BorderWare™

A Taxonomy of VoIP Security Threats

An outline of the security threats that face SIP based VoIP and other real-time applications

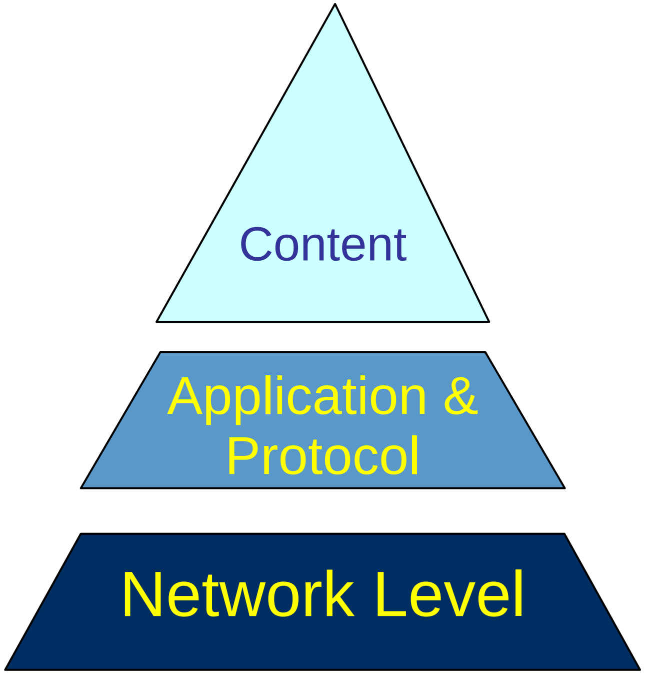
Peter Cox

CTO Borderware Technologies Inc

VoIP Security Threats

VoIP Applications Run over IP Networks

- Network Level Threats, in common with all IP applications
- Application and Protocol specific threats
- Content Related Threats



Network Level Threats

Threats propagated via low-level protocols, IP and TCP/UDP

- Malformed packet attacks
- Flooding attacks, including connection flooding
- Denial of Service Attacks
- Buffer overflow attacks

Consequences

- Full or partial service loss
- Loss of system control

Application and Protocol Threats

VoIP applications use a mix of standards based and proprietary protocols including:

- H.323 Legacy protocol used in Microsoft’s NetMeeting and in some commercial VoIP products
- Skinny, Cisco proprietary protocol, used by Call Manager
- Skype, proprietary protocol designed to use a number of transports to find a way through Firewalls
- Session Initiation Protocol, emerging as the Internet Standard
  - Implemented in new products
  - Implemented in virtually all legacy products for interoperability
  - Scope is much wider than VoIP

Session Initiation Protocol (SIP)

- A relatively new protocol (first proposed March 1999)
- Designed to support *Internet based* real-time messaging
  - Voice Telephony (VoIP)
  - Video Conferencing
  - Instant Messaging
- Many of these services already exist as regular telecommunications applications
- The First time a major new Internet protocol has emerged to drive existing applications

Date	*Protocol*	*Application*
1982	SMTP	Email, new service concept
1991	HTTP	Web, new service concept
1999	SIP	Real-time messaging, existing service concept

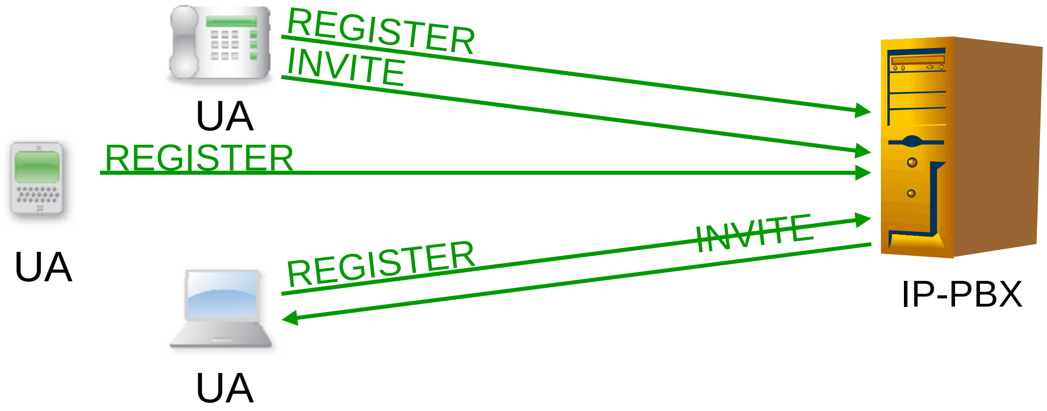
What role does SIP Play

SIP is responsible primarily for session control

- Device registration,
- Call setup
- Call termination
- Advanced features such as call transfer
- VoIP and Video conferencing use other protocols for call data, typically **RTP** (real-time transport protocol)
- Call data parameters negotiated via **SDP** (Session Description Protocol)
- Instant Messaging and related services use SIP directly for message transfer

