

# Incorporate Active Fingerprinting into SPIT Prevention Systems

Hong Yan, Hui Zhang (CMU, USA)

Kunwadee Sripanidkulchai (NECTEC, Thailand)

Zon-Yin Shae, Debanjan Saha (IBM T.J. Watson Research, USA)

# Agenda

- Motivations
- Related works
- Passive fingerprinting
- Active fingerprinting
- Experiment setup and results
- Summary

# Motivations

- Expect SIP spamming software to have different implementation from legitimate user agents
  - For small code size and better speed
- Each device with different SIP stack implementation can have different fingerprinting
  - A large number of SIP devices, at least 70 soft-phones and 60 servers (from wiki)
- As the network grows in scale and heterogeneity, potential abuse of the VoIP technology (e.g. SPIT) and the interoperability problems between SIP devices.
- To explore the additional knowledge of the remote devices for SPIT prevention and to protect the domain by rejecting the INVITE requests from non-interoperable SIP devices

# Related Works

- Black/white lists
- Reputation-based social networks (Rebahi, et. al. June, 2005)
- Combine black/white lists, trust and reputation functions and media quarantining (Dantu, et. al. July, 2005)
- Progressive Multi Gray-Leveling to learn calling patterns of spammer (Shin, et. al., June 2005)
- Our proposed fingerprinting techniques can be incorporated into these SPIT preventing systems.

# Passive Fingerprinting

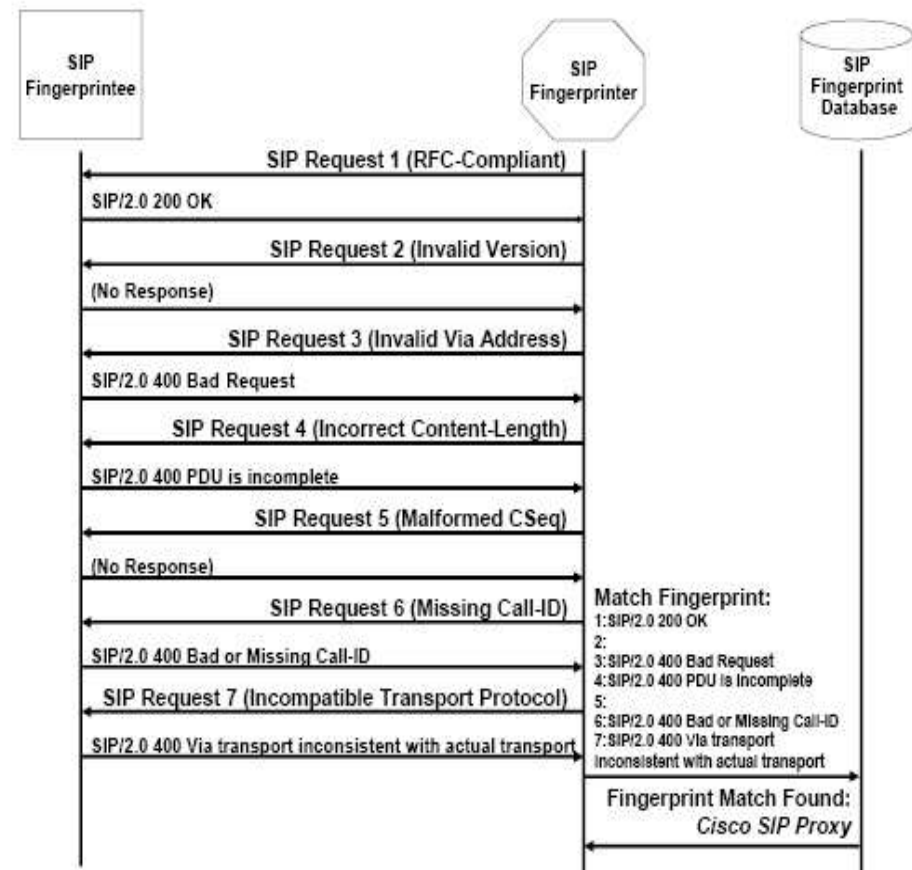
- Analyzing the header fields of INVITE messages
- Experiment using 13 different hard-phones and soft-phones for their popularities, various OS platforms, and countries
- Existence and ordering of the header fields form passive fingerprinting vector
- Able to distinguish different devices, but easy to be spoofed

