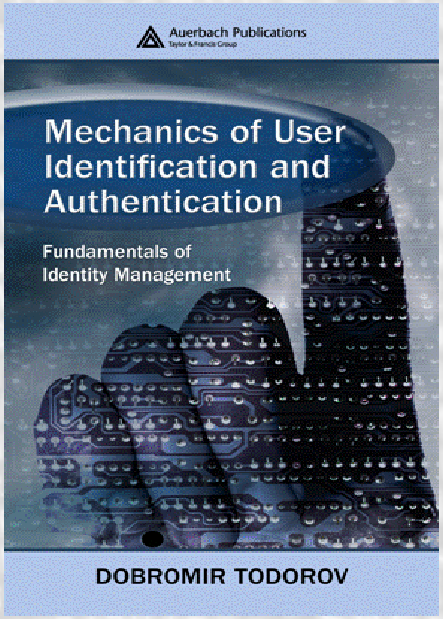
Unified Security for Unified Communications

Dobromir Todorov | BT Global Services | 28/10/08 | Session Code: DEV-208



Auerbach Publications

Taylor & Francis Group

Mechanics of User Identification and Authentication

Fundamentals of Identity Management

DOBROMIR TODOROV

RSA CONFERENCE EUROPE 2008

Overview

- Security vs UC(C)
- Identification and Authentication
- Signalling, IM and Presence
- Audio and Video Communications Security
- Summary
- Q&A

Security vs UC(C)

- Identity Management
  - Requirements ranging from anonymous communication to strong authentication
- UC is an application network on top of the telecommunications network
  - As such, it is effectively a tunnelling technology
- How seamless should communication between users be?
  - UC allows users to communicate; how do you prevent them from communicating?
- 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)
- Users must communicate securely.
  - How do we provide compliance capabilities (CDR, content retention, voice recording)?
  - How do we protect users from spreading malware across “secure” channels?

Identification and Authentication

Unified Communications Identity

- Identity
  - Identity of each party in the communication
  - SIP From and To fields is used for user Identity
    - However, the caller can put any ID there
  - XMPP potentially handles caller IDs better
- Caller Perspective
  - How do we ensure that the call has been routed to the party we wanted to call?
- Called Party Perspective
  - How do I verify the identity of the party that has just called me?
  - Do I receive anonymous and/or calls from an unverifiable callers?

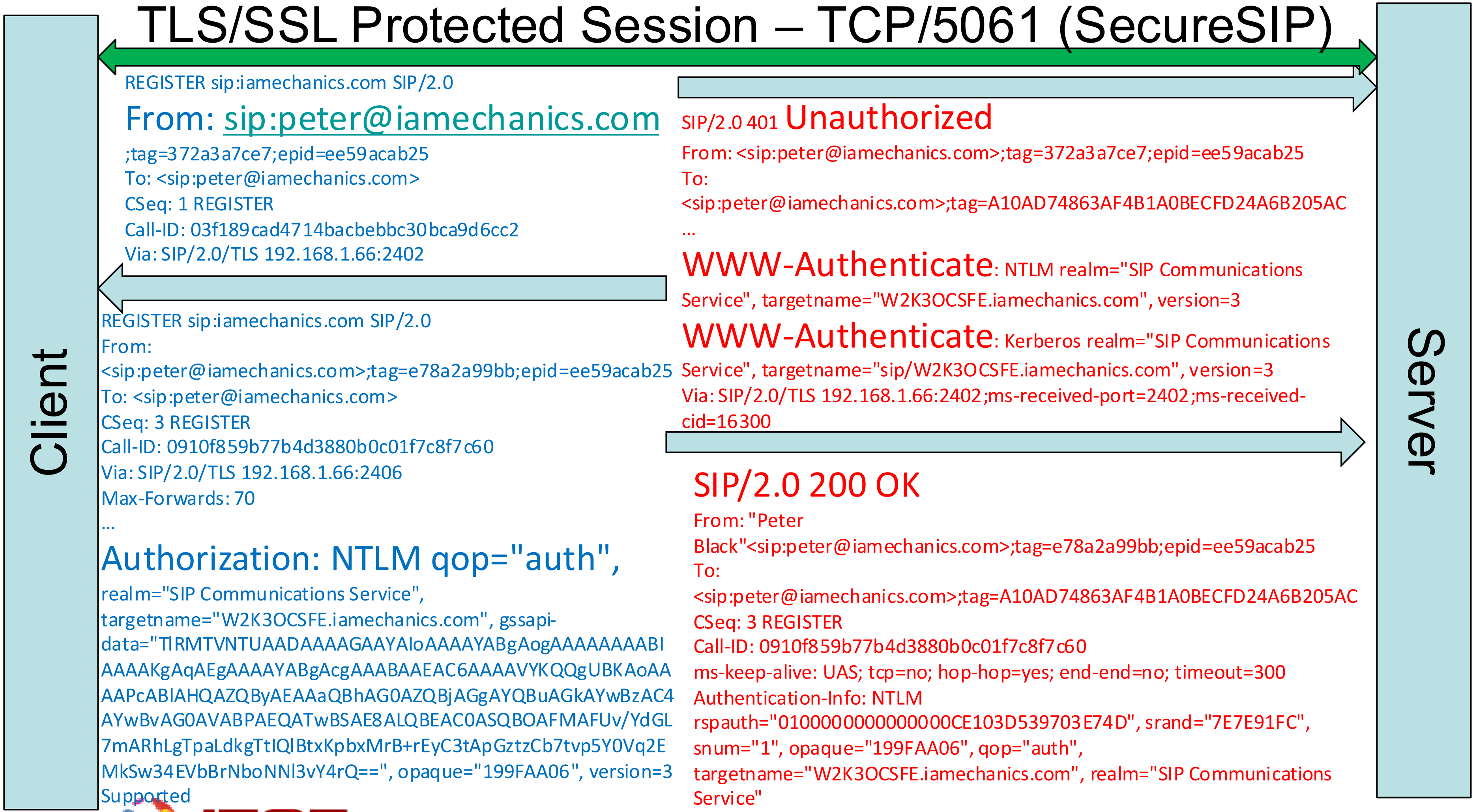
UC(C) Identity Scenarios

- 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
- I&A Mechanisms
  - Authenticate users
    - SIP Proxy-authenticate header
    - SIP Authenticate header – end-to-end
  - Registration Server checks peer identity