SIP Network Components

- SIP Application Server, Proxy Server, IP-PBX, Soft-switch
  - Routes calls, holds local user database
  - Equivalent to the *Private Branch Exchange* (Telephone switch)
- SIP phones, User agents (UA)
  - Hardware phones
  - Softphones
- UA’s *REGISTER* with the IP-PBX
- Calls established with *INVITE* requests



SIP Protocol Details

- Text based protocol, similar to Web (HTTP) and Email (SMTP) protocols
- Shares many of the same security risks and vulnerabilities
- Easy to monitor/spoof

```
REGISTER sip:sip.borderware.co.uk SIP/2.0
Via: SIP/2.0/UDP 192.168.19.12:5060;branch=z9hG4bK927ec13a8c04928
Max-Forwards: 70
To: <sip:johnsmith0@borderware.co.uk>
From: <sip:johnsmith0@borderware.co.uk>;tag=9600645
Call-ID: 1da1@192.168.19.12
Cseq: 20482 REGISTER
Contact: <sip:johnsmith0@192.168.19.12>
User-Agent: SIP desktop phone
Content-Length: 0
```

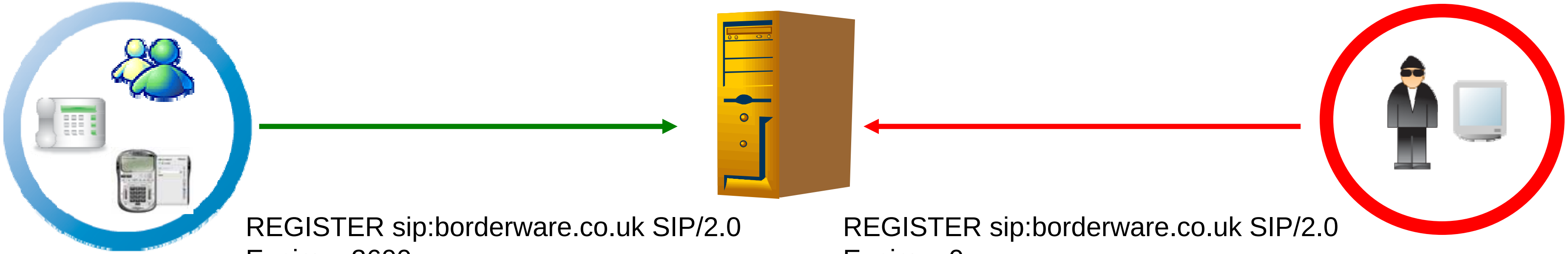
Registration Attacks (Protocol Level)

Denial of Service Attacks

- Registration flooding (PBX can’t make or accept calls)
- De-registration attacks (device can’t receive calls)

