Acquired by:

AVAYA

VIPER Lab

WWW.VIPERLAB.NET

The End of the PSTN As You Know It

DEF CON 20

July 28, 2012

Agenda

- "Islands of VoIP"
  - Tool release
- UC Federation
  - Surprise UCF Vendor Research
- Open Source Software

Small Disclaimer

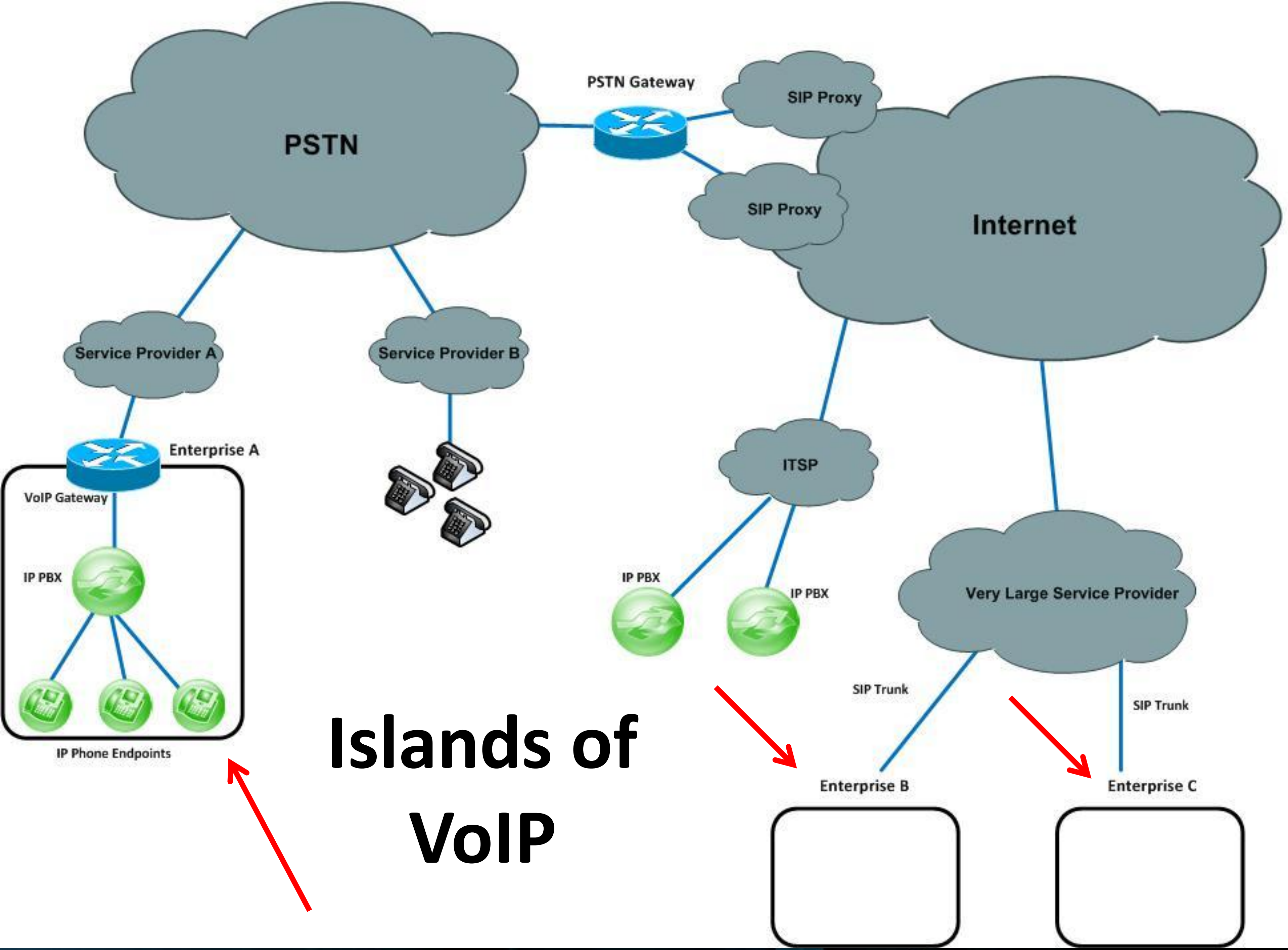
- These are our opinions based on experience
  - Not necessarily the official position of our employer
  - These issues are large and complex
    - We are here to explore an idea
  - We’re not finished with this research
    - (In fact, we’re just getting started)

About VIPER

- VIPER Lab (Voice over IP Exploit Research)
  - 1. Security Assessment for VoIP/UC
  - 2. R&D Lab for vulnerability research around UC/VoIP

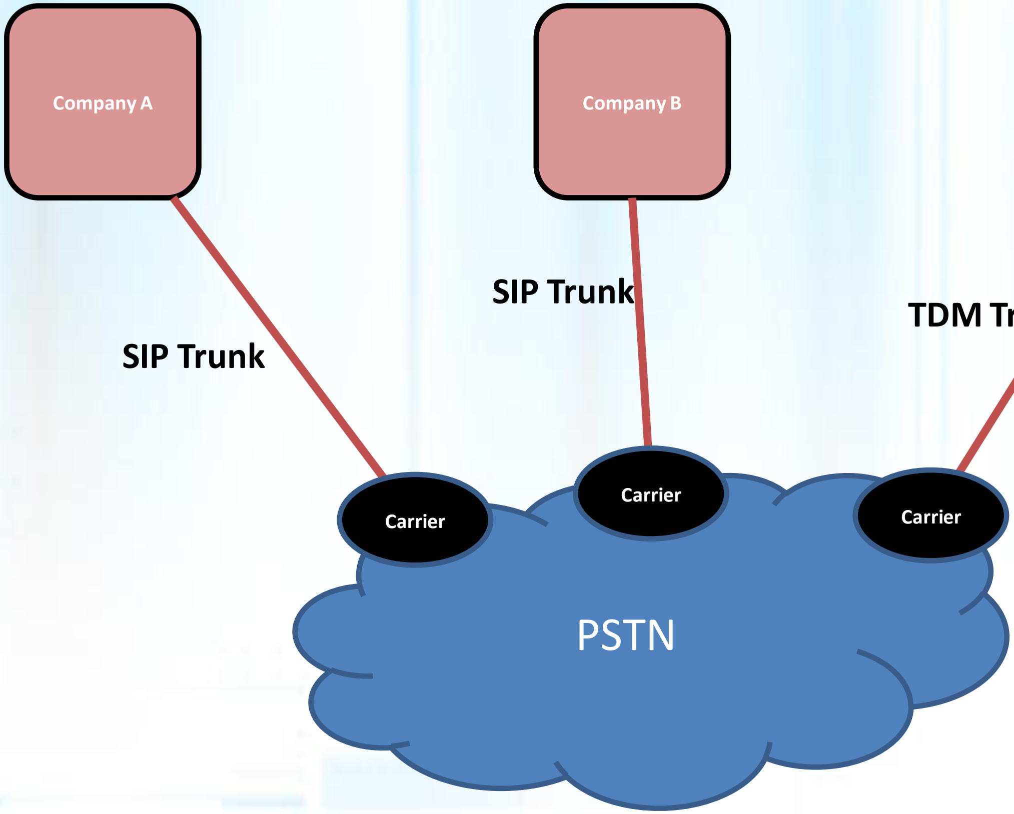
A long time ago, in a land far away…

A VoIP Pentest took place…



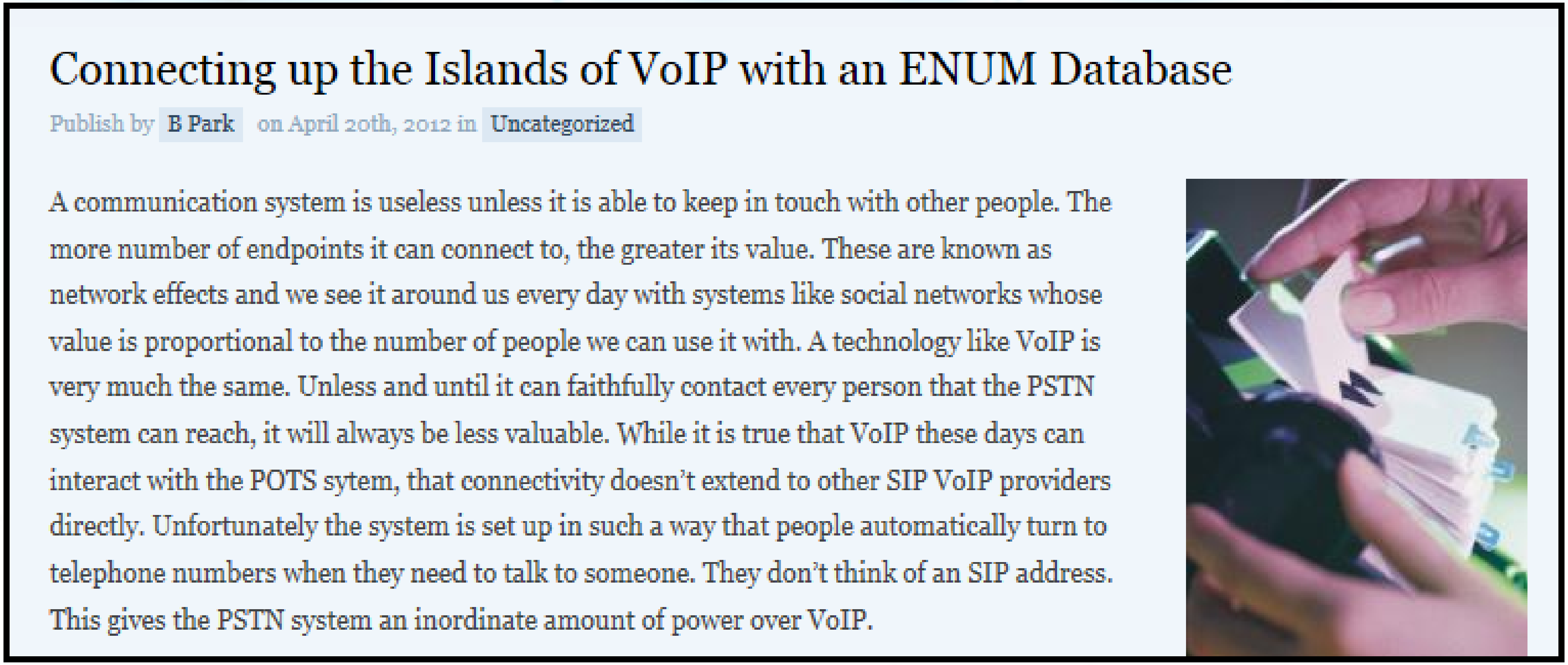
Islands of VoIP

"Islands of VoIP"



How to Connect “Islands of VoIP”?

- ENUM



Connecting up the Islands of VoIP with an ENUM Database

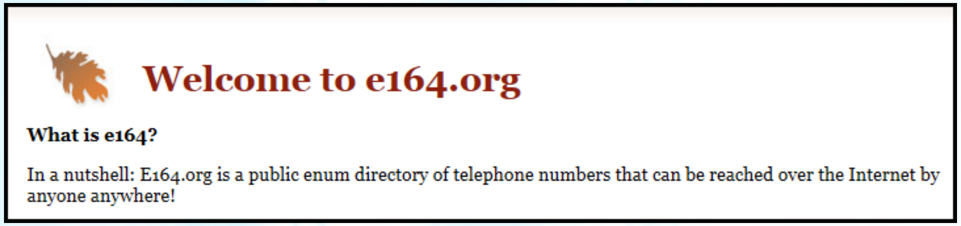
Publish by B Park on April 20th, 2012 in Uncategorized

A communication system is useless unless it is able to keep in touch with other people. The more number of endpoints it can connect to, the greater its value. These are known as network effects and we see it around us every day with systems like social networks whose value is proportional to the number of people we can use it with. A technology like VoIP is very much the same. Unless and until it can faithfully contact every person that the PSTN system can reach, it will always be less valuable. While it is true that VoIP these days can interact with the POTS sytem, that connectivity doesn’t extend to other SIP VoIP providers directly. Unfortunately the system is set up in such a way that people automatically turn to telephone numbers when they need to talk to someone. They don’t think of an SIP address. This gives the PSTN system an inordinate amount of power over VoIP.

ENUM

- How it works
  - Uses DNS NAPTR records to map E.164 telephone numbers to a URI (SIP URI)
  - When you dial a telephone number, you don’t know for certain if it’s connected to PSTN or a SIP network
  - Solves problem of dialing between SIP networks when you only have a telephone number
- Adoption rate
  - Hasn’t seen widespread adoption
  - Political, Economic reasons

ENUM Experiment



Welcome to e164.org

What is e164?

In a nutshell: E164.org is a public enum directory of telephone numbers that can be reached over the Internet by anyone anywhere!

- www.e164.org
  - Public ENUM Directory
  - They have a form and validation procedure for adding your telephone number and SIP URI to their directory
  - We tried adding ourselves in using their procedure
- Result
  - Failure
  - Process didn't appear to work & multiple emails to their contact address - no response.

No more “Islands of VoIP”!

(There has to be a better way)

The Superior Solution:

SIP Peering using DNS SRV

SIP Peering using DNS SRV

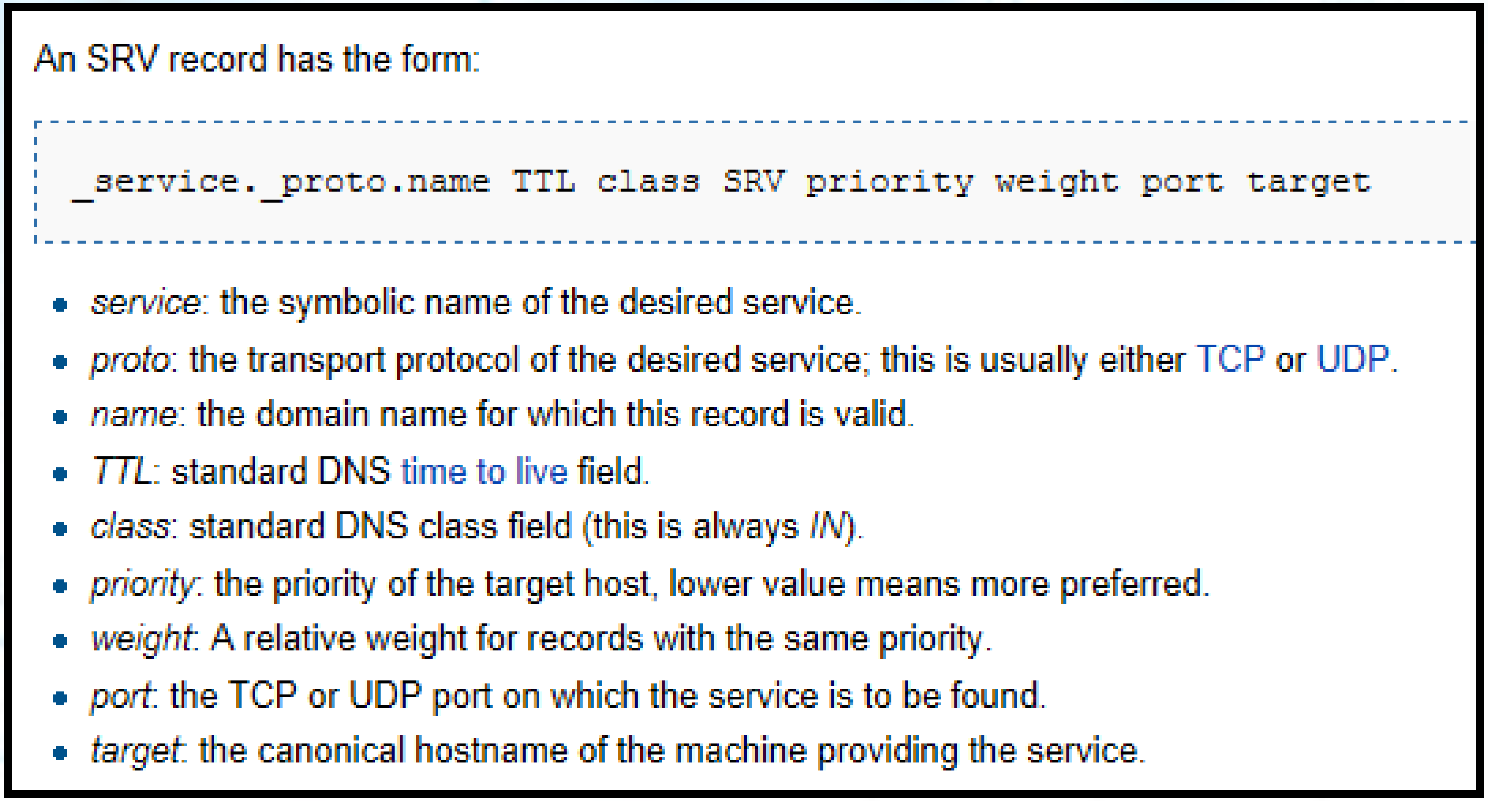
- We propose an idea to have everyone use DNS for SIP Peering
  - Can interconnect all "Islands of VoIP" directly between organizations using DNS
  - DNS built for HA and load balancing
  - Calls via your SIP URI
    - Easier to remember
    - No more dial by numbers
    - Use your email address as your SIP URI / address
  - Large cost saving for direct SIP peering
  - PSTN will be increasingly diminished

DNS SRV: RFC 2782

- A special DNS resource record for the location of Services (SRV)
- For fault tolerance and load balancing
- Multiple *priorities* and *weights*, just like MX records for MTAs
- Clients look up lower *priority* records first, and then fallback to records of equal or higher priority
- If multiple records with same priority, *weight* value is used
- RFC 3263 specifies usage of DNS SRV for SIP

DNS SRV: RFC 2782

› Record Format



An SRV record has the form:

```
_service._proto.name TTL class SRV priority weight port target
```

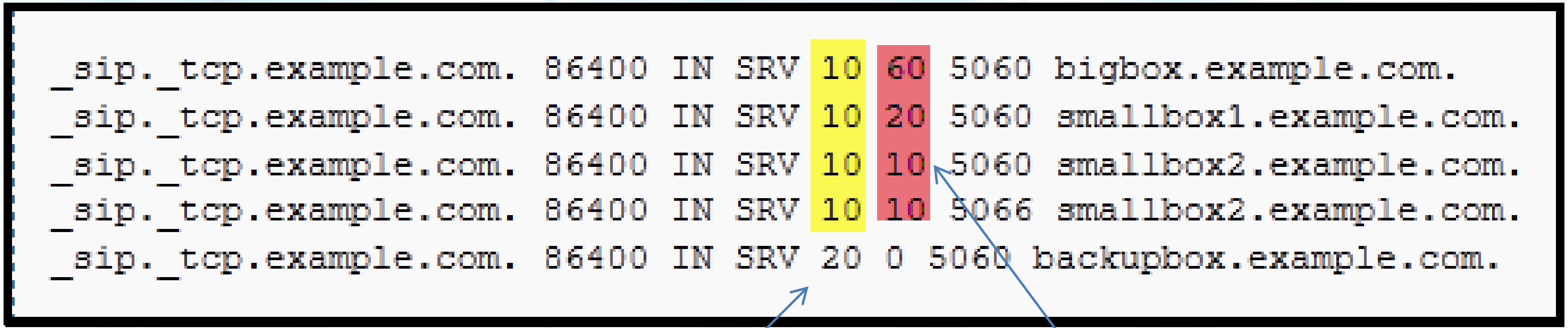
- *service*: the symbolic name of the desired service.
- *proto*: the transport protocol of the desired service; this is usually either TCP or UDP.
- *name*: the domain name for which this record is valid.
- *TTL*: standard DNS time to live field.
- *class*: standard DNS class field (this is always *IN*).
- *priority*: the priority of the target host, lower value means more preferred.
- *weight*: A relative weight for records with the same priority.
- *port*: the TCP or UDP port on which the service is to be found.
- *target*: the canonical hostname of the machine providing the service.

