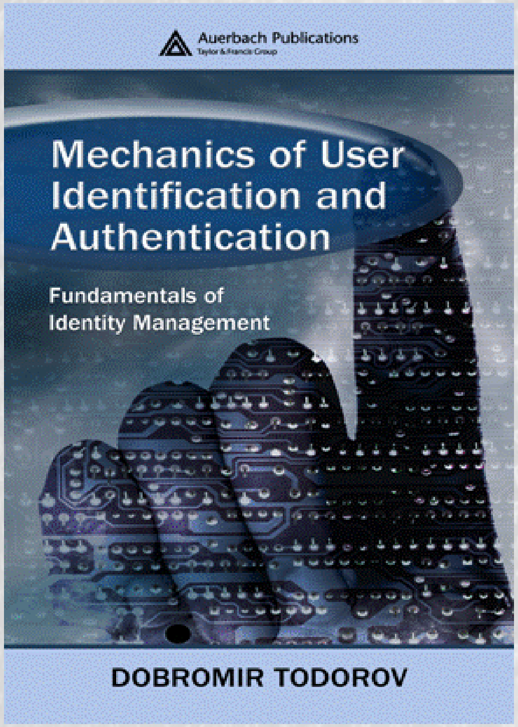
Unified Security for Unified Communications

Security and Protection of Information | Brno, CZ
Dobromir Todorov | BT Global Services | 05 May 2009

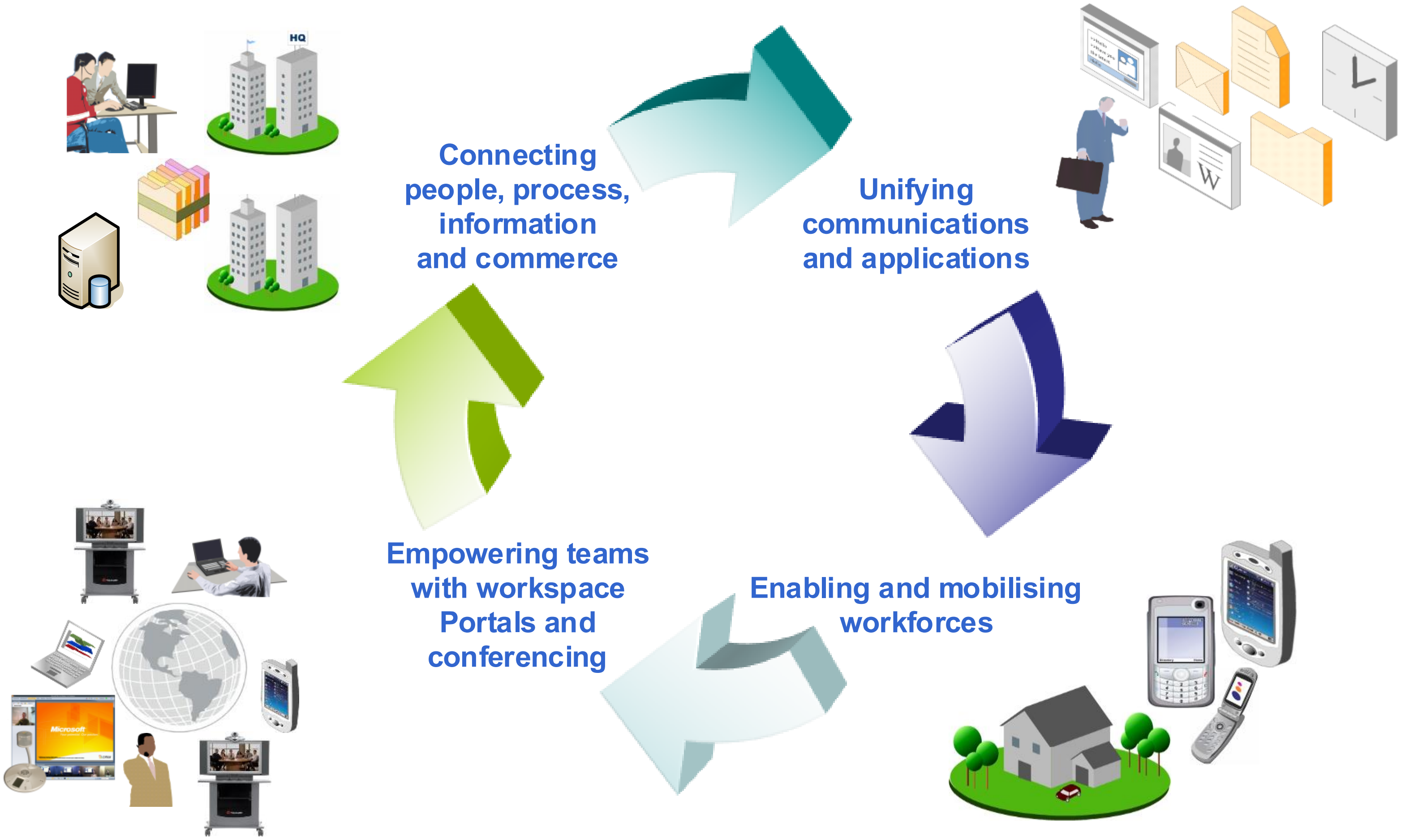

Auerbach Publications
Taylor & Francis Group
Mechanics of User Identification and Authentication
Fundamentals of Identity Management
DOBROMIR TODOROV

Overview

- Unified Communications for the Business
- Overview of Products and Technologies
- Identification and Authentication
- Signalling, IM and Presence
- Audio and Video Communications Security
- Security for the Social Web
- Summary
- Q&A

Unified Communications for the Business

The UCC Landscape



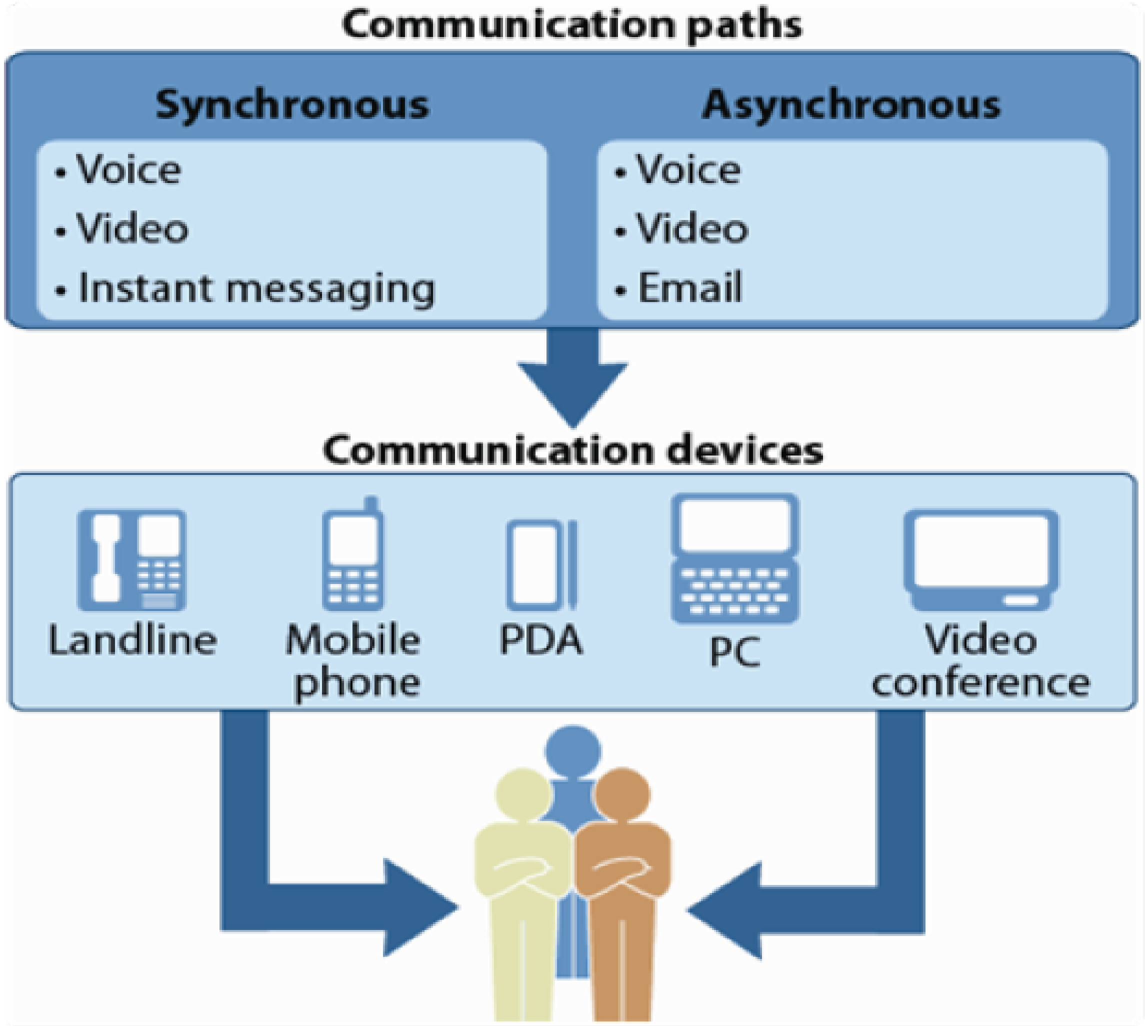
Connecting people, process, information and commerce

Unifying communications and applications

Enabling and mobilising workforces

Empowering teams with workspace Portals and conferencing

Unified Communications Defined



Communication paths

Synchronous
- Voice
- Video
- Instant messaging

Asynchronous
- Voice
- Video
- Email

Communication devices

UC(C) is on CIO's Agenda

- Forrester Research, March 2008
  - European Union:
    - 25% consider UC a priority
    - 10% consider UC a critical priority
  - North America
    - 24% consider UC a priority
    - 10% consider UC a critical priority

UC(C) Futures

- Presence as a dial tone
- One number (address) – one device
- Convergence with CRM and Contact Centres
- Communication Enabled Business Processes (CEBP) = Service Oriented Communications (SOC)
- …

CEBP Example

- A customer calls for a mortgage into a call centre
- The level of the mortgage is such that the agent cannot authorise it
- The agent initiates a CE business process to find three out of five higher level managers that can approve the mortgage
- The UC system finds three managers which are currently avaialble and conferences them in
- The customer has the mortgage approved, and a deal is closed.

CEBP Challenges

- Unified Communications provide for seamless communication between users and applications
  - How seamless does it need to be?
  - Should each user communicate with each application?
  - CEBP level firewalls – they don't exist
  - An infected client computer may spread malware using the UC platform; UC level firewalls
  - Antivirus software with UC support
- CEBP applications are yet to be developed and adopted; watch this space
- DO NOT implement CEBP unless you trust your UC platform

Products and Technologies

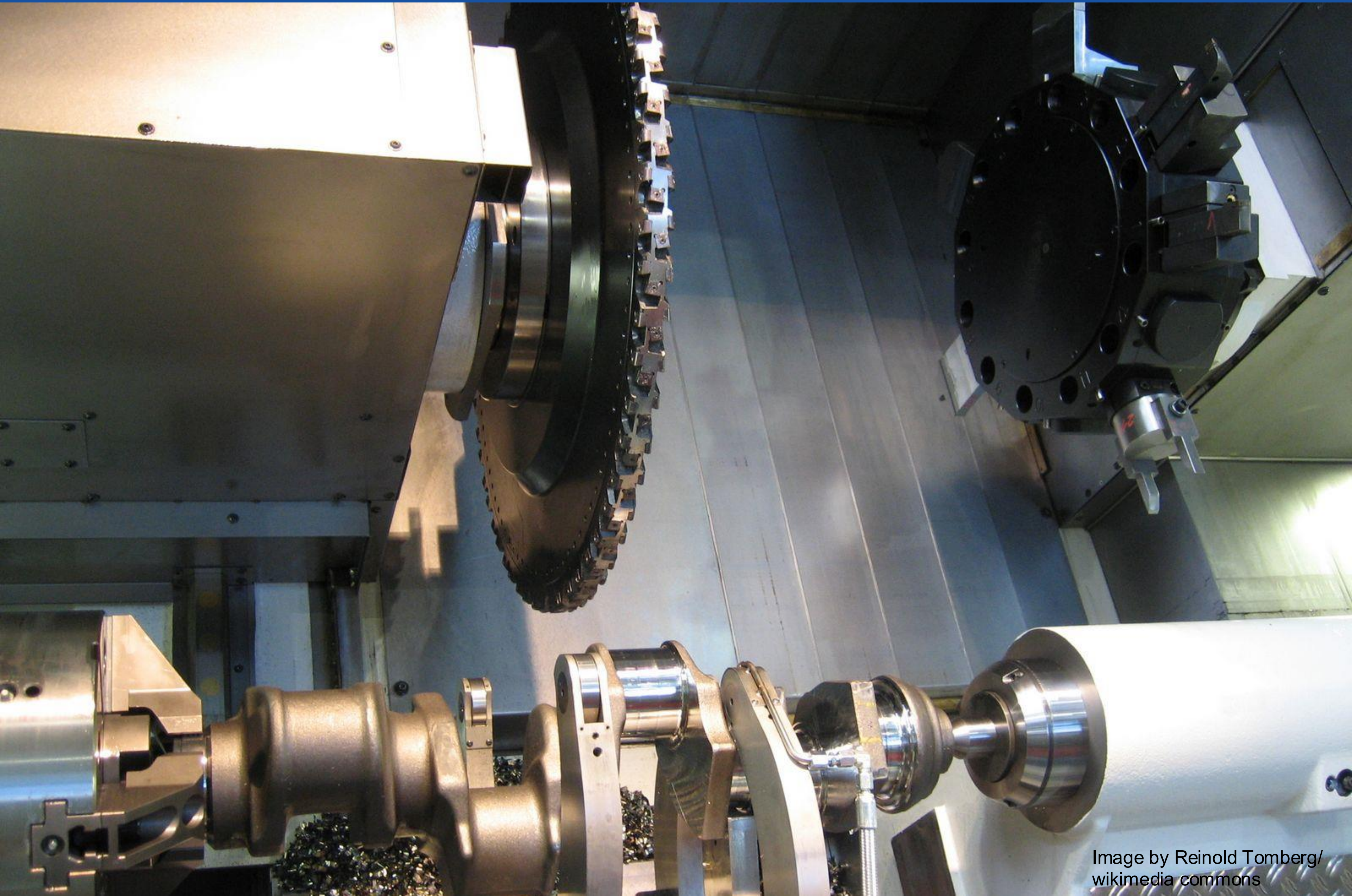
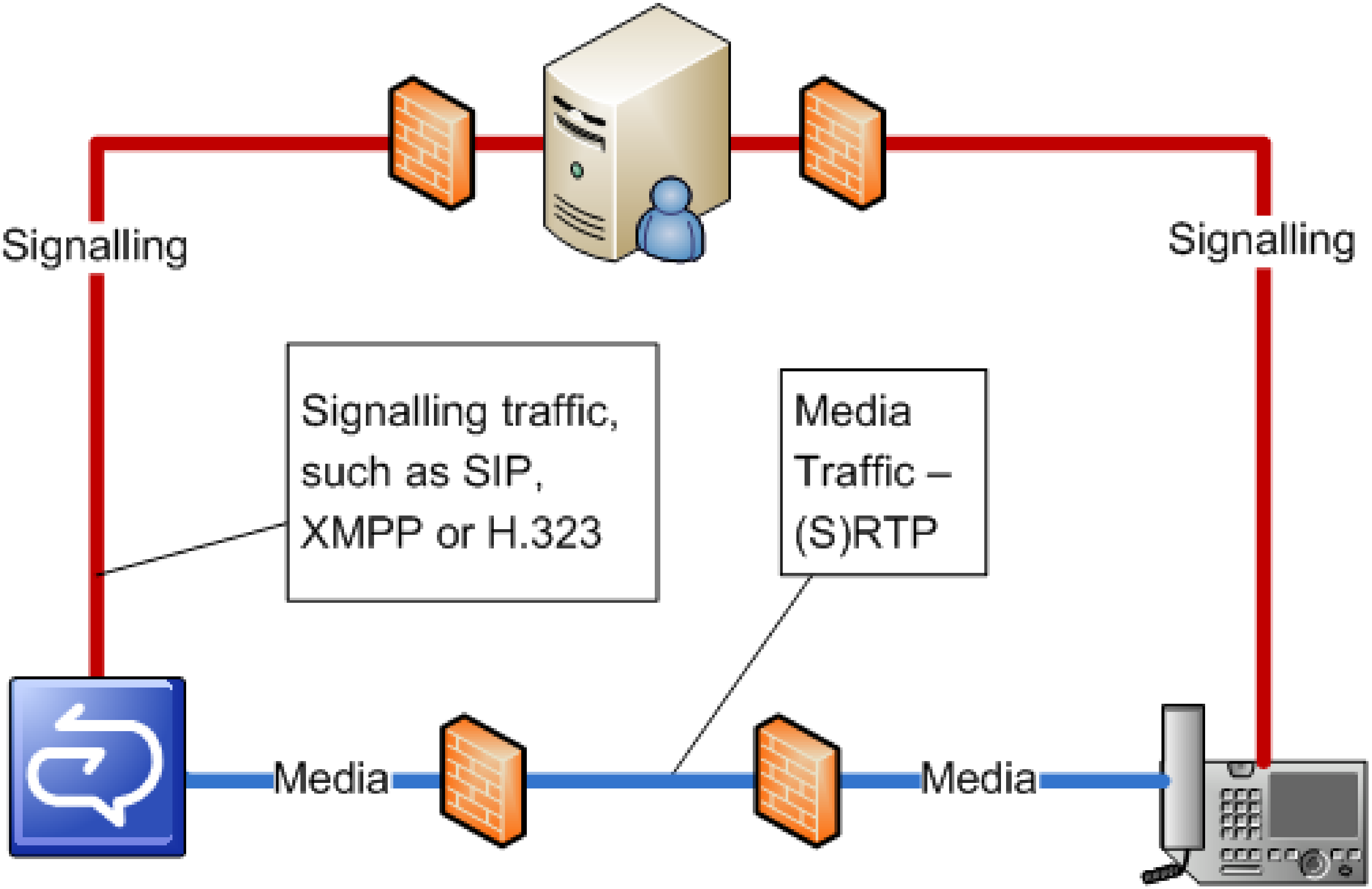


Image by Reinold Tomberg/ wikimedia commons

Products and Technologies Overview

Product	Areas	Vendor
Office Communications Server 2007 (inc R2)	Presence, IM, Voice, Video, Web Conferencing	Microsoft
Sametime	Presence, IM, Voice, Video, Web Conferencing	IBM
Call Manager/Unified Communications Manager & Unified Presence Server	Presence, IM, Voice, Video	Cisco
CS1K/CS2K	Voice, Video	Nortel
Asterisk (and derivatives)	Voice, Video	Digium/ Community/ OpenSource
WildFire/OpenFire	Presence, IM, (Voice, Video)	Jive Software

Signalling vs Media



Signalling vs Media/Payload

Type	Signalling	Media/Payload	Protocol Stack
Presence	SIP, XMPP	In-band (presence info)	SIP over TCP/TLS XMPP over TCP/TLS
Instant Messaging	SIP, XMPP	In-band (text messages)	SIP over TCP/TLS XMPP over TCP/TLS
E-mail	SMTP, IMAP, POP3, MAPI	In-band (MIME, Plaintext, RTF, HTML)	SMTP over TCP/TLS IMAP over TCP/TLS POP3 over TCP/TLS MAPI over MS-RPC
Directory Access	LDAP	In-band (LDAP PDUs)	LDAP over TCP/TLS
Voice & Video	SIP, XMPP, H.323	Out of Band: RTP, SRTP	SIP over TCP/TLS XMPP over TCP/TLS RTP & SRTP
Web Conferencing	HTTP, PSOM (MS)	In-band	Java over HTTP(s) Ajax over HTTP(s) PSOM over TCP

Security vs UC(C) [1/3]

- UC is an application network on top of the telecommunications network
  - As such, it is effectively a **tunnelling technology**

Security vs UC(C) [2/3]

- How seamless should communication between users be?
  - UC allows users (and applications) to communicate; how do you **prevent** them from communicating?
    - Policies, prevention of virus spread...