Attacks possible because of

- Optional authentication service
- No automatic message verification



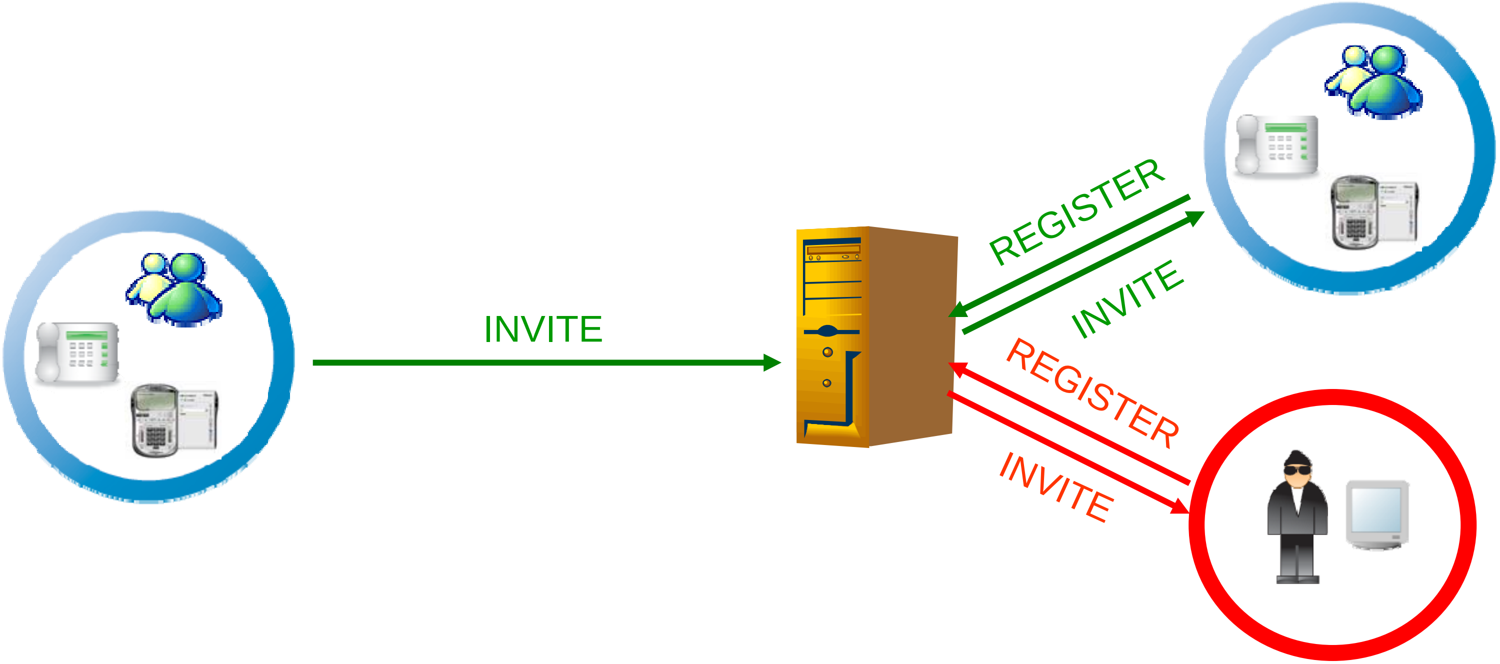
REGISTER sip:borderware.co.uk SIP/2.0
Expires: 3600

REGISTER sip:borderware.co.uk SIP/2.0
Expires: 0

Unlawful Session Intercept (Protocol Level)

Unauthorised device registration and eavesdropping

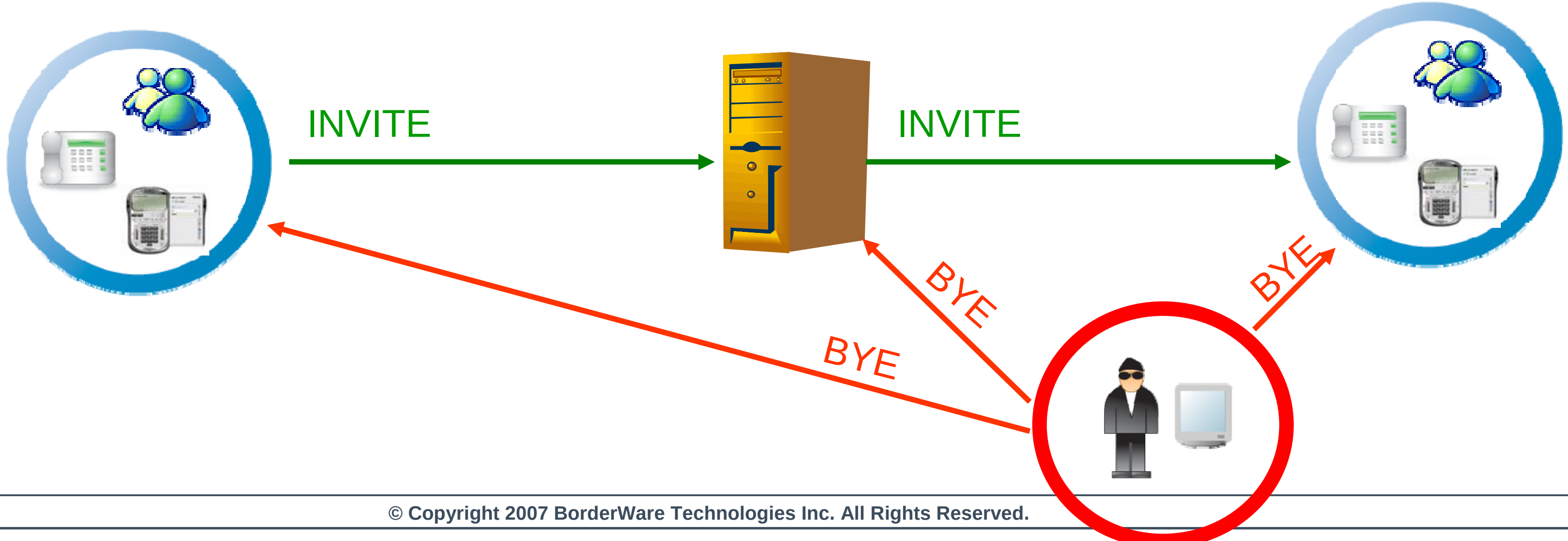
- Attacker registers additional devices under user's SIP URL
- Calls to user also received by attacker