Source: Wikipedia

DNS SRV: RFC 2782

- Sample Record

Source: Wikipedia



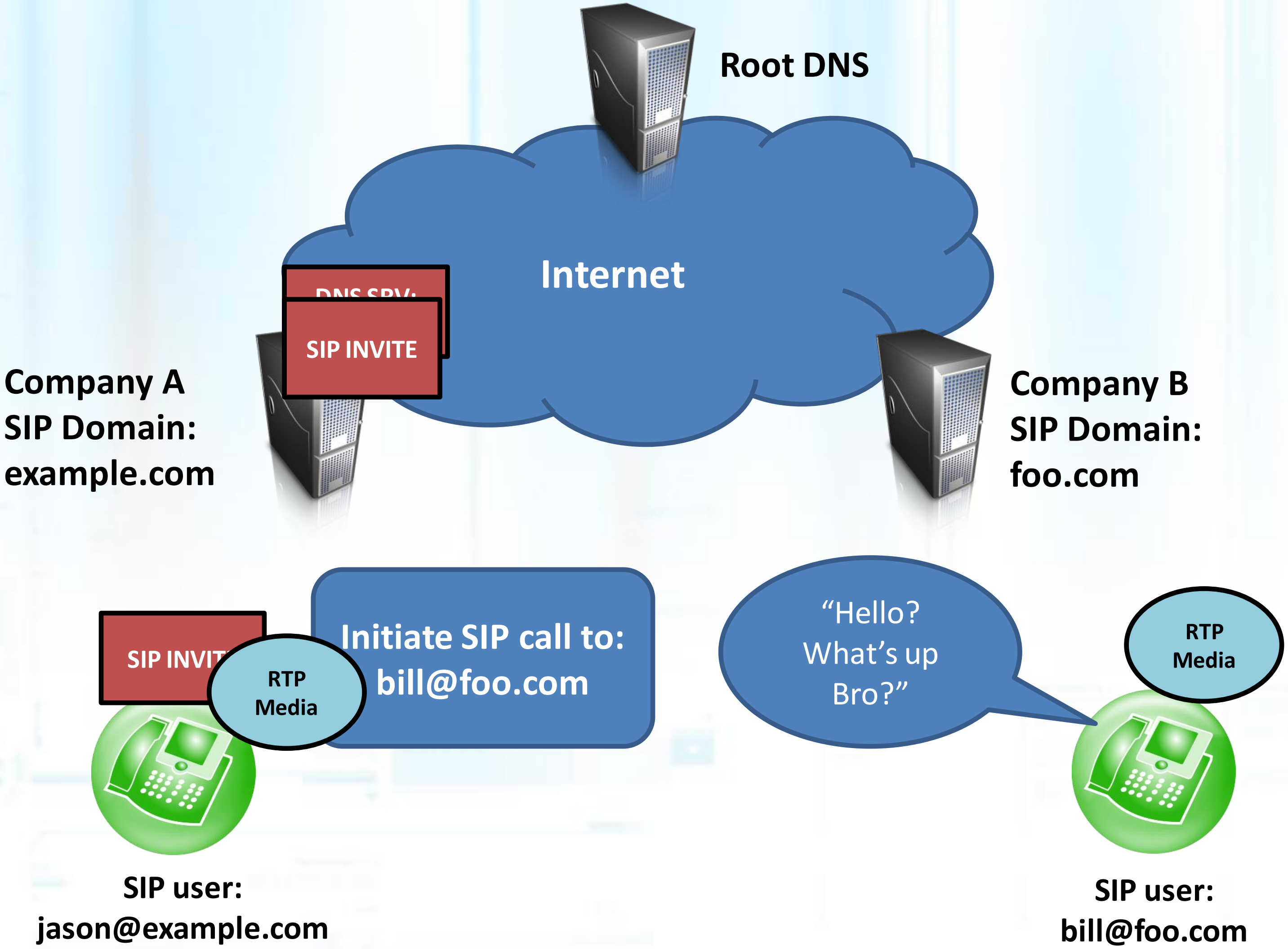
```
_sip._tcp.example.com. 86400 IN SRV 10 60 5060 bigbox.example.com.
_sip._tcp.example.com. 86400 IN SRV 10 20 5060 smallbox1.example.com.
_sip._tcp.example.com. 86400 IN SRV 10 10 5060 smallbox2.example.com.
_sip._tcp.example.com. 86400 IN SRV 10 10 5066 smallbox2.example.com.
_sip._tcp.example.com. 86400 IN SRV 20 0 5060 backupbox.example.com.
```

Automatic load balancing group created with equal priority of “10”

Weight values added up to 100.

60% of traffic to bigbox
20% of traffic to smallbox
10% to each remaining

SIP DNS SRV Deployment



Root DNS

Internet

DNS SRV:

SIP INVITE

Company A
SIP Domain:
example.com

Company B
SIP Domain:
foo.com

SIP INVIT

RTP
Media

Initiate SIP call to:
bill@foo.com

"Hello?
What's up
Bro?"

RTP
Media

SIP user:
jason@example.com

SIP user:
bill@foo.com

Research Goal

- Objective: Wanted to measure growth of SIP peering on IPv4 Internet, over period of time.
  - Proliferation of DNS SRV records, plotted over time
  - Proliferation of ENUM for selected e.164 blocks, plotted over time
  - Proliferation of listening SIP services for every IPv4 address, plotted over time

Introducing Enumerator Tool

- Releasing a new intelligence gathering tool that we developed for this research
  - Tool Name: enumerator
  - Website: http://enumerator.sourceforge.net
  - Written in C
  - Uses the "libresolv" library
  - Can be used for R&D purposes like we did, or for VoIP pentesting in the Recon phase
  - Optimized for VoIP and a large number of domains

Enumerator

- Key Features
  - DNS SRV lookups for single domain, or text input list
    - Partial support for Microsoft specific targets
  - DNS MX lookups for single domain, or text input list
  - DNS ENUM lookups for single number, or input list

Enumerator Phase I “Scan”

- Ran an enumerator SRV lookup “Scan”
  - Procured all TLD (Top-level domains) from Network Solutions, Org
  - Goal was to find number of SRV enabled domains potentially enabled for SIP
  - Idea was to run several of these “scans” over a year and plot how the data changes over time

Data Input

- Received from Network Solutions and Org
  - .com domains: 234,638,894 (4.231 GB)
  - .net domains: 34,232,716 (578.313 MB)
  - .org domains: 23,409,623 (430.455 MB)
- Total: 292,281,233 domains

4 SRV Target Queries

- *Benchmarking*
  - *140 Domain queries per second on each server (11 servers)*
  - *4 SRV queries per domain*
  - *Split enumerator into 800 separate processes, 800 files*
  - *Command: ./enum-launcher.pl –f largefile.txt –c 800*
- *4 SRV queries*
  - *_sip._udp.<domain>*
  - *_sip._tcp.<domain>*
  - *_sip._tls.<domain>*
  - *_sipfederationtls._tcp.<domain>*

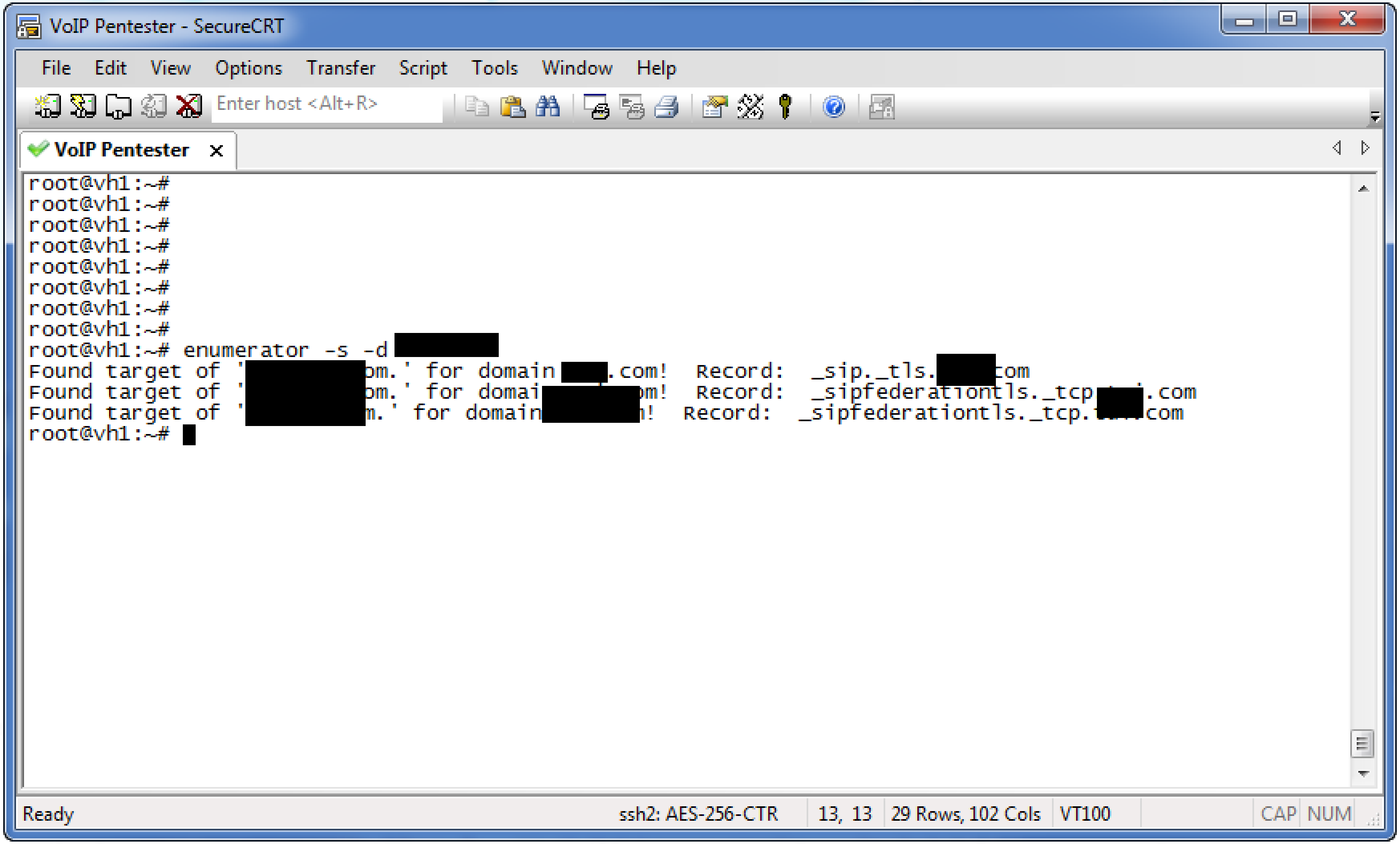
Results from Enumerator Scan #1

- Total domains checked:
  - 265,710,178
- Without SRV:
  - 256,947,303
  - 96.70%
- With SRV for SIP:
  - **8,762,875 Top Level Domains (.com/.net/.org) with SRV SIP enabled**
  - **3.30%**

8 Million TLD domains enabled for SIP SRV!

3.30%

Enumerator In Action

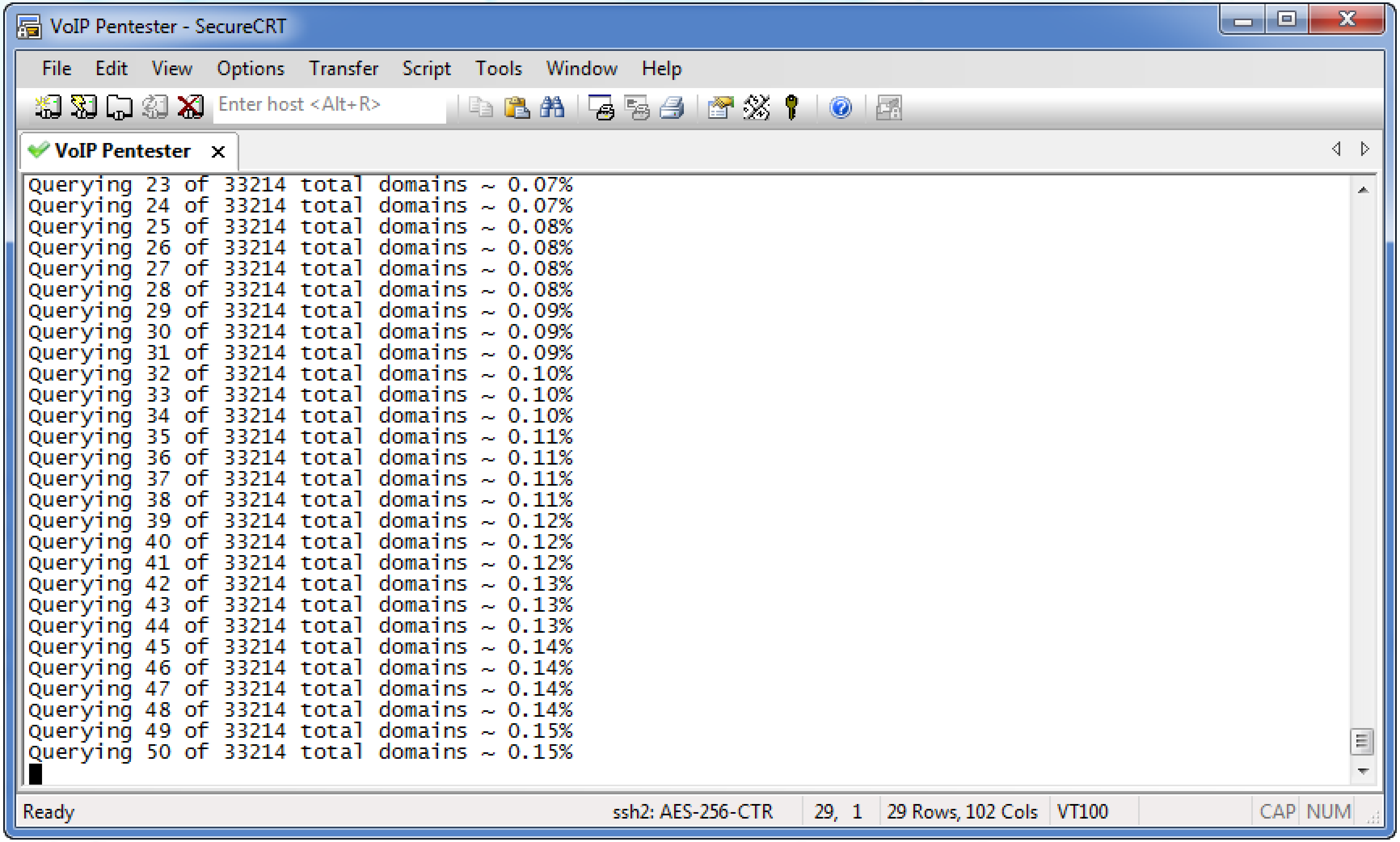


```
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~# enumerator -s -d [redacted]
Found target of '[redacted]om.' for domain [redacted].com!  Record:  _sip._tls.[redacted]com
Found target of '[redacted]om.' for domai[redacted]om!  Record:  _sipfederationtls._tcp[redacted].com
Found target of '[redacted]m.' for domain[redacted]!  Record:  _sipfederationtls._tcp.[redacted]com
root@vh1:~# █
```

Other Examples

- Example: enumerator –s –l domains.txt
  - Takes domains.txt as input and looks up all domains
- Example: enumerator –m –d example.com
  - MX Record lookup of single domain

Enumerator In Action



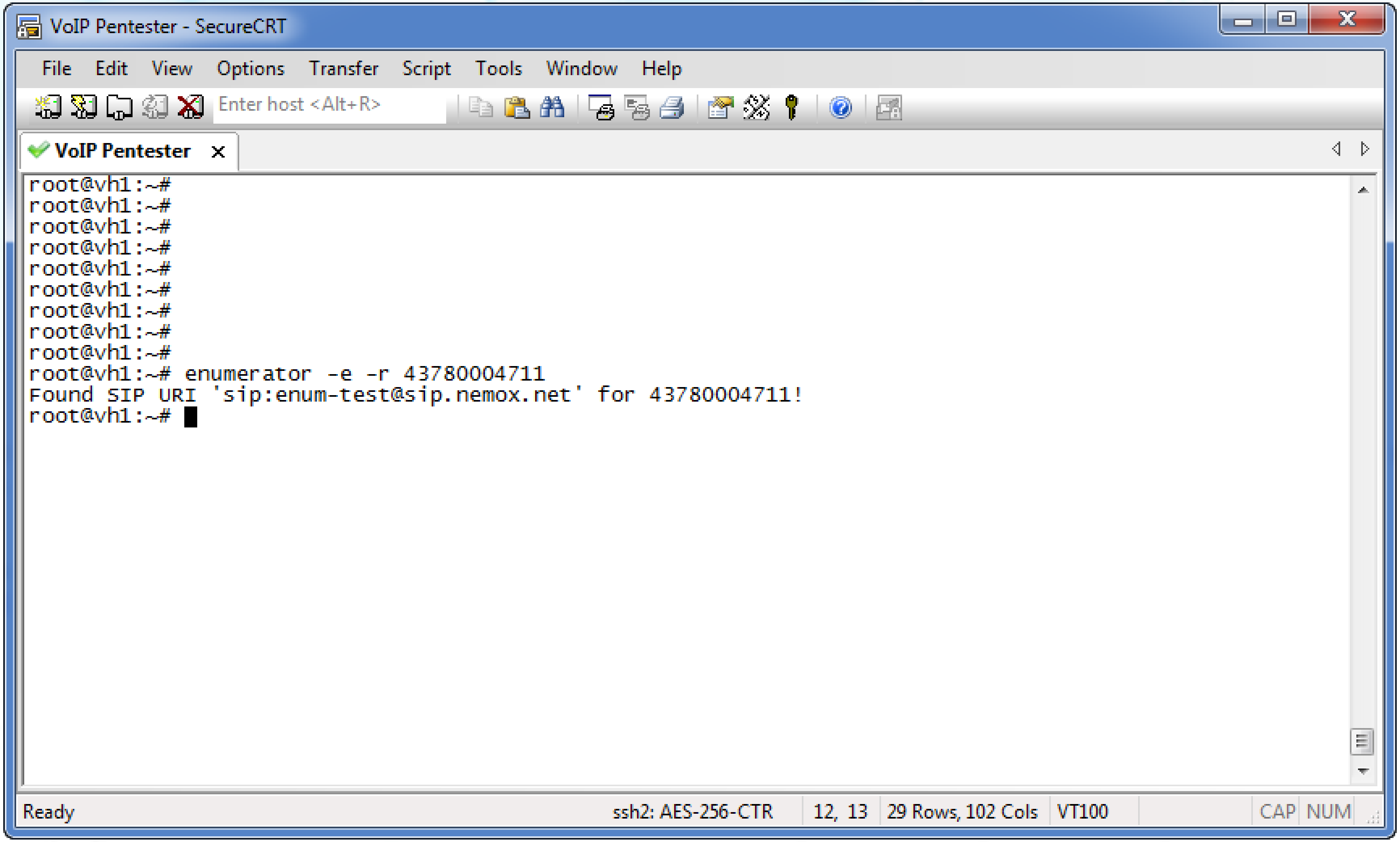
VoIP Pentester - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
VoIP Pentester

```
Querying 23 of 33214 total domains ~ 0.07%
Querying 24 of 33214 total domains ~ 0.07%
Querying 25 of 33214 total domains ~ 0.08%
Querying 26 of 33214 total domains ~ 0.08%
Querying 27 of 33214 total domains ~ 0.08%
Querying 28 of 33214 total domains ~ 0.08%
Querying 29 of 33214 total domains ~ 0.09%
Querying 30 of 33214 total domains ~ 0.09%
Querying 31 of 33214 total domains ~ 0.09%
Querying 32 of 33214 total domains ~ 0.10%
Querying 33 of 33214 total domains ~ 0.10%
Querying 34 of 33214 total domains ~ 0.10%
Querying 35 of 33214 total domains ~ 0.11%
Querying 36 of 33214 total domains ~ 0.11%
Querying 37 of 33214 total domains ~ 0.11%
Querying 38 of 33214 total domains ~ 0.11%
Querying 39 of 33214 total domains ~ 0.12%
Querying 40 of 33214 total domains ~ 0.12%
Querying 41 of 33214 total domains ~ 0.12%
Querying 42 of 33214 total domains ~ 0.13%
Querying 43 of 33214 total domains ~ 0.13%
Querying 44 of 33214 total domains ~ 0.13%
Querying 45 of 33214 total domains ~ 0.14%
Querying 46 of 33214 total domains ~ 0.14%
Querying 47 of 33214 total domains ~ 0.14%
Querying 48 of 33214 total domains ~ 0.14%
Querying 49 of 33214 total domains ~ 0.15%
Querying 50 of 33214 total domains ~ 0.15%
```