SIP Registration Example



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

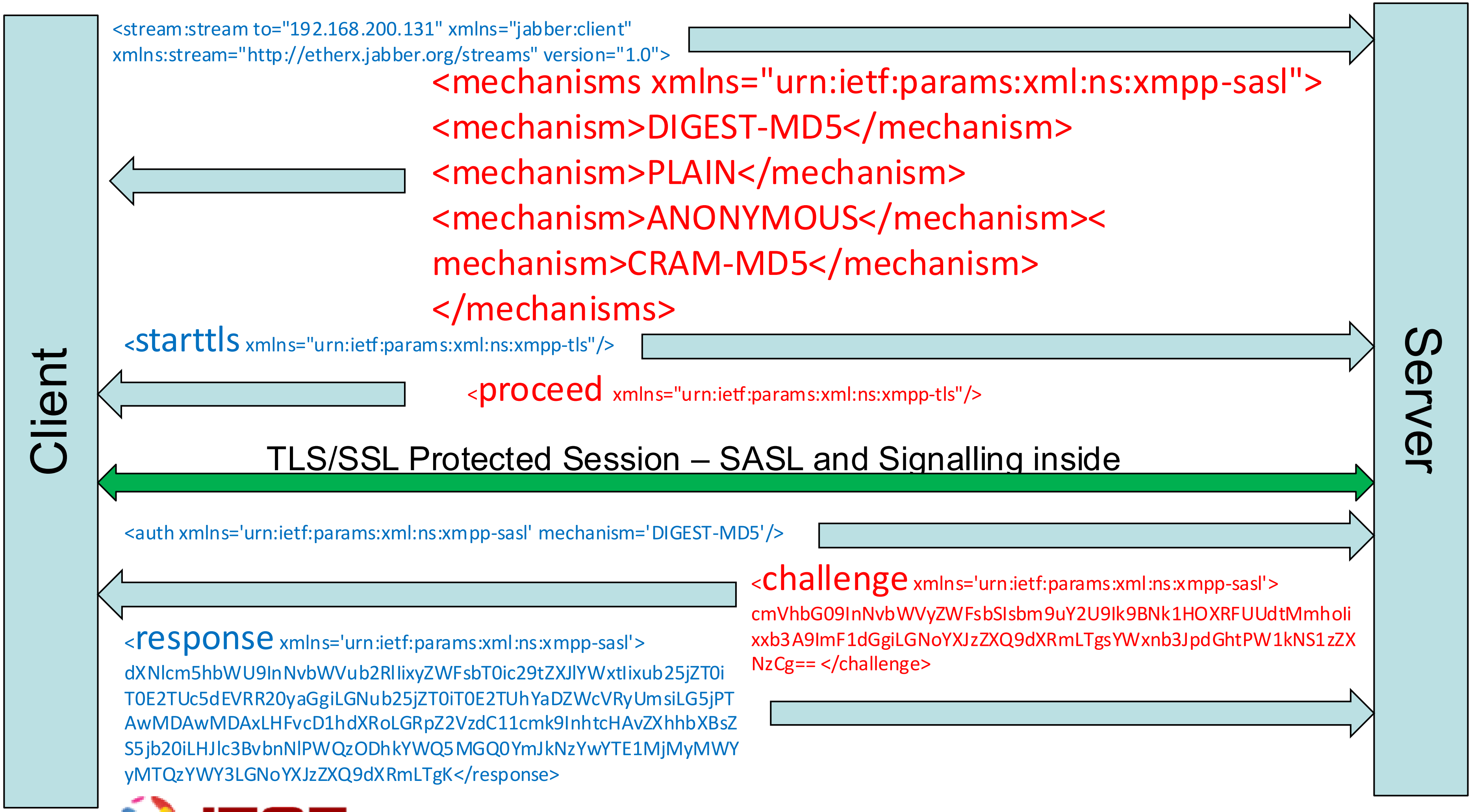
REGISTER sip:iamechanics.com SIP/2.0
From: sip:peter@iamechanics.com
;tag=372a3a7ce7;epid=ee59acab25
To: <sip:peter@iamechanics.com>
CSeq: 1 REGISTER
Call-ID: 03f189cad4714bacbebbc30bca9d6cc2
Via: SIP/2.0/TLS 192.168.1.66:2402

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

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
Max-Forwards: 70
...
Authorization: NTLM qop="auth",
realm="SIP Communications Service",
targetname="W2K3OCSFE.iamechanics.com", gssapi-data="TlRMTVNTUAADAAAAGAAYAIoAAAAYABgAogAAAAAAAABIAAAAKgAqAEgAAAAYABgAcgAAABAAEAC6AAAAVYKQQgUBKAoAAAAPcABlAHQAZQByAEAAaQBhAG0AZQBjAGgAYQBuAGkAYwBzAC4AYwBvAG0AVABPAEQATwBSAE8ALQBEAC0ASQBOAFMAFUv/YdGL7mARhLgTpaLdkgTtIQlBtxKpbxMrB+rEyC3tApGztzCb7tvp5Y0Vq2EMkSw34EVbBrNboNNl3vY4rQ==", opaque="199FAA06", version=3
Supported