BYE Attack, Call Termination (Protocol Level)

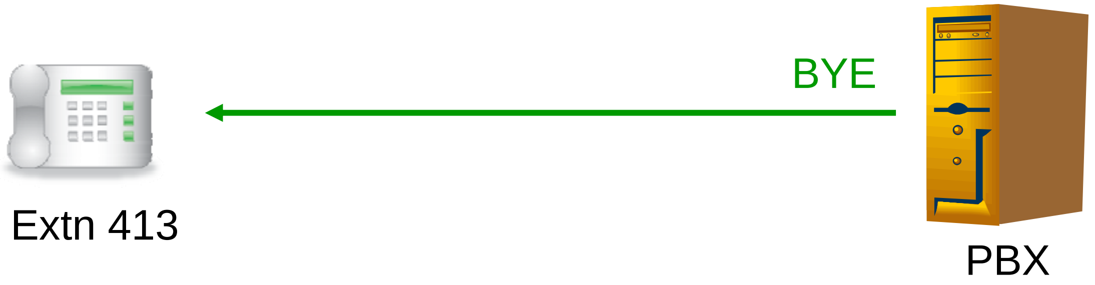
SIP Calls Terminated with a “BYE” message

- Originating from a call participant
- Originating from the IP-PBX or Administrator
- An unauthorised “BYE” will prematurely terminate the call
- 3 Vulnerability Points:



Dissecting a Bye Attack (1)

Call from PBX to Extension 413

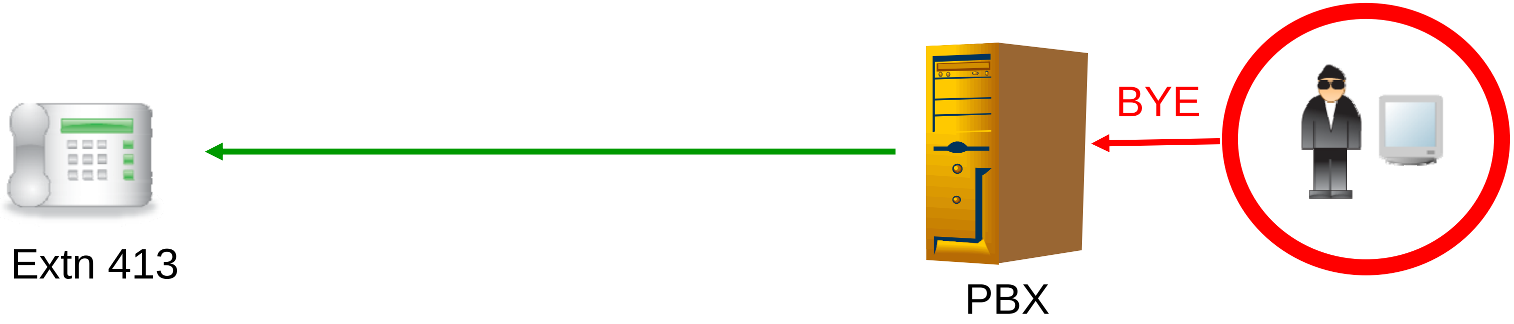


- Normal Termination

```
BYE sip:413@192.168.4.75:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.4.28:5060;branch=z9hG4bK28107c34;rport
From: "Sales Desk" <sip:414@192.168.4.28>;tag=as466c284f
To: <sip:413@192.168.4.8:5060>;tag=4ab274367f880505i0
Call-ID: 456e14f3615c4fa714a164920de4702a@192.168.4.28
CSeq: 103 BYE
User-Agent: Branch Office PBX
Max-Forwards: 70
Content-Length: 0
```

Dissecting a Bye Attack (2)

Call from PBX to Extension 413



- BYE Attack

```
BYE sip:victim@1.2.3.4 SIP/2.0
Via: SIP/2.0/UDP 192.168.4.28:5060;branch=z9hG4bK3028e41a
Max-Forwards: 70
To: <sip:123@random.com>
From: <sip:attacker@hostile.org>;tag=e0ae24c56f1952bfi0
Call-ID: 26adb57535734f41413514ac09fc043d@192.168.4.28
CSeq: 102 BYE
Expires: 240
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER
Contact: <sip:456:6.7.8.9>
Content-Length: 0
```