ENUM Support

- Example: enumerator –e –r 12145551212
  - Looks up single e.164 telephone number
- Example: enumerator –e –r 12145551212-12145559999
  - Looks up a range
- Example: enumerator –e –l numbers.txt
  - Takes numbers.txt as input and looks up all numbers in text file

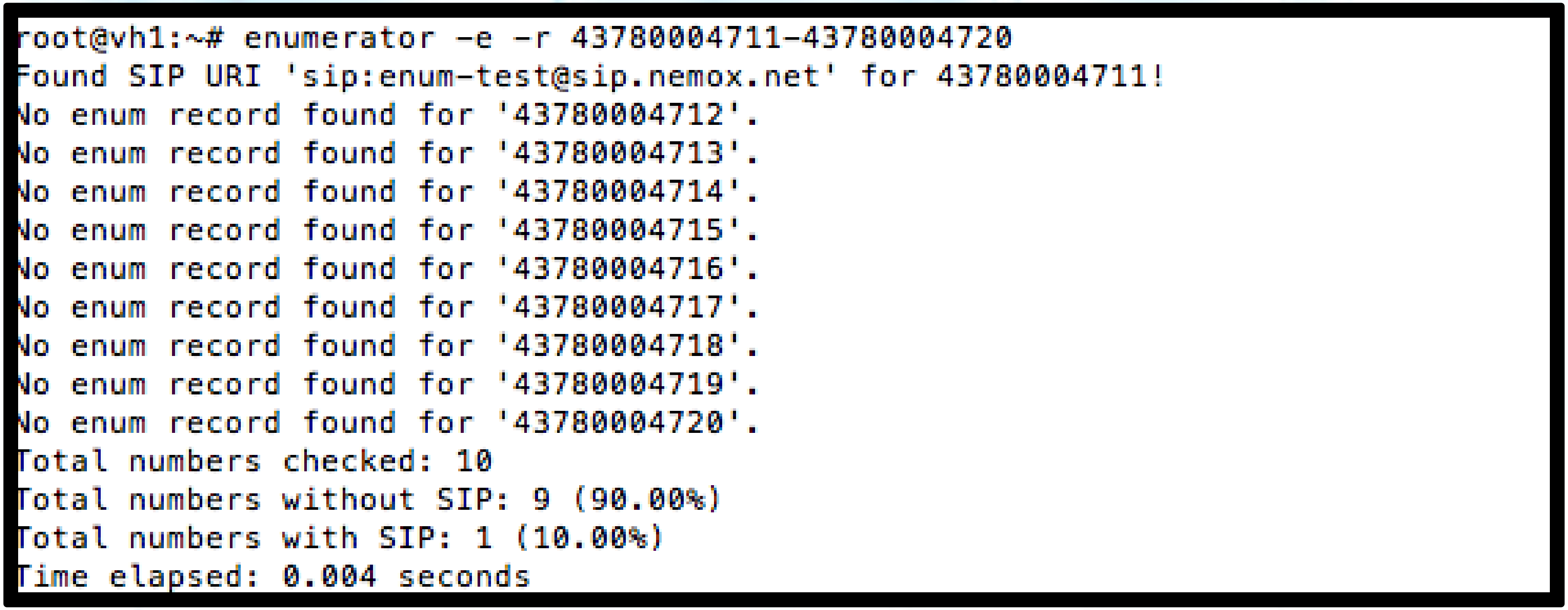
Enumerator In Action - ENUM



VoIP Pentester - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
VoIP Pentester

```
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~#
root@vh1:~# enumerator -e -r 43780004711
Found SIP URI 'sip:enum-test@sip.nemox.net' for 43780004711!
root@vh1:~#
```

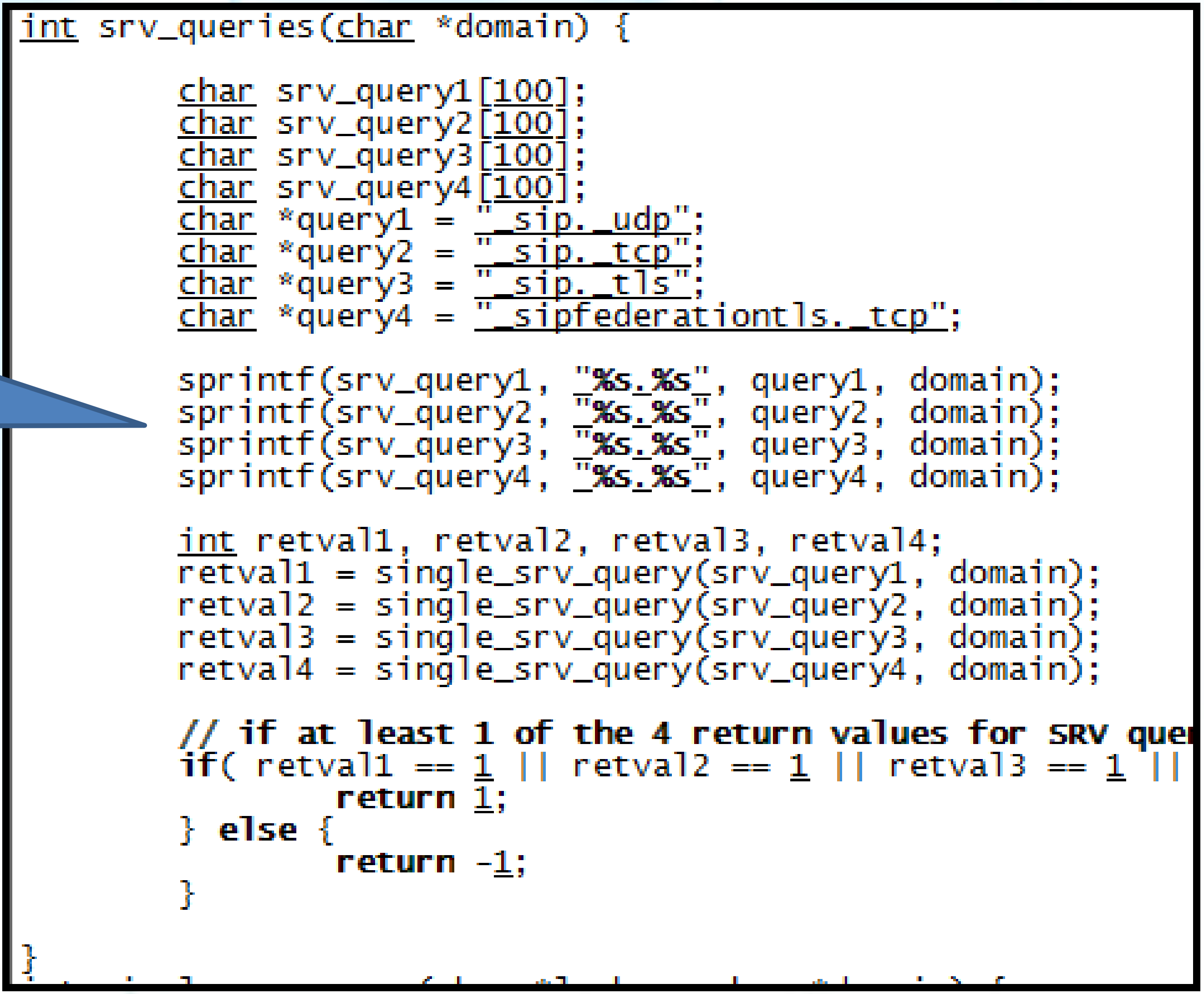
Enumerator In Action - ENUM



```
root@vh1:~# enumerator -e -r 43780004711-43780004720
Found SIP URI 'sip:enum-test@sip.nemox.net' for 43780004711!
No enum record found for '43780004712'.
No enum record found for '43780004713'.
No enum record found for '43780004714'.
No enum record found for '43780004715'.
No enum record found for '43780004716'.
No enum record found for '43780004717'.
No enum record found for '43780004718'.
No enum record found for '43780004719'.
No enum record found for '43780004720'.
Total numbers checked: 10
Total numbers without SIP: 9 (90.00%)
Total numbers with SIP: 1 (10.00%)
Time elapsed: 0.004 seconds
```

srv.c

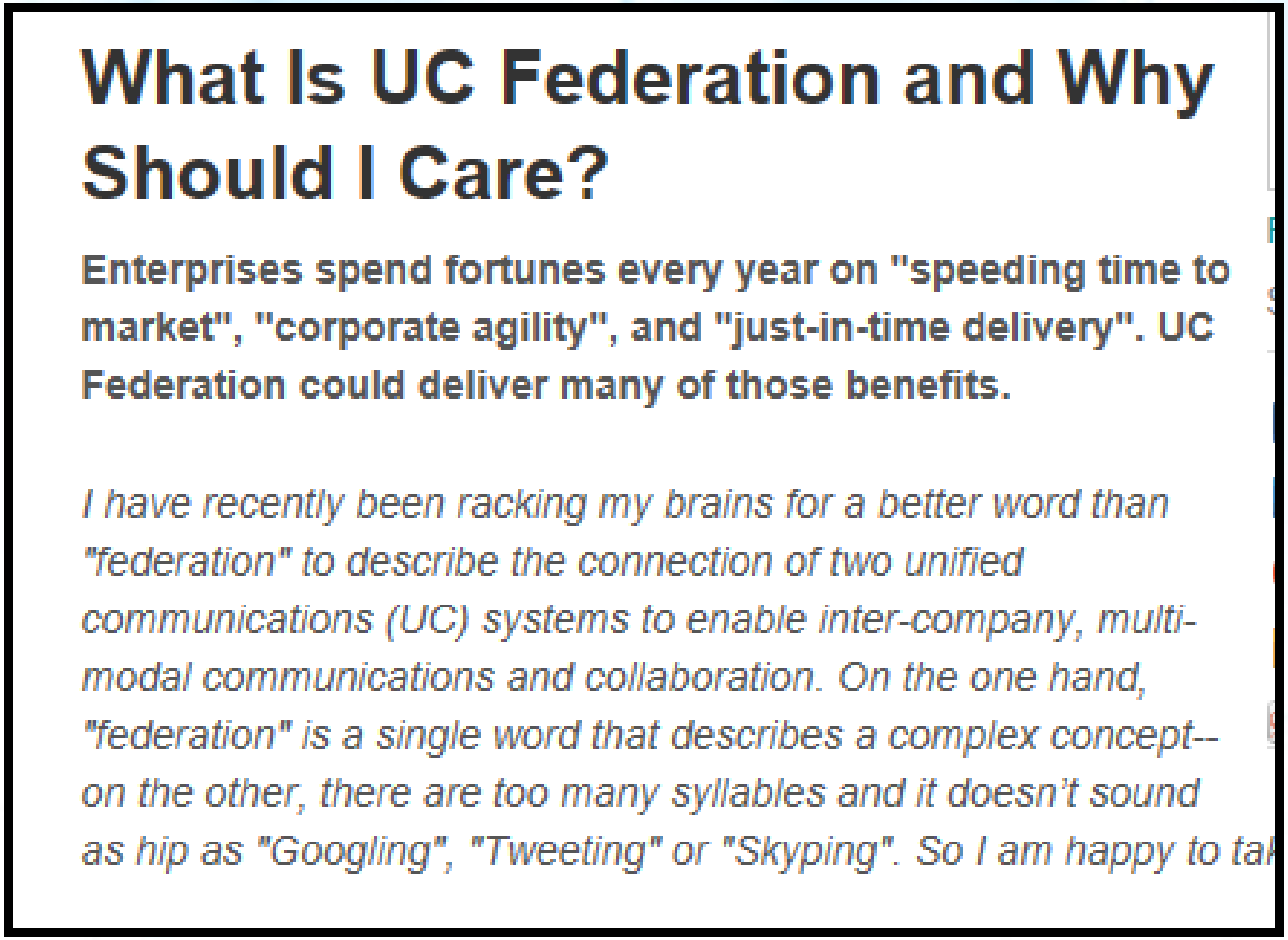
You can make changes to srv.c, adding support for new SRV queries.



```
int srv_queries(char *domain) {

        char srv_query1[100];
        char srv_query2[100];
        char srv_query3[100];
        char srv_query4[100];
        char *query1 = "_sip._udp";
        char *query2 = "_sip._tcp";
        char *query3 = "_sip._tls";
        char *query4 = "_sipfederationtls._tcp";

        sprintf(srv_query1, "%s.%s", query1, domain);
        sprintf(srv_query2, "%s.%s", query2, domain);
        sprintf(srv_query3, "%s.%s", query3, domain);
        sprintf(srv_query4, "%s.%s", query4, domain);

        int retval1, retval2, retval3, retval4;
        retval1 = single_srv_query(srv_query1, domain);
        retval2 = single_srv_query(srv_query2, domain);
        retval3 = single_srv_query(srv_query3, domain);
        retval4 = single_srv_query(srv_query4, domain);

        // if at least 1 of the 4 return values for SRV quer
        if( retval1 == 1 || retval2 == 1 || retval3 == 1 ||
                return 1;
        } else {
                return -1;
        }

}
```

Enumerator can measure the usage of UC Federation services, or SIP enabled DNS SRV records, enabled on the public Internet.

UC Federation – next “Killer App”?



What Is UC Federation and Why Should I Care?

Enterprises spend fortunes every year on "speeding time to market", "corporate agility", and "just-in-time delivery". UC Federation could deliver many of those benefits.

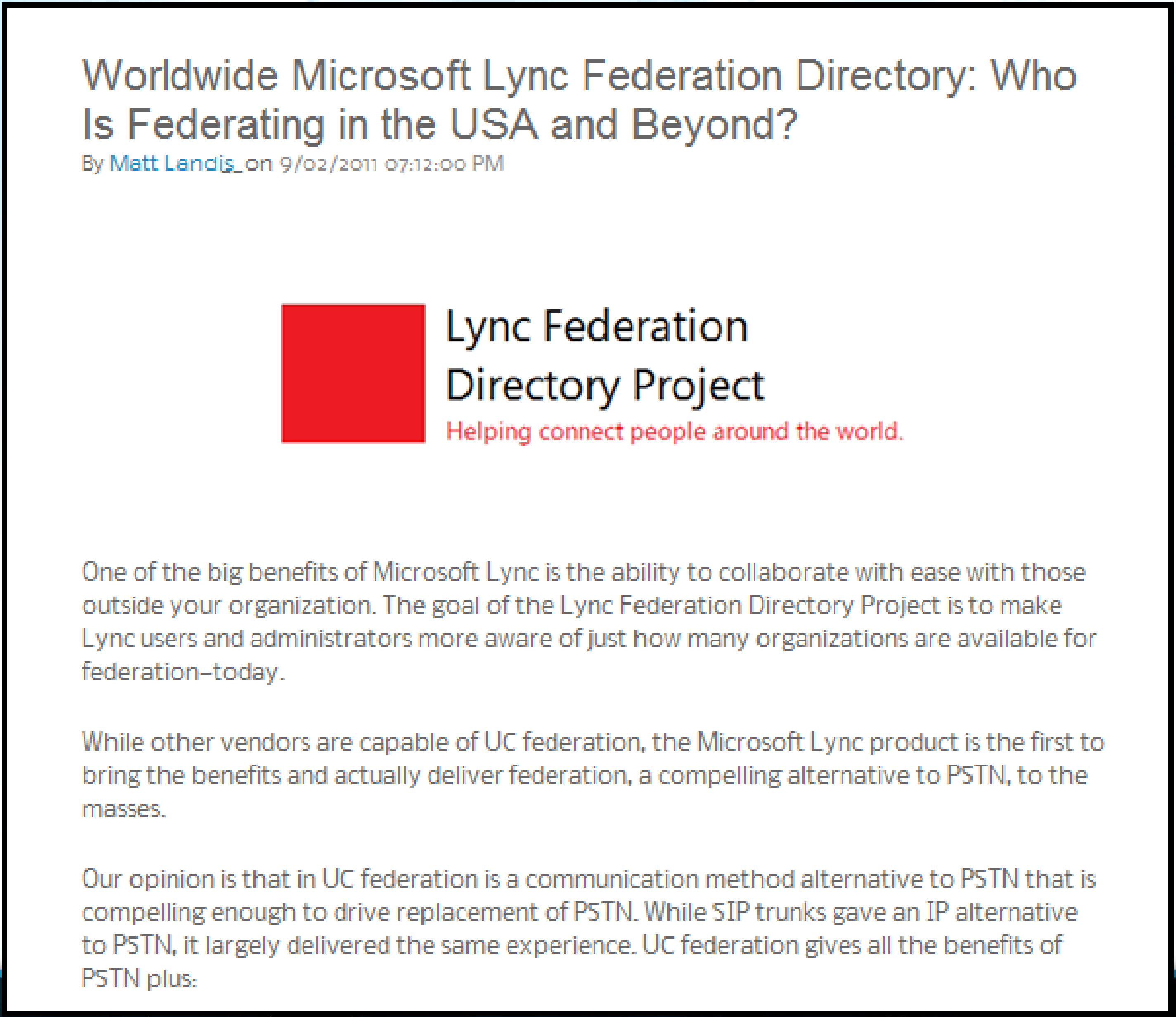
I have recently been racking my brains for a better word than "federation" to describe the connection of two unified communications (UC) systems to enable inter-company, multi-modal communications and collaboration. On the one hand, "federation" is a single word that describes a complex concept--on the other, there are too many syllables and it doesn’t sound as hip as "Googling", "Tweeting" or "Skyping". So I am happy to tak

Some great insight from www.ucinsights.com

UC Federation

- Market Definition:
  - Being able to use UC between companies in the same way that it is used within the company (B2B Comms)
  - IM / Presence
  - VoIP
  - HD Video
  - Collaboration, Desktop sharing, white boarding
  - Promises many business benefits!
- Looked at two vendors initially
  - Cisco
  - Microsoft

Who is Federating? Matt Landis' Federation Directory (This is a public directory)



Worldwide Microsoft Lync Federation Directory: Who Is Federating in the USA and Beyond?