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="0100000000000000CE103D539703E74D", srand="7E7E91FC", snum="1", opaque="199FAA06", qop="auth", targetname="W2K3OCSFE.iamechanics.com", realm="SIP Communications Service"

XMPP Session Example



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

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

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

<proceed xmlns="urn:ietf:params:xml:ns:xmpp-tls"/>

TLS/SSL Protected Session – SASL and Signalling inside

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

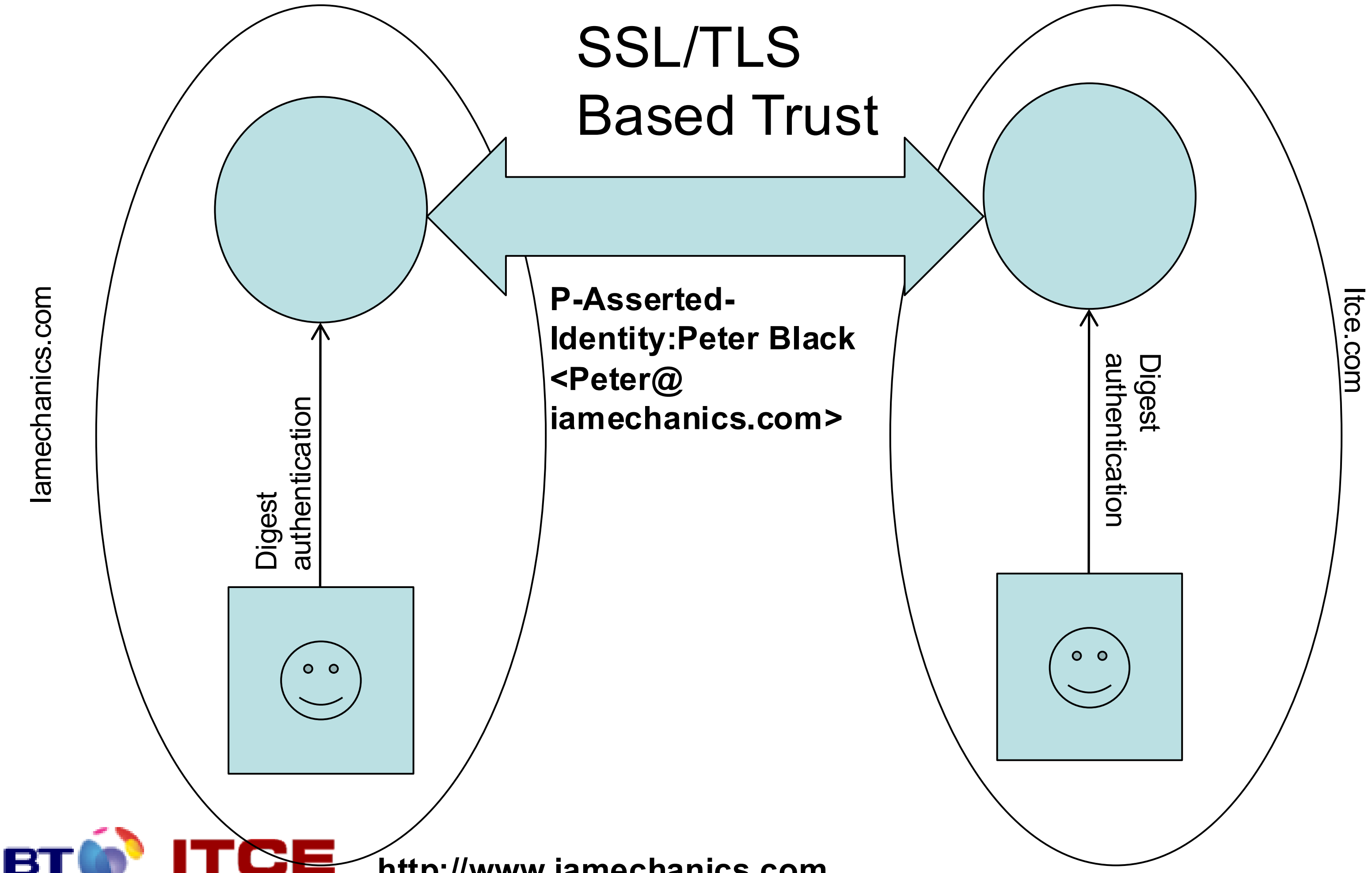
<challenge xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
cmVhbG09InNvbWVyZWFsbSIsbm9uY2U9Ik9BNk1HOXRFUUdtMmholi
xxb3A9ImF1dGgiLGNoYXJzZXQ9dXRmLTgsYWxnb3JpdGhtPW1kNS1zZX
NzCg== </challenge>

<response xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
dXNlcm5hbWU9InNvbWVub2RlIixyZWFsbT0ic29tZXJlYWxtIixub25jZT0i
T0E2TUc5dEVRR20yaGgiLGNub25jZT0iT0E2TUhYaDZWcVRyUmsiLG5jPT
AwMDAwMDAxLHFvcD1hdXRoLGRpZ2VzdC11cmk9InhtcHAvZXhhbXBsZ
S5jb20iLHJlc3BvbnNlPWQzODhkYWQ5MGQ0YmJkNzYwYTE1MjMyMWY
yMTQzYWY3LGNoYXJzZXQ9dXRmLTgK</response>