SIP Component	Header Fields in INVITE Message
Hardphones	
Cisco Phone	Via,Record-Route,Via,From,To,Call-ID,Date,CSeq,User-Agent>Contact,Expires,Content-Type,Content-Length,Accept
Pingtel Phone	Via,Record-Route,From,To,Call-ID,CSeq>Contact,Content-Type,Content-Length,Accept-Language,Allow,Supported,User-Agent,Date,Via
Softphones	
Adore Softphone	Via,Max-Forwards,From,To,Call-ID,CSeq>Contact,User-Agent,Content-Type,Content-Length
Express Talk	Via,To,From,Call-ID,CSeq,Max-Forwards,User-Agent>Contact,Allow,Supported,Content-Type,Content-Length
eyeBeam	Via,Max-Forwards>Contact,To,From,Call-ID,CSeq,Allow,Content-Type,Supported,User-Agent,Content-Length
KPhone	Via,CSeq,To,Content-Type,From,Call-ID,Subject,Content-Length,User-Agent>Contact
LinPhone	Via,From,To,Call-ID,CSeq,Max-Forwards,User-Agent,Subject,Expires,Allow,Content-Length
Phoner	Via,From,To,Call-ID,CSeq>Contact,Max-Forwards,User-Agent,Allow,Content-Type,Content-Length
Sipps	Via,From,To,Call-ID,CSeq,User-Agent,Expires,Accept,Content-Type,Content-Length>Contact,Max-Forwards,Allow
sipXphone	From,To,Call-ID,CSeq>Contact,Content-Type,Content-Length,Date,Max-Forwards,User-Agent,Accept-Language,Allow,Supported,Via
STPhone	Via,Content-Length>Contact,Call-ID,Content-Type,CSeq,From,Max-Forwards,To
WinSip	Via,Max-Forwards,From,To,User-Agent,Call-ID,CSeq>Contact,Allow,Accept,Accept-Language,Content-Type,Content-Disposition,Content-Length
Yate	Max-Forwards,Via,From,To,Call-ID,CSeq,User-Agent,Allow,Content-Type,Content-Length

Table 1: Passive fingerprints obtained from INVITE messages of SIP hardphones and softphones.

# Active Fingerprinting

- Active probe the remote device using a set of specially crafted standard compliant and non-compliant SIP messages (e.g., OPTIONS)
- The returned status code and the values in response headers form active fingerprinting vector
- There are large number of possible ways to manipulate the OPTIONS that can be used as probes. A random selection of the subset can be used.
- We argue that malicious user agents can not easily rely on the pre-canned response to spoof identity, and this mechanism can fingerprint the SIP stack used.



# Response to Standard Compliant OPTIONS

```
OPTIONS sip:128.2.181.221 SIP/2.0
Via: SIP/2.0/UDP 155.98.39.84;branch=z9hG4bKhjhs8as877
CSeq: 1 OPTIONS
Call-ID: a84b4c76e66710
To: <sip:128.2.181.221>
From: Anonymous <sip:anonymous@sipfw.org>;tag=1928301774
Max-Forwards: 70
```