SIP Protocol Threats, Summary

SIP Method	Attacks	Consequences
REGISTER	• Registration Flood • Dictionary Attack • DeRegistration Attack	• Loss of service • Password compromise • Call disruption
INVITE	• Call Flooding • Call Transfer Attack • Call Intercept	• Loss of service • Denial of Service • Confidentiality breach
REFER	• Unauthorised Forwarding	• Confidentiality breach
BYE	• Call Termination Attack	• Call disruption • Service Degredation

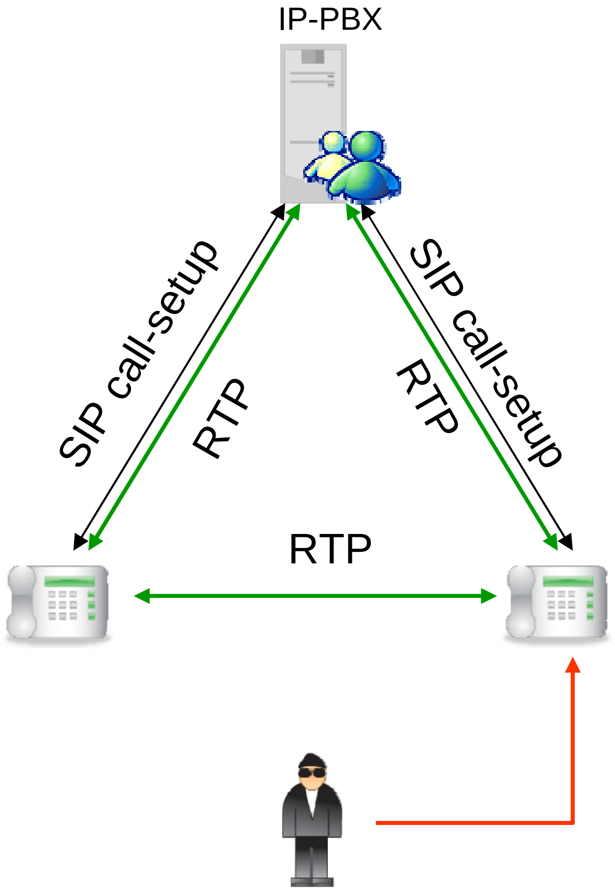
RTP Protocol Attacks

RTP Carries call media between end-points

- Peer-to-Peer
- Via Server
- Defaults to clear-text

RTP Injection

- Send an RTP stream to and end-point
- Replace or combine with valid stream



Content Threats

Threats at the Call Content Level

- Unwanted Calls
- VoIP Spam
- Unauthorised Monitoring
- Malicious Payloads (Worms, Viruses)

Is VoIP Spam a reality?

The explosion of email spam lagged email growth

- Spammers need a critical mass of users for Spam to be cost effective
- Don’t wait, even a low level of Spam will make VoIP unusable

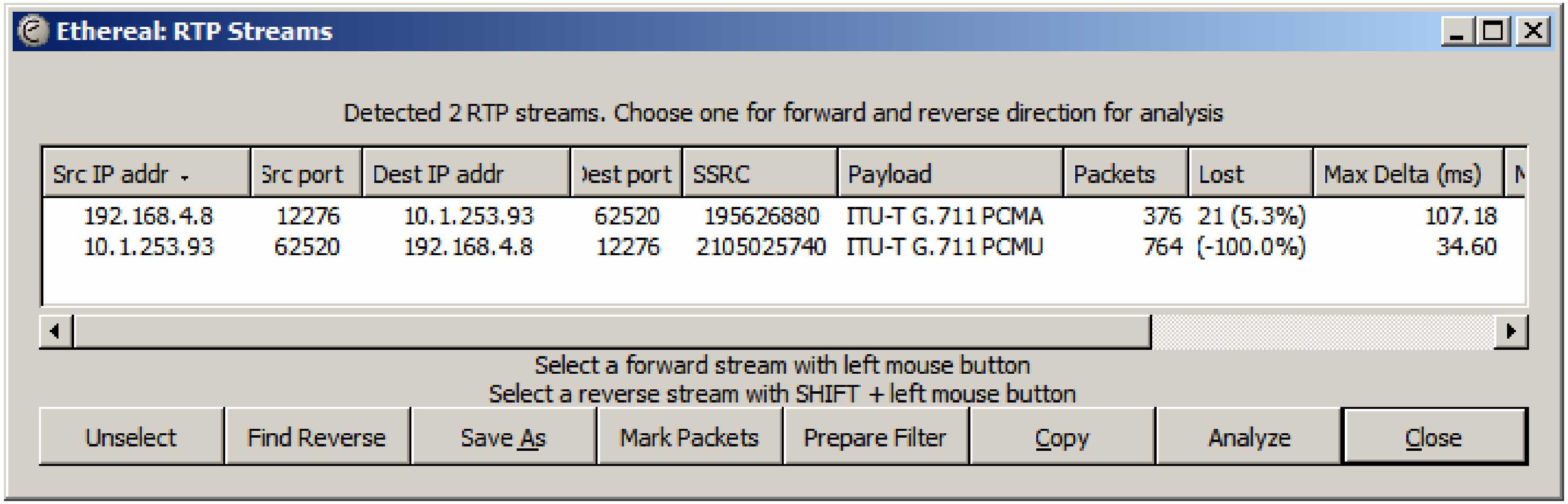
“Spam, defined as the transmission of bulk unsolicited email, has been a plague on the Internet email system, rendering it nearly useless. Many solutions have been documented and deployed to counter the problem. None of these solutions is ideal. However, one thing is clear: the spam problem would be much less significant had solutions been deployed ubiquitously before the problem became widespread.”