UC Identity Solutions – Cross Domain

- **Whitelists:** Explicit Federation Policies: only federate with parties you trust
- **Blacklists:** Explicit Non-trust List: establish and manage blacklists
- **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
- **Dialback (XMPP):** Target server resolves source domain and goes for a key exchange

RFC 3325: Network Asserted Identity



SSL/TLS Based Trust

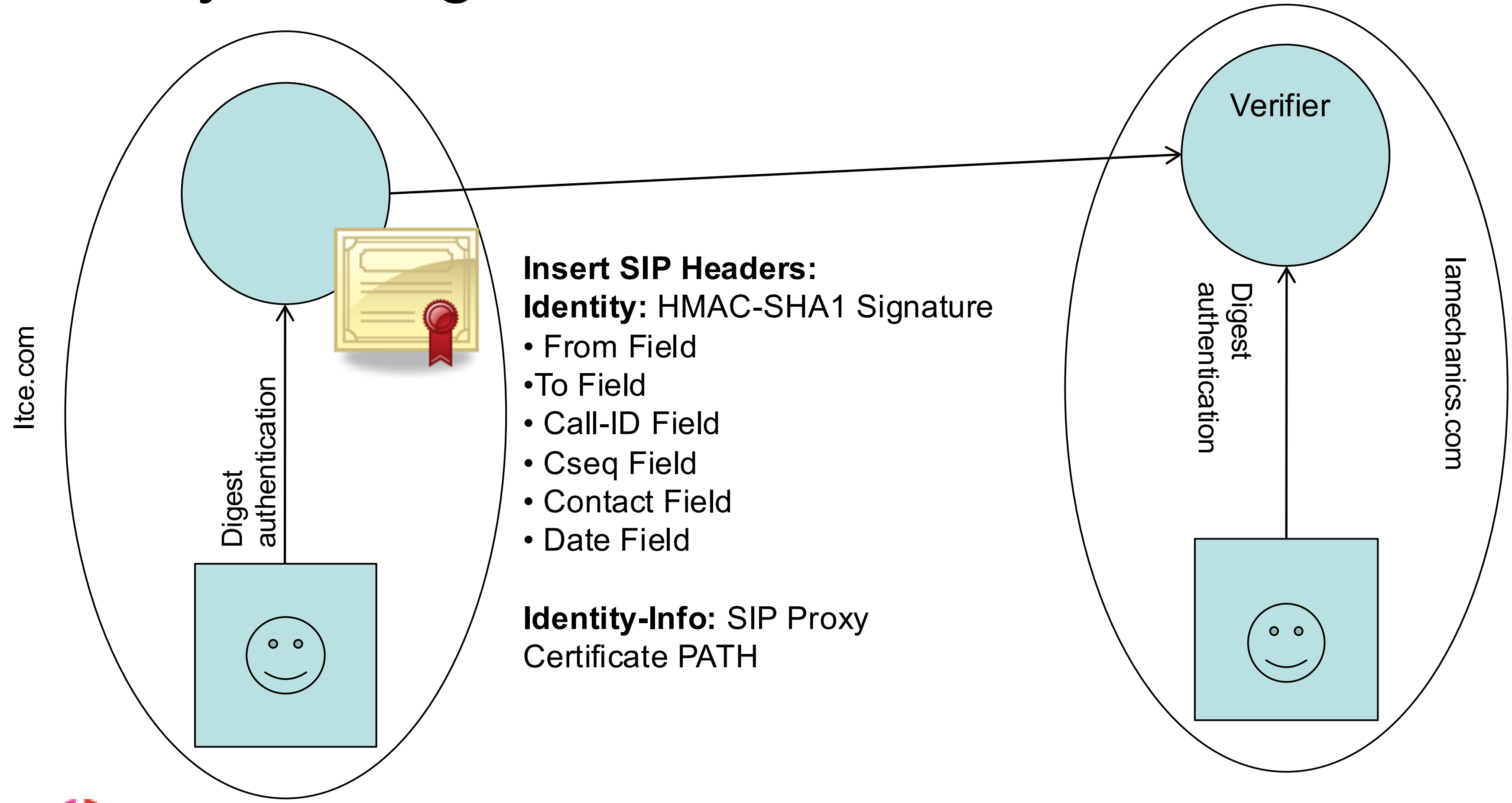
P-Asserted-Identity:Peter Black <Peter@iamechanics.com>