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 155.98.39.84;branch=z9hG4bKhjhs8as877
Contact: <sip:128.2.181.221:5060>
To: <sip:128.2.181.221>;tag=7c3d124c
From: Anonymous <sip:anonymous@sipfw.org>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 1 OPTIONS
Accept: application/sdp
Accept-Language: en
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,MESSAGE,
      SUBSCRIBE,INFO
```

# Response to Non-Compliant OPTIONS

- Invalid Version (SIP/99.9)
- Invalid Via Address (via = "localhost")
- Incorrect Content-Length (non-zero length without body)
- Malformed CSeq (remove the OPTIONS)
- Missing Call-ID (remove Call-ID field)
- Incompatible Transport Protocol (use UDP to send request but claim to have TCP in Via)

# Active Fingerprinting Feature Vector

Component	SIP Fingerprint						
	RFC-Compliant	Invalid Version	Incorrect Via Address	Incorrect Content Length	Malformed CSeq	Missing Call-ID	Incorrect Transport Protocol
SIP Servers							
3Com SIP Proxy (siphappens.com)	405	405	NR	405	NR	NR	NR
Cisco Voice Gateway (Cisco-SIPGateway/IOS-12.x)	200	400	200	NR	NR	400	400
Cisco Voice Gateway	400	400	400	NR	NR	400	400
Cisco SIP proxy	NR	NR	400	400	NR	400	400
MCI SIP Proxy (sipaccount.mci.com)	302	400	NR	302	NR	NR	400
Microappliances SIP Proxy (zdots.com MA-1000-2.1)	403	400	403	403	NR	NR	400
SIP Express Router Proxy (iptel.org 0.0.0udpfifo i386/linux)	404	NR	404	404	NR	404	NR
Hardphones							
Cisco Phone (cisco.com)	200	NR	200	400	NR	400	NR
Pingtel Phone (pingtel.com)	200	505	200	200	NR	NR	NR
Softphones							
Adore Softphone (adoresoftphone.com)	200	481	NR	400	NR	400	NR
Express Talk (nch.com.au)	200	200	200	200	NR	200	200
eyeBeam (counterpath.com)	200	200	200	200	405	NR	200
KPhone (wirllab.net)	200	200	NR	200	200	200	NR
LinPhone (linphone.org)	200	200	200	200	NR	NR	NR
Phoner (phoner.de)	200	200	200	200	NR	NR	200
Sipps (nero.com)	200	200	200	200	400	NR	NR
sipXphone (sipfoundry.org)	200	505	200	200	NR	NR	200
SJPhone (sjlabs.com)	405	NR	405	NR	NR	NR	NR
WinSip (touchstone-inc.com)	200	NR	200	200	NR	481	481
Yate (yate.null.ro)	501	NR	NR	501	NR	501	501

Table 2: Fingerprints of various SIP components. “NR” denotes no response.

# Allow Header Feature Vector

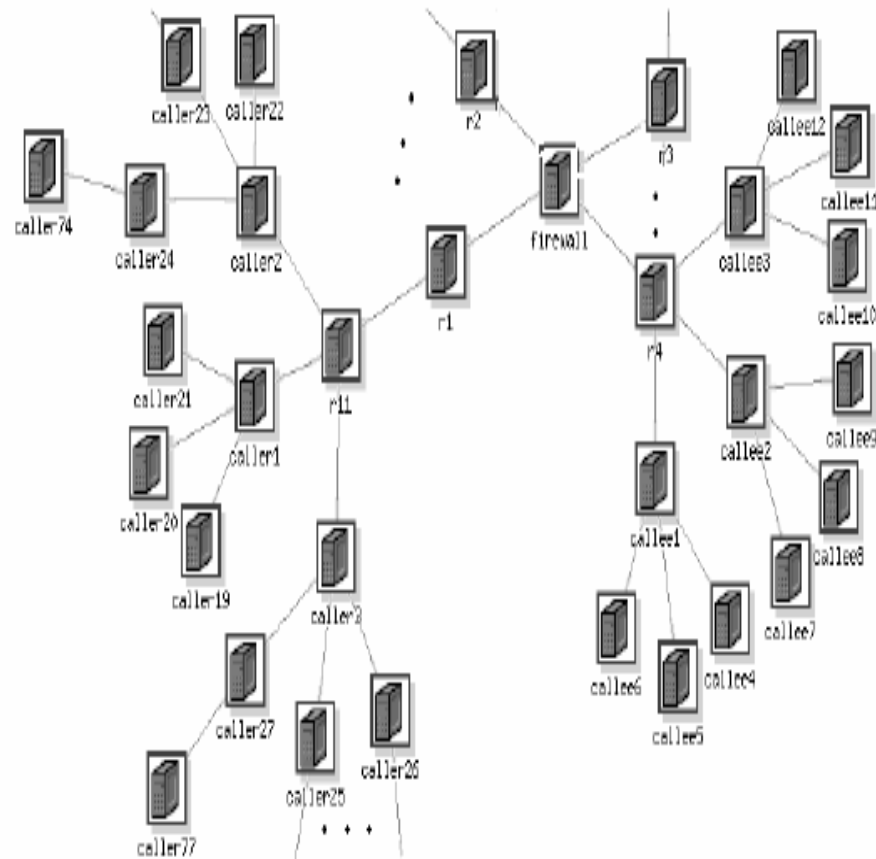
Component	SIP Allowed Field in OPTIONS Response
SIP Servers	
Cisco Voice Gateway (Cisco-SIPGateway/IOS-12.x)	INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE, NOTIFY, INFO, UPDATE, REGISTER
Hardphones	