By Matt Landis on 9/02/2011 07:12:00 PM

Lync Federation Directory Project

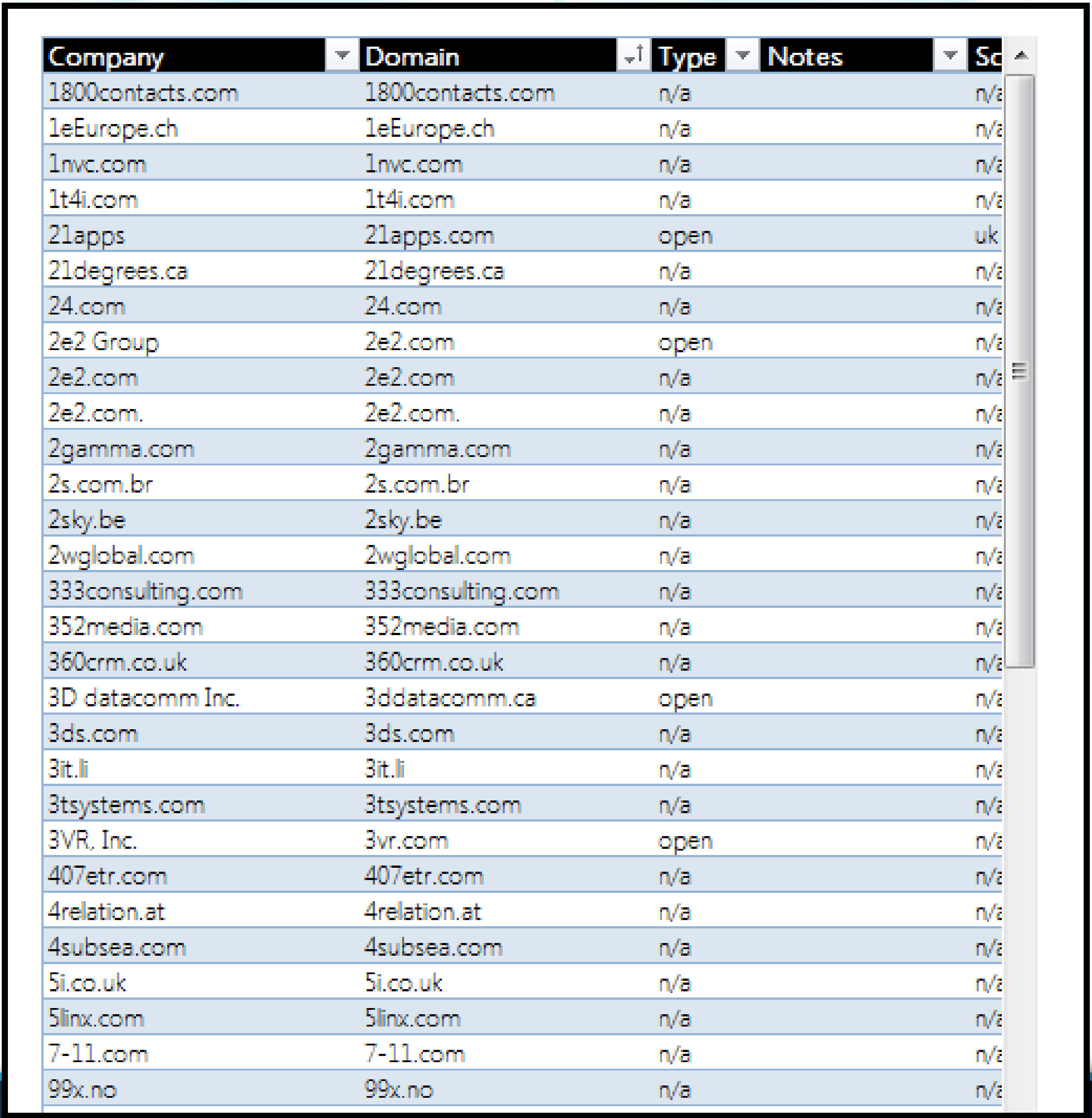
Helping connect people around the world.

One of the big benefits of Microsoft Lync is the ability to collaborate with ease with those outside your organization. The goal of the Lync Federation Directory Project is to make Lync users and administrators more aware of just how many organizations are available for federation-today.

While other vendors are capable of UC federation, the Microsoft Lync product is the first to bring the benefits and actually deliver federation, a compelling alternative to PSTN, to the masses.

Our opinion is that in UC federation is a communication method alternative to PSTN that is compelling enough to drive replacement of PSTN. While SIP trunks gave an IP alternative to PSTN, it largely delivered the same experience. UC federation gives all the benefits of PSTN plus:

Who is Federating?   Matt Landis' (Public) Federation Directory



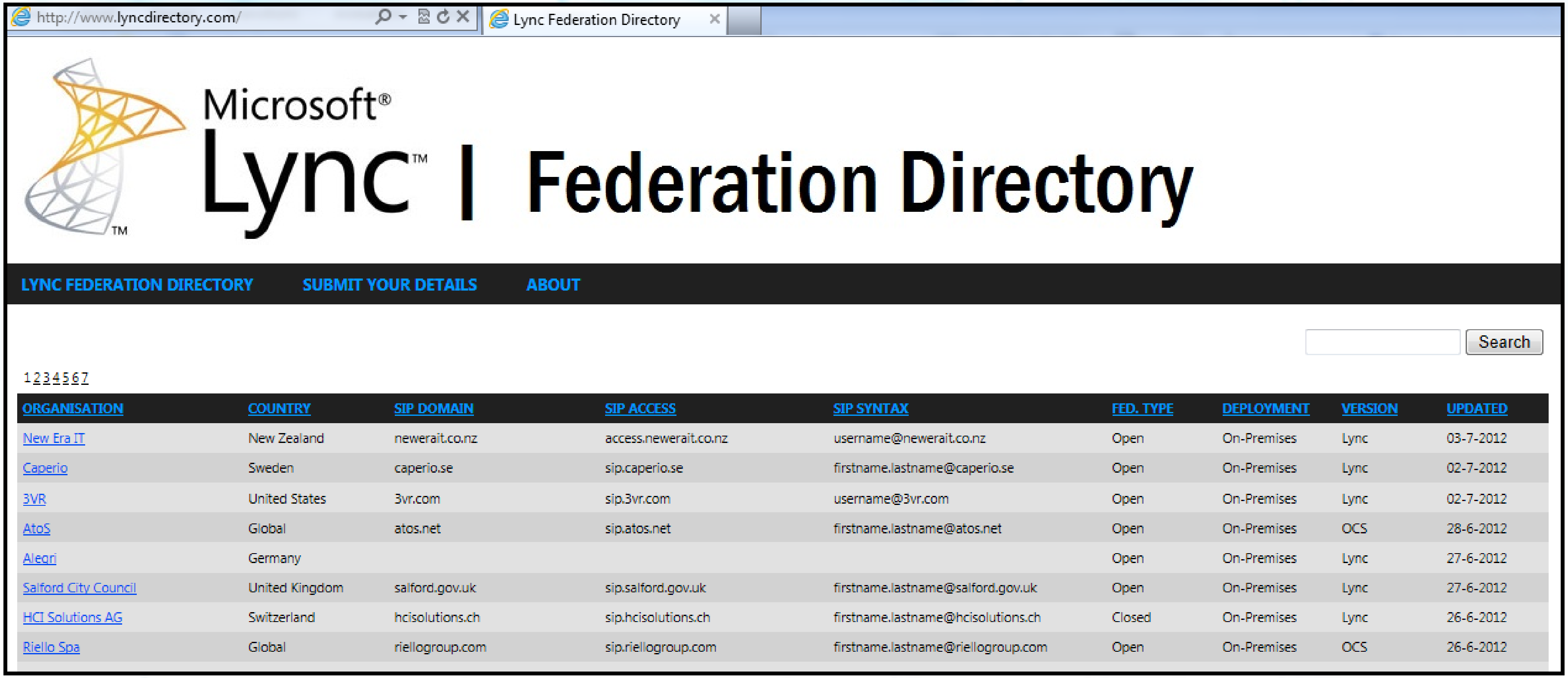
Company	Domain	Type	Notes	Sc
1800contacts.com	1800contacts.com	n/a		n/a
1eEurope.ch	1eEurope.ch	n/a		n/a
1nvc.com	1nvc.com	n/a		n/a
1t4i.com	1t4i.com	n/a		n/a
21apps	21apps.com	open		uk
21degrees.ca	21degrees.ca	n/a		n/a
24.com	24.com	n/a		n/a
2e2 Group	2e2.com	open		n/a
2e2.com	2e2.com	n/a		n/a
2e2.com.	2e2.com.	n/a		n/a
2gamma.com	2gamma.com	n/a		n/a
2s.com.br	2s.com.br	n/a		n/a
2sky.be	2sky.be	n/a		n/a
2wglobal.com	2wglobal.com	n/a		n/a
333consulting.com	333consulting.com	n/a		n/a
352media.com	352media.com	n/a		n/a
360crm.co.uk	360crm.co.uk	n/a		n/a
3D datacomm Inc.	3ddatacomm.ca	open		n/a
3ds.com	3ds.com	n/a		n/a
3it.li	3it.li	n/a		n/a
3tsystems.com	3tsystems.com	n/a		n/a
3VR, Inc.	3vr.com	open		n/a
407etr.com	407etr.com	n/a		n/a
4relation.at	4relation.at	n/a		n/a
4subsea.com	4subsea.com	n/a		n/a
5i.co.uk	5i.co.uk	n/a		n/a
5linx.com	5linx.com	n/a		n/a
7-11.com	7-11.com	n/a		n/a
99x.no	99x.no	n/a		n/a

Tried adding our test deployment into this directory. Not successful.

Data from Matt Landis' Public directory

- 9,705 domains for Microsoft UC Federation
- Top 3 countries:
  - Canada
  - USA
  - Norway

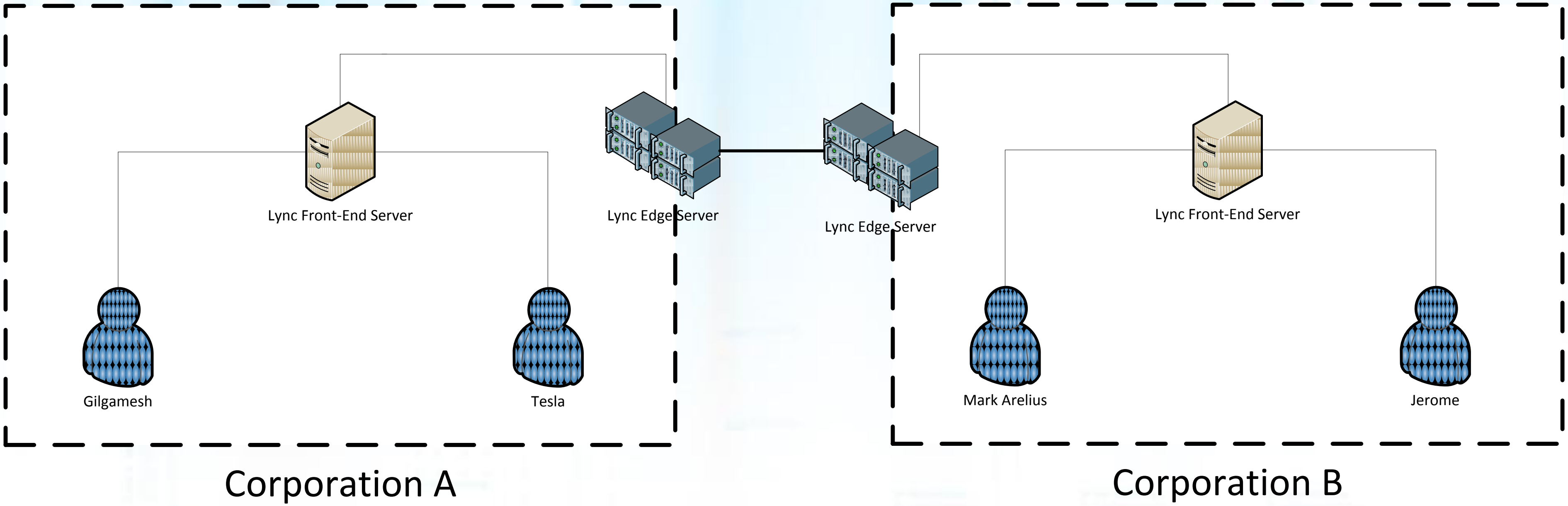
Another Lync Federation Public Directory


http://www.lyncdirectory.com/
Lync Federation Directory
Microsoft®
Lync™ | Federation Directory
LYNC FEDERATION DIRECTORY
SUBMIT YOUR DETAILS
ABOUT
Search
1234567

ORGANISATION	COUNTRY	SIP DOMAIN	SIP ACCESS	SIP SYNTAX	FED. TYPE	DEPLOYMENT	VERSION	UPDATED
New Era IT	New Zealand	newerait.co.nz	access.newerait.co.nz	username@newerait.co.nz	Open	On-Premises	Lync	03-7-2012
Caperio	Sweden	caperio.se	sip.caperio.se	firstname.lastname@caperio.se	Open	On-Premises	Lync	02-7-2012
3VR	United States	3vr.com	sip.3vr.com	username@3vr.com	Open	On-Premises	Lync	02-7-2012
AtoS	Global	atos.net	sip.atos.net	firstname.lastname@atos.net	Open	On-Premises	OCS	28-6-2012
Alegri	Germany				Open	On-Premises	Lync	27-6-2012
Salford City Council	United Kingdom	salford.gov.uk	sip.salford.gov.uk	firstname.lastname@salford.gov.uk	Open	On-Premises	Lync	27-6-2012
HCI Solutions AG	Switzerland	hcisolutions.ch	sip.hcisolutions.ch	firstname.lastname@hcisolutions.ch	Closed	On-Premises	Lync	26-6-2012
Riello Spa	Global	riellogroup.com	sip.riellogroup.com	firstname.lastname@riellogroup.com	Open	On-Premises	OCS	26-6-2012

We were able to add our test UC Federation deployment into this directory.

Lync Federation - Architecture



Lync Federation - Types

- Dynamic (SRV Discovery)
  - Allows anyone to communicate with anyone
  - Some restrictions apply (traffic throttling, contact lists)
- Enhanced/Direct Federation (Whitelist)
  - For trusted partners
- Blacklist
  - Specifically disallow Federation with a certain domain

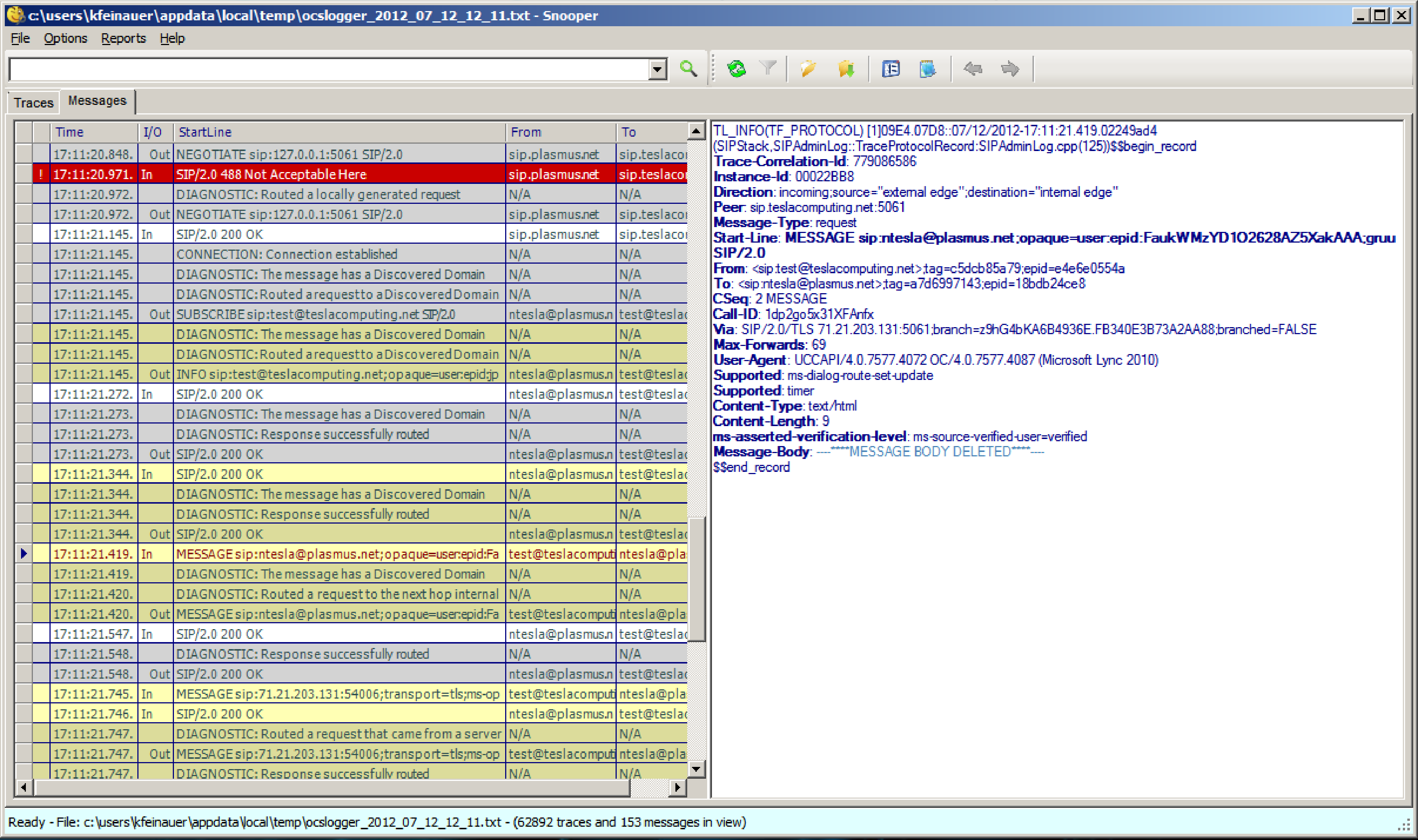
Lync Federation - Security

- Dynamic Federation seems like the weak point…
- If Dynamic Federation is employed by a company, their infrastructure is publicly accessible to all
- Knowing this, what can we exploit?

Lync – Reverse Engineering

- To see what we could do with Dynamic Federation, we reverse engineered the Lync Client
- Registered two domains to Federate
- Made extensive use of the Lync Server Logging Tool and Lync Client
- Official Microsoft documentation sparse and unclear – reverse engineering much easier!