Security vs UC(C) [3/3]

- What happens if a user is infected with a virus, or accidentally runs a Trojan?
  - Malware may spread across the UC network completely bypassing firewalls and IDS/IPS systems....
  - Malware may compromise service availability (denial of service attacks)

Identification and Authentication

Telephony Security Quiz

- Question 1: What identification is there on the PSTN for both caller and called party?
  - PSTN (or PBX) port ID
  - Telephone number (potentially)

- Question 2: What authentication is there on the PSTN or both caller and called party(or TDM PBX telephony infrastructure)?
  - Physical access (to the socket in the wall)
  - Extension mobility (modern world - user login with a PIN)

Identity Challenges in the UCC/IPT World

- Endpoint may reside anywhere on the network (wired in the building, wireless in the building, across the WAN, on the Internet...)
- IPT phones have limited resources
  - Device and user authentication not very common: resource constraints
- IPT phone keyboard cumbersome to use for long and complex passwords
  - Alternative password - or PIN (4-6 digits) – is often used
  - "As strong as the weakest link..."
- SSL/TLS Client (Phone) Authentication
  - Requires secure storage of private key – but phones are easy to steal...

UCC/IPT Identity At the Data Link Layer

- 802.1x Authentication (port authentication)
- Port-level Security based on MAC address (limited protection/not scalable)
- Dedicated VLANs (requires other technologies)

Secure UCC/IPT Phones

- Specialised Phones
  - Limited
  - Too expensive
- Physical Security for IP phones
- Softphones
  - Computer security is much better
  - TPMs available
- Futures
  - Biometric authentication in phones (actually, available on Tanjay phones…)
  - SmartCard readers in phones
  - TPMs in phones

Unified Communications Identity

- Caller Identity – who is initiating the call?
  - SIP From field is used for user Identity
    - However, the caller can put any ID there; servers must check ID
  - XMPP To and From attributes
- Called party identity - How do we ensure that the call has been routed to the party we wanted to call (aka peer identity authentication)?
  - SIP To field is used for user identity of called party
    - However, communication will typically go via a proxy
  - XMPP To and From attributes

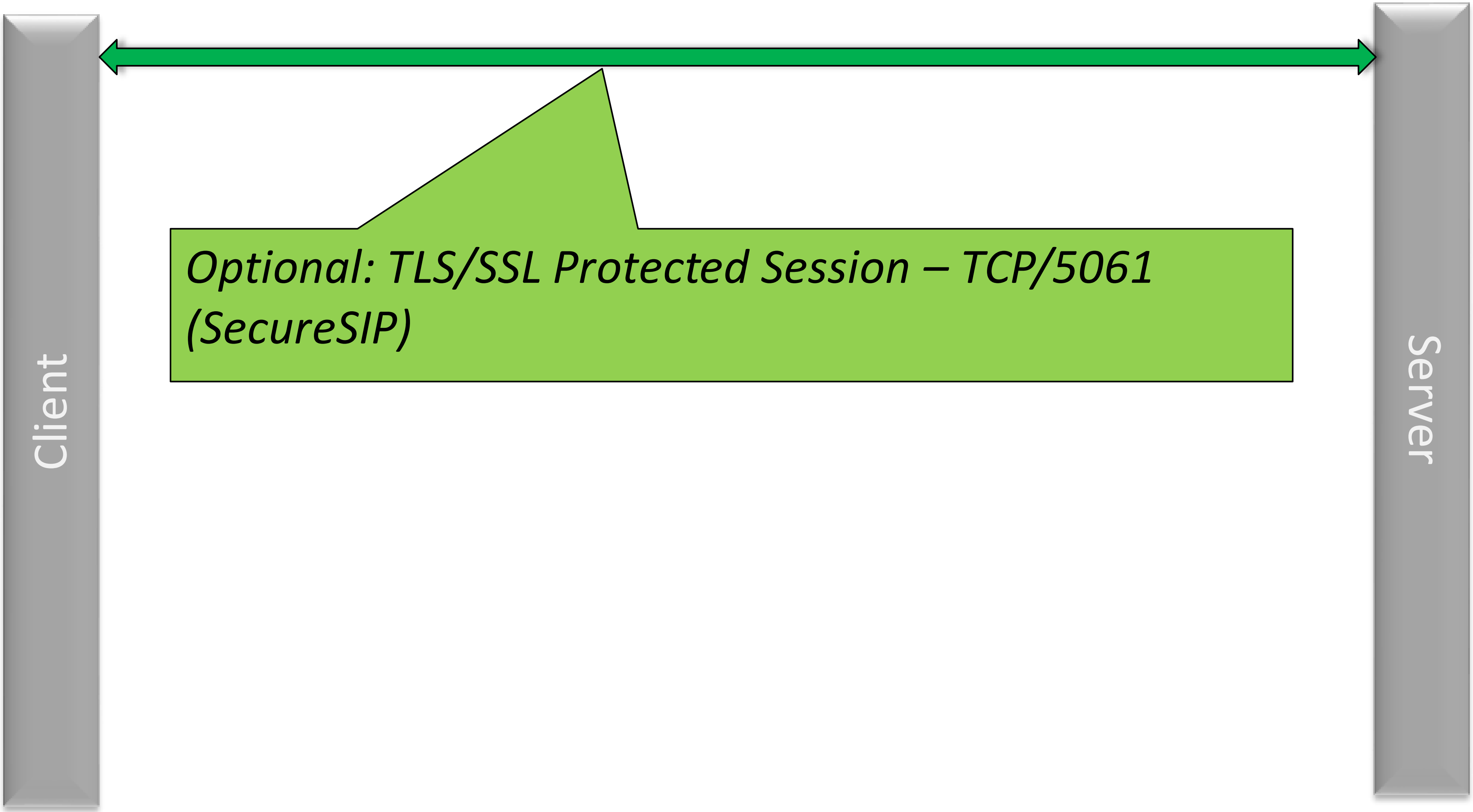
UC(C) Identity Scenarios

- Internal User
  - Authenticate against internal domain
- Remote User
  - Authenticate against internal domain
- Federated User
  - Authenticated by another domain
  - Requires trust in external parties
  - Explicit trust: federated only with known domains
  - Implicit trust: federate with anyone
  - Indicate to users that identity is federated ("Beware...")
- Public IM Services User – Limited Trust
  - Identified and Authenticated
  - Identity cannot be trusted - authentication meaningless
  - Indicate to users that identity is federated ("Beware...")

UC(C) Identity Solutions within the Domain

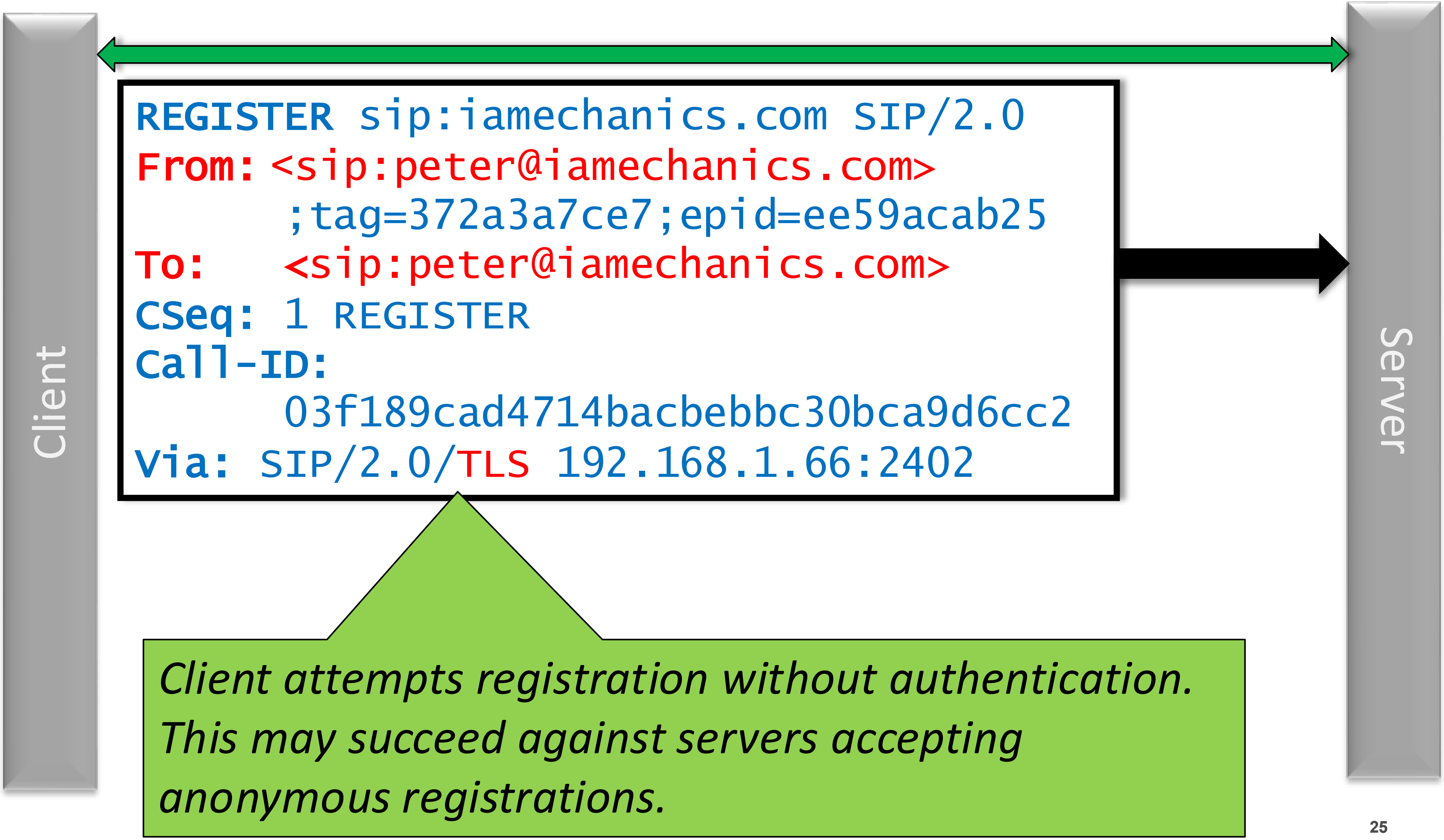
- Authentication against Directory (often AD)
  - SIP supports digest authentication (similar to HTTP)
  - XMPP supports SASL
- Caller identity
  - Authenticate users (use the SIP Proxy-authenticate header) against a domain-wide authentication source
- Called party identity
  - All servers trust each other to verify and pass peer identity
  - Registration Server checks peer identity (authenticates peer) upon registration
  - Maintain the integrity of the authentication database

SIP Registration Example [1/5]



Optional: TLS/SSL Protected Session – TCP/5061 (SecureSIP)

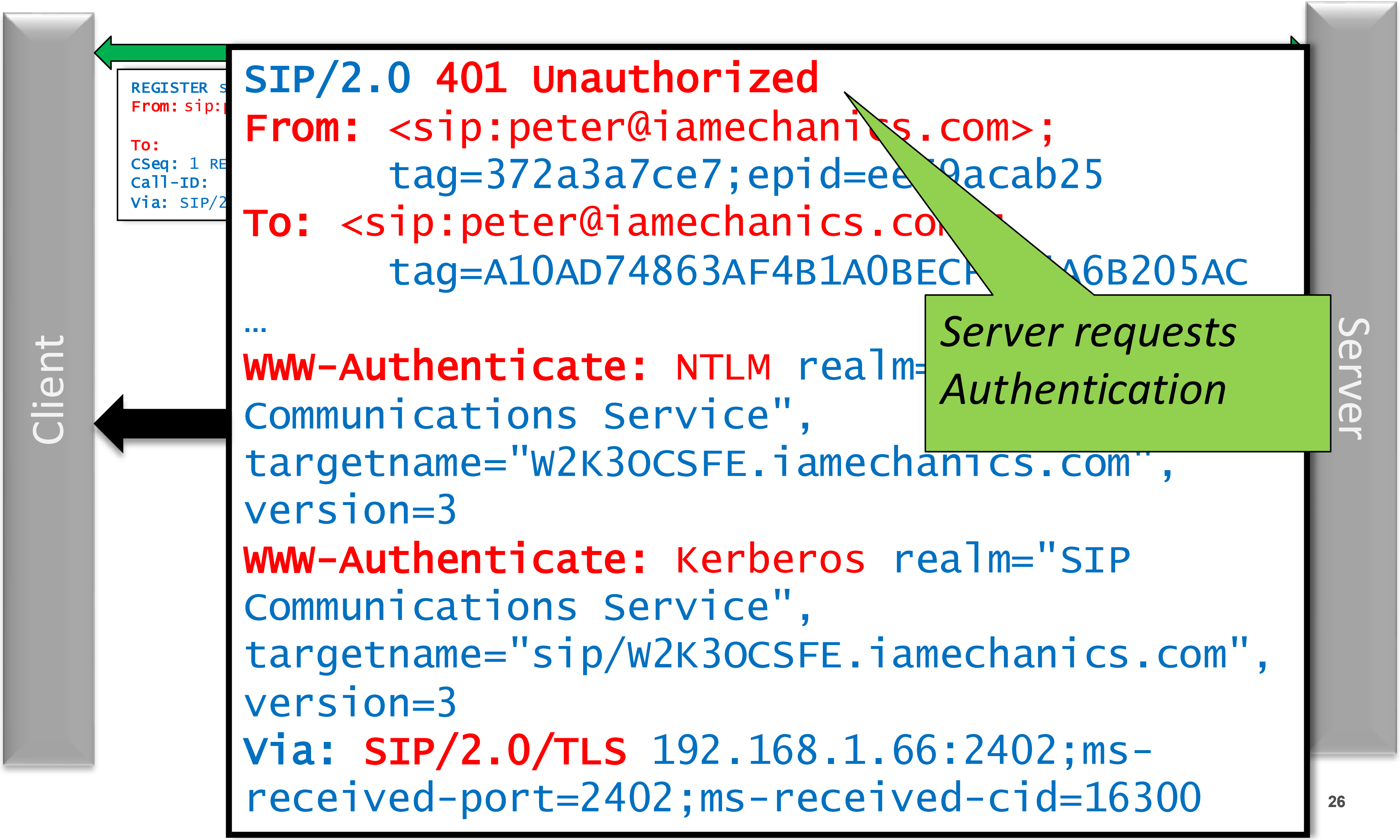
SIP Registration Example [2/5]



```
REGISTER sip:iamechanics.com SIP/2.0
From: <sip:peter@iamechanics.com>
      ;tag=372a3a7ce7;epid=ee59acab25
To:    <sip:peter@iamechanics.com>
CSeq: 1 REGISTER
Call-ID:
      03f189cad4714bacbebbc30bca9d6cc2
Via: SIP/2.0/TLS 192.168.1.66:2402
```

Client attempts registration without authentication. This may succeed against servers accepting anonymous registrations.

SIP Registration Example [3/5]



```
REGISTER s
From: sip:

To:
CSeq: 1 RE
Call-ID:
Via: SIP/2
```

```
SIP/2.0 401 Unauthorized
From: <sip:peter@iamechani s.com>;
      tag=372a3a7ce7;epid=ee 9acab25
To: <sip:peter@iamechanics.co
      tag=A10AD74863AF4B1A0BEC A6B205AC
…
WWW-Authenticate: NTLM realm=
Communications Service",
targetname="W2K3OCSFE.iamechanics.com",
version=3
WWW-Authenticate: Kerberos realm="SIP
Communications Service",
targetname="sip/W2K3OCSFE.iamechanics.com",
version=3
Via: SIP/2.0/TLS 192.168.1.66:2402;ms-
received-port=2402;ms-received-cid=16300
```

Server requests Authentication

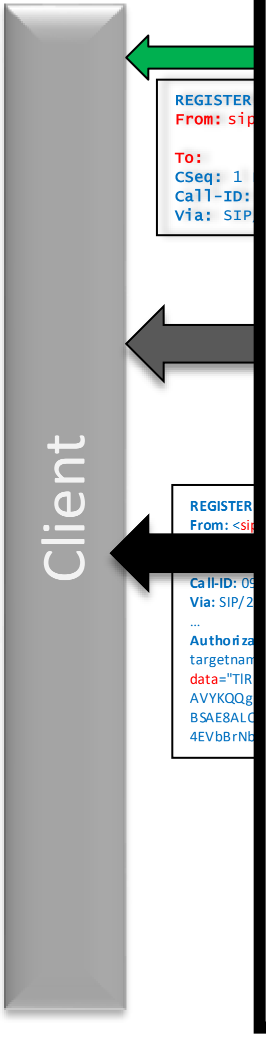
http://www.iamechanics.com

SIP Registration Example [4/5]

```
REGISTER sip:iamechanics.co
From:
<sip:peter@iamechanics.com>                    d=
ee59acab25
To: <sip:peter@iamechanics.
CSeq: 3 REGISTER
Call-ID: 0910f859b77b4d388    c01f7c8f7c60
Via: SIP/2.0/TLS 192.16    1.66:2406
…
Authorization: NTLM qop="auth", realm="SIP
Communications Service",
targetname="W2K3OCSFE.iamechanics.com", gssapi-
data="TlRMTVNTUAADAAAAGAAYAIoAAAAYABgAogAAAAAAA
BIAAAAKgAqAEgAAAAYABgAcgAAABAAEAC6AAAAVYKQQgUBKA
oAAAAPcABlAHQAZQByAEAAaQBhAG0AZQBjAGgAYQBuAGkAYw
BzAC4AYwBvAG0AVABPAEQATwBSAE8ALQBEAC0ASQBOAFMAFU
v/YdGL7mARhLgTpaLdkgTtIQlBtxKpbxMrB+rEyC3tApGztz
Cb7tvp5Y0Vq2EMkSw34EVbBrNboNNl3vY4rQ==",
opaque="199FAA06", version=3
```