Cisco Phone (cisco.com)	OPTIONS, INVITE, BYE, CANCEL, REGISTER, ACK, NOTIFY, REFER
Pingtel Phone (pingtel.com)	INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE
Softphones	
Adore Softphone (adoresoftphone.com)	INVITE, BYE, OPTIONS, MESSAGE, ACK, CANCEL, NOTIFY, SUBSCRIBE, INFO, REFER
Express Talk (nch.com.au)	INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
eyeBeam (counterpath.com)	INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, INFO
KPhone	INVITE, OPTIONS, ACK, BYE, MSG, CANCEL, MESSAGE, SUBSCRIBE, NOTIFY, INFO, REFER
LinPhone (linphone.org)	INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, MESSAGE, INFO
Phoner (phoner.de)	INVITE, ACK, CANCEL, BYE, NOTIFY
Sipps (nero.com)	INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, INFO
SJPhone (sjlabs.com)	INVITE, ACK, CANCEL, BYE, REFER, NOTIFY
WinSip (touchstone-inc.com)	INVITE, ACK, BYE, CANCEL, OPTIONS, MESSAGE, INFO
Yate (yate.null.ro)	ACK, INVITE, BYE, CANCEL

Table 3: Allow fields of various SIP components. “N/A” indicates that the Allow field is not included in the response.



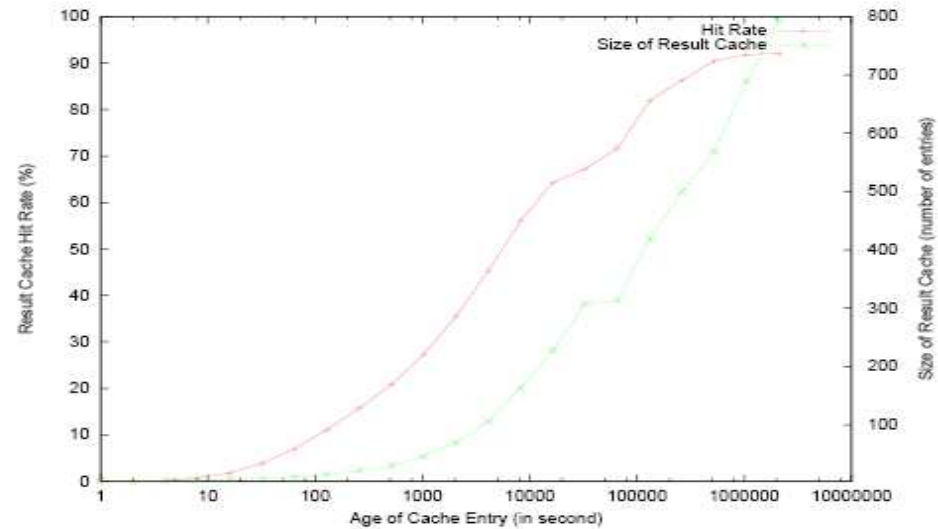
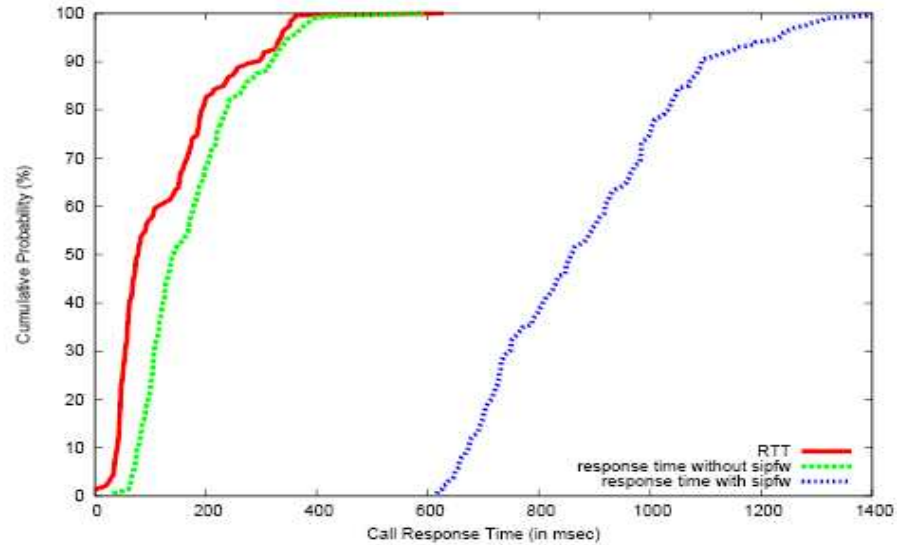
# Throughput Experiments

- SIP firewall : 2.0 GHz Pentium 4, 512 MB, Linux 2.6.14
- Callers/callees: 850 MHz pentium III, 512 MB, Linux 2.6.14
- 100 emulab nodes for callers and 100 nodes for callees. All links have 100 Mbps bandwidth
- Run LinPhone on callers and callees.
- Modify LinPhone to repeatedly make calls at specified rate and callee automatically answer and terminate calls.
- Results: 1000 calls/second when CPU is 80%



# Response Time Experiments

- 200 Planetlab machines as callers for realistic network delay and conditions
- Response time Increase 600 to 800 ms. The response time can be shorten by Caching
- To study the effectiveness for caching, we use 2 months long call traces data collected from a small enterprise VoIP deployment with call rate 5-10 calls/minutes
- Cache aging increase to 1000 second, hit rate is 25%, and 6 days with 90% hit rate
- Cache table size is very small (about 70 KB)



# Summary

- Propose active fingerprinting to explore the additional knowledge of the remote user agents for SPIT prevention and rejecting the non-interoperable SIP devices
- Study the feasibility of active fingerprinting firewall implementation
- Fingerprinted 20 SIP devices and find each device has a unique fingerprint and can be uniquely identified using a small number of probes.