Lync – Reverse Engineering



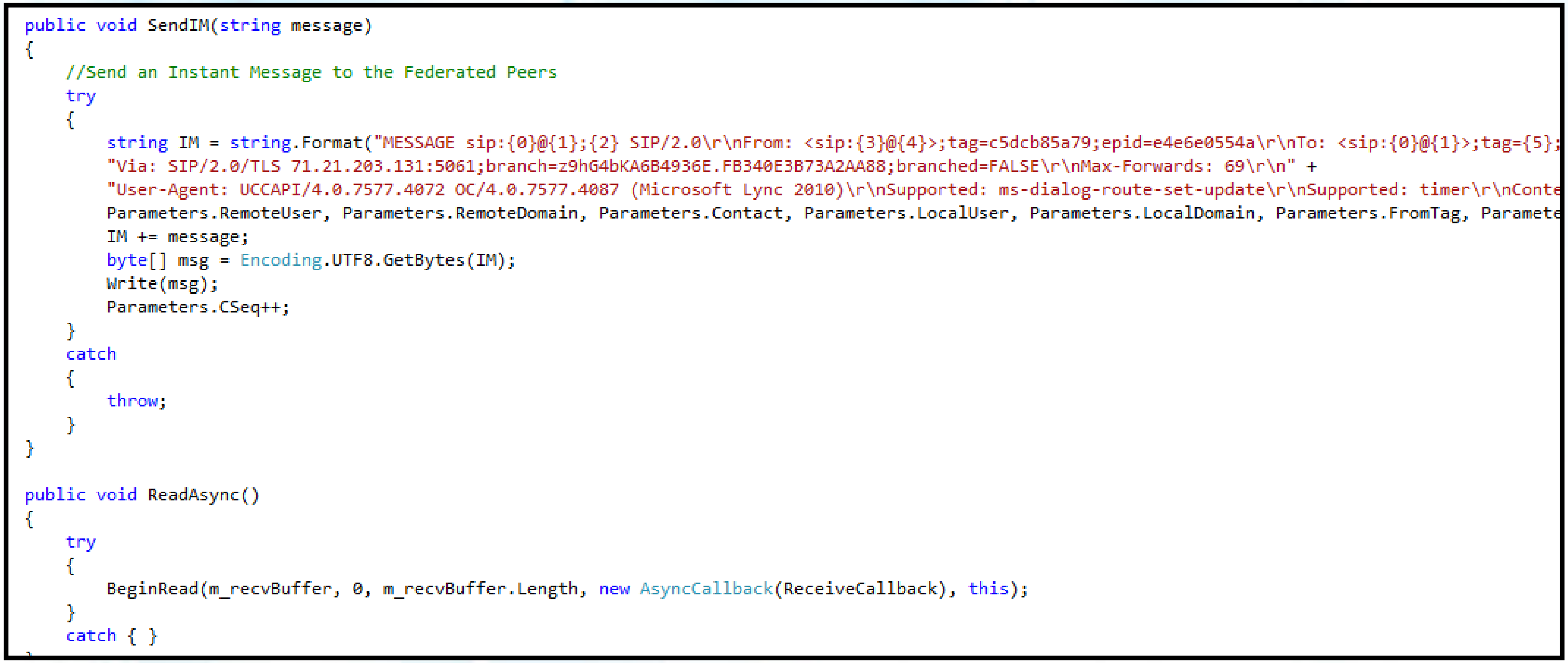
c:\users\kfeinauer\appdata\local\temp\ocslogger_2012_07_12_12_11.txt - Snooper

	Time	I/O	StartLine	From	To
	17:11:20.848.	Out	NEGOTIATE sip:127.0.0.1:5061 SIP/2.0	sip.plasmus.net	sip.teslacoı
!	17:11:20.971.	In	SIP/2.0 488 Not Acceptable Here	sip.plasmus.net	sip.teslacoı
	17:11:20.972.		DIAGNOSTIC: Routed a locally generated request	N/A	N/A
	17:11:20.972.	Out	NEGOTIATE sip:127.0.0.1:5061 SIP/2.0	sip.plasmus.net	sip.teslacoı
	17:11:21.145.	In	SIP/2.0 200 OK	sip.plasmus.net	sip.teslacoı
	17:11:21.145.		CONNECTION: Connection established	N/A	N/A
	17:11:21.145.		DIAGNOSTIC: The message has a Discovered Domain	N/A	N/A
	17:11:21.145.		DIAGNOSTIC: Routed a request to a Discovered Domain	N/A	N/A
	17:11:21.145.	Out	SUBSCRIBE sip:test@teslacomputing.net SIP/2.0	ntesla@plasmus.n	test@teslac
	17:11:21.145.		DIAGNOSTIC: The message has a Discovered Domain	N/A	N/A
	17:11:21.145.		DIAGNOSTIC: Routed a request to a Discovered Domain	N/A	N/A
	17:11:21.145.	Out	INFO sip:test@teslacomputing.net;opaque=user:epid:jp	ntesla@plasmus.n	test@teslac
	17:11:21.272.	In	SIP/2.0 200 OK	ntesla@plasmus.n	test@teslac
	17:11:21.273.		DIAGNOSTIC: The message has a Discovered Domain	N/A	N/A
	17:11:21.273.		DIAGNOSTIC: Response successfully routed	N/A	N/A
	17:11:21.273.	Out	SIP/2.0 200 OK	ntesla@plasmus.n	test@teslac
	17:11:21.344.	In	SIP/2.0 200 OK	ntesla@plasmus.n	test@teslac
	17:11:21.344.		DIAGNOSTIC: The message has a Discovered Domain	N/A	N/A
	17:11:21.344.		DIAGNOSTIC: Response successfully routed	N/A	N/A
	17:11:21.344.	Out	SIP/2.0 200 OK	ntesla@plasmus.n	test@teslac
▶	17:11:21.419.	In	MESSAGE sip:ntesla@plasmus.net;opaque=user:epid:Fa	test@teslacomput	ntesla@pla
	17:11:21.419.		DIAGNOSTIC: The message has a Discovered Domain	N/A	N/A
	17:11:21.420.		DIAGNOSTIC: Routed a request to the next hop internal	N/A	N/A
	17:11:21.420.	Out	MESSAGE sip:ntesla@plasmus.net;opaque=user:epid:Fa	test@teslacomput	ntesla@pla
	17:11:21.547.	In	SIP/2.0 200 OK	ntesla@plasmus.n	test@teslac
	17:11:21.548.		DIAGNOSTIC: Response successfully routed	N/A	N/A
	17:11:21.548.	Out	SIP/2.0 200 OK	ntesla@plasmus.n	test@teslac
	17:11:21.745.	In	MESSAGE sip:71.21.203.131:54006;transport=tls;ms-op	test@teslacomput	ntesla@pla
	17:11:21.746.	In	SIP/2.0 200 OK	ntesla@plasmus.n	test@teslac
	17:11:21.747.		DIAGNOSTIC: Routed a request that came from a server	N/A	N/A
	17:11:21.747.	Out	MESSAGE sip:71.21.203.131:54006;transport=tls;ms-op	test@teslacomput	ntesla@pla
	17:11:21.747.		DIAGNOSTIC: Response successfully routed	N/A	N/A

```
TL_INFO(TF_PROTOCOL) [1]09E4.07D8::07/12/2012-17:11:21.419.02249ad4
(SIPStack,SIPAdminLog::TraceProtocolRecord:SIPAdminLog.cpp(125))$$begin_record
Trace-Correlation-Id: 779086586
Instance-Id: 00022BB8
Direction: incoming;source="external edge";destination="internal edge"
Peer: sip.teslacomputing.net:5061
Message-Type: request
Start-Line: MESSAGE sip:ntesla@plasmus.net;opaque=user:epid:FaukWMzYD1O2628AZ5XakAAA;gruu
SIP/2.0
From: <sip:test@teslacomputing.net>;tag=c5dcb85a79;epid=e4e6e0554a
To: <sip:ntesla@plasmus.net>;tag=a7d6997143;epid=18bdb24ce8
CSeq: 2 MESSAGE
Call-ID: 1dp2go5x31XFAnfx
Via: SIP/2.0/TLS 71.21.203.131:5061;branch=z9hG4bKA6B4936E.FB340E3B73A2AA88;branched=FALSE
Max-Forwards: 69
User-Agent: UCCAPI/4.0.7577.4072 OC/4.0.7577.4087 (Microsoft Lync 2010)
Supported: ms-dialog-route-set-update
Supported: timer
Content-Type: text/html
Content-Length: 9
ms-asserted-verification-level: ms-source-verified-user=verified
Message-Body: ----****MESSAGE BODY DELETED****----
$$end_record
```

Ready - File: c:\users\kfeinauer\appdata\local\temp\ocslogger_2012_07_12_12_11.txt - (62892 traces and 153 messages in view)

Lync – Reverse Engineering



```
public void SendIM(string message)
{
    //Send an Instant Message to the Federated Peers
    try
    {
        string IM = string.Format("MESSAGE sip:{0}@{1};{2} SIP/2.0\r\nFrom: <sip:{3}@{4}>;tag=c5dcb85a79;epid=e4e6e0554a\r\nTo: <sip:{0}@{1}>;tag={5};
        "Via: SIP/2.0/TLS 71.21.203.131:5061;branch=z9hG4bKA6B4936E.FB340E3B73A2AA88;branched=FALSE\r\nMax-Forwards: 69\r\n" +
        "User-Agent: UCCAPI/4.0.7577.4072 OC/4.0.7577.4087 (Microsoft Lync 2010)\r\nSupported: ms-dialog-route-set-update\r\nSupported: timer\r\nConte
        Parameters.RemoteUser, Parameters.RemoteDomain, Parameters.Contact, Parameters.LocalUser, Parameters.LocalDomain, Parameters.FromTag, Paramete
        IM += message;
        byte[] msg = Encoding.UTF8.GetBytes(IM);
        Write(msg);
        Parameters.CSeq++;
    }
    catch
    {
        throw;
    }
}

public void ReadAsync()
{
    try
    {
        BeginRead(m_recvBuffer, 0, m_recvBuffer.Length, new AsyncCallback(ReceiveCallback), this);
    }
    catch { }
```

Lync – Reverse Engineering

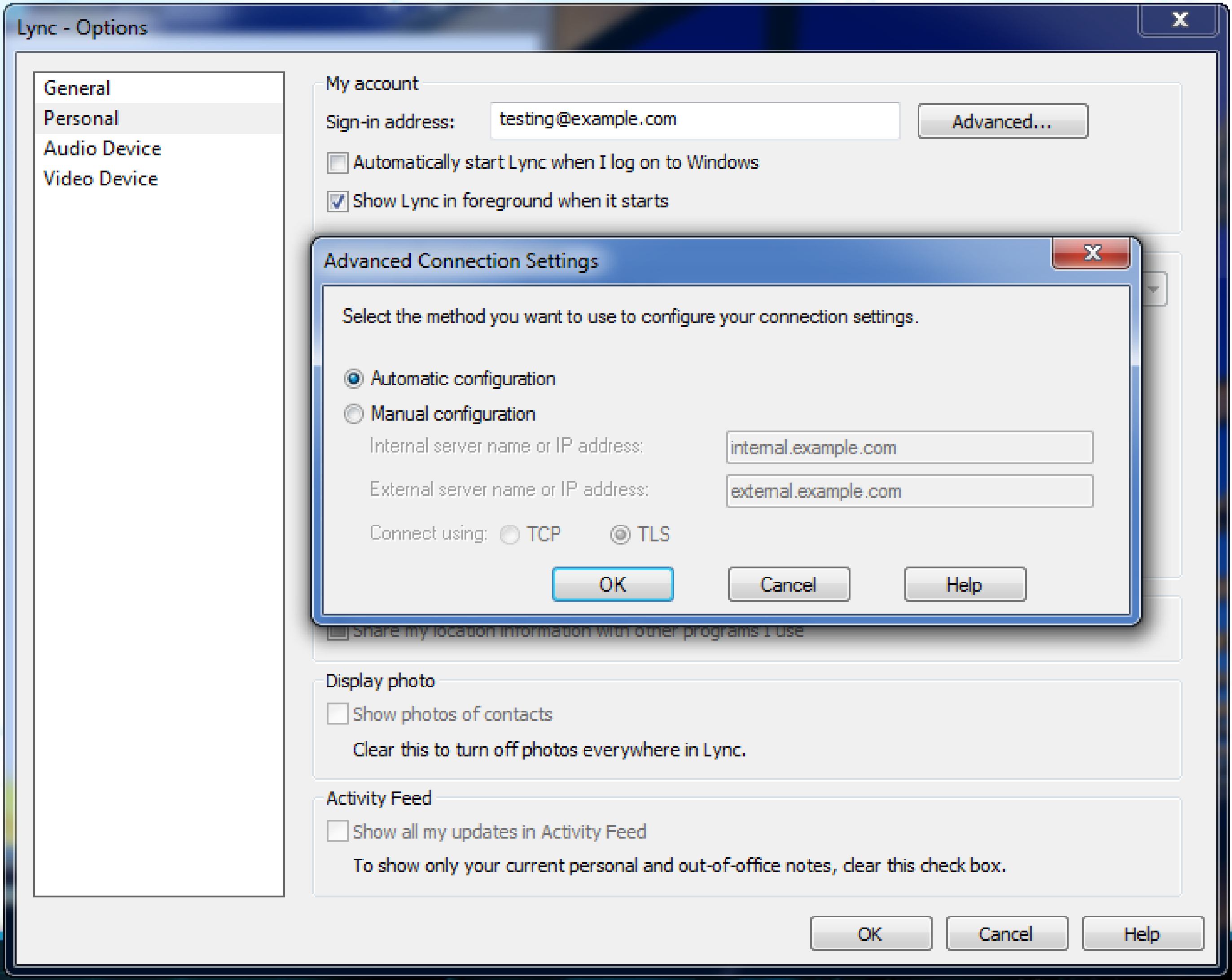
- It wasn’t all fun and games!
- For non-federated connections, messages require signing and NTLM authentication
- Convoluted, sometimes incorrect documentation!
- Results of this showed that the security is much tighter for non-federated connections

Outcome of Reverse Engineering

- LyncSpoof
  - Acts as a legitimate Lync client and connects to Lync Front-End Server
  - Uses NTLM Authentication and message signing
- Federator
  - Acts as a legitimate Lync Server and connects to another Lync Server via Federation
  - Requires a cert from a public CA

Video Demos

Lync client SRV Automatic Sign-In



Lync - Options

My account

Sign-in address: testing@example.com

□ Automatically start Lync when I log on to Windows

☑ Show Lync in foreground when it starts

Advanced Connection Settings

Select the method you want to use to configure your connection settings.

● Automatic configuration

○ Manual configuration

Internal server name or IP address: internal.example.com

External server name or IP address: external.example.com

Connect using: ○ TCP ● TLS

□ Share my location information with other programs I use

Display photo

□ Show photos of contacts

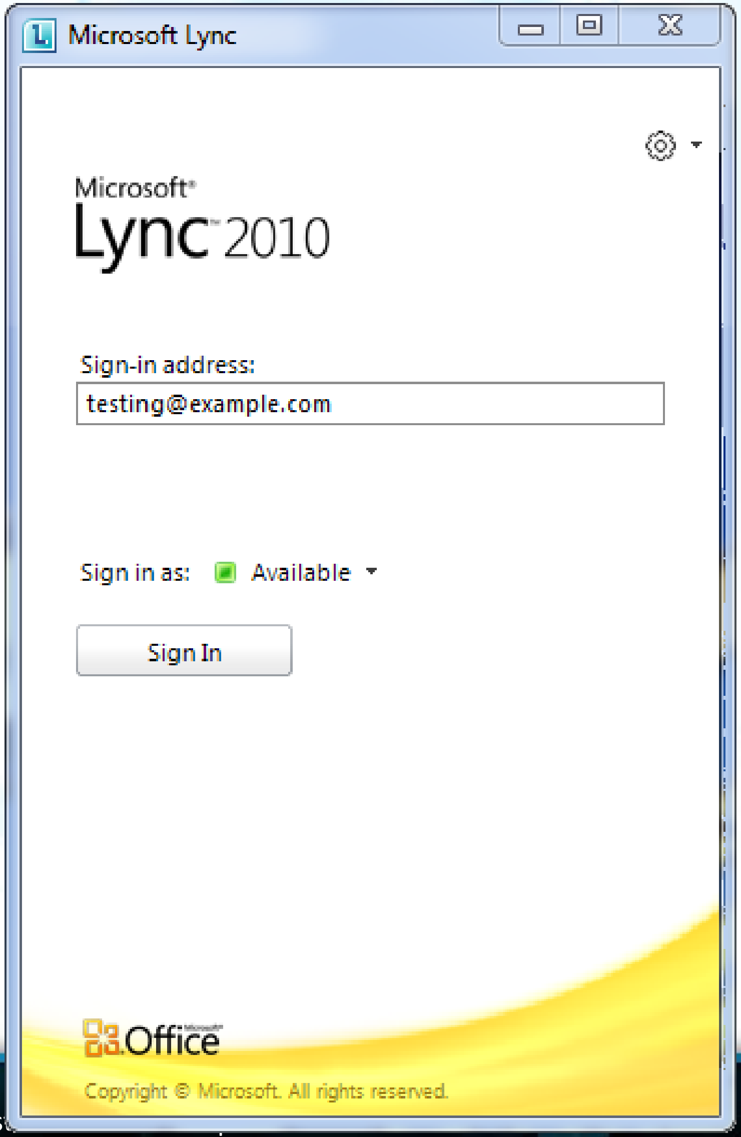
Clear this to turn off photos everywhere in Lync.

Activity Feed

□ Show all my updates in Activity Feed

To show only your current personal and out-of-office notes, clear this check box.

Lync client SRV Automatic Sign-In



Sign-in address: testing@example.com

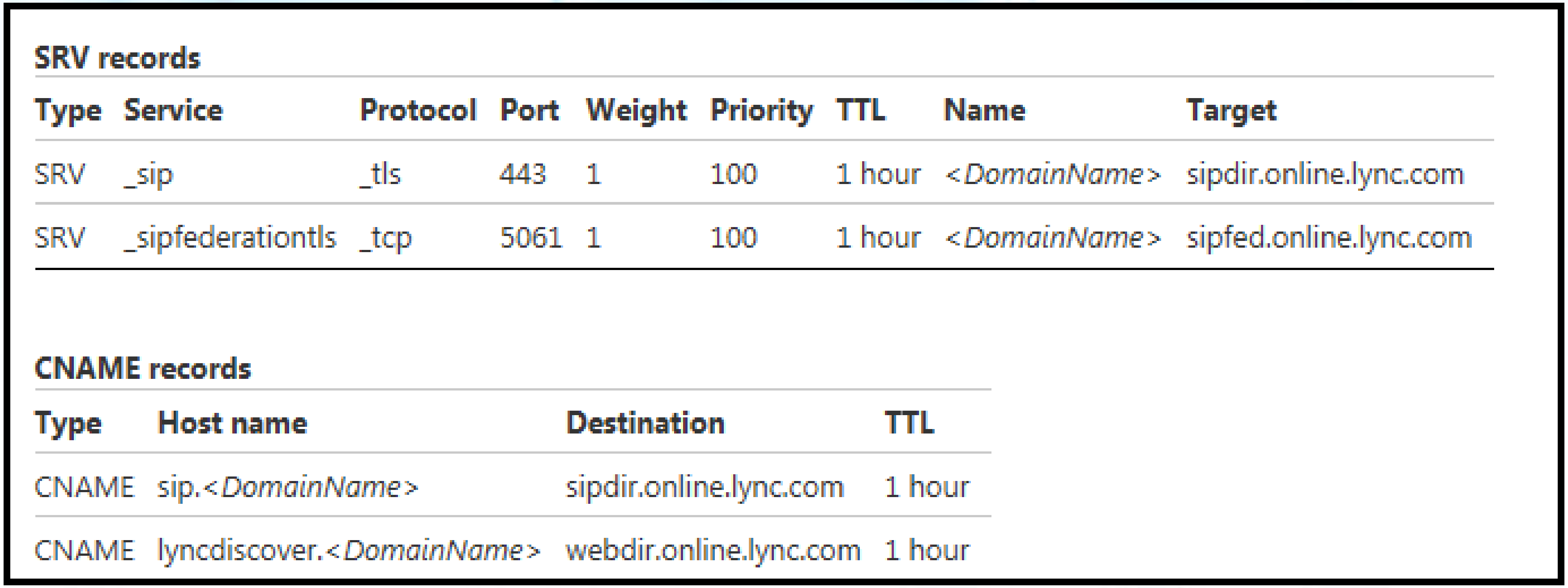
Sign in as: 🟩 Available

Copyright © Microsoft. All rights reserved.