Client authenticates using NTLM over Digest Authentication

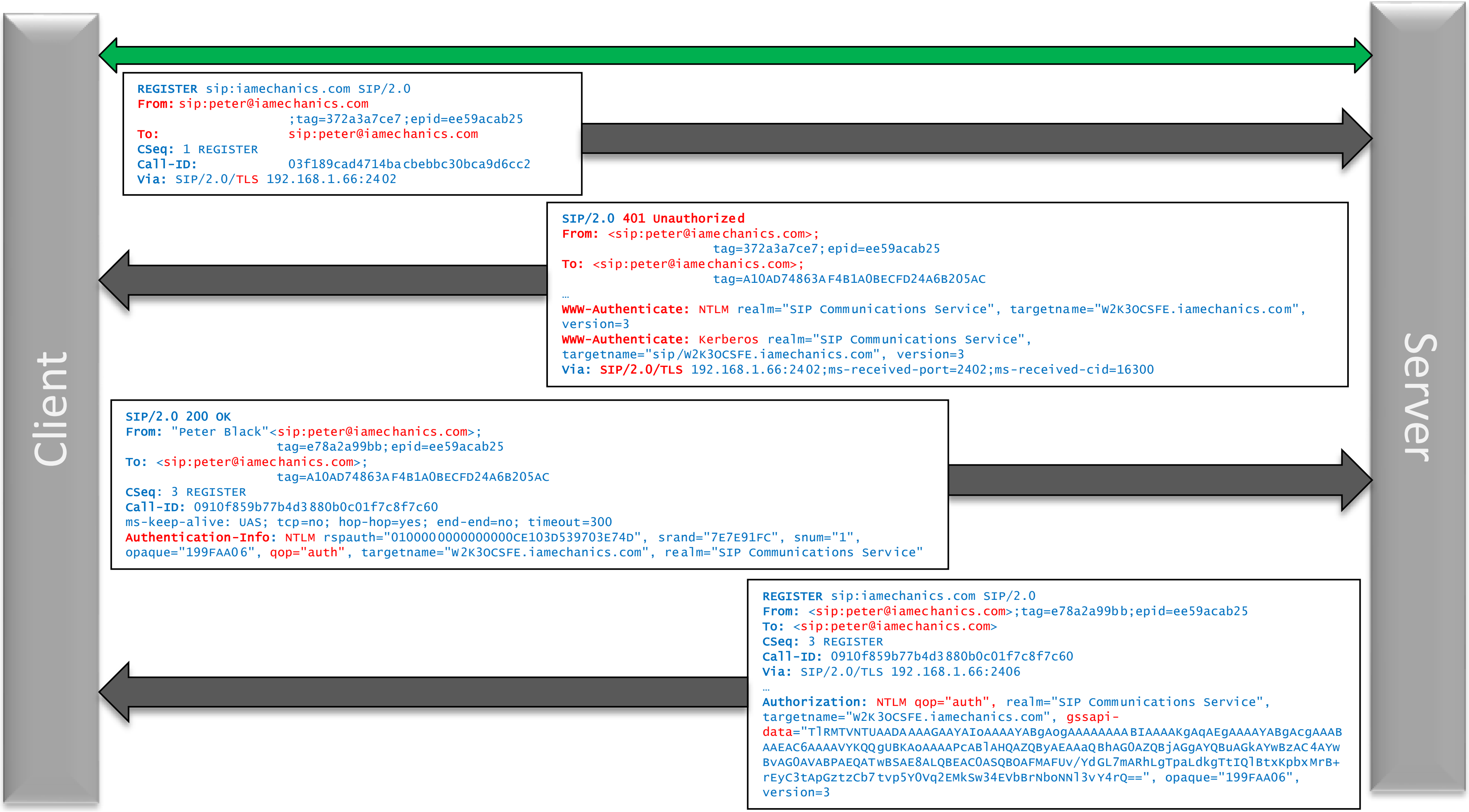
SIP Registration Example [5/5]



```
SIP/2.0 200 OK
From: "Peter
Black"<sip:peter@iamechanics.com>;
      tag=e78a2a99bb;epid=ee5
To: <sip:peter@iamechanics.co
      tag=A10AD74863AF4B1A0BE
CSeq: 3 REGISTER
Call-ID: 0910f859b77b4d3880
ms-keep-alive: UAS; tcp=n, h
end=no; timeout=300
Authentication-Info: NTLM
rspauth="01000000000000CE103D539703E74D",
srand="7E7E91FC", snum="1",
opaque="199FAA06", qop="auth",
targetname="W2K3OCSFE.iamechanics.com",
realm="SIP Communications Service"
```

Server authenticates using NTLM over HTTP/digest Authentication

SIP Registration Example



```
REGISTER sip:iamechanics.com SIP/2.0
From: sip:peter@iamechanics.com
                     ;tag=372a3a7ce7;epid=ee59acab25
To:                  sip:peter@iamechanics.com
CSeq: 1 REGISTER
Call-ID:             03f189cad4714bacbebbc30bca9d6cc2
Via: SIP/2.0/TLS 192.168.1.66:2402
```

```
SIP/2.0 401 Unauthorized
From: <sip:peter@iamechanics.com>;
                    tag=372a3a7ce7;epid=ee59acab25
To: <sip:peter@iamechanics.com>;
                    tag=A10AD74863AF4B1A0BECFD24A6B205AC
…
WWW-Authenticate: NTLM realm="SIP Communications Service", targetname="W2K3OCSFE.iamechanics.com",
version=3
WWW-Authenticate: Kerberos realm="SIP Communications Service",
targetname="sip/W2K3OCSFE.iamechanics.com", version=3
Via: SIP/2.0/TLS 192.168.1.66:2402;ms-received-port=2402;ms-received-cid=16300
```

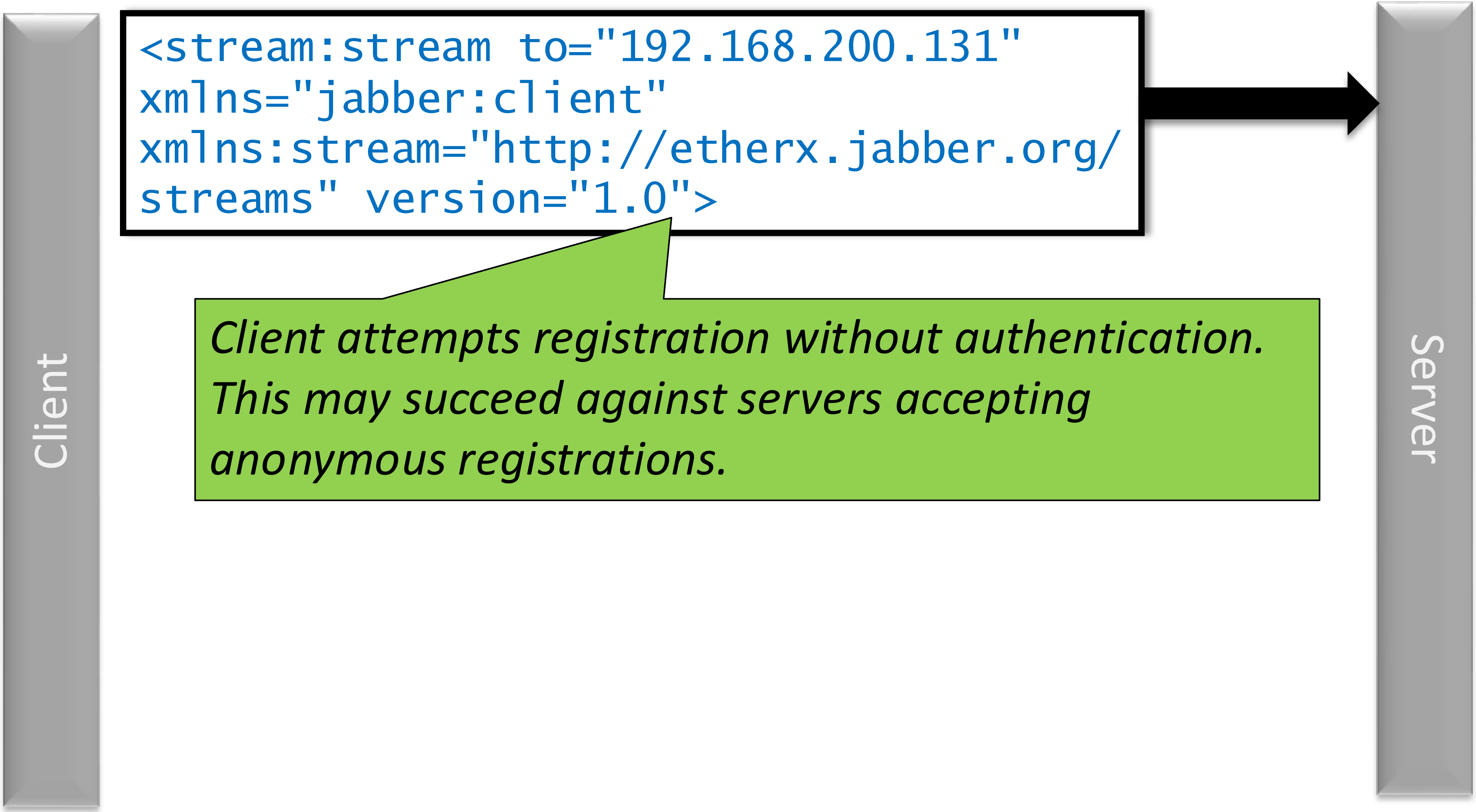
```
SIP/2.0 200 OK
From: "Peter Black"<sip:peter@iamechanics.com>;
                    tag=e78a2a99bb;epid=ee59acab25
To: <sip:peter@iamechanics.com>;
                    tag=A10AD74863AF4B1A0BECFD24A6B205AC
CSeq: 3 REGISTER
Call-ID: 0910f859b77b4d3880b0c01f7c8f7c60
ms-keep-alive: UAS; tcp=no; hop-hop=yes; end-end=no; timeout=300
Authentication-Info: NTLM rspauth="01000000000000000CE103D539703E74D", srand="7E7E91FC", snum="1",
opaque="199FAA06", qop="auth", targetname="W2K3OCSFE.iamechanics.com", realm="SIP Communications Service"
```

```
REGISTER sip:iamechanics.com SIP/2.0
From: <sip:peter@iamechanics.com>;tag=e78a2a99bb;epid=ee59acab25
To: <sip:peter@iamechanics.com>
CSeq: 3 REGISTER
Call-ID: 0910f859b77b4d3880b0c01f7c8f7c60
Via: SIP/2.0/TLS 192.168.1.66:2406
…
Authorization: NTLM qop="auth", realm="SIP Communications Service",
targetname="W2K3OCSFE.iamechanics.com", gssapi-
data="TlRMTVNTUAADAAAAGAAYAIoAAAAYABgAogAAAAAAAABIAAAAKgAqAEgAAAAYABgAcgAAAB
AAEAC6AAAAVYKQQgUBKAoAAAAPCABlAHQAZQByAEAAaQBhAG0AZQBjAGgAYQBuAGkAYwBzAC4AYw
BvAG0AVABPAEQATwBSAE8ALQBEAC0ASQBOAFMAFUv/YdGL7mARhLgTpaLdkgTtIQlBtxKpbxMrB+
rEyC3tApGztzCb7tvp5Y0Vq2EMkSw34EvbBrNboNNl3vY4rQ==", opaque="199FAA06",
version=3
```

XMPP and SASL Authentication

- SASL = Simple Authentication and Security Layer (RFC 2222)
- Layer of abstractions for applications to access user authentication functions and have their network traffic protected
- Widely used by legacy TCP interactive applications (SMTP, POP3, IMAP, LDAP (modified))
- Applications include a command verb to enter SASL negotiation
- SASL relies upon pluggable authentication mechanisms to do the actual job:
  - Kerberos IV
  - GSS-API
  - S/Key
  - CRAM-MD5/Digest-MD5

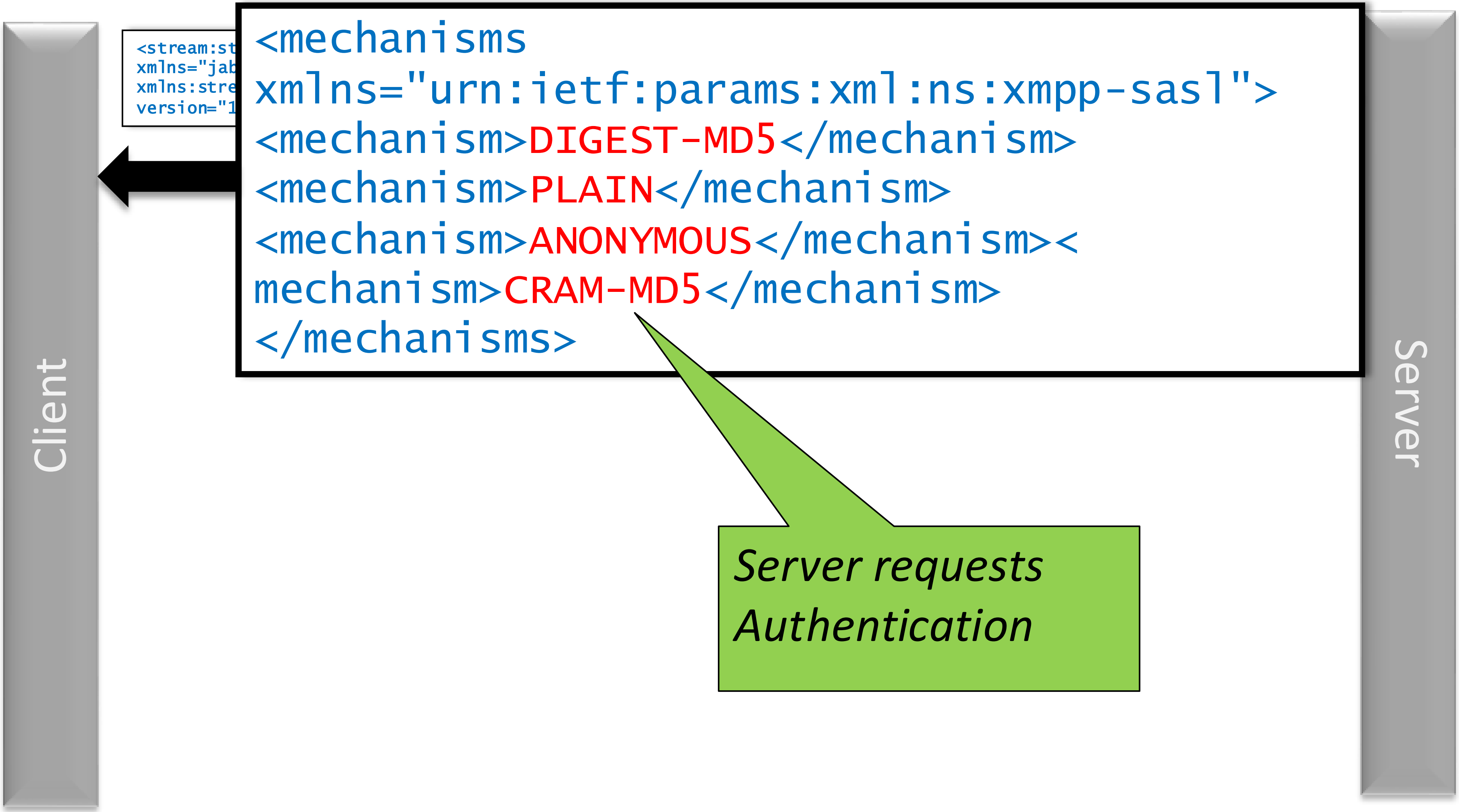
XMPP Registration Example [1/7]



```
<stream:stream to="192.168.200.131"
xmlns="jabber:client"
xmlns:stream="http://etherx.jabber.org/
streams" version="1.0">
```

Client attempts registration without authentication. This may succeed against servers accepting anonymous registrations.

XMPP Registration Example [2/7]

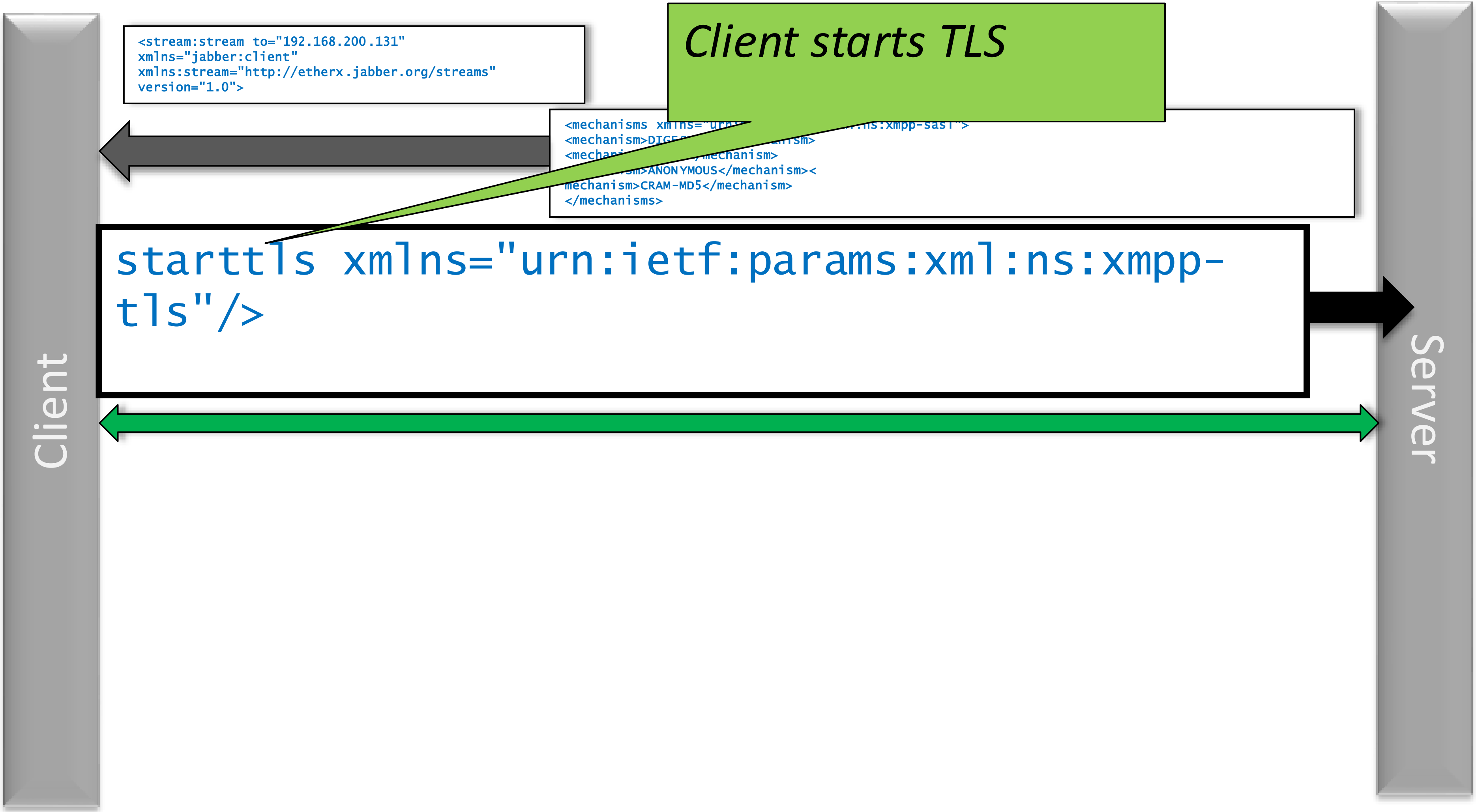


```
<stream:st
xmlns="jab
xmlns:stre
version="1
```

```
<mechanisms
xmlns="urn:ietf:params:xml:ns:xmpp-sasl">
<mechanism>DIGEST-MD5</mechanism>
<mechanism>PLAIN</mechanism>
<mechanism>ANONYMOUS</mechanism><
mechanism>CRAM-MD5</mechanism>
</mechanisms>
```