The Session Initiation Protocol (SIP) and Spam
http://www.ietf.org/internet-drafts/draft-ietf-sipping-spam-03.txt

Eavesdropping / Unlawful Monitoring

Monitor and record the call…

- The old fashioned way using packet sniffers and other tools:



Ethereal: RTP Streams

Detected 2 RTP streams. Choose one for forward and reverse direction for analysis

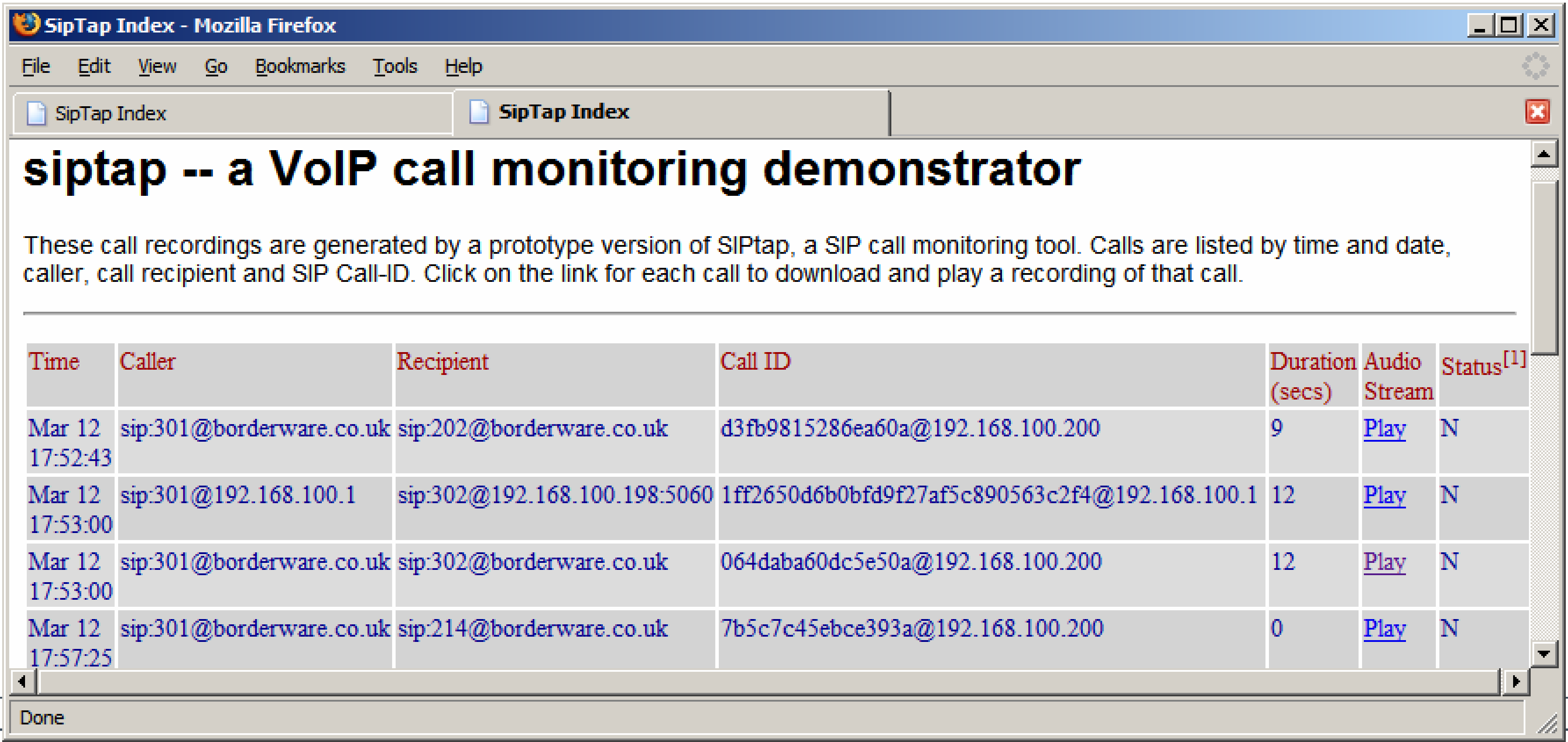
Src IP addr	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost	Max Delta (ms)	M
192.168.4.8	12276	10.1.253.93	62520	195626880	ITU-T G.711 PCMA	376	21 (5.3%)	107.18	
10.1.253.93	62520	192.168.4.8	12276	2105025740	ITU-T G.711 PCMU	764	(-100.0%)	34.60	