SRV records for Automatic Sign-In

- Queries automatically sent by Lync:
  - _sipinternaltls._tcp.example.com
  - _sip._tls.example.com

Other DNS RRs



SRV records

Type	Service	Protocol	Port	Weight	Priority	TTL	Name	Target
SRV	_sip	_tls	443	1	100	1 hour	<*DomainName*>	sipdir.online.lync.com
SRV	_sipfederationtls	_tcp	5061	1	100	1 hour	<*DomainName*>	sipfed.online.lync.com

CNAME records

Type	Host name	Destination	TTL
CNAME	sip.<*DomainName*>	sipdir.online.lync.com	1 hour
CNAME	lyncdiscover.<*DomainName*>	webdir.online.lync.com	1 hour

Source: Microsoft

Summary

Source: Russell Bennett

- Security vs. Usability
  - Balance between "Discovery vs. Privacy" (or Confidentiality)
  - The easier it is for a company to be "discovered" for UCF, the easier for business ~ the easier to attack
- Federation Technically speaking
  - Using SIP for signaling / control plane
  - RTP for apps requiring real-time communications
  - DNS SRV for service lookups, so anyone can look up a target company using DNS!
- Microsoft appears to be market leader in UC Federation
- Strong default security with SIP TLS and SRTP
- Very difficult to peak into the encrypted messaging used, or is it?....

We should actually be able to decrypt those messages.

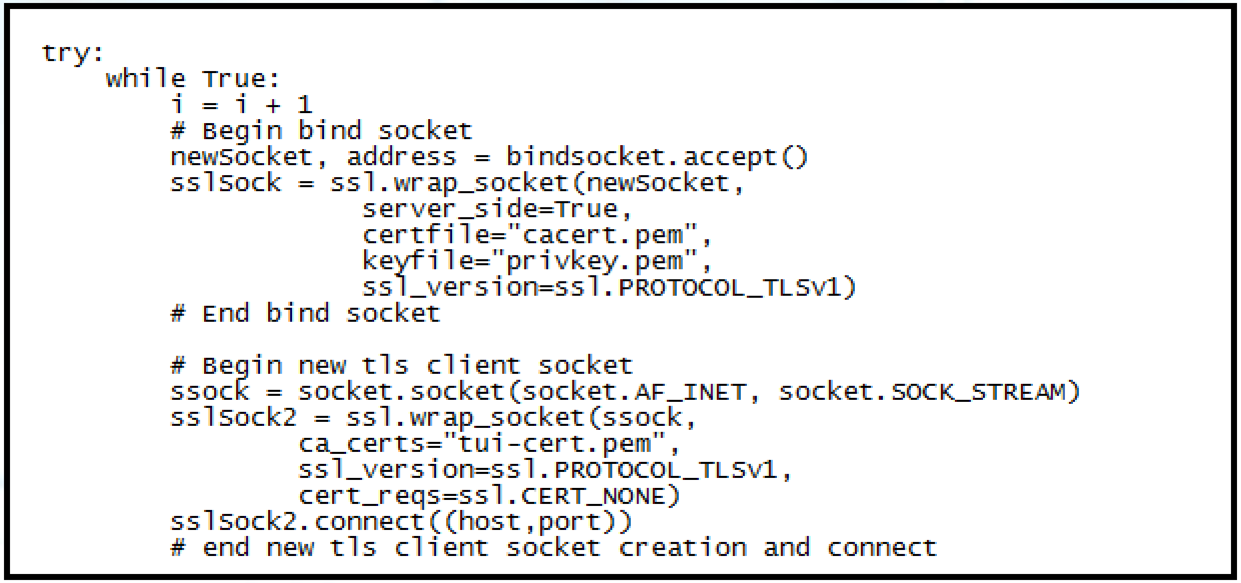
We like to understand things

So that’s what we did

SIP TLS Proxy Tool

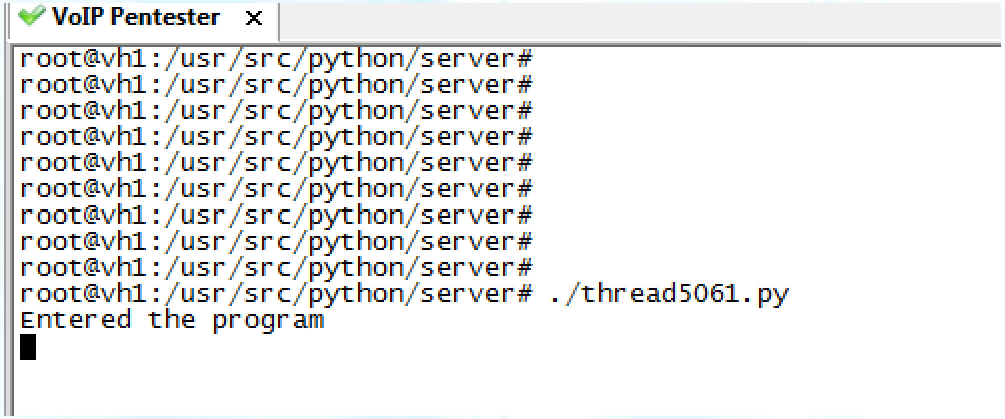
Objective 1: Decrypt the SIP TLS message flow and learn how it works (Complete)

Objective 2: Fuzzing engine (In development)

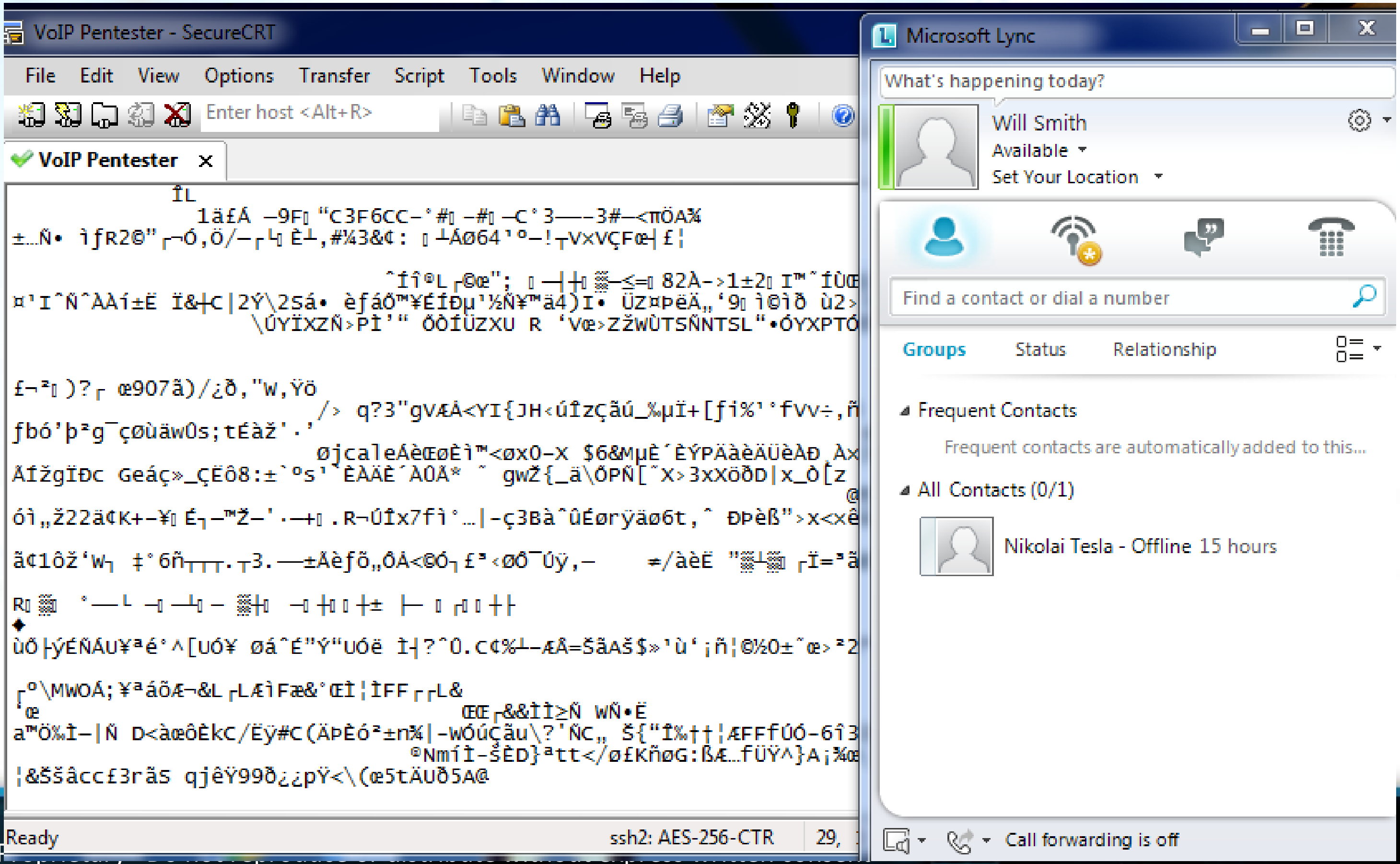


```
try:
    while True:
        i = i + 1
        # Begin bind socket
        newSocket, address = bindsocket.accept()
        sslSock = ssl.wrap_socket(newSocket,
                    server_side=True,
                    certfile="cacert.pem",
                    keyfile="privkey.pem",
                    ssl_version=ssl.PROTOCOL_TLSv1)
        # End bind socket

        # Begin new tls client socket
        ssock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sslSock2 = ssl.wrap_socket(ssock,
                ca_certs="tui-cert.pem",
                ssl_version=ssl.PROTOCOL_TLSv1,
                cert_reqs=ssl.CERT_NONE)
        sslSock2.connect((host,port))
        # end new tls client socket creation and connect
```

How it works



```
root@vh1:/usr/src/python/server#
root@vh1:/usr/src/python/server#
root@vh1:/usr/src/python/server#
root@vh1:/usr/src/python/server#
root@vh1:/usr/src/python/server#
root@vh1:/usr/src/python/server#
root@vh1:/usr/src/python/server#
root@vh1:/usr/src/python/server#
root@vh1:/usr/src/python/server#
root@vh1:/usr/src/python/server# ./thread5061.py
Entered the program
█
```

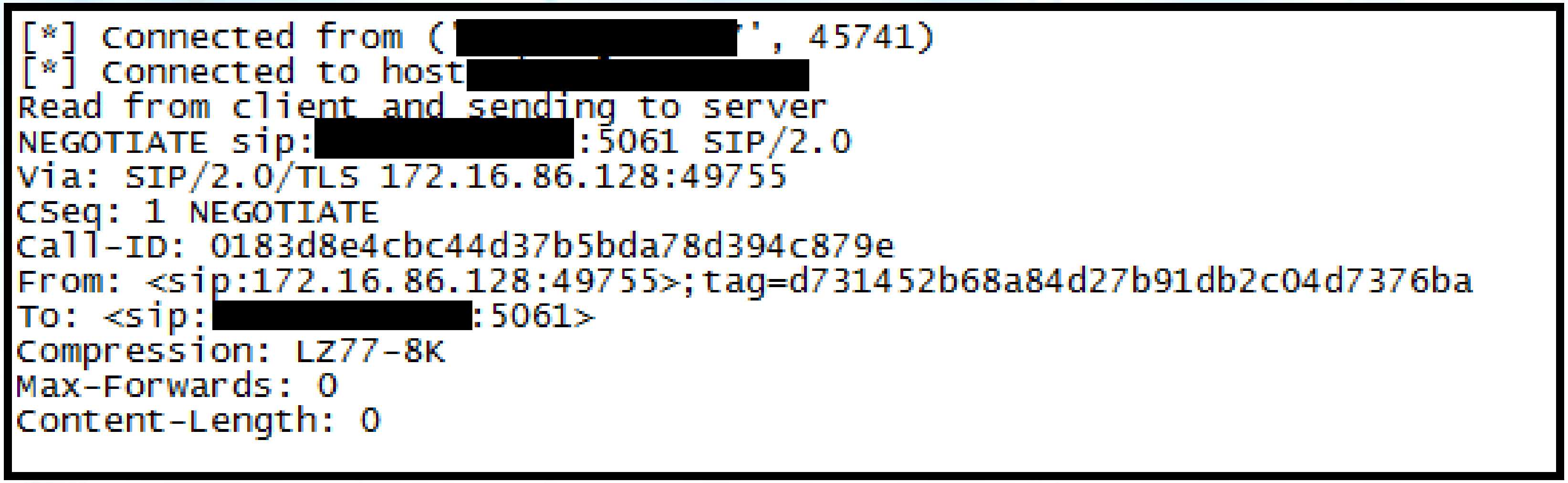


```
          ÎL
             1äfÁ —9F▯ "C3F6CC–°#▯ –#▯ –C° 3——-3#—<ΠÖA%
±…Ñ• ìƒR2©"┌¬Ó,Ö/—┌┘ È┴,#¼3&¢: ▯ ┴Á064¹º—!┬VxVÇFœ┤£¦

                       ˆÎî©L┌©œ"; ▯ ─┤┼▯ ▒—≤═▯ 82À–›1±2▯ I™ˆÎÙŒ
¤'IˆÑˆÀÀí±Ë Ï&┼C|2Ý\2Sá• èƒáÖ™¥ÉÍÐµ'½Ñ¥™ä4)I• ÜZ¤ÞëÄ„'9▯ ì©ìð ù2›
                 \ÚYÏXZÑ›PÌ'" ÖÒÎÜZXU R 'Vœ›ZŽWÙTSÑNTSL"•ÓYXPTÓ


£¬²▯ )?┌ œ907ã)/¿ð,"W,Ÿö
                     /› q?3"gVÆÁ<YI{JH‹úÎzÇãú_‰µÏ+[ƒi%'°fVv÷,ñ
ƒbó'þ²g¯çøùäw0s;tÉàž'·'
                    øjcaleÁèŒøÈì™<øx0–X $6&MµÈ´ÈÝPÄàèÄÜèÀÐ Àx
ÀÎžgÏÐc Geáç»_ÇËô8:±`ºs' ÈÀÄÈ´ÀÖÄ* ˜ gwŽ{_ä\ÔPÑ[˜X›3xXöðD|x_ô[z
                                                               @
óì„ž22ä¢K+–¥▯ É┐—™Ž–'·—┼▯ .R¬ÚÎx7fì°…|-ç3Bàˆûɸrÿäø6t,ˆ ÐÞèß"›x<xê

ä¢1ôž'W┐ ‡°6ñ┬┬┬.┬3.——±Àèƒõ„ÕÁ<©Ó┐£³‹øð¯Úÿ,—    ≠/àèË "▒┴▒ ┌Ï=²ä

R▯ ▒  °—└ ─▯ ─┤▯ – ▒┼▯  ─┤┼▯ ▯ ┼± ├─ ▯ ┌▯ ▯ ┼┼
◆
ùÓ├ýÉÑÃU¥ªé°^[UÓ¥ øáˆÉ"Ý"uÓë Ì┤?ˆ0.C¢%┴–ÆÂ=ŠãAš$»'ù'¡ñ¦©½0±˜œ›²2

┌º\MWOÁ;¥ªãõÆ¬&L┌LÆìFæ&°ŒÌ¦ÌFF┌┌L&
 œ                    ŒE┌&&ÌÌ≥Ñ WÑ•Ë
a™Ö‰Ì–|Ñ D<àœôÈkC/Ëÿ#C(ÄPÈó²±n%|-wÓúÇãu\?'ÑC„ Š{"Ì‰†┼¦ÆFFfÚÓ-6î3
                      ©NmíÌ-šÈD}ªtt</øfKñøG:ßÆ…fÜÝ^}A¡¾œ
¦&Ššâccƒ3rãs qjêŸ99ð¿¿pŸ<\(œ5tÄUð5A@
```

How it works

- Microsoft Lync client points to SIP TLS Proxy
- Proxy decrypts client traffic as a TLS server
- View traffic
- Proxy connects as TLS client to real Edge Server
- Proxy encrypts traffic
- Uses Python TLS module, sockets, multi-threading

Decrypted SIP TLS Message #1



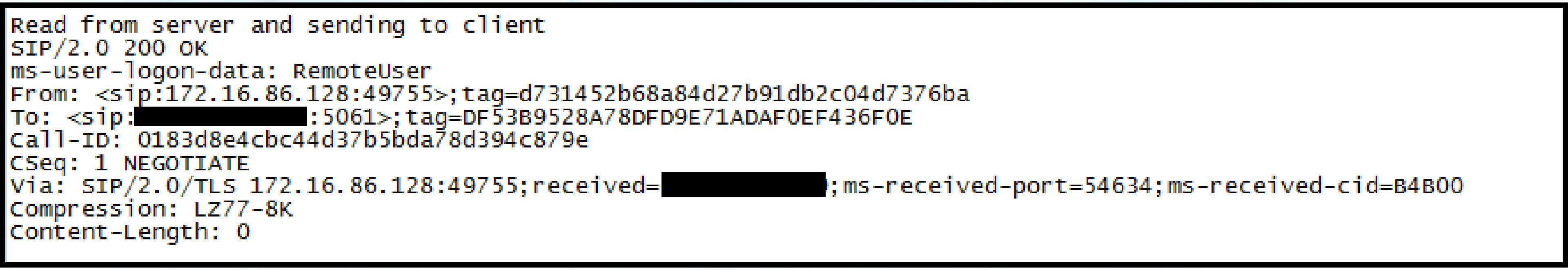
```
[*] Connected from ('[redacted]', 45741)
[*] Connected to host[redacted]
Read from client and sending to server
NEGOTIATE sip:[redacted]:5061 SIP/2.0
Via: SIP/2.0/TLS 172.16.86.128:49755
CSeq: 1 NEGOTIATE
Call-ID: 0183d8e4cbc44d37b5bda78d394c879e
From: <sip:172.16.86.128:49755>;tag=d731452b68a84d27b91db2c04d7376ba
To: <sip:[redacted]:5061>
Compression: LZ77-8K
Max-Forwards: 0
Content-Length: 0
```

Client → Server

Negotiate

Client sends a NEGOTIATE message with Compression of LZ77-8K

Decrypted SIP TLS Message #2



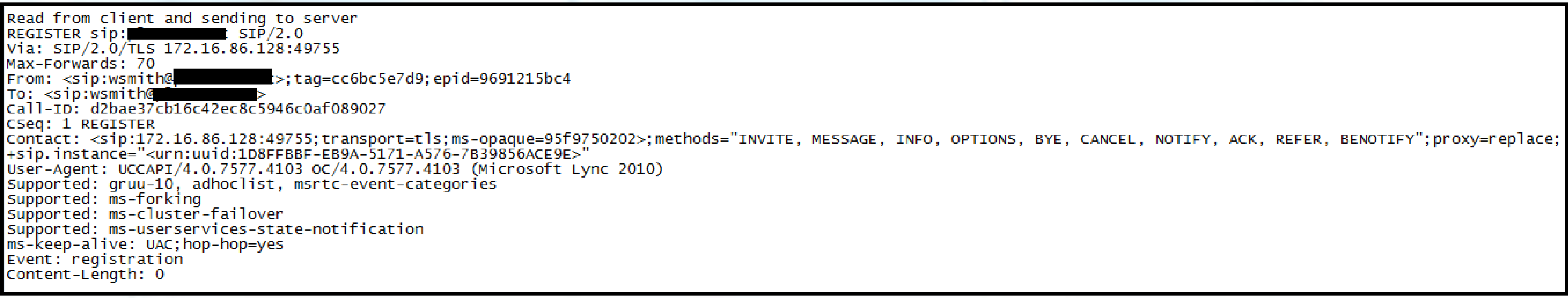
```
Read from server and sending to client
SIP/2.0 200 OK
ms-user-logon-data: RemoteUser
From: <sip:172.16.86.128:49755>;tag=d731452b68a84d27b91db2c04d7376ba
To: <sip:[redacted]:5061>;tag=DF53B9528A78DFD9E71ADAF0EF436F0E
Call-ID: 0183d8e4cbc44d37b5bda78d394c879e
CSeq: 1 NEGOTIATE
Via: SIP/2.0/TLS 172.16.86.128:49755;received=[redacted];ms-received-port=54634;ms-received-cid=B4B00
Compression: LZ77-8K
Content-Length: 0
```

Client ← Server

200 OK

Server inspects compression header field and matches the value of LZ77-8K. Server responds with 200 OK, will support compression.