Server requests Authentication

XMPP Registration Example [3/7]



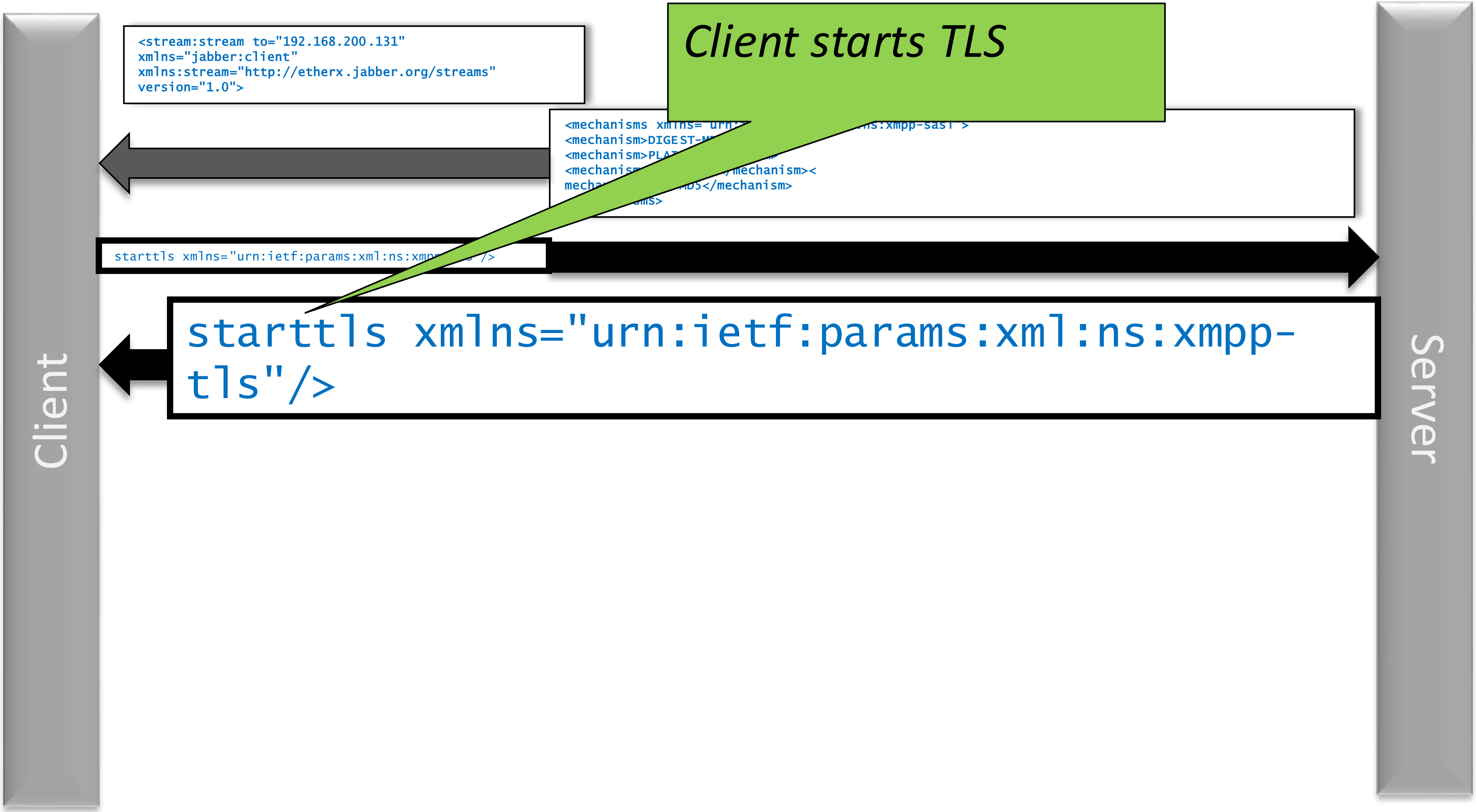
```
<stream:stream to="192.168.200.131"
xmlns="jabber:client"
xmlns:stream="http://etherx.jabber.org/streams"
version="1.0">
```

```
<mechanisms xmlns="urn[illegible]:ns:xmpp-sasl">
<mechanism>DIGE[illegible]anism>
<mechani[illegible]/mechanism>
[illegible]sm>ANONYMOUS</mechanism><
mechanism>CRAM-MD5</mechanism>
</mechanisms>
```

Client starts TLS

```
starttls xmlns="urn:ietf:params:xml:ns:xmpp-
tls"/>
```

XMPP Registration Example [4/7]



```
<stream:stream to="192.168.200.131"
xmlns="jabber:client"
xmlns:stream="http://etherx.jabber.org/streams"
version="1.0">
```

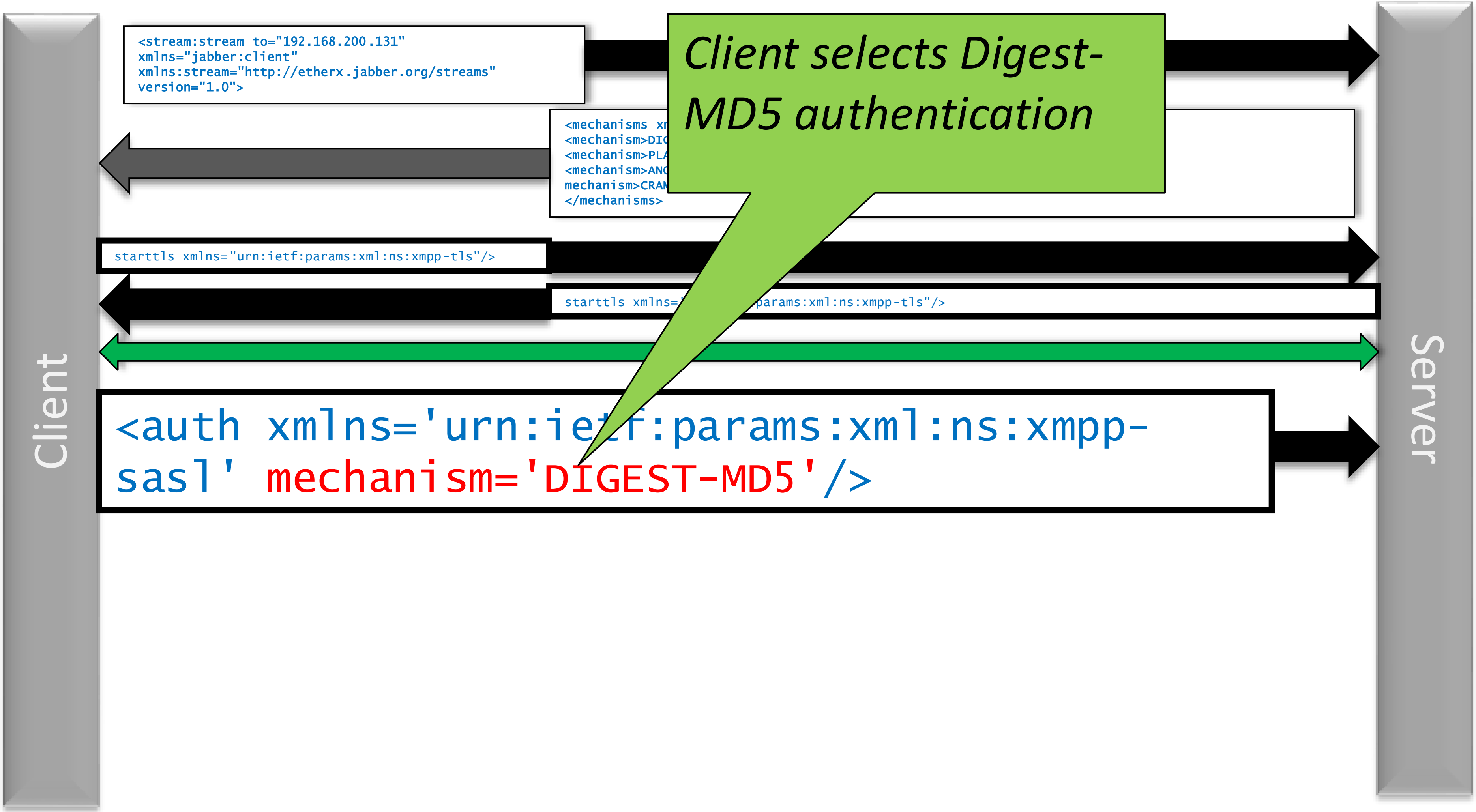
```
<mechanisms xmlns="urn:              ns:xmpp-sasl">
<mechanism>DIGEST-M
<mechanism>PLA
<mechanism              /mechanism><
mecha              MD5</mechanism>
              sms>
```

Client starts TLS

```
starttls xmlns="urn:ietf:params:xml:ns:xmp       s"/>
```

```
starttls xmlns="urn:ietf:params:xml:ns:xmpp-
tls"/>
```

XMPP Registration Example [5/7]



```
<stream:stream to="192.168.200.131"
xmlns="jabber:client"
xmlns:stream="http://etherx.jabber.org/streams"
version="1.0">
```

```
<mechanisms xm
<mechanism>DIG
<mechanism>PLA
<mechanism>ANO
mechanism>CRAM
</mechanisms>
```

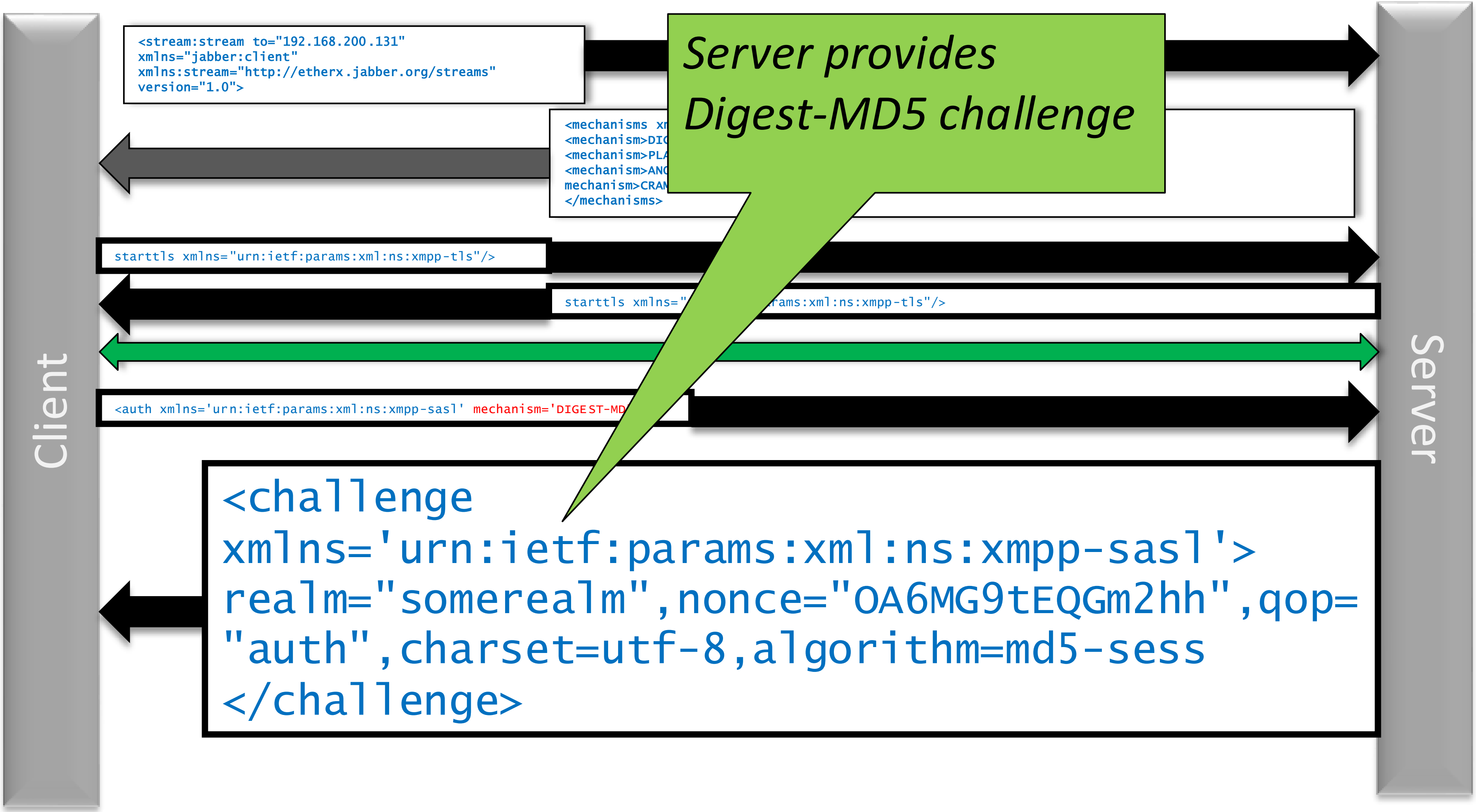
```
starttls xmlns="urn:ietf:params:xml:ns:xmpp-tls"/>
```

```
starttls xmlns=          params:xml:ns:xmpp-tls"/>
```

```
<auth xmlns='urn:ietf:params:xml:ns:xmpp-
sasl' mechanism='DIGEST-MD5'/>
```

Client selects Digest-MD5 authentication

XMPP Registration Example [6/7]



```
<stream:stream to="192.168.200.131"
xmlns="jabber:client"
xmlns:stream="http://etherx.jabber.org/streams"
version="1.0">
```

```
<mechanisms xm
<mechanism>DIG
<mechanism>PLA
<mechanism>ANO
mechanism>CRAM
</mechanisms>
```

```
starttls xmlns="urn:ietf:params:xml:ns:xmpp-tls"/>
```

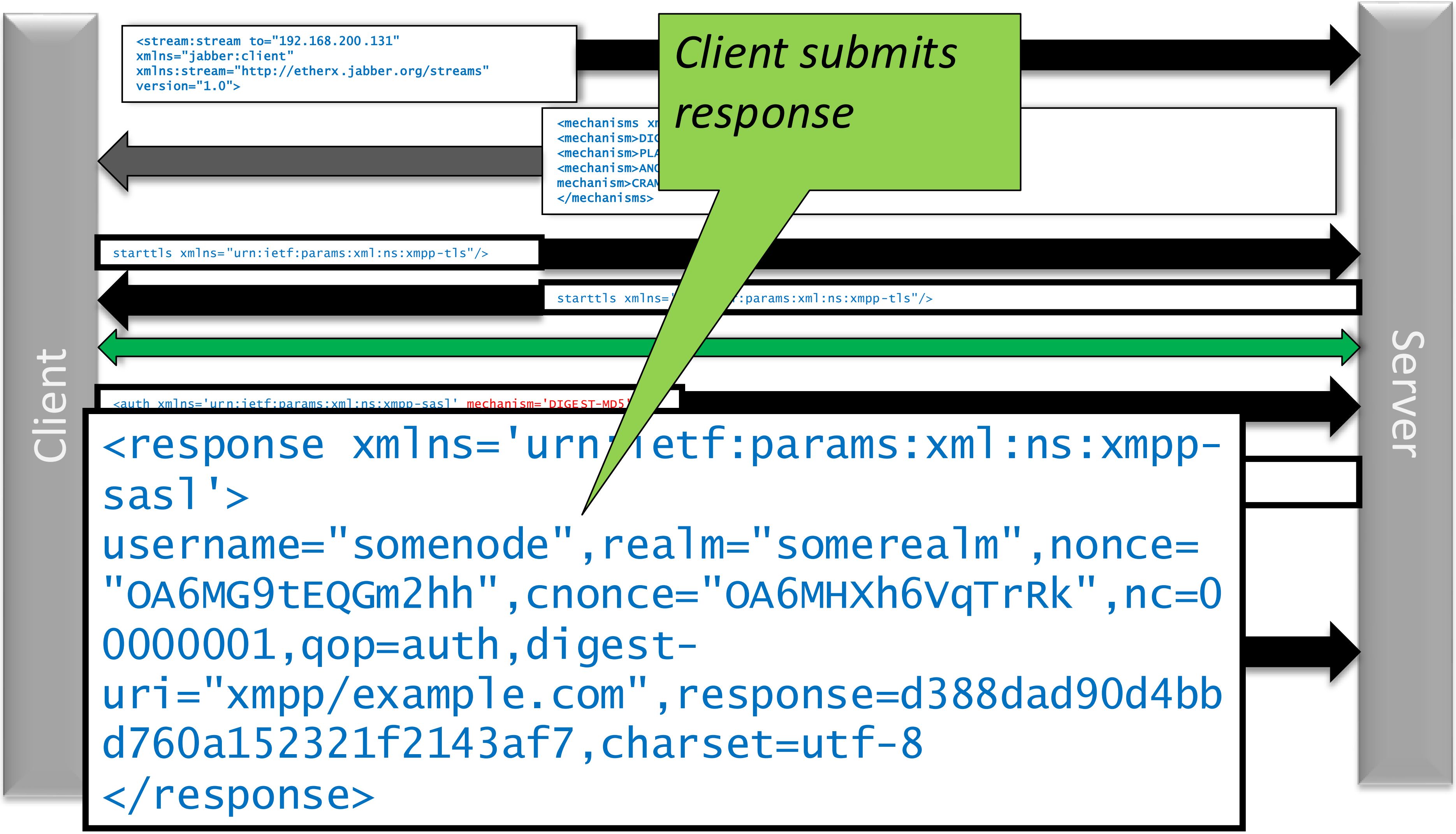
```
starttls xmlns="                 rams:xml:ns:xmpp-tls"/>
```

```
<auth xmlns='urn:ietf:params:xml:ns:xmpp-sasl' mechanism='DIGEST-MD
```

Server provides Digest-MD5 challenge

```
<challenge
xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
realm="somerealm",nonce="OA6MG9tEQGm2hh",qop=
"auth",charset=utf-8,algorithm=md5-sess
</challenge>
```

XMPP Registration Example [7/7]



```
<stream:stream to="192.168.200.131"
xmlns="jabber:client"
xmlns:stream="http://etherx.jabber.org/streams"
version="1.0">
```

```
<mechanisms xm
<mechanism>DIG
<mechanism>PLA
<mechanism>ANO
mechanism>CRAM
</mechanisms>
```

```
starttls xmlns="urn:ietf:params:xml:ns:xmpp-tls"/>
```

```
starttls xmlns=' :params:xml:ns:xmpp-tls"/>
```

```
<auth xmlns='urn:ietf:params:xml:ns:xmpp-sasl' mechanism='DIGEST-MD5'
```

Client submits response

```
<response xmlns='urn:ietf:params:xml:ns:xmpp-
sasl'>
username="somenode",realm="somerealm",nonce=
"OA6MG9tEQGm2hh",cnonce="OA6MHXh6VqTrRk",nc=0
0000001,qop=auth,digest-
uri="xmpp/example.com",response=d388dad90d4bb
d760a152321f2143af7,charset=utf-8
</response>
```

Identity on the Internet

"On the Internet, nobody knows you're a dog."

http://www.iamechanics.com

UC Identity Solutions – Cross Domain [1/2]

Old School

- **Whitelists:** Explicit Federation Policies: only federate with parties you trust
- **Blacklists:** Explicit Non-trust List: establish and manage blacklists