Example: MS OC 2007 Asserted Identity

```
INVITE sip:john@itce.com SIP/2.0
From:
        <sip:peter@iamechanics.com>;tag=94d432861a;epid=c36d93ba
        3
To: <sip:john@itce.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:+441628503002>
```

```
INVITE sip:131.107.2.101:2143;transpo tls;ms-
        opaque=81883e18f1;ms-received-c 6400 SIP/2.0
From: "Peter
        Black"<sip:peter@iamechanics.com> d432861a;epid=c36d
        93ba53
To: <sip:john@itce.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:+441628503002>
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

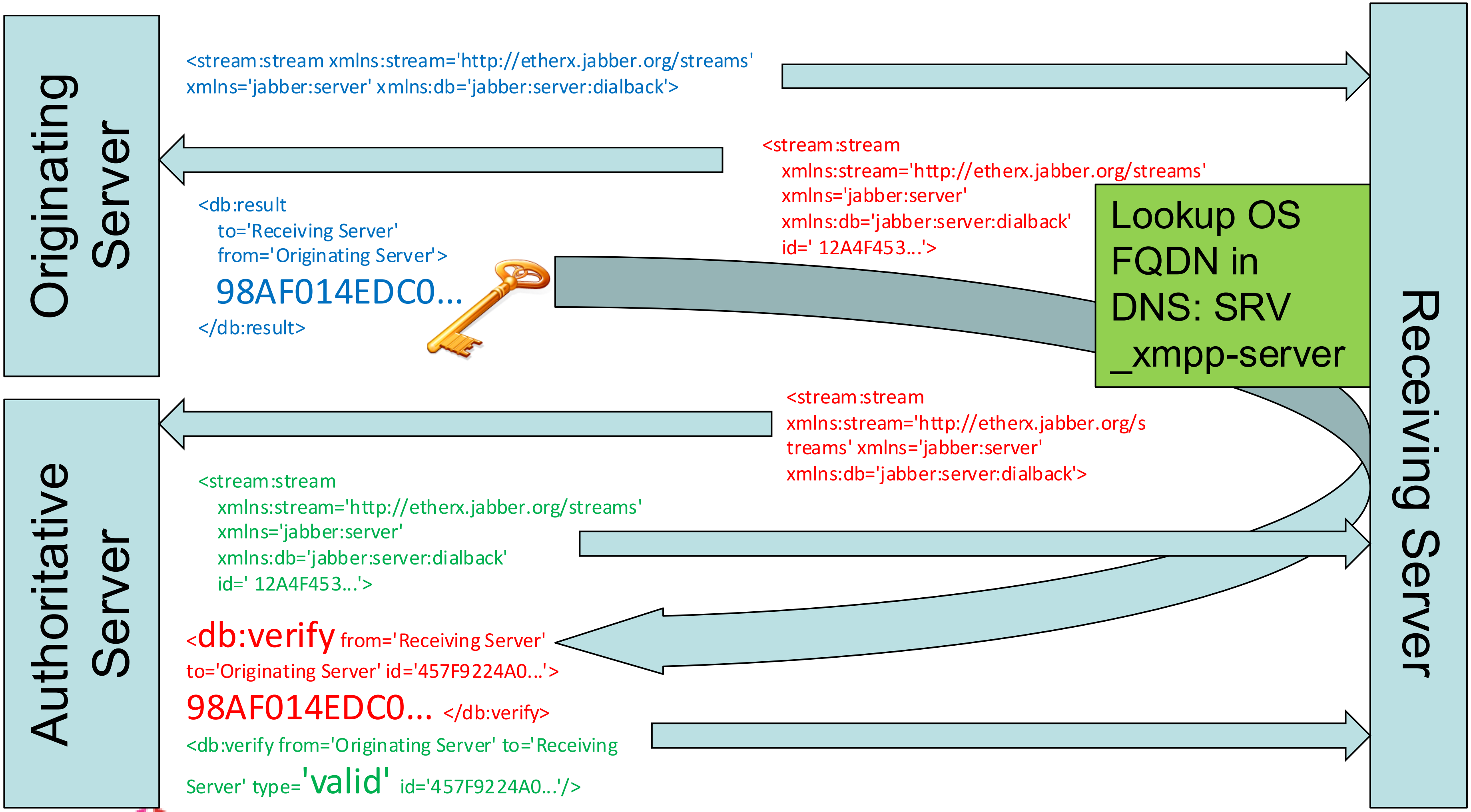


Insert SIP Headers:
Identity: HMAC-SHA1 Signature

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

Identity-Info: SIP Proxy Certificate PATH

XMPP Server Dialback – use DNS



<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/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...'>

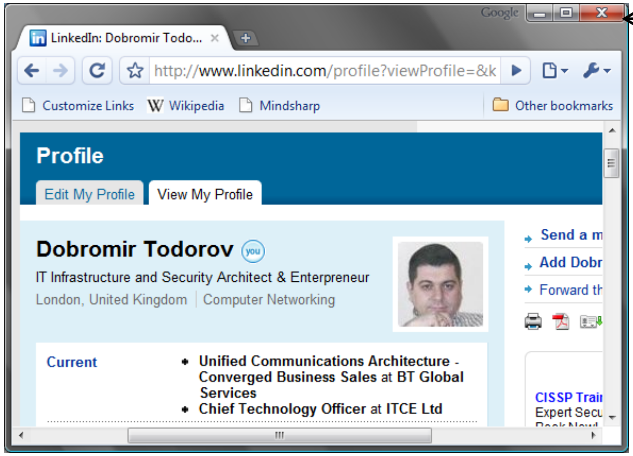
<db:verify from='Receiving Server' to='Originating Server' id='457F9224A0...'>