Select a forward stream with left mouse button
Select a reverse stream with SHIFT + left mouse button

Eavesdropping / Unlawful Monitoring

Monitor and record the call…

- The easy way, point and click wire-tapping from anywhere on the net….

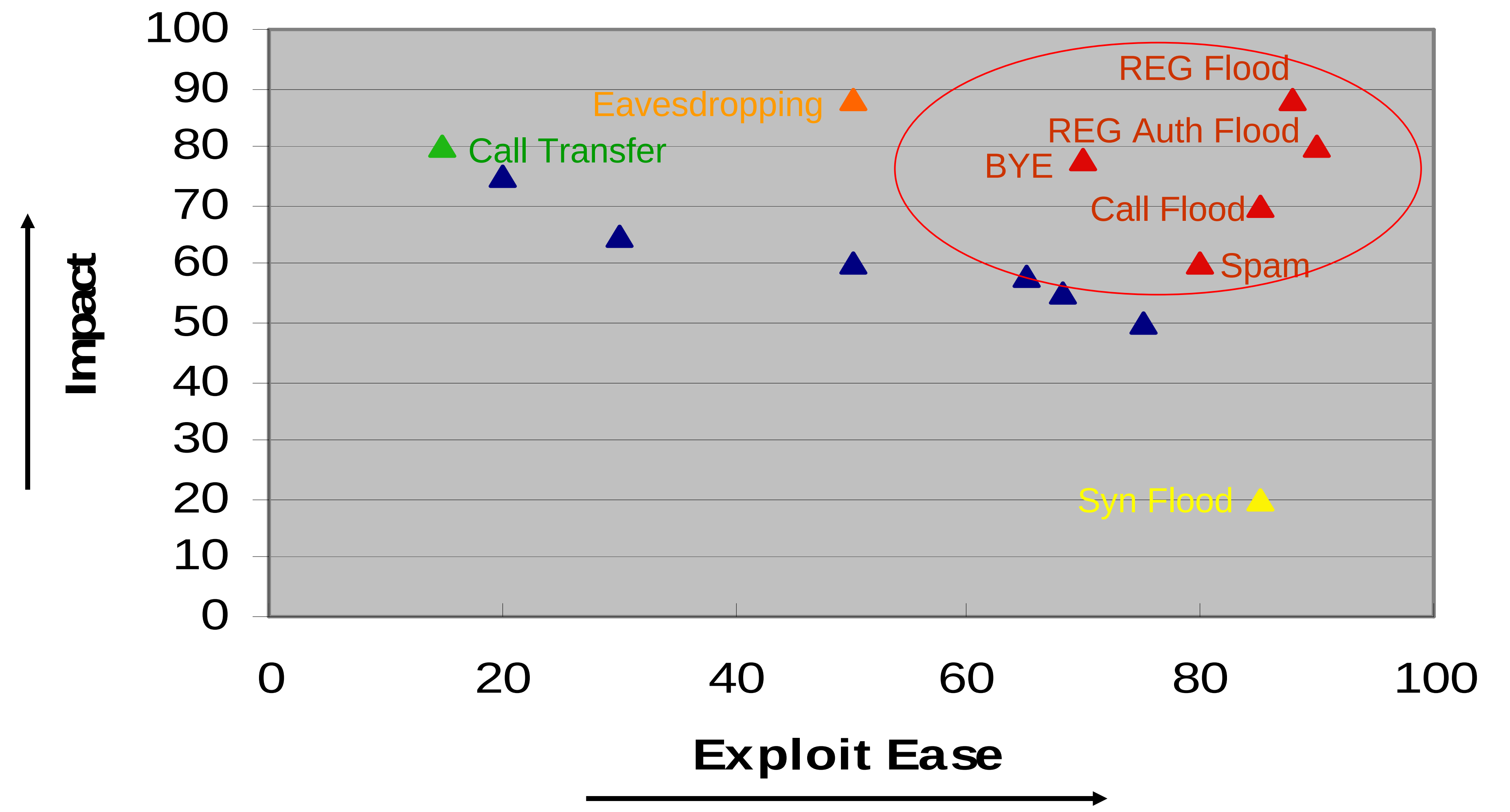

SipTap Index - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
SipTap Index
SipTap Index
Done

siptap -- a VoIP call monitoring demonstrator

These call recordings are generated by a prototype version of SIPtap, a SIP call monitoring tool. Calls are listed by time and date, caller, call recipient and SIP Call-ID. Click on the link for each call to download and play a recording of that call.

Time	Caller	Recipient	Call ID	Duration (secs)	Audio Stream	Status[1]
Mar 12 17:52:43	sip:301@borderware.co.uk	sip:202@borderware.co.uk	d3fb9815286ea60a@192.168.100.200	9	Play	N
Mar 12 17:53:00	sip:301@192.168.100.1	sip:302@192.168.100.198:5060	1ff2650d6b0bfd9f27af5c890563c2f4@192.168.100.1	12	Play	N
Mar 12 17:53:00	sip:301@borderware.co.uk	sip:302@borderware.co.uk	064daba60dc5e50a@192.168.100.200	12	Play	N
Mar 12 17:57:25	sip:301@borderware.co.uk	sip:214@borderware.co.uk	7b5c7c45ebce393a@192.168.100.200	0	Play	N