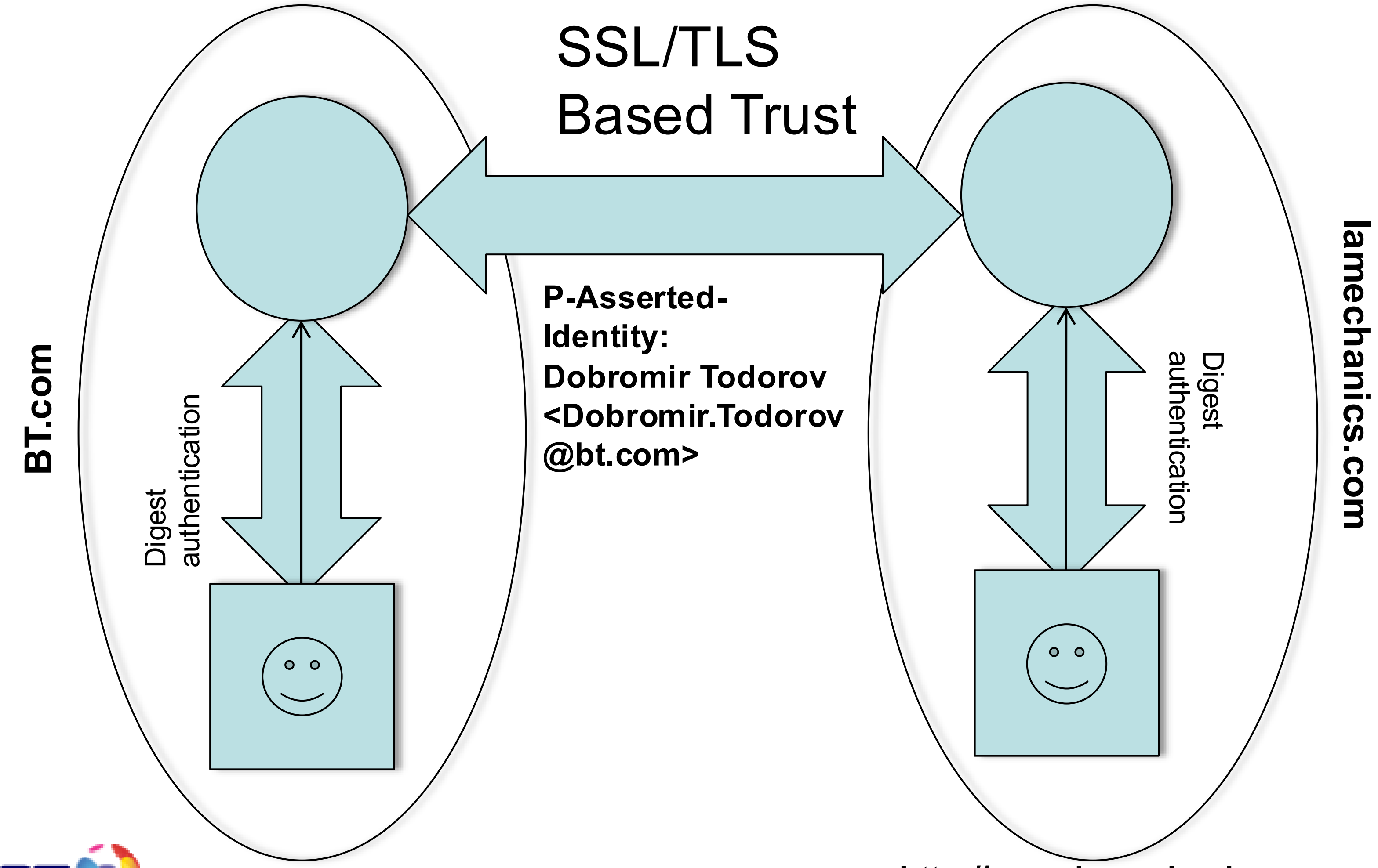
Neither of these is scalable...

UC Identity Solutions – Cross Domain [2/2]

Advanced

- **SIP**
  - **RFC 3325 (SIP):** use the SIP P-Asserted-Identity attribute within and across domains. Attribute always exchanged between trusted parties; uses SSL/TLS to extend trust
  - **RFC 4474 (SIP):** domain proxy generates authentication token and signs it using domain certificate and private key; uses Identity (for signature) and Identity-Info (points to domain certificate) attributes
- **XMPP**
  - **Dialback (XMPP):** Target server resolves source domain and goes for a key exchange

RFC 3325: Network Asserted Identity



http://www.iamechanics.com

Example: MS OC 2007 Asserted Identity

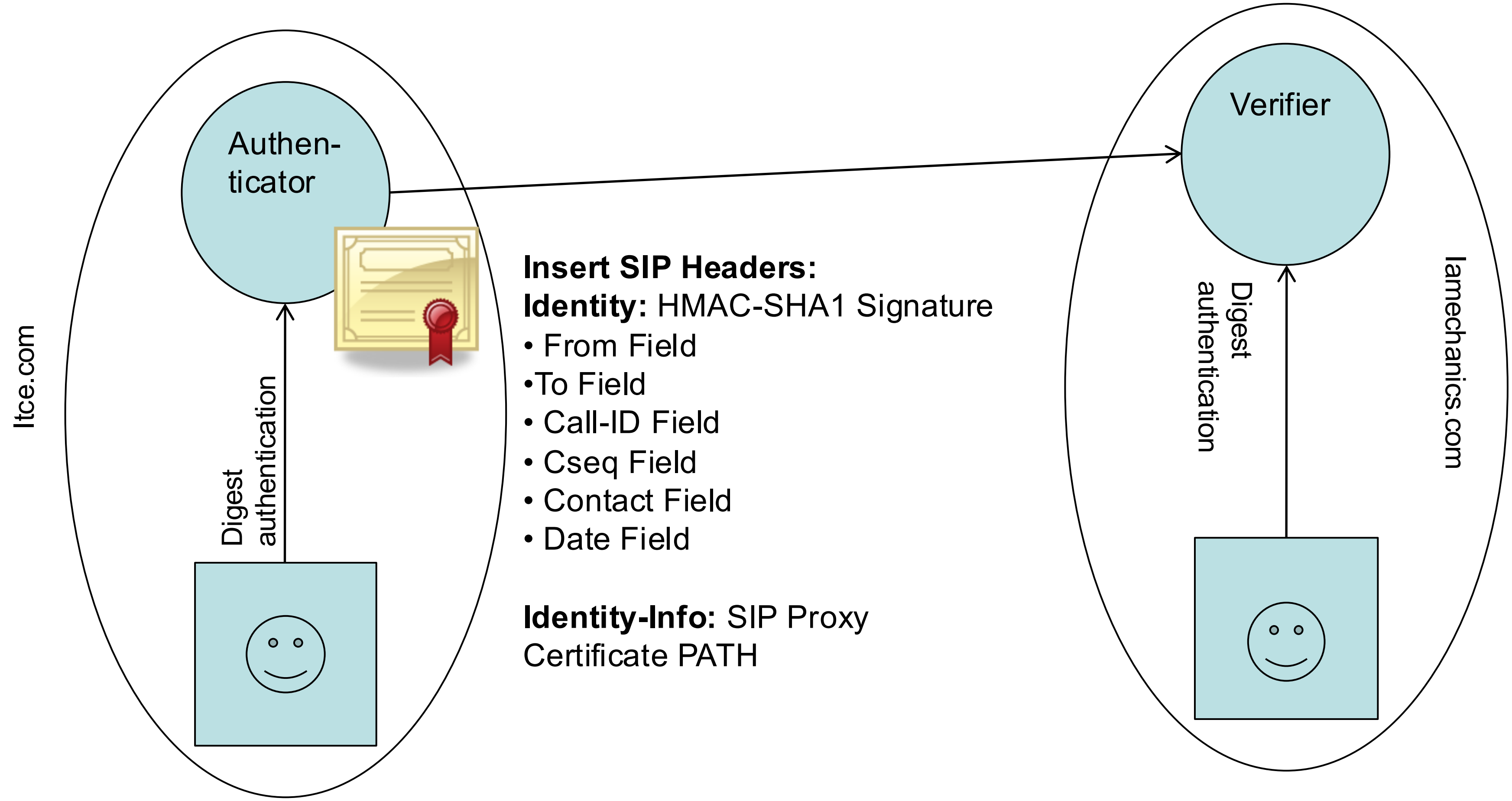
Caller to Server

```
INVITE sip:john@iamechanics.com SIP/2.0
From: <sip:peter@iamechanics.com>;tag=94d432861a;epid=c36d93ba53
To: <sip:john@iamechanics.com>
CSeq: 1 INVITE
Call-ID: fd408ecc016b4db8917fd5dd3bfb91eb
Via: SIP/2.0/TCP 192.168.1.73:50301
Max-Forwards: 70
Contact: <sip:peter@iamechanics.com;opaque=user:epid:dpArCJD5sFG-
        SZmdSUbqawAA;gruu>
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Microsoft Office Communicator)
Ms-Conversation-ID: Ackv4OPalY6CEllqSBuZ7RejeSgB0Q==
Supported: timer
Supported: ms-sender
Supported: ms-early-media
ms-keep-alive: UAC;hop-hop=yes
P-Preferred-Identity: <sip:peter@iamechanics.com>, <tel:+441628504002>
```

Server to Called Party

```
INVITE sip:131.107.2.101:2143;transport=tls;ms-
        opaque=81883e18f1;ms-received-cid=6400 SIP/2.0
From: "Peter
        Black"<sip:peter@iamechanics.com>;tag=94d432861a;epid=c36d
        93ba53
To: <sip:john@iamechanics.com>;epid=9ff97062ca
CSeq: 1 INVITE
Call-ID: fd408ecc016b4db8917fd5dd3bfb91eb
ms-user-data: ms-publiccloud=true;ms-federation=true
Record-Route:
        <sip:W2K3OCSFE.iamechanics.com:5061;transport=tls;ms-role-
        rs-to;ms-role-rs-
        from;lr>;tag=A10AD74863AF4B1A0BECFD24A6B205AC
Via: SIP/2.0/TLS
        192.168.200.102:5061;branch=z9hG4bK5BE6F3FF.092E6AF0;bra
        nched=TRUE
Authentication-Info: NTLM
        rspauth="0100000000000000025EEE2C9C285641A",
        srand="F1C8CF5A", snum="11", opaque="7CEBF860",
        qop="auth", targetname="W2K3OCSFE.iamechanics.com",
        realm="SIP Communications Service"
Max-Forwards: 69
Content-Length: 1072
P-Asserted-Identity: "Peter
        Black"<sip:peter@iamechanics.com>,<tel:+441628504002>
Contact:
        <sip:peter@iamechanics.com;opaque=user:epid:dpArCJD5sFG-
        SZmdSUbqawAA;gruu>
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Microsoft Office
        Communicator)
```

RFC 4474: Enhancements for Authenticated Identity Management



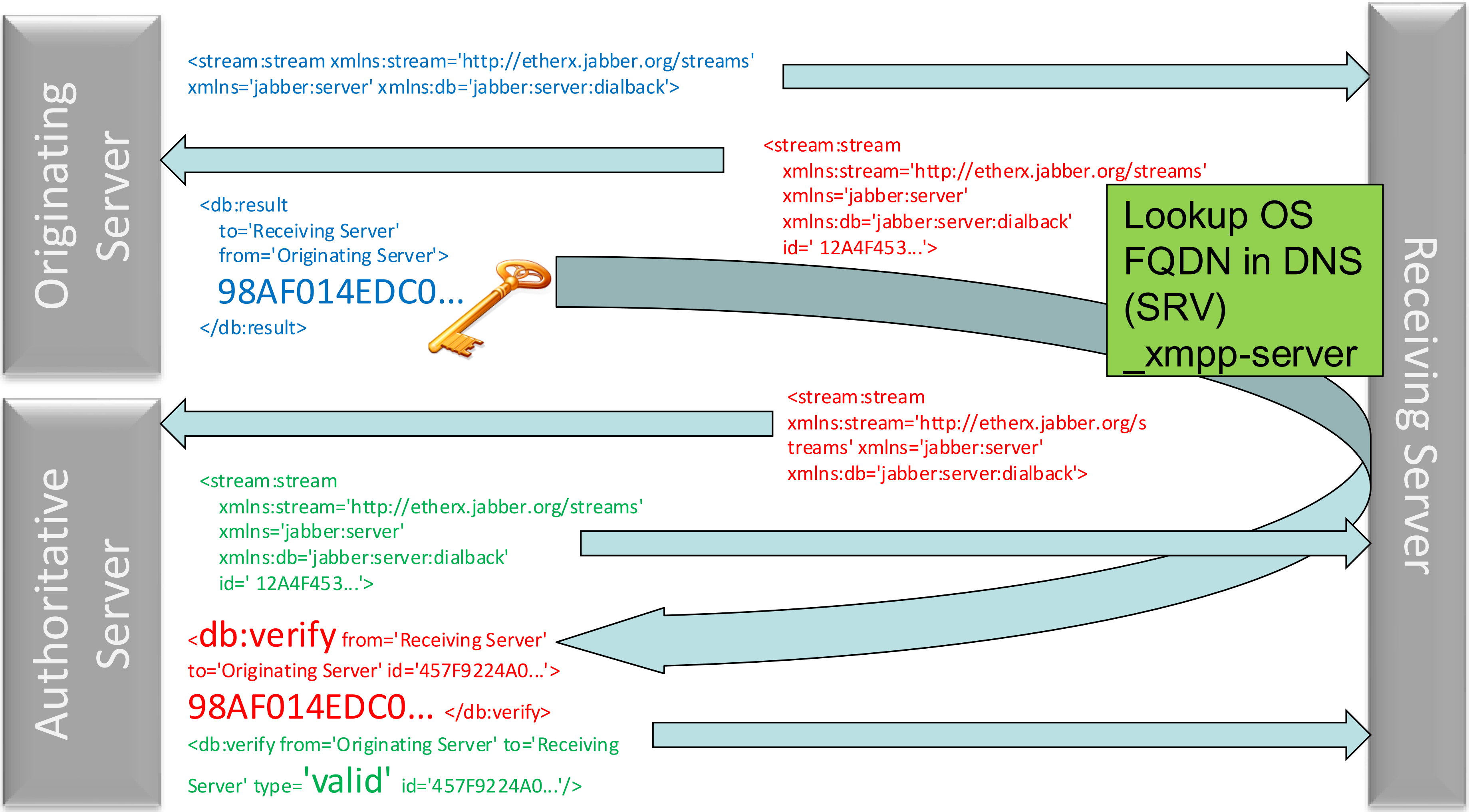
Insert SIP Headers:

Identity: HMAC-SHA1 Signature

- From Field
- To Field
- Call-ID Field
- Cseq Field
- Contact Field
- Date Field

Identity-Info: SIP Proxy Certificate PATH

XMPP Server Dialback – DNS for Caller Identity



<stream:stream xmlns:stream='http://etherx.jabber.org/streams'
xmlns='jabber:server' xmlns:db='jabber:server:dialback'>

<stream:stream
xmlns:stream='http://etherx.jabber.org/streams'
xmlns='jabber:server'
xmlns:db='jabber:server:dialback'
id=' 12A4F453...'>

<db:result
to='Receiving Server'
from='Originating Server'>
98AF014EDC0...
</db:result>

Lookup OS
FQDN in DNS
(SRV)
_xmpp-server

<stream:stream
xmlns:stream='http://etherx.jabber.org/s
treams' xmlns='jabber:server'
xmlns:db='jabber:server:dialback'>

<stream:stream
xmlns:stream='http://etherx.jabber.org/streams'
xmlns='jabber:server'
xmlns:db='jabber:server:dialback'
id=' 12A4F453...'>

<db:verify from='Receiving Server'
to='Originating Server' id='457F9224A0...'>
98AF014EDC0... </db:verify>

<db:verify from='Originating Server' to='Receiving
Server' type='valid' id='457F9224A0...'/>

UC(C) Identity and Privacy [1/2]

- The goal of UC: a single number/address
  - A single identity for the user
- Personal Privacy Aspects
  - By default, called party knows who the caller is
  - More powerful than cookies: the user may have been authenticated!
- EU Data Protection Directives
  - Prohibit unnecessary collection of personal data
  - Prohibit correlation of personal information

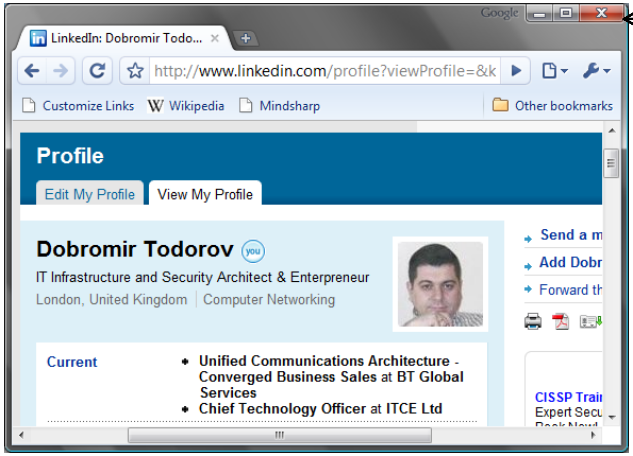
UC(C) Identity and Privacy [2/2]

- Case Study: Caller ID 2.0 – User A calls user B with full Caller ID information
- Beneficial: User B is an agent in a call centre. He receives a screen pop-up with all the details of the caller.
- Undesirable: User B performs a full lookup of User A and finds personal information for User A on Facebook, Linked-In, and RSS feeds.
- Recommendations:
  - Use separate personal and business UCC identities (so more than one number/address) – similar to personal and business SIM cards
  - For personal identity, use non-intuitive address
  - Do NOT forward caller ID to untrusted domains.

Caller-ID 2.0: Privacy Concerns

Caller ID

Search & Correlate



LinkedIn: Dobromir Todo...

http://www.linkedin.com/profile?viewProfile=&k

Customize Links | Wikipedia | Mindsharp | Other bookmarks

Profile

Edit My Profile | View My Profile

Dobromir Todorov (you)

IT Infrastructure and Security Architect & Enterpreneur

London, United Kingdom | Computer Networking

Send a m

Add Dobr

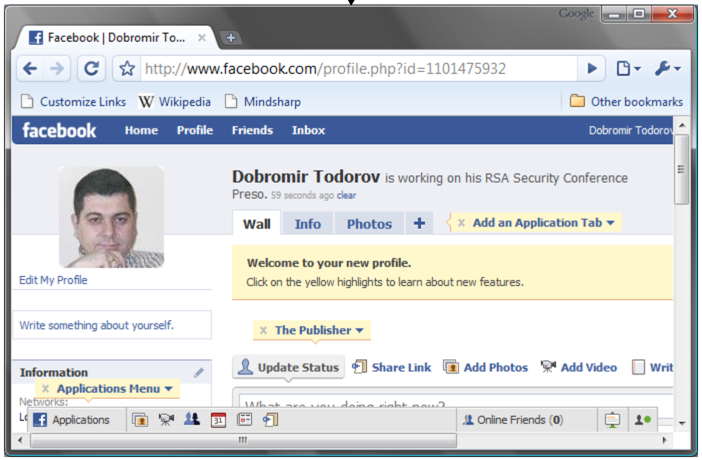
Forward th

Current

- Unified Communications Architecture - Converged Business Sales at BT Global Services
- Chief Technology Officer at ITCE Ltd

CISSP Trai

Expert Secu



Facebook | Dobromir To...

http://www.facebook.com/profile.php?id=1101475932

Customize Links | Wikipedia | Mindsharp | Other bookmarks

facebook | Home | Profile | Friends | Inbox | Dobromir Todorov

Dobromir Todorov is working on his RSA Security Conference Preso. 59 seconds ago clear

Wall | Info | Photos | + | Add an Application Tab

Welcome to your new profile.