98AF014EDC0... </db:verify>

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

Caller-ID 2.0: Privacy Concerns

Caller ID

Search & Correlate



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

Profile

Dobromir Todorov

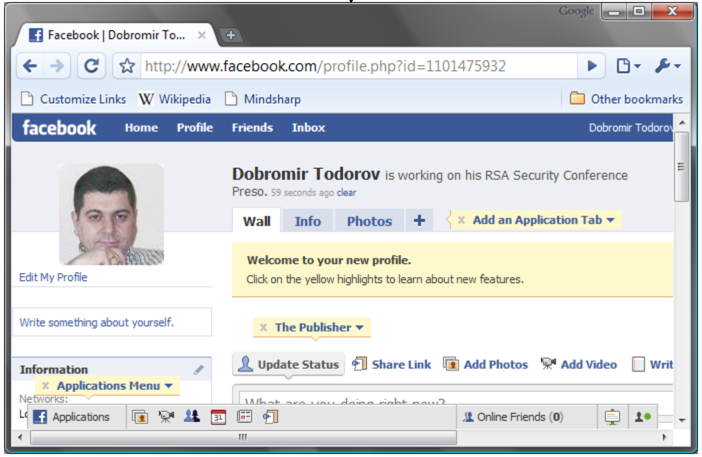
IT Infrastructure and Security Architect & Enterpreneur

London, United Kingdom | Computer Networking

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

Send a m
Add Dobr
Forward th

CISSP Trai
Expert Secu



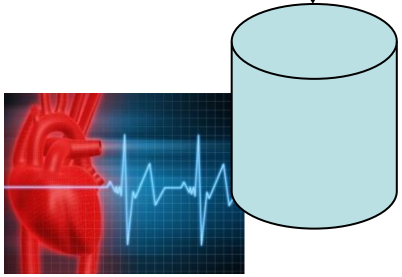
http://www.facebook.com/profile.php?id=1101475932

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

Welcome to your new profile.
Click on the yellow highlights to learn about new features.

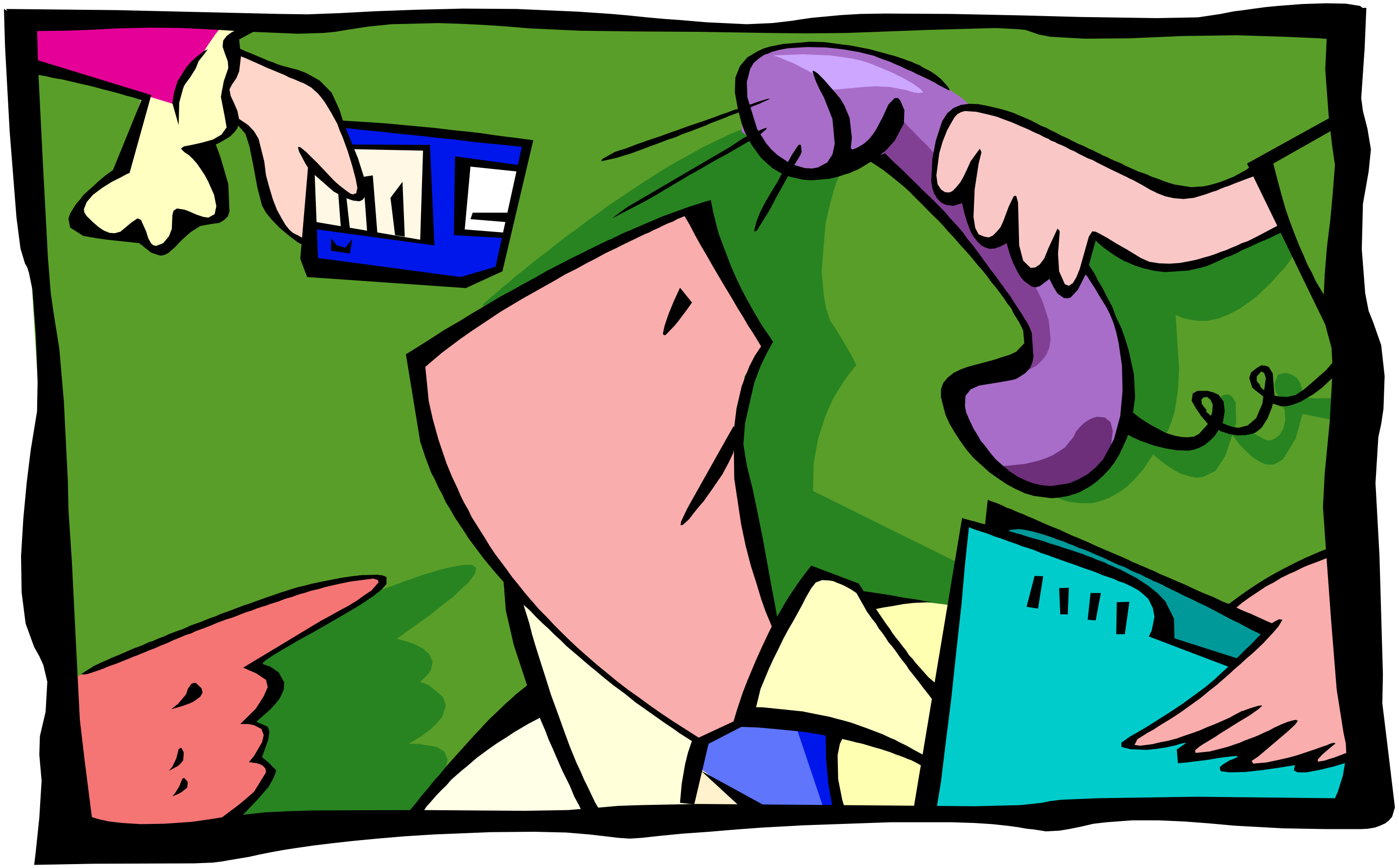
Write something about yourself.

What are you doing right now?



Patient DB

Signalling, IM and Presence



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, encryption, integrity)
- SSL/TLS and IPSec best suited to protect signalling
- 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