Threat Impact



Information Sources

White Papers

- VoIP Threat Landscape
- Far-end NAT Traversal
- Securing and Federating VoIP using Encryption

VoIP Threat Demonstration (Podcast)

http://www.youtube.com/watch?v=UA1quyLOTdg

http://tinyurl.com/2s42jr

VoIP Threat Demonstration

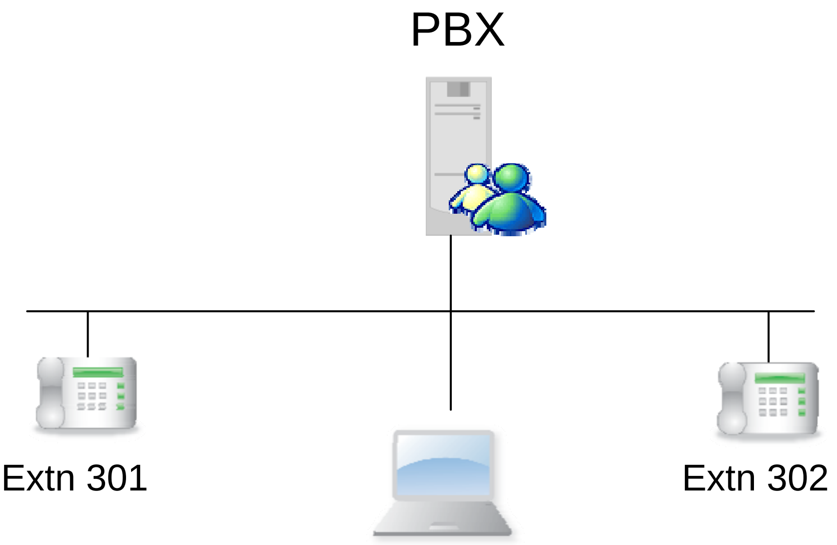
Protocol and Application

- Call Termination Attack
- Call Flooding
- Caller ID Spoofing

Content

- VoIP Spam
- Unauthorised Monitoring

At our vendor booth



Contacts

Stuart Morrice

- stuart@sipserviceseurope.com
- +44 7855 416126

Peter Cox

- peter@voipcode.org
- +44 7785 333832

Introducing SIPassure

SIP Security gateway for VoIP, Video Conferencing, IM and other applications

- Appliance form factor
- Firewall grade secure operating system
- Application level protection against flooding attacks and call disruption
- Call pattern analysis for Spam and malicious call threats
- Advanced reputation services for tracking abuse sources
- SIP TLS encryption, SRTP for RTP encryption and caller/call recipient verification
- Comprehensive management and auditing
- Compliancy and policy control including legal call monitoring