Click on the yellow highlights to learn about new features.

Edit My Profile

Write something about yourself.

The Publisher

Information

Applications Menu

Networks:

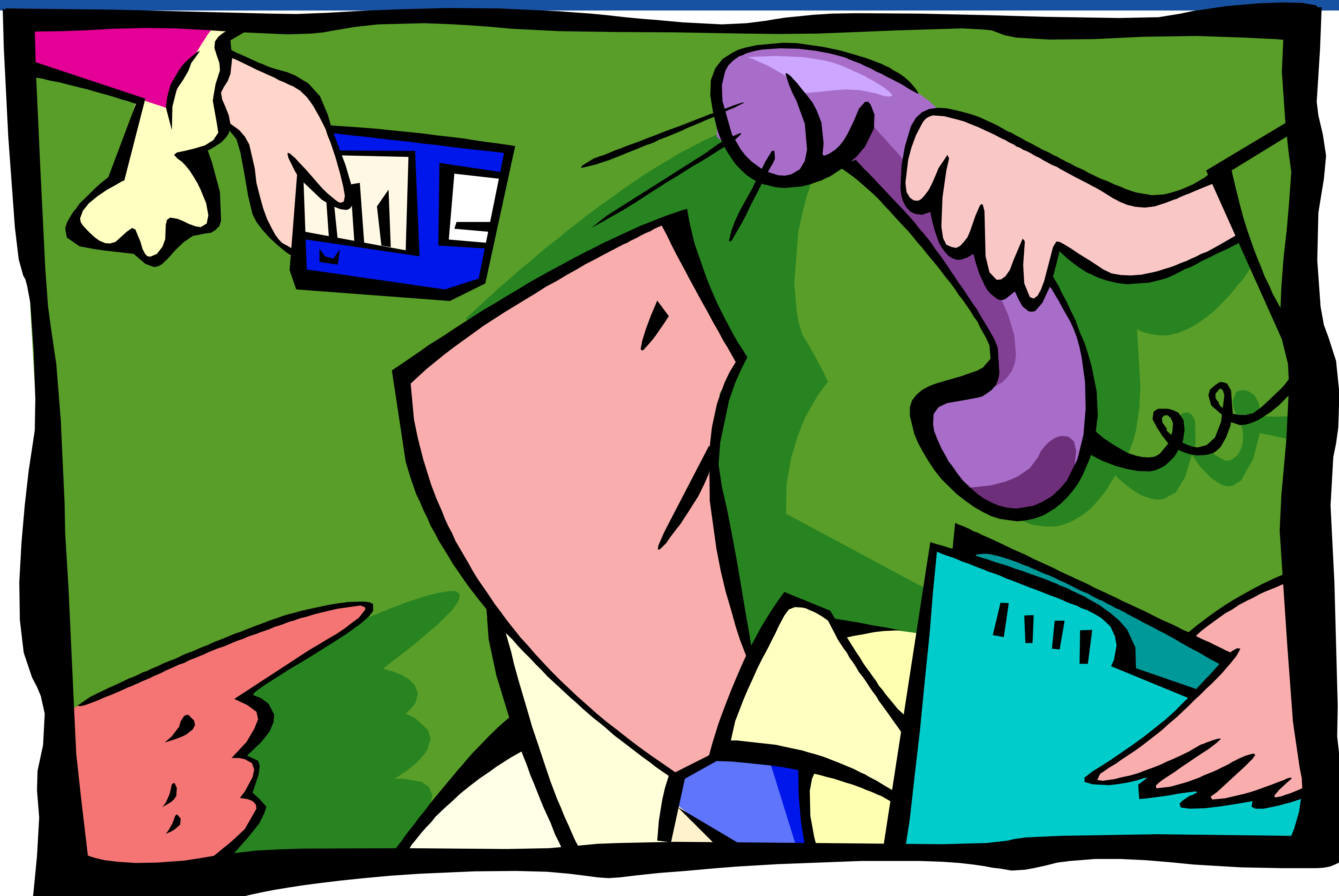
Update Status | Share Link | Add Photos | Add Video | Writ

What are you doing right now?

Applications | Online Friends (0)

http://www.iamechanics.com

Signalling, IM and Presence



Multifaceted Presence

- Connected: Online/Offline
- Willing to Communicate: Available, DnD
- Able to Communicate: Busy, On the phone...
- Location: Desk, Room, Floor, Building, Office, Town
- Skills: Technical, Personal, Languages...
- Rich Presence
- Presence Access Levels
  - Personal
  - Team
  - Company
  - Public

Presence, Availability, Location...

- Presence (and Availability) is the new dial tone
  - Users in DND mode don’t receive (all) calls
  - Availability may be an issue if presence information is compromised
  - Requires integrity services
- Location is geographical presence
  - Protect from disclosure: confidentiality or personal privacy
  - Protect integrity
  - Location based services, authentication and presence
  - Requires integrity and confidentiality services
- Compromised presence, availability or location is compromise of service in the CEBP world

Presence Security

- Presence carried over signalling channel
- The signalling channel has to be protected (peer identity,
- SSL/TLS and IPSec best suited to protect signalling
  - PKI more important than ever
- XMPP supports S/MIME & PGP as well (end-to-end security)

Instant Messaging Security

- Both SIP and XMPP can carry IMs in the signalling channel
- Signalling Channel protection for IM

SIP Protocol Security

- SIP over UDP doesn’t protect the channel (DTLS/RFC 4347 vendor support limited to none)
- SIP over TLS/SSL supported by some vendors
- Native peer identification: via From/To fields
- Native authentication via Digest Authentication – good
- Native data integrity authentication: none (use SDP)
- Native encryption: none (use SDP)
- End-to-End Protection: good to limited
  - Compliance logging can be enforced on the server

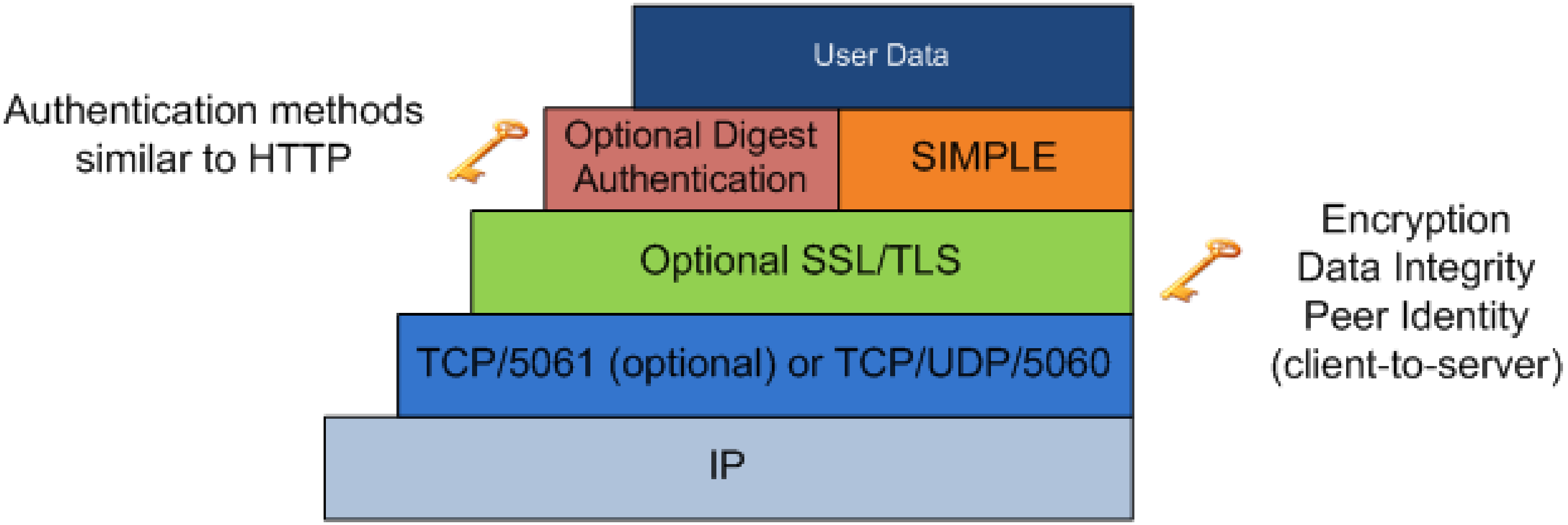
XMPP Protocol Security

- SIP over TLS supported as standard
- Native peer identification: via From/To/ID fields
- Native authentication via SASL and pluggable modules: very good
- Native data integrity authentication: SMIME, PGP
- Native encryption: SMIME, PGP
- End-to-End Protection: very good
  - Compliance logging may be restricted on the server: apply on the client
  - Requires trusted client...

Sample Message in SIP

```
MESSAGE sip:W2K3OCSFE.iamechanics.com:5061;transport=tls;ms-role-rs-
   from;ms-role-rs-to;ms-ent-dest;lr;ms-route-
   sig=cpvBz2lI0gHnVEgMK6rZn8ApFNCCl0tcVvJQ8HEQAA SIP/2.0
From: <sip:peter@iamechanics.com>;tag=c908d9b884;epid=ee59acab25
To: "" <sip:administrator@iamechanics.com>;epid=99d752bb74;tag=83427b067e
CSeq: 2 MESSAGE
Call-ID: 8da2a980f6fb451db5537b942477e65b
Via: SIP/2.0/TLS 192.168.1.66:2406
Max-Forwards: 70
Route: <sip:administrator@iamechanics.com;opaque=user:epid:bh1TvRpc9Faehf-
   1-jQjGwAA;gruu>
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Microsoft Office Communicator)
Supported: timer
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service",
   opaque="199FAA06", crand="2085b746", cnum="26",
   targetname="W2K3OCSFE.iamechanics.com",
   response="0100000061646d6981b1bd289703e74d"
Content-Type: text/rtf
Content-Length: 273
Message-Body: “Hello! How are you?”
```

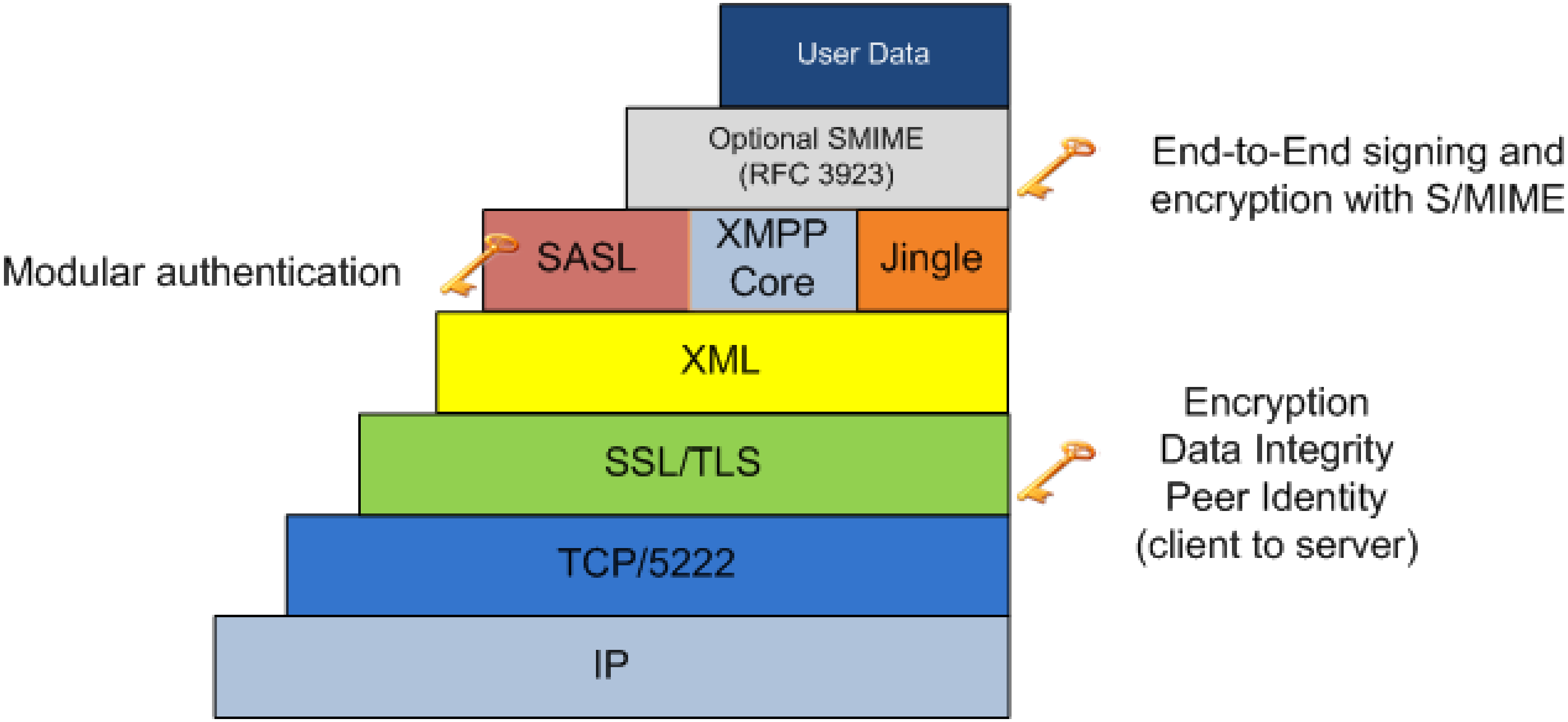
SIP Security Layers


User Data
Optional Digest Authentication
SIMPLE
Optional SSL/TLS
TCP/5061 (optional) or TCP/UDP/5060
IP

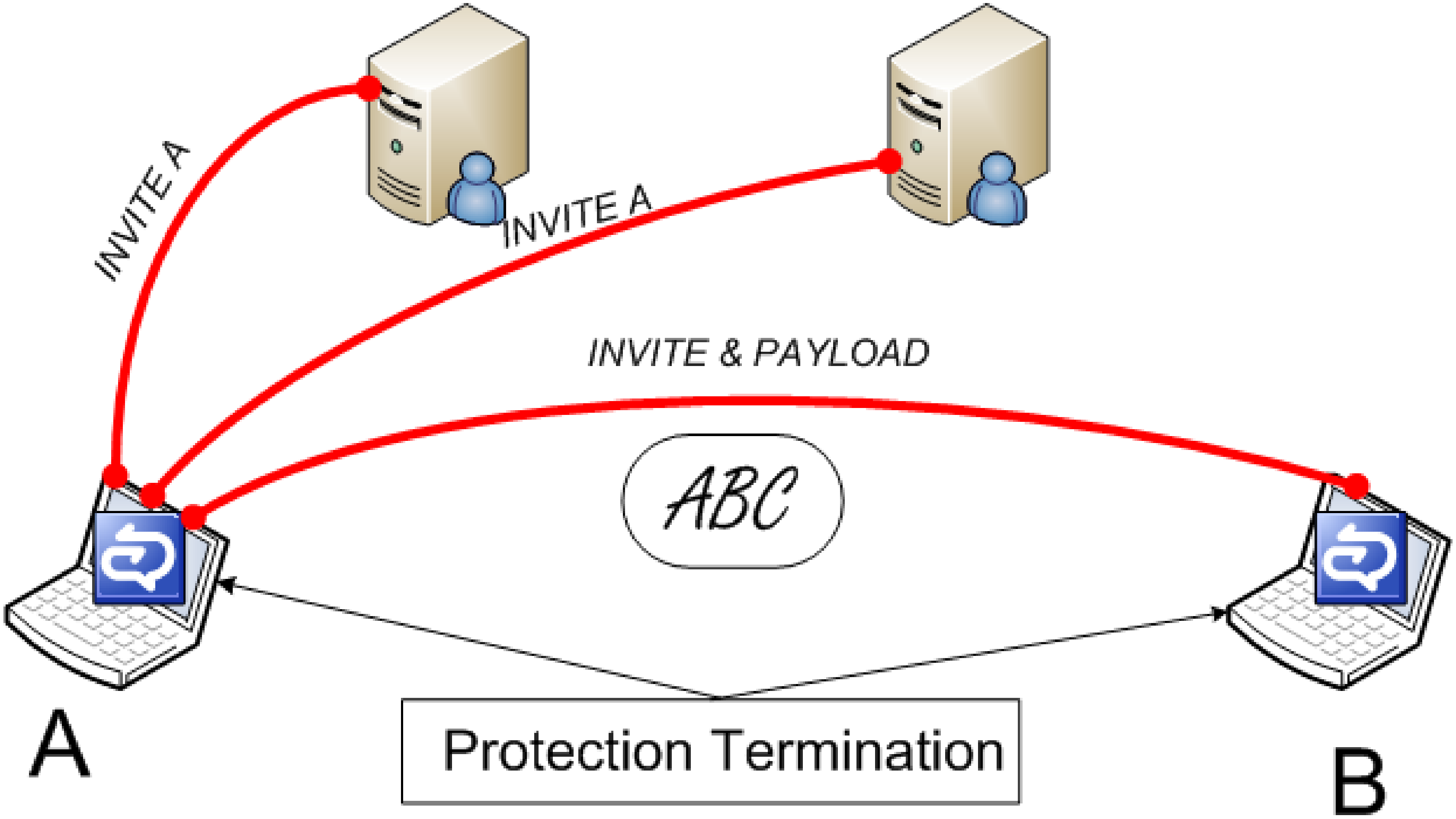
Authentication methods similar to HTTP

Encryption
Data Integrity
Peer Identity
(client-to-server)

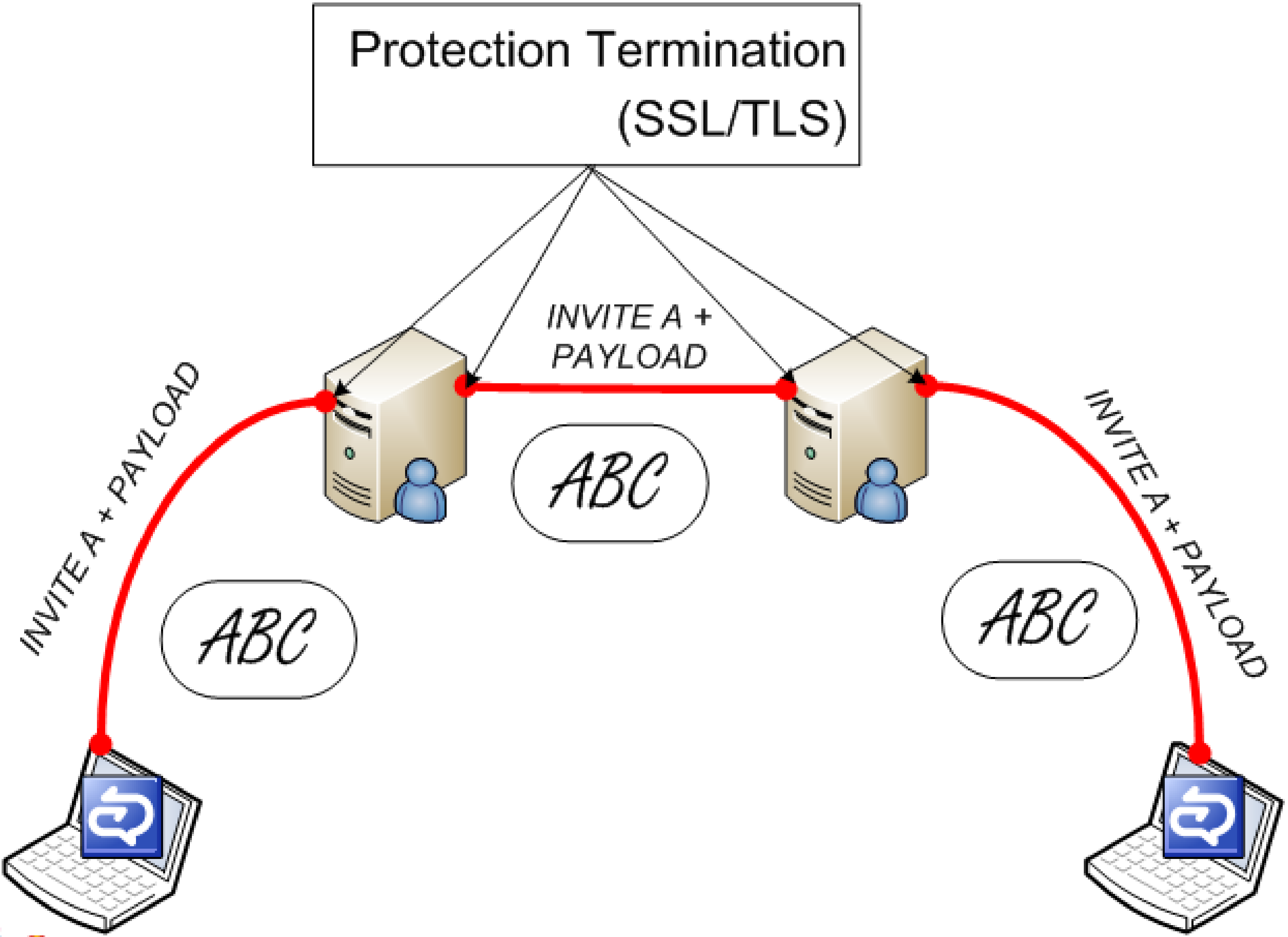
XMPP Security Layers



Original SIP End-to-End Protection

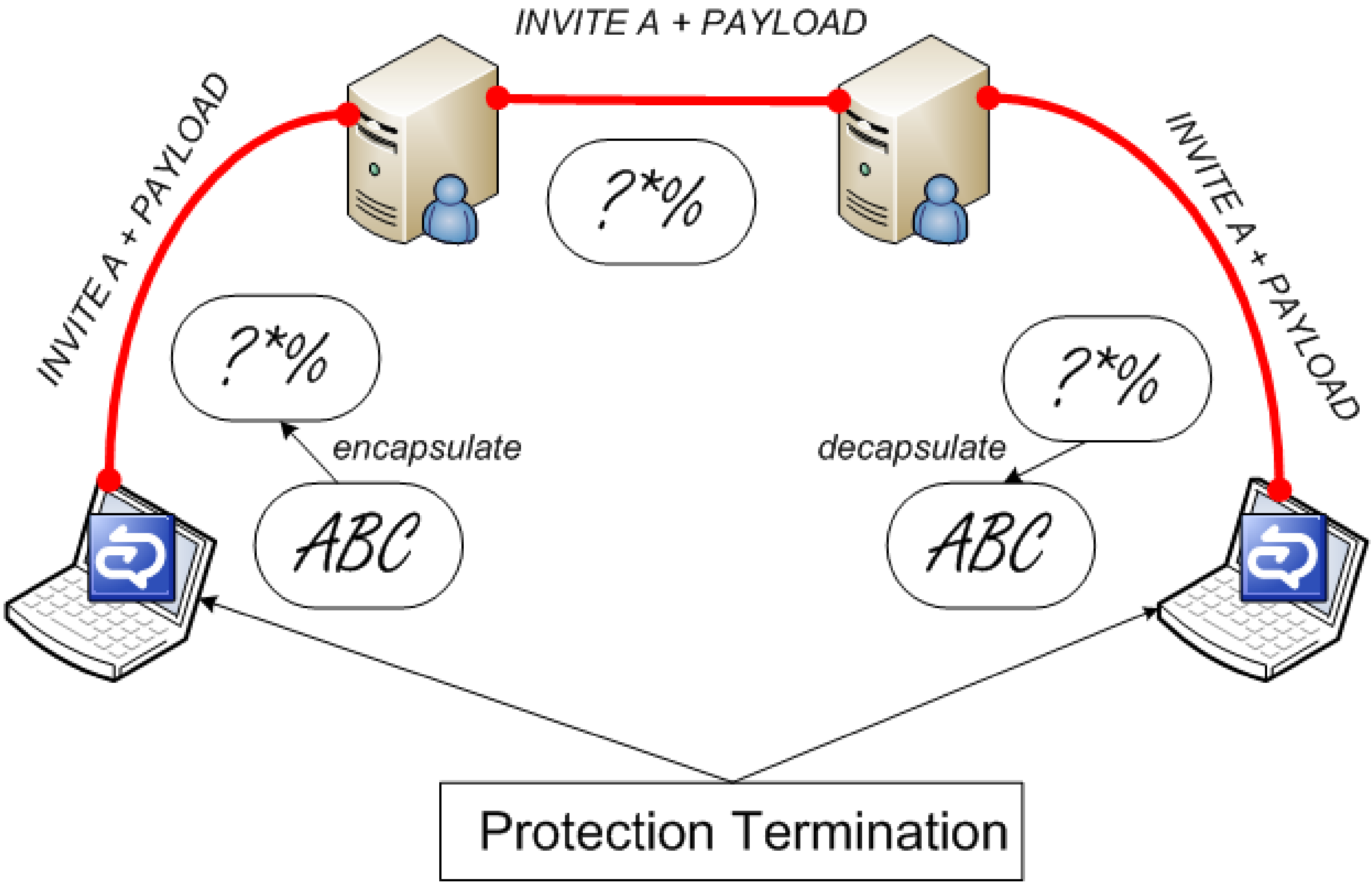


Channel Protection: SIP Inline Proxy & B2BUA



http://www.iamechanics.com

End-to-End Protection via Proxy: SMIME, PGP, RSA (XMPP)



UC(C) Signalling and Firewalls

- Shallow Inspection
  - IP addresses and TCP/UDP ports
  - Stateful firewalls
  - Often bypassed using tunnelling (VPN, STUN/ICE, HTTP, HTTPS)
  - Everything is HTTP/HTTPS these days...
- Deep Packet Inspection
  - Application intelligence
  - Protocol verbs: HTTP, SMTP, FTP, SIP
- Still missing (some SBCs support limited functionality)
  - SIP SERVICE verb inspection
  - XMPP Stanza inspection

Example: SIP SERVICE verb

SERVICE sip:John@iamechanics.com SIP/2.0

From: <sip:John@iamechanics.com>;tag=59ce8636c2;epid=9ff97062ca

To: sip:John@iamechanics.com

Content-Type: application/msrtc-category-publish+xml

Message-Body: <publish xmlns="http://schemas.microsoft.com/2006/09/sip/rich-presence"><publications uri="sip:john@iamechanics.com"><publication categoryName="state" instance="975921213" container="2" version="0" expireType="endpoint"><state xmlns="http://schemas.microsoft.com/2006/09/sip/state" manual="false" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="machineState"><availability>3500</availability><endpointLocation></endpointLocation></state></publication><publication categoryName="state" instance="975921213" container="3" version="0" expireType="endpoint"><state xmlns="http://schemas.microsoft.com/2006/09/sip/state" manual="false" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="machineState"><availability>3500</availability><endpointLocation></endpointLocation></state></publication><publication categoryName="device" instance="2729837529" container="2" version="0" expireType="endpoint"><device xmlns="http://schemas.microsoft.com/2006/09/sip/device" endpointId="305F6746-243B-5A9C-A89C-8A647910E9F2"><capabilities preferred="false" uri="sip:john@iamechanics.com"><text capture="true" render="true" publish="false"/><gifInk capture="false" render="true" publish="false"/><isfInk capture="false" render="true" publish="false"/></capabilities><timezone>00:00:00+01:00</timezone><machineName>XPCLIENT</machineName></device></publication></publications></publish>

Mobility vs Physical Security

- A mobile phone in malicious hands can:
  - Provide identity to attackers (calls/e-mails/IMs/presence...)
    - Also stored passwords, certificates, credit card numbers...
  - Disclose information (address book/IM/e-mail)
  - Compromise data integrity (access to information)
  - Incur call charges
- Recommendation: Protect mobile phones with biometric authentication or PIN

Presence-Location Spoofing

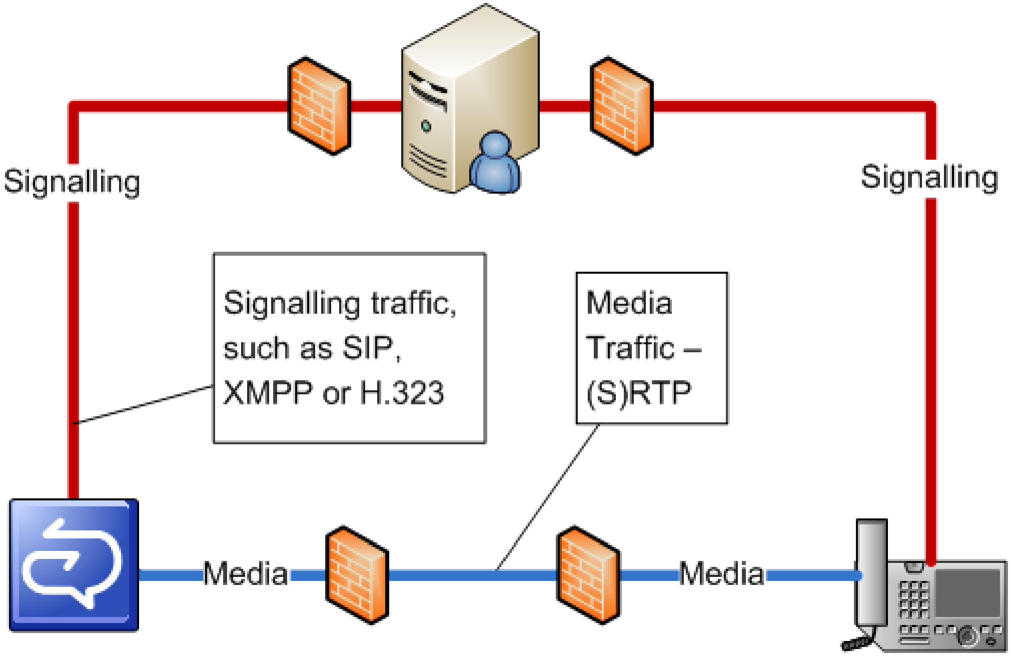
- Location information based on triangulation
- Detect active/passive RFID or Wireless NIC
- Passive RFID can be spoofed
- Active RFID can be spoofed
  (see http://rfidiot.org)
- Wireless NIC MAC address can be spoofed
- RFID authentication – not available
- NICs can be authenticated using 802.11i/EAP

Malware in the UC(C) world

- Unified Communications allows users, applications and malware to communicate seamlessly
- Eliminate malware from the communications path
- Implement Anti-virus/Anti-spam/Anti-fishing software on the endpoints
  - More important than ever

Audio and Video Communications Security

Audio/Video Security Model



Protecting Signalling – SIP/XMPP/SameTime/ Skinny/UniSTIM...

- SSL/TLS
- IPSec (rare)
- Protocol Specific

Protecting Media

- Secure RTP (key exchange over secure signalling channel)
- IPSec (rare)

http://www.iamechanics.com

IAX2 (Asterisk and derivatives)

- Exception to the rule
- A single channel used for signalling and media
- No need to track secondary sessions on firewalls!
- UDP/4569

SRTP [1/2]

- Defined in RFC 3711
  - Data Encryption
  - Data Integrity Authentication
  - Replay Protection
  - Re-keying
  - Keys derived from master key – typically external
- Scale SRTP (SSRTP) is Microsoft’s variation
  - Proprietary
  - Published by MS on 27 Jul 2008

SRTP [2/2]

- Master Key Negotiation Out of Band
  - MIKEY
    - Defined in RFC 3830
    - Certificates, pre-shared keys and Diffie-Hellman supported
    - Works on top of SIP/SDP
  - IKE
    - Rarely used
    - Can be in SIP/SDP, or out of signalling band

SDP and SRTP

- **k=<method>:<encryption key>** in RFC 4566 (2327)
  - Old model – NOT recommended
- **a=crypto** introduced in RFC 4568

  a=crypto:<tag> <crypto-suite> <key-params>

  [<session-params>]
- **a=cryptoscale** - Microsoft-specific for SSRTP
  - Similar to a=crypto

Example: SDP key provisioning for SRTP [1/2]

```
INVITE sip:john@iamechanics.com SIP/2.0
From: <sip:peter@iamechanics.com>;tag=94d432861a;epid=c36d93ba53
To: <sip:john@iamechanics.com>
CSeq: 1 INVITE
Call-ID: fd408ecc016b4db8917fd5dd3bfb91eb
Via: SIP/2.0/TCP 192.168.1.73:50301
Max-Forwards: 70
Contact: <sip:peter@iamechanics.com;opaque=user:epid:dpArCJD5sFG-SZmdSUbqawAA;gruu>
User-Agent: UCCP/2.0.6362.0 OC/2.0.6362.0 (Microsoft Office Communicator)
Ms-Conversation-ID: Ackv4OPalY6CEllqSBuZ7RejeSgB0Q==
Supported: timer
Supported: ms-sender
Supported: ms-early-media
ms-keep-alive: UAC;hop-hop=yes
P-Preferred-Identity: <sip:peter@iamechanics.com>, <tel:+441628504002>
Supported: ms-conf-invite
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service", opaque="3212BCAE", crand="b1c43407",
        cnum="10", targetname="W2K3OCSFE.iamechanics.com", response="01000000e8228b06a5af7a6ccb05798e"
Content-Type: application/sdp
Content-Length: 1072
Message-Body: v=0
o=- 0 0 IN IP4 192.168.1.73
s=session
c=IN IP4 192.168.1.73
b=CT:47980
t=0 0
m=audio 21504 RTP/AVP 114 111 112 115 116 4 8 0 97 101
```

Example: SDP key provisioning for SRTP [2/2]

```
k=base64:SIwGi1zyiU2I+0ALoPq7y2mA5jZbTJRnXywosg9NohRTbF9XKeYxjezrtlLx
a=candidate:/T0b/1X7sJfZ39m5We+V5EyjP7XTyKNCtTxZA0dog4g 1 DBcwIyZt9dWG/1+dP7njGA UDP 0.830 192.168.1.73 21504
a=candidate:/T0b/1X7sJfZ39m5We+V5EyjP7XTyKNCtTxZA0dog4g 2 DBcwIyZt9dWG/1+dP7njGA UDP 0.830 192.168.1.73 26752
a=cryptoscale:1 client AES_CM_128_HMAC_SHA1_80 inline:8jyLzhwNHOKQlqmxNUrXQfJwwi4tQ13qysiT8Lvx|2^31|1:1
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:rnAn3U1VRQA+pK13NNCVYUwwhrG7CMm44le/qjOA|2^31|1:1
a=maxptime:200
a=rtcp:26752
a=rtpmap:114 x-msrta/16000
a=fmtp:114 bitrate=29000
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:112 G7221/16000
a=fmtp:112 bitrate=24000
a=rtpmap:115 x-msrta/8000
a=fmtp:115 bitrate=11800
a=rtpmap:116 AAL2-G726-32/8000
a=rtpmap:4 G723/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:97 RED/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=encryption:optional
```

ZRTP

- Similar to SRTP but with in-band key establishment
- Works only on the media channel (RTP)
- Diffie-Hellman key negotiation
- Does not protect from Man-in-the-Middle attack by itself
- The two parties can mitigate MITM attacks by reading an optional signature string to each other...
  - Their speech though may potentially be spoofed as well...
- Used by zfone and PGPfone
- IETF Draft draft-zimmermann-avt-zrtp-09

Audio/Video Media: The 10K Ports Problem

- Media path different from signalling path
- RTP ports dynamic – negotiated in signalling conversation
- RTP uses UDP as a transport
- Signalling conversation encrypted
- How do we allow dynamic media ports?

Audio/Video Media: Solution 1

- Just open the 10K (or 16K) UDP ports bidirectionally!
- Cisco use UDP/16384-32768 by default
- MS use ALL dynamic UDP ports by default...
- Threats:
  - Tunnelling: Hide virtually any traffic in a UDP tunnel; traffic may be coming in or out
  - Internet users can access applications using this set of ports on internal hosts (UDP/1812-1813 is RADIUS, UDP/1701 is L2TP, UDP/2049 is NFSD...)
  - Flooding attacks against internal hosts
- Conclusion: weak from a security point of view

Audio/Video Media: Solution 2

- Inspect SSL/TLS protected SIP sessions (transparent inspection)
  - SBCs designed to do this
- Dynamically open UDP ports seen in active SIP dialogues
- Supported in Cisco ASA 8.0; can be scripted using open source products – TLS Proxy
- Requires trusted certificate and private key on the inspection device...
  - Ensure that physical and admin access to the inspection device is secure

Audio/Video Media: Solution 3

- Terminate SIP and Relay SRTP
  - SBCs and Edges
- All traffic goes via a single relay host
- Allows SIP to be inspected
- Stateful SRTP: only relay between source and destination ports/IP addresses that have been seen in SIP negotiations
- Good security
- Changes the media path; different bandwidth and QoS requirements
- Single relay host may become a bottleneck

Audio/Video Media: The NAT&Firewall Problem

- Bidirectional UDP communication required for RTP/SRTP streams
- ‘Symmetric’ NAT is a funnel
  - internal clients are mapped to public IP addresses as the source of outbound traffic
  - inbound traffic is not translated
  - If both clients are behind NAT, no end-to-end session can be established
  - No bidirectional communication with symmetric NAT

STUN, TURN, and ICE [1/2]

- STUN: Simple Traversal of UDP over NATs
  - Determine own IP address, type and presence of NAT
  - ‘Symmetric’ NAT means clients can’t communicate
- TURN: Traversal Using Relay NAT
  - Relay host for UDP traffic
  - REQUIRES authentication and authorisation
  - Tunnel traffic to destination over UDP/3478
  - Server decapsulates UDP/3478 tunnel and relays traffic
  - Allows communication over any type of NAT
  - Tunnelling is bad for security: enable application firewall, or a shallow inspection firewall on the TURN server
  - SBC is strongly recommended

STUN, TURN, and ICE [2/2]

- ICE: Interactive Connectivity Establishment
  - Try direct communication using all local IP addresses
  - Try STUN
  - Try TURN
- ICE can establish the best connectivity over any type of NAT
- The result of ICE is a peer-to-peer session between the two hosts: another tunnel
- To manage the P2P tunnel, ensure that the relay host:
  - Allows only RTP/UDP streams for active SIP dialogues
  - Authenticates SIP users and content

File Transfers

- Often point to point
- Use a different set of ports (MS OCS uses TCP/6891-TCP/6901 by default.
- Some implementations (MS OCS 2007) protect content but not actual commands
- Generally insecure; users should use portals to exchange files
- Protect the endpoints: Antivirus/Antispam

UC(C) Solution Availability

- Failover Clustering
- Load-balancing
- Geographic clusters
- Call admission control
  - Deep packet inspection can be poorman’s CAC
- QoS techniques
- Flood protection

Session Border Controllers

- Essentially “VoIP firewalls”
- Central policy
- Attack containment and mitigation
- Signalling inspection (sanity checking, state)
- “Stateful” (media-session) firewall rules
- Authentication, Authorisation, Accounting (AAA)
- Signalling conversion
- Media termination
- Media transcoding
- NAT-traversal technologies

QoS Security: Audio/Video Availability

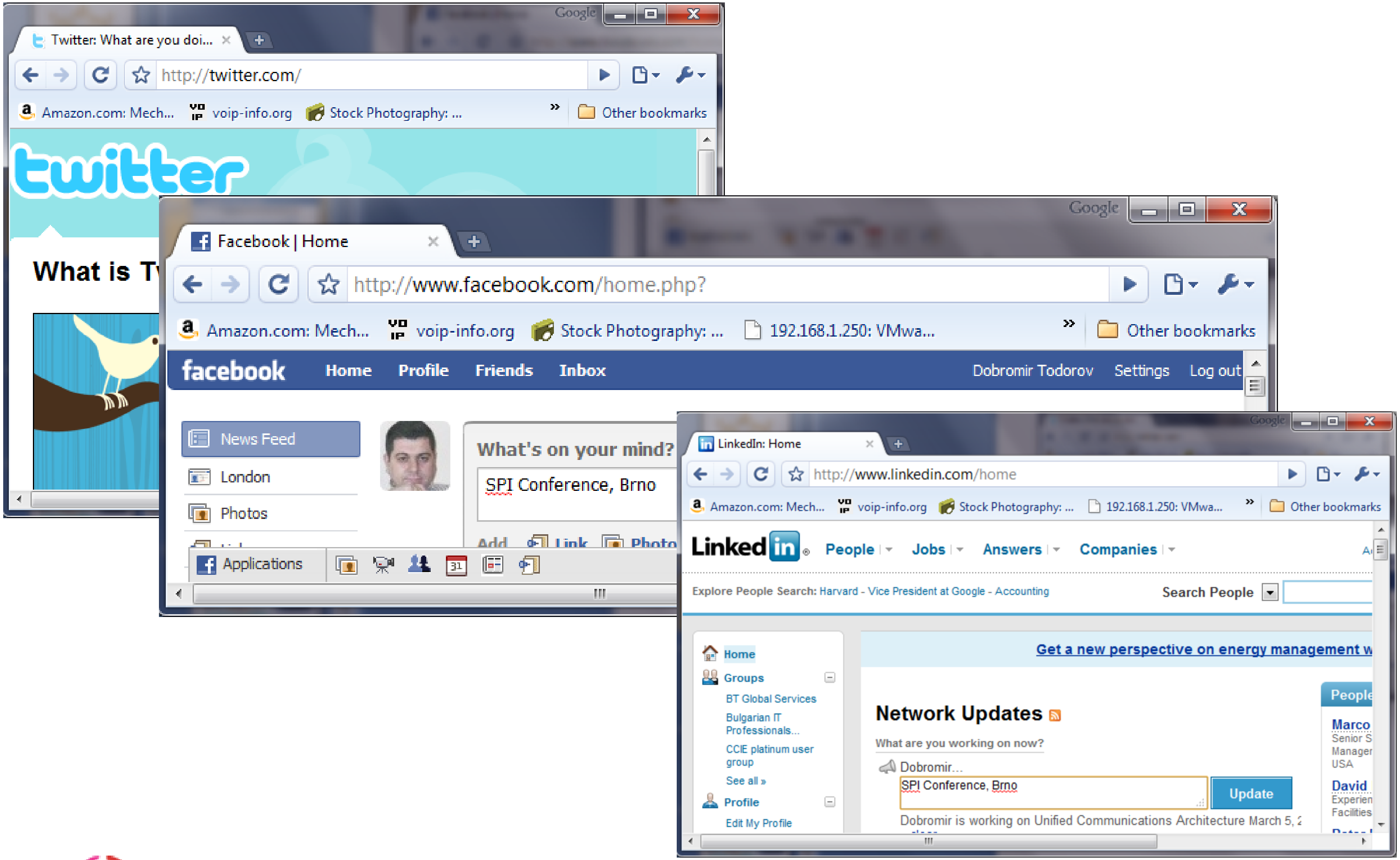
- Bandwidth typically shared on the data network
- Virtually all codecs require strict QoS policies
  - RTT < 200ms, Packet Loss < 1%, Jitter < 40ms, BW 20-80Kbps
- Maximum allocated voice/video “channels”: Call Admission Control
- QoS marking on the endpoints
  - Requires trusted endpoints
  - NAC/NAP – not bulletproof
- QoS on the network
  - Trust CoS: potentially insecure
  - Trust DSCP/ToS: potentially insecure
  - Dedicated VLANs and associated CoS/DSCP trust + 802.1x

CEBP Security Challenges

Security for The Social Web

Image by Tom Burke/
wikimedia commons

Facebook, Twitter, LinkedIn...



Twitter: What are you doi...

http://twitter.com/

Amazon.com: Mech... voip-info.org Stock Photography: ... Other bookmarks

twitter

What is T

Facebook | Home

http://www.facebook.com/home.php?

Amazon.com: Mech... voip-info.org Stock Photography: ... 192.168.1.250: VMwa... Other bookmarks

facebook Home Profile Friends Inbox Dobromir Todorov Settings Log out

News Feed

London

Photos

Applications

What's on your mind?

SPI Conference, Brno

LinkedIn: Home

http://www.linkedin.com/home

Amazon.com: Mech... voip-info.org Stock Photography: ... 192.168.1.250: VMwa... Other bookmarks

LinkedIn People Jobs Answers Companies

Explore People Search: Harvard - Vice President at Google - Accounting

Search People

Home

Groups

BT Global Services

Bulgarian IT Professionals...

CCIE platinum user group

See all »

Profile

Edit My Profile

Get a new perspective on energy management w

Network Updates

What are you working on now?

Dobromir...

SPI Conference, Brno

Update

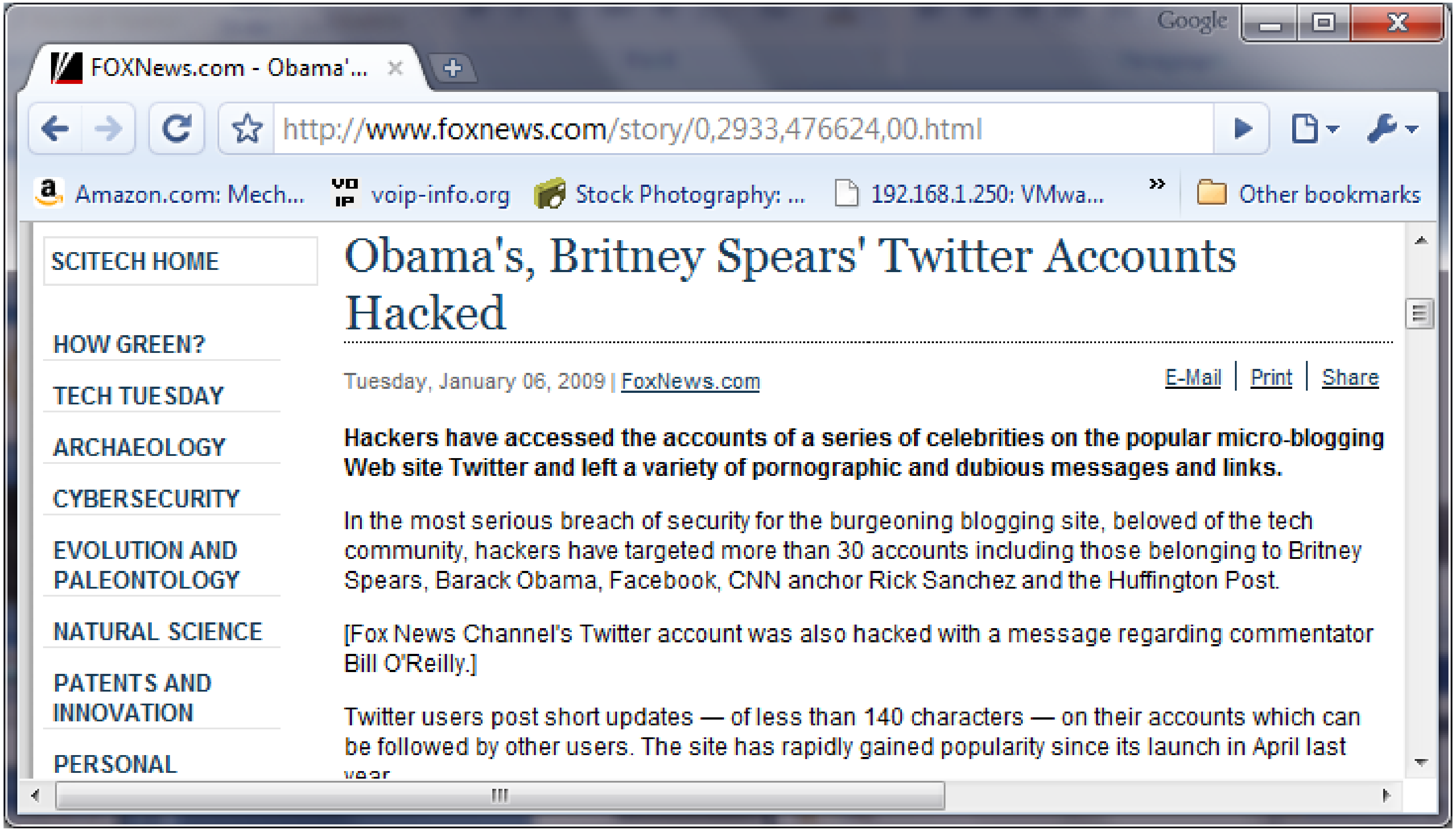
Dobromir is working on Unified Communications Architecture March 5, 2

People

Marco
Senior S
Manager
USA

David
Experien
Facilities

Social Web Security in the Press



Obama's, Britney Spears' Twitter Accounts Hacked

Tuesday, January 06, 2009 | FoxNews.com

Hackers have accessed the accounts of a series of celebrities on the popular micro-blogging Web site Twitter and left a variety of pornographic and dubious messages and links.

In the most serious breach of security for the burgeoning blogging site, beloved of the tech community, hackers have targeted more than 30 accounts including those belonging to Britney Spears, Barack Obama, Facebook, CNN anchor Rick Sanchez and the Huffington Post.

[Fox News Channel's Twitter account was also hacked with a message regarding commentator Bill O'Reilly.]

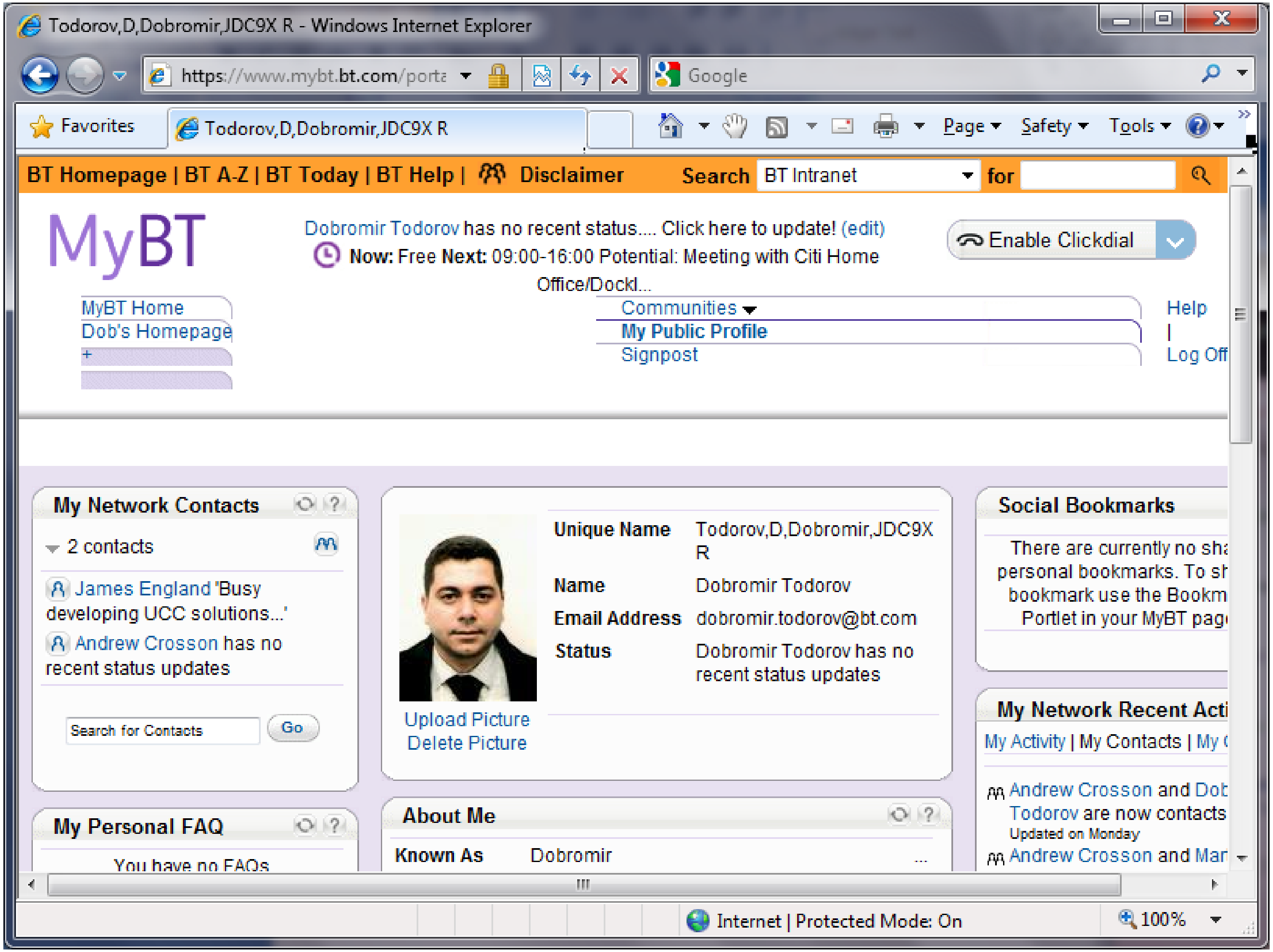
Twitter users post short updates — of less than 140 characters — on their accounts which can be followed by other users. The site has rapidly gained popularity since its launch in April last year

http://www.iamechanics.com

Security Challenges with Public Social Web

- Disclosure of Personal Information: people tell more than they should
  - Identity theft (name, address, DoB…)
  - Sexual abuse
  - …
- Some personal information may be limited to friends
- Disclosure of Company Confidential Information
- No identity verification: web of trust (friend of a friend)
  - Impersonation (imposters)
- False endorsements (falsifying trust)
- Central storage: everyone can be found there
- Searchable!

Taming the Beast: 'Corporate' Facebook


Todorov,D,Dobromir,JDC9X R - Windows Internet Explorer
https://www.mybt.bt.com/porta
Google
Favorites
Todorov,D,Dobromir,JDC9X R
Page
Safety
Tools
BT Homepage | BT A-Z | BT Today | BT Help | Disclaimer
Search
BT Intranet
for
MyBT
Enable Clickdial
MyBT Home
Dob's Homepage
+
Communities
My Public Profile
Signpost
Help
|
Log Off
Upload Picture
Delete Picture
Go
Internet | Protected Mode: On
100%

Dobromir Todorov has no recent status.... Click here to update! (edit)

Now: Free Next: 09:00-16:00 Potential: Meeting with Citi Home Office/Dockl...

My Network Contacts

2 contacts

James England 'Busy developing UCC solutions...'

Andrew Crosson has no recent status updates

Search for Contacts

Unique Name	Todorov,D,Dobromir,JDC9X R
Name	Dobromir Todorov
Email Address	dobromir.todorov@bt.com
Status	Dobromir Todorov has no recent status updates

Social Bookmarks

There are currently no sha personal bookmarks. To sh bookmark use the Bookm Portlet in your MyBT pag

My Network Recent Acti

My Activity | My Contacts | My

Andrew Crosson and Dob Todorov are now contacts

Updated on Monday

Andrew Crosson and Mar

My Personal FAQ

You have no FAQs

About Me

Known As	Dobromir

http://www.iamechanics.com

‘Corporate’ Facebook Security

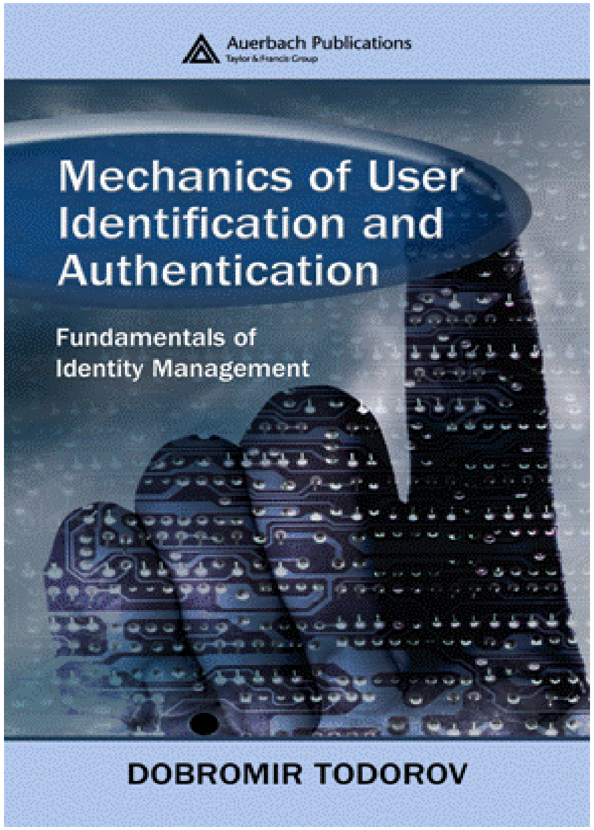
- Personal information is personal even inside the organisation
  - Consider confidentiality
  - EU directives apply (company responsible for protection)
  - Educate users
  - Provide access levels for personal information
  - Allow building a web of trust
- Impersonation may be an issue even inside the organisation: consider trust and integrity of information
  - “I am a big boss”
  - “I am an expert”
- Access Control: DAC/RBAC
- Harden the Web server and the database

In Summary: UC(C) Security Ingredients

- Security Policies, Guidelines, and Compliance
- Directory Services (most often AD)
  - User identification and authentication
  - User policies and settings, provisioning
- PKI is a must
- SSL/TLS accelerators required for large organisations
- Firewalls with deep packet inspection & SBCs
- Antivirus and Antispam Software
- Consider implementing SRTP

Questions and Answers

- All questions are welcome
- Questions can be taken offline
  - Anytime by e-mail – contact details below


Auerbach Publications
Taylor & Francis Group
Mechanics of User Identification and Authentication
Fundamentals of Identity Management
DOBROMIR TODOROV

Dobromir Todorov

UC Architect, BT Global Services

mailto:Dobromir.Todorov@bt.com

http://www.iamechanics.com