Decrypted SIP TLS Message #3



```
Read from client and sending to server
REGISTER sip:[redacted] SIP/2.0
Via: SIP/2.0/TLS 172.16.86.128:49755
Max-Forwards: 70
From: <sip:wsmith@[redacted]>;tag=cc6bc5e7d9;epid=9691215bc4
To: <sip:wsmith@[redacted]>
Call-ID: d2bae37cb16c42ec8c5946c0af089027
CSeq: 1 REGISTER
Contact: <sip:172.16.86.128:49755;transport=tls;ms-opaque=95f9750202>;methods="INVITE, MESSAGE, INFO, OPTIONS, BYE, CANCEL, NOTIFY, ACK, REFER, BENOTIFY";proxy=replace;
+sip.instance="<urn:uuid:1D8FFBBF-EB9A-5171-A576-7B39856ACE9E>"
User-Agent: UCCAPI/4.0.7577.4103 OC/4.0.7577.4103 (Microsoft Lync 2010)
Supported: gruu-10, adhoclist, msrtc-event-categories
Supported: ms-forking
Supported: ms-cluster-failover
Supported: ms-userservices-state-notification
ms-keep-alive: UAC;hop-hop=yes
Event: registration
Content-Length: 0
```

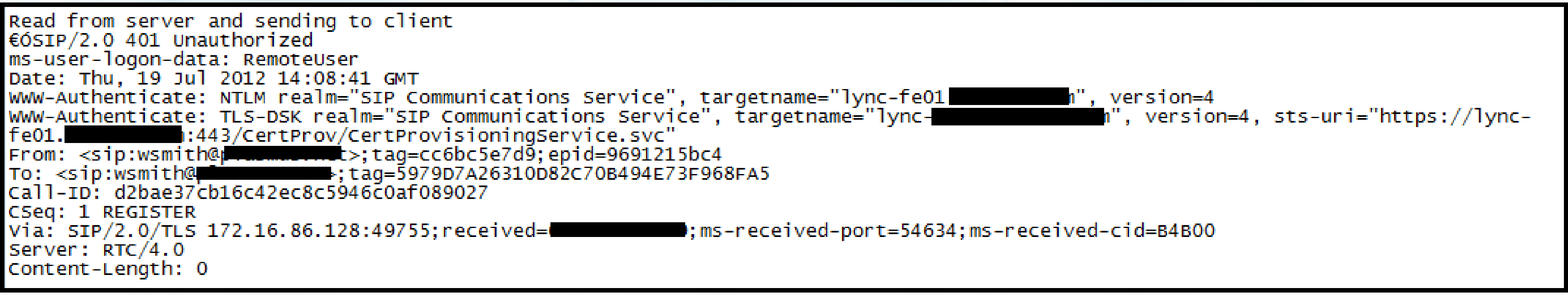
Client → Server

REGISTER

Client sends first SIP REGISTER message to Edge Server

Decrypted SIP TLS Message #4

Server responds with 401 Unauthorized and WWW-Authenticate header, telling client supported authentication methods (NTLM, TLS-DSK)

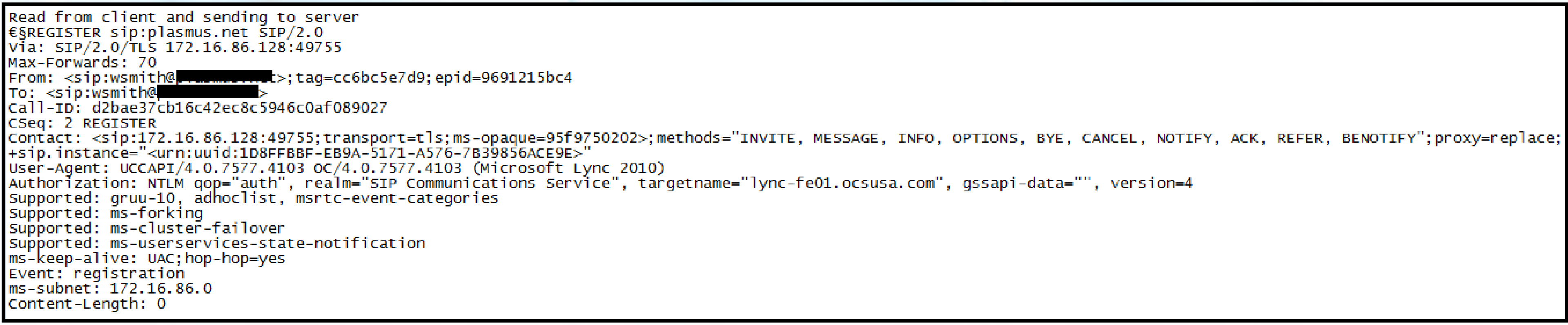


```
Read from server and sending to client
€ÓSIP/2.0 401 Unauthorized
ms-user-logon-data: RemoteUser
Date: Thu, 19 Jul 2012 14:08:41 GMT
WWW-Authenticate: NTLM realm="SIP Communications Service", targetname="lync-fe01 [redacted]", version=4
WWW-Authenticate: TLS-DSK realm="SIP Communications Service", targetname="lync-[redacted]", version=4, sts-uri="https://lync-
fe01.[redacted]:443/CertProv/CertProvisioningService.svc"
From: <sip:wsmith@[redacted]>;tag=cc6bc5e7d9;epid=9691215bc4
To: <sip:wsmith@[redacted];tag=5979D7A26310D82C70B494E73F968FA5
Call-ID: d2bae37cb16c42ec8c5946c0af089027
CSeq: 1 REGISTER
Via: SIP/2.0/TLS 172.16.86.128:49755;received=[redacted];ms-received-port=54634;ms-received-cid=B4B00
Server: RTC/4.0
Content-Length: 0
```

Client ← Server

401 Unauthorized

Decrypted SIP TLS Message #5



```
Read from client and sending to server
€§REGISTER sip:plasmus.net SIP/2.0
Via: SIP/2.0/TLS 172.16.86.128:49755
Max-Forwards: 70
From: <sip:wsmith@[redacted]>;tag=cc6bc5e7d9;epid=9691215bc4
To: <sip:wsmith@[redacted]>
Call-ID: d2bae37cb16c42ec8c5946c0af089027
CSeq: 2 REGISTER
Contact: <sip:172.16.86.128:49755;transport=tls;ms-opaque=95f9750202>;methods="INVITE, MESSAGE, INFO, OPTIONS, BYE, CANCEL, NOTIFY, ACK, REFER, BENOTIFY";proxy=replace;
+sip.instance="<urn:uuid:1D8FFBBF-EB9A-5171-A576-7B39856ACE9E>"
User-Agent: UCCAPI/4.0.7577.4103 OC/4.0.7577.4103 (Microsoft Lync 2010)
Authorization: NTLM qop="auth", realm="SIP Communications Service", targetname="lync-fe01.ocsusa.com", gssapi-data="", version=4
Supported: gruu-10, adhoclist, msrtc-event-categories
Supported: ms-forking
Supported: ms-cluster-failover
Supported: ms-userservices-state-notification
ms-keep-alive: UAC;hop-hop=yes
Event: registration
ms-subnet: 172.16.86.0
Content-Length: 0
```

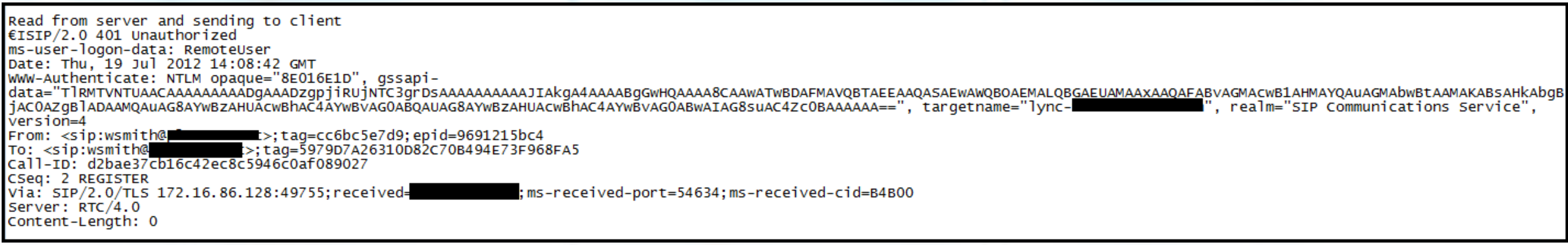
Client → Server

REGISTER

Client sends second SIP REGISTER message with Authorization header NTLM

Decrypted SIP TLS Message #6

Server responds with 401 Unauthorized and WWW-Authenticate header, containing gsappi-data for client NTLM authentication.

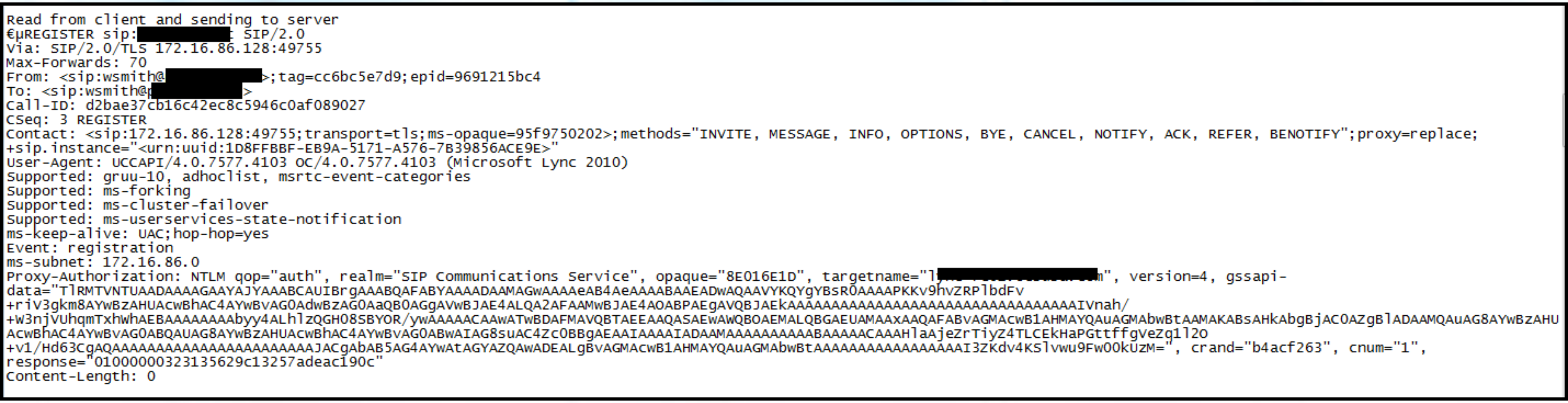


```
Read from server and sending to client
€ISIP/2.0 401 Unauthorized
ms-user-logon-data: RemoteUser
Date: Thu, 19 Jul 2012 14:08:42 GMT
WWW-Authenticate: NTLM opaque="8E016E1D", gssapi-
data="TlRMTVNTUAACAAAAAAAAAADgAAADzgpjiRUjNTC3grDsAAAAAAAAAAJIAkgA4AAAABgGwHQAAAA8CAAwATwBDAFMAVQBTAEEAAQASAEwAWQBOAEMALQBGAEUAMAAxAAQAFABvAGMAcwB1AHMAYQAuAGMAbwBtAAMAKABsAHkAbgB
jAC0AZgBlADAAMQAuAG8AYwBzAHUAcwBhAC4AYwBvAG0ABQAUAG8AYwBzAHUAcwBhAC4AYwBvAG0ABwAIAG8suAC4Zc0BAAAAAA==", targetname="lync-[redacted]", realm="SIP Communications Service",
version=4
From: <sip:wsmith@[redacted]>;tag=cc6bc5e7d9;epid=9691215bc4
To: <sip:wsmith@[redacted]>;tag=5979D7A26310D82C70B494E73F968FA5
Call-ID: d2bae37cb16c42ec8c5946c0af089027
CSeq: 2 REGISTER
Via: SIP/2.0/TLS 172.16.86.128:49755;received=[redacted];ms-received-port=54634;ms-received-cid=B4B00
Server: RTC/4.0
Content-Length: 0
```

Client ← Server

401 Unauthorized

Decrypted SIP TLS Message #7



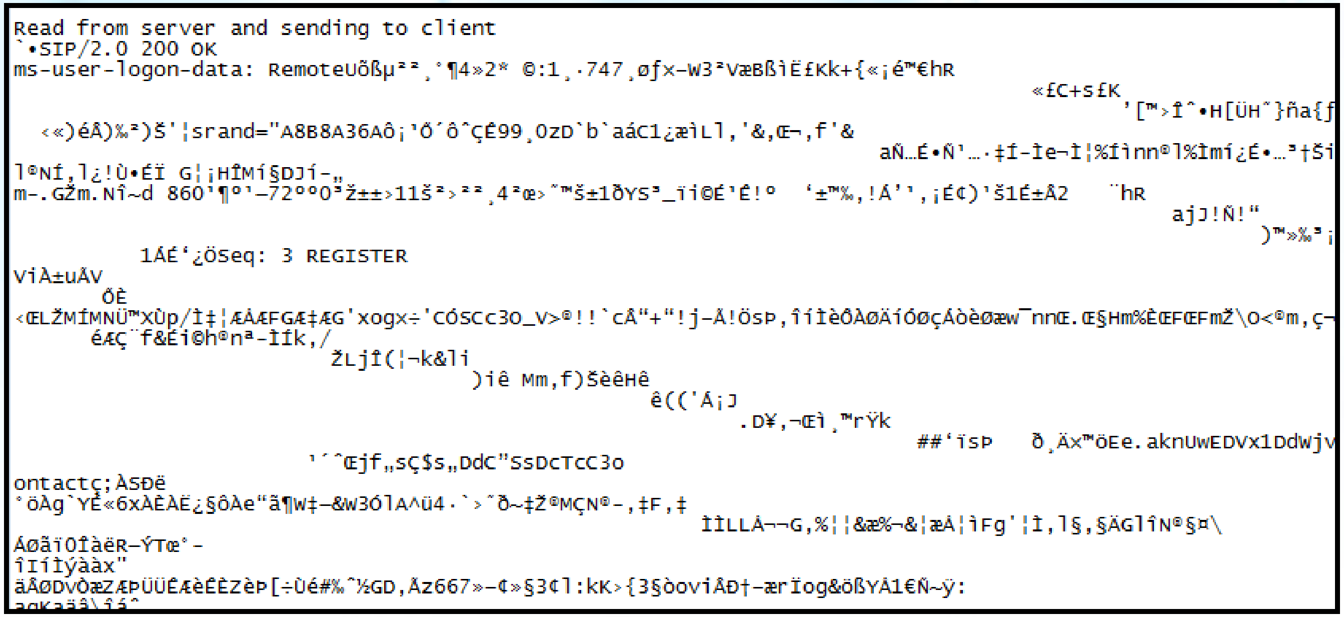
```
Read from client and sending to server
€µREGISTER sip:[redacted] SIP/2.0
Via: SIP/2.0/TLS 172.16.86.128:49755
Max-Forwards: 70
From: <sip:wsmith@[redacted]>;tag=cc6bc5e7d9;epid=9691215bc4
To: <sip:wsmith@[redacted]>
Call-ID: d2bae37cb16c42ec8c5946c0af089027
CSeq: 3 REGISTER
Contact: <sip:172.16.86.128:49755;transport=tls;ms-opaque=95f9750202>;methods="INVITE, MESSAGE, INFO, OPTIONS, BYE, CANCEL, NOTIFY, ACK, REFER, BENOTIFY";proxy=replace;
+sip.instance="<urn:uuid:1D8FFBBF-EB9A-5171-A576-7B39856ACE9E>"
User-Agent: UCCAPI/4.0.7577.4103 OC/4.0.7577.4103 (Microsoft Lync 2010)
Supported: gruu-10, adhoclist, msrtc-event-categories
Supported: ms-forking
Supported: ms-cluster-failover
Supported: ms-userservices-state-notification
ms-keep-alive: UAC;hop-hop=yes
Event: registration
ms-subnet: 172.16.86.0
Proxy-Authorization: NTLM qop="auth", realm="SIP Communications Service", opaque="8E016E1D", targetname="l[redacted]m", version=4, gssapi-
data="TlRMTVNTUAADAAAAGAAYAJYAAABCAUIBrgAAABQAFABYAAAADAAMAGwAAAAeAB4AeAAAABAAEADwAQAAVYKQYgYBsR0AAAAPKKv9hvZRPlbdFv
+riV3gkm8AYwBzAHUAcwBhAC4AYwBvAG0AdwBzAG0AaQB0AGgAVwBJAE4ALQA2AFAAMwBJAE4AOABPAEgAVQBJAEkAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIVnah/
+W3njVUhqmTxhWhAEBAAAAAAAAbyy4ALhlzQGH08SBYOR/ywAAAAACAAwATwBDAFMAVQBTAEEAAQASAEwAWQBOAEMALQBGAEUAMAAxAAQAFABvAGMAcwB1AHMAYQAuAGMAbwBtAAMAKABsAHkAbgBjAC0AZgBlADAAMQAuAG8AYwBzAHU
AcwBhAC4AYwBvAG0ABQAUAG8AYwBzAHUAcwBhAC4AYwBvAG0ABwAIAG8suAC4ZcOBBgAEAAIAAAAIADAAMAAAAAAAAAAABAAAAAACAAAHlaAjeZrTiyZ4TLCEkHaPGttffgVeZq1l2O
+v1/Hd63CgAQAAAAAAAAAAAAAAAAAAAAAAAAAJACgAbAB5AG4AYwAtAGYAZQAwADEALgBvAGMAcwB1AHMAYQAuAGMAbwBtAAAAAAAAAAAAAAAAAI3ZKdv4KSlvwu9FwOOkUzM=", crand="b4acf263", cnum="1",
response="0100000323135629c13257adeac190c"
Content-Length: 0
```

Client → Server

REGISTER

Client sends third SIP REGISTER message with Proxy-Authorization header and data, for NTLM.

