VOIP in XKEYSCORE