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"

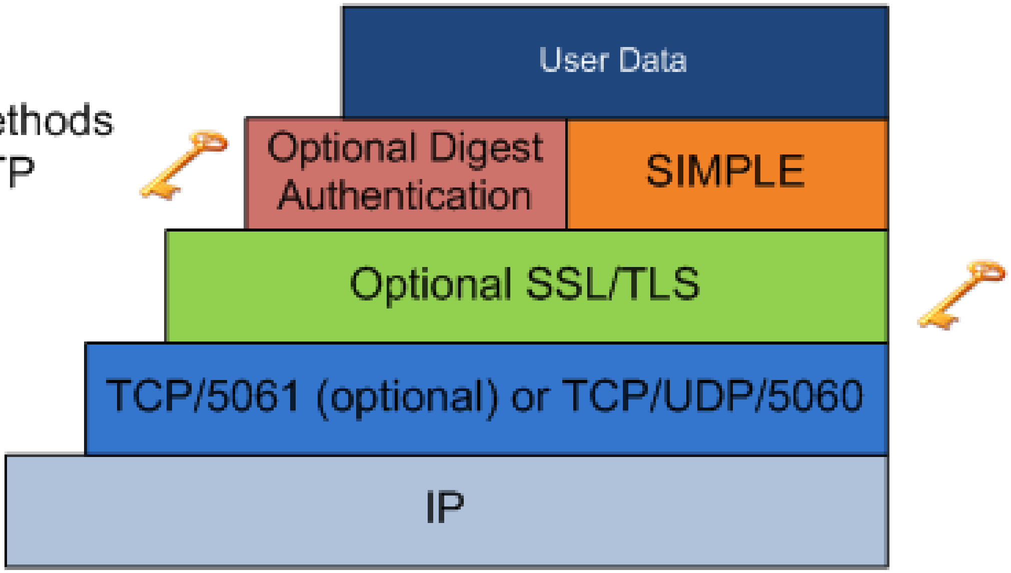
Content-Type: text/rtf

Content-Length: 273

Message-Body: “Hello! How are you?”

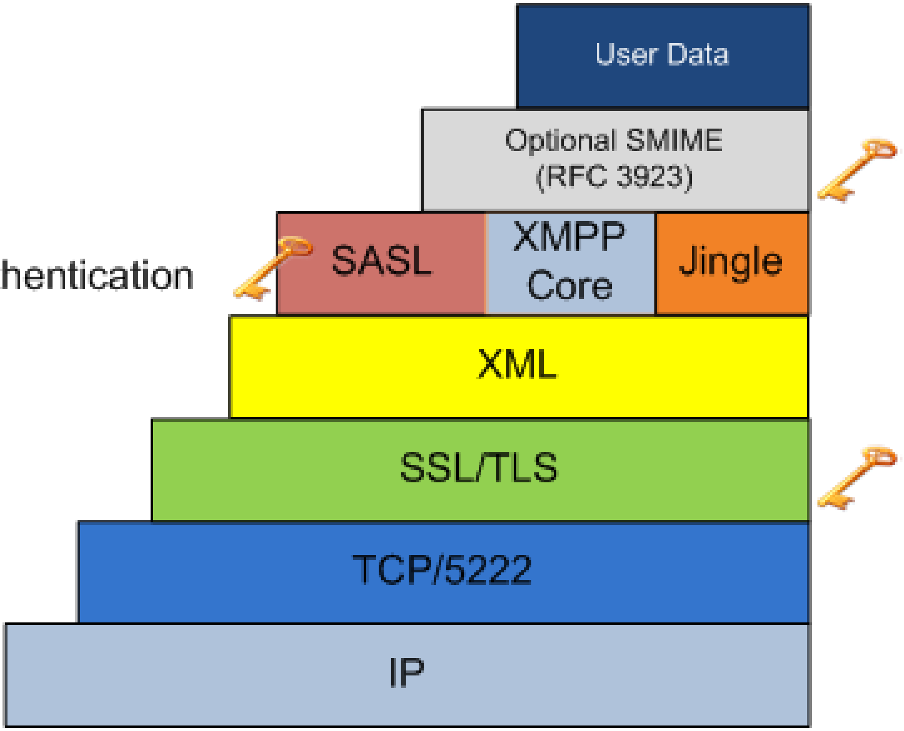
SIP Security Layers

Authentication methods similar to HTTP


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

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

XMPP Security Layers



Modular authentication

End-to-End signing and encryption with S/MIME

Encryption
Data Integrity
Peer Identity
(client to server)

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
  - SIP SERVICE verb inspection
  - XMPP Stanza inspection

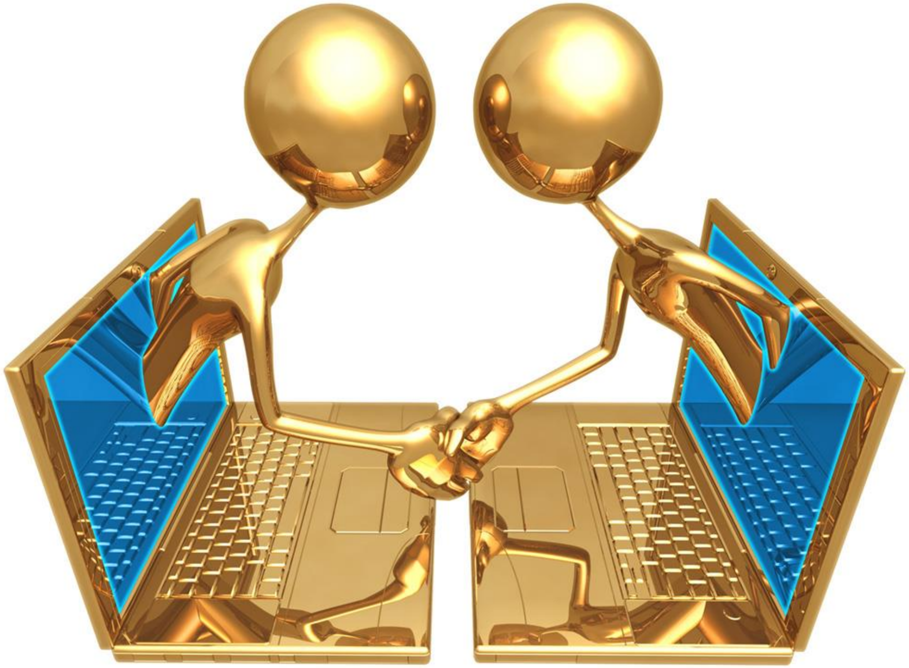
Example: Location Spoofing

- 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

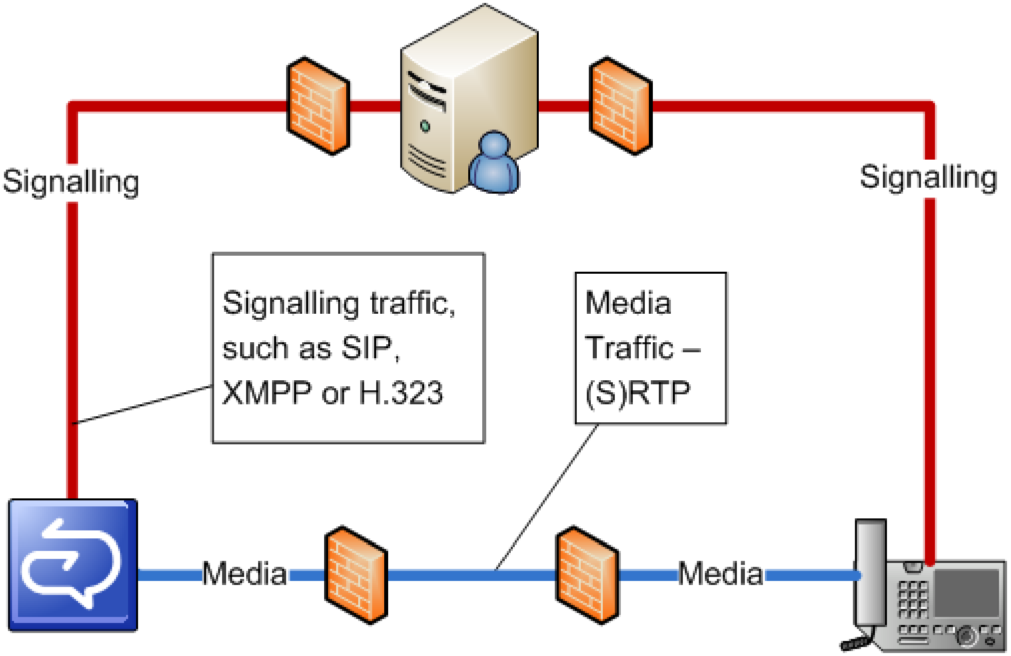
Malware in the UC(C) world

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

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)

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
  - SDP (over SIP over SSL/TLS)