Decrypted SIP TLS Message #8



```
Read from server and sending to client
`•SIP/2.0 200 OK
ms-user-logon-data: RemoteUõßµ²²¸°¶4»2* ©:1¸·747¸øƒx–W3²VæBßìË£Kk+{«¡é™€hR
                                                                                «£C+s£K
                                                                                       '[™›î^•H[ÜH˜}ña{ƒ
  <«)éÅ)‰²)Š'¦srand="A8B8A36Aô¡'Ő´ô^ÇÊ99¸OzD`b`aáC1¿æìL1,'&,Œ¬,f'&
                                                                    aÑ…É•Ñ¹…·‡Î–Ìe¬Ì¦%Îìnn®1%Ìmí¿É•…³†Ši
1®Ní,1¿!Ù•ÉÏ G¦¡HÎMí§DJí–„
m–.GŽm.Nî~d 860¹¶º¹–72ºººO³Ž±±›11š²›²²¸4²œ›˜™š±1ðYS³_ïi©É¹Ê!º  ‘±™‰,!Á'¹,¡É¢)¹š1É±Å2    ¨hR
                                                                                           ajJ!Ñ!“
                                                                                                  )™»‰³¡
          1ÁÉ‘¿ÖSeq: 3 REGISTER
ViÀ±uÄV
       ÕÈ
<ŒLŽMÍMNÜ™XÛp/Ì‡¦ÆÅÆFGÆ‡ÆG'xogx÷'CÓSCc3O_V>®!!`cÅ"+"!j–Å!ÖsÞ,îíÌèÕÀØÄíÓØçÁòèØæw¯nnŒ.Œ§Hm%ÈŒFŒFmŽ\O<®m,ç¬
      éÆÇ¨f&Éi©h®nª–Ìík,/
                         ŽLjî(¦¬k&1i
                                    )iê Mm,f)ŠèêHê
                                                  ê(('Á¡J
                                                         .D¥,¬Œì¸™rŸk
                                                                     ##‘ïsÞ   ð¸Äx™öEe.aknUwEDVx1DdWjv
                       '´ˆŒjf„sÇ$s„DdC"SsDcTcC3o
ontactç;ÀSÐë
°öÀg`YË«6xÀÈÀË¿§ôÀe“ã¶W‡–&W3Ó1A^ü4·`›˜ð~‡Ž®MÇN®–,‡F,‡
                                                      ÌÌLLÀ¬¬G,%¦¦&æ%¬&¦æÀ¦ìFg'¦Ì,1§,§ÄG1îN®§¤\
ÁØãïOîàëR–ÝTœ°–
îIíÌýàáx"
äÅØDvÒæZÆÞÜÜÊÆèÊÈZèÞ[÷Ûé#‰ˆ½GD,ÄZ667»–¢»§3¢1:kK›{3§òoviÅÐ†–ærÏog&ößYÀ1€Ñ~ÿ:
aqKaääâ\îá^
```

Client ← Server

200 OK

Server responds with 200 OK. You can see the compressed stream of data sent by the server.

Download

Co-Author (Anil Mahale)

- Thanks Anil

- Python SIP TLS proxy is available for download
  - http://enumerator.sourceforge.net/
  - Goal of building education and awareness

Thanks Anil!

Thanks Karl Feinauer

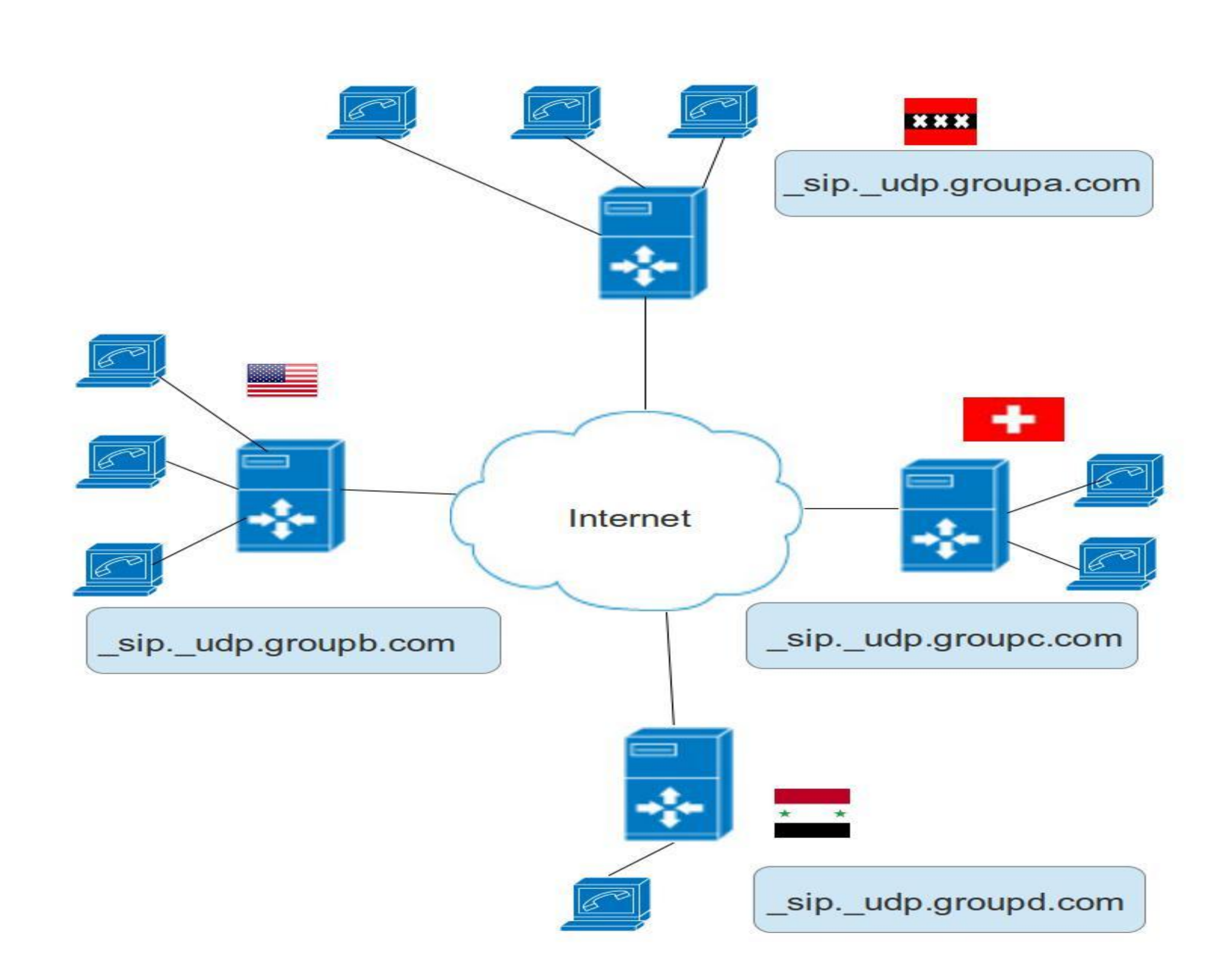
- Karl Feinauer
  - VIPER Lab Developer
  - DEF CON 20 Speaker
  - Couldn’t make it here today
  - Reverse engineered SIP messaging of Lync
  - Authored LyncSpoof, Federator
  - Somewhat of a mystery…

Thanks Karl Feinauer

Open Source UC Federation

- Can be used for inexpensive and out of band communication between groups of friends.
- Can be used for audio, video and instant messaging.
- Saves money by using open source software for servers and end points.

Open Source Federation - Architecture



Asterisk Federation and How it Works

- SRV Lookups
  - When a user that is registered to a federated Asterisk server calls another user registered to another federated server his server simply performs an SRV lookup and places the call to the other user.
  - In this scenario there is no need for SIP trunks to terminate calls at the PSTN.
  - This means no long distance or international charges for phone calls between federated users.

Our Open Source Federation Project

- SIP Federation Project
  - Servers can appear to be in any part of the world by IP address (Linodes).
  - We set up fake companies with SIP servers.
  - We can call one another using SIP user agents on our cell phones and computers.
  - This would be a great way for DefCon groups to stay in touch.
  - If each group had a server and federated with one another using SRV records they could communicate very inexpensively.

Our Configuration Files

- To get started doing this you can go to

http://enumerator.sf.net and download a version of our configuration files.

Conclusion

- One idea
  - You could move your Asterisk server from internal network to Edge, with a public IP address (No NAT)
  - Asterisk could function as a B2BUA - “Poor Man’s SBC”
    - RTP Media Anchoring
    - No NAT or Topology Hiding
    - Proof of Concept for business communication (offers No Security)
  - Then host your own SIP for your organization using DNS SRV, using your domain
  - Peer directly to other organizations using SIP and DNS SRV
  - Remote SIP users could register and place calls as a local extension
  - Keep your carrier SIP Trunk, for access to legacy PSTN
  - IP QoS

The “UC Cloud” - UC Federation and SIP DNS SRV Peering

http://www.linode.com/

Linode - Xen VPS Hosting

linode.com

Deploy and Manage Linux Virtual Servers in the Linode Cloud.

Get a server running in minutes with your choice of Linux distro, resources, and node location.

Servers on demand. Support that cares.

Conclusion – Peering in the New “UC Federation” Cloud

- Another Idea
  - New UC/VoIP Cloud services using DNS SRV for SIP peering
    - Create your own new product/service for Cloud hosting for SIP DNS SRV peering (Linode.com)
    - Host your SIP server for your company in the cloud and experiment with SIP DNS SRV peering for Fun! (Linode.com)
    - IP QoS

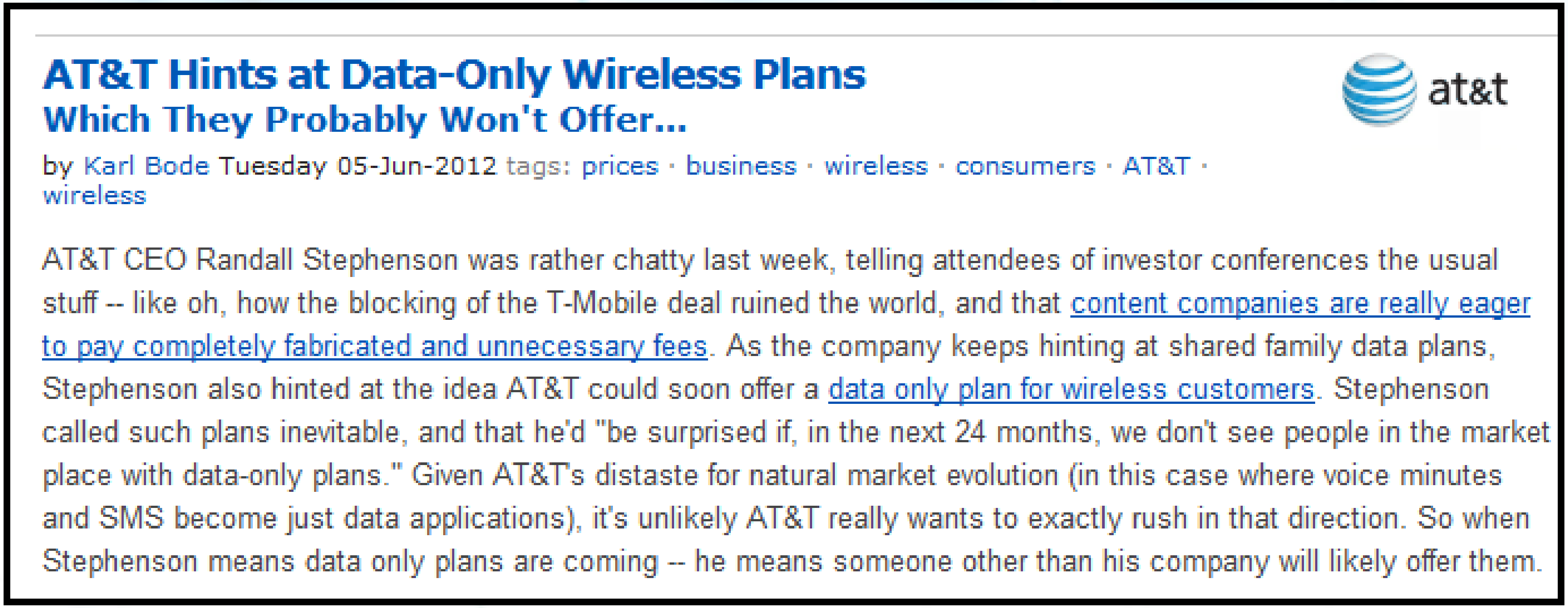
linode.com

Mobile Carriers & Smartphones

- SIP and Federation on smartphones
  - Very slow adoption
  - In the US, it appears subscribers can’t opt for Data Only plans on Cellular/3GPP carrier networks
  - Less incentive to use VoIP on my smartphone if I already have to pay my carrier for Voice
  - Data only plans would be a compelling option and help build exciting new applications
  - IP QoS for RealTime communications on Cellular/3GPP networks

Mobile Carriers

- Data-Only plans just around the corner?



AT&T Hints at Data-Only Wireless Plans

Which They Probably Won't Offer...

by Karl Bode Tuesday 05-Jun-2012 tags: prices · business · wireless · consumers · AT&T · wireless

AT&T CEO Randall Stephenson was rather chatty last week, telling attendees of investor conferences the usual stuff -- like oh, how the blocking of the T-Mobile deal ruined the world, and that content companies are really eager to pay completely fabricated and unnecessary fees. As the company keeps hinting at shared family data plans, Stephenson also hinted at the idea AT&T could soon offer a data only plan for wireless customers. Stephenson called such plans inevitable, and that he'd "be surprised if, in the next 24 months, we don't see people in the market place with data-only plans." Given AT&T's distaste for natural market evolution (in this case where voice minutes and SMS become just data applications), it's unlikely AT&T really wants to exactly rush in that direction. So when Stephenson means data only plans are coming -- he means someone other than his company will likely offer them.

NSA Secure Mobility

Mobility Capability Package

February 27

2012

This document defines the first phase of the Enterprise Mobility Architecture and focuses on the architectural components of providing a Secure VoIP capability using commercial grade products.

Secure VoIP
Version 1.1

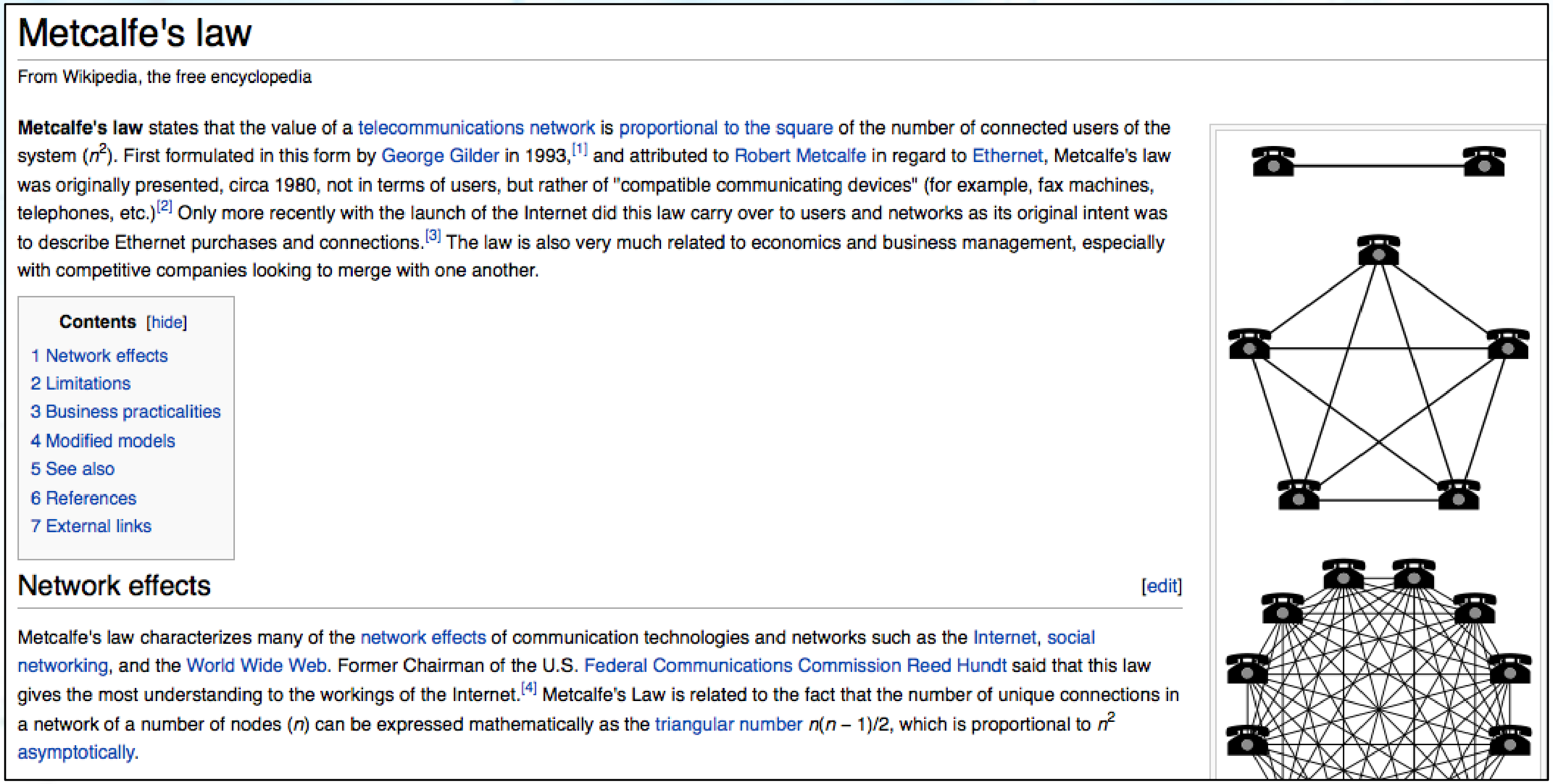
WebRTC + Google

- WebRTC could be disruptive to all of this
- http://www.webrtc.org
- Realtime communications with Javascript and HTML5 natively in the browser (no plugins required)

WebRTC

Metcalfe’s law

The more people using SIP DNS SRV peering and/or UC Federation, the more valuable the network becomes.



Metcalfe's law

From Wikipedia, the free encyclopedia

Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2). First formulated in this form by George Gilder in 1993,[1] and attributed to Robert Metcalfe in regard to Ethernet, Metcalfe's law was originally presented, circa 1980, not in terms of users, but rather of "compatible communicating devices" (for example, fax machines, telephones, etc.)[2] Only more recently with the launch of the Internet did this law carry over to users and networks as its original intent was to describe Ethernet purchases and connections.[3] The law is also very much related to economics and business management, especially with competitive companies looking to merge with one another.

Contents [hide]

Network effects

[edit]

Metcalfe's law characterizes many of the network effects of communication technologies and networks such as the Internet, social networking, and the World Wide Web. Former Chairman of the U.S. Federal Communications Commission Reed Hundt said that this law gives the most understanding to the workings of the Internet.[4] Metcalfe's Law is related to the fact that the number of unique connections in a network of a number of nodes (n) can be expressed mathematically as the triangular number $n(n – 1)/2$, which is proportional to n^2 asymptotically.

Thanks

Acquired by:

AVAYA

- Contact Information
  - William Borskey (wborskey@avaya.com)
  - Jason Ostrom (jostrom@viperlab.net)
  - Karl Feinauer (kfeinauer@viperlab.net)
- For more information
  - About VIPER: http://www.viperlab.net
  - For live participants, presentation can be downloaded from http://enumerator.sf.net