice contacts node 215 to get Bob's IP-address (without using the overlay)

(7) Alice and Bob negotiate parameters and set up their session directly (without using the overlay)

P2P Paradigm introduces new security problems

- **No central authority in the network**
  - No trust in other nodes in the network
- **Distributed Hash Table is highly dynamic**
  - Node responsible for storing location of a SIP-URI changes frequently
- **Adversary nodes can:**
  - Spoof identity
  - Falsify messages in the overlay
  - Insert false messages in the overlay
  - ...

Previous work on DHT security

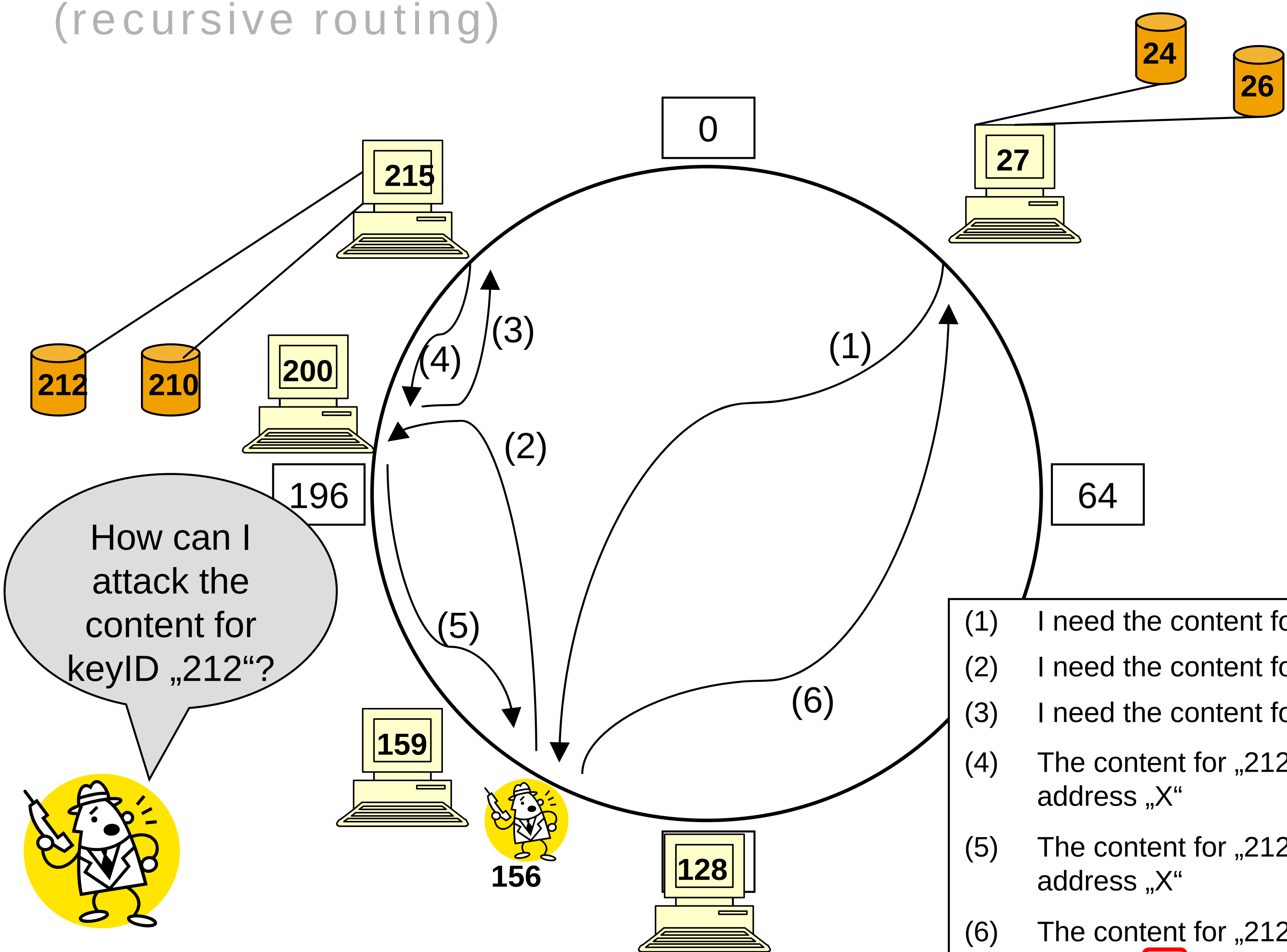
- **Focuses on availability of the (whole) network**

Threats for Real-time communication

- **Attacks on single nodes and single keys have to be considered**
- **Performance is important**
- **Application protocol (e.g. SIP) has to be considered**
  - **Attacks depend on content stored in the network**
  - **might be exploited for attacks/protection**

=> DHT security is application specific

Man-in-the-middle attack on P2P SIP (recursive routing)



(1) I need the content for „212“
(2) I need the content for „212“
(3) I need the content for „212“
(4) The content for „212“ is IP-address „X“
(5) The content for „212“ is IP-address „X“
(6) The content for „212“ is IP-address „Y“

Adding a central authority

- Takes away most benefits of P2P computing
  - Not scalable
  - Single point of failure / attack

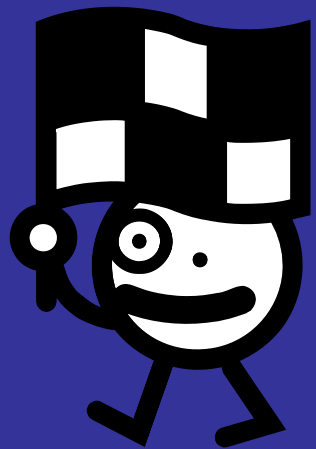
Using a distributed reputation management system to build „trust“

- Gain reputation for what?

Self-certifying approaches

=> Due to the lack of a central authority, authentication in peer-to-peer systems is a tough problem

Conclusion



Jan Seedorf - seedorf@informatik.uni-hamburg.de
SVS - Security in Distributed Systems

Conclusion

- **Differences to PSTN have significant security implications for VoIP/SIP**
- **Many efforts to secure SIP-based VoIP**
- **SIP-Security is an interesting, still evolving field**
- **P2P-SIP will impose new and different security challenges**

Thank you for your attention

Jan Seedorf

seedorf@informatik.uni-hamburg.de

University of Hamburg

SVS - Security in Distributed Systems