  - 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@itce.com SIP/2.0
From: <sip:peter@iamechanics.com>;tag=94d432861a;epid=c36d93ba53
To: <sip:john@itce.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 DBcwlyZt9dWG/1+dP7njGA UDP 0.830 192.168.1.73 21504
a=candidate:/T0b/1X7sJfZ39m5We+V5EyjP7XTyKNCtTxZA0dog4g 2 DBcwlyZt9dWG/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? ICE/TURN/STUN Tunnelling
- Application Layer Gateways required

In Summary: UC(C) Security Ingredients

- 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
- Antivirus and Antispam Software
- Considering implementing SRTP
- Security Policies, Guidelines, and Compliance

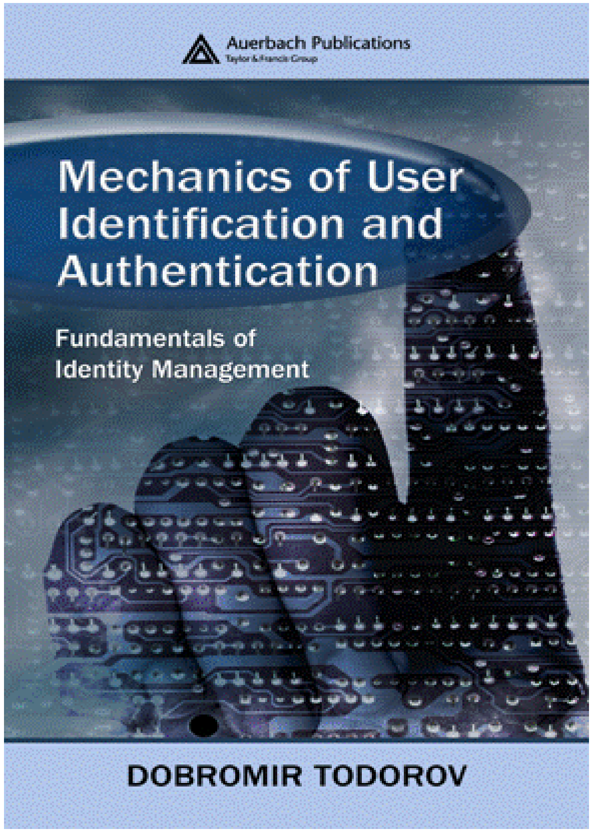
Questions and Answers

- All questions are welcome
- Questions can be taken offline
  - After this session for the duration of the conference
  - Anytime by e-mail – contact details below

Dobromir Todorov

UC Architect, BT Global Services

mailto:Dobromir.Todorov@bt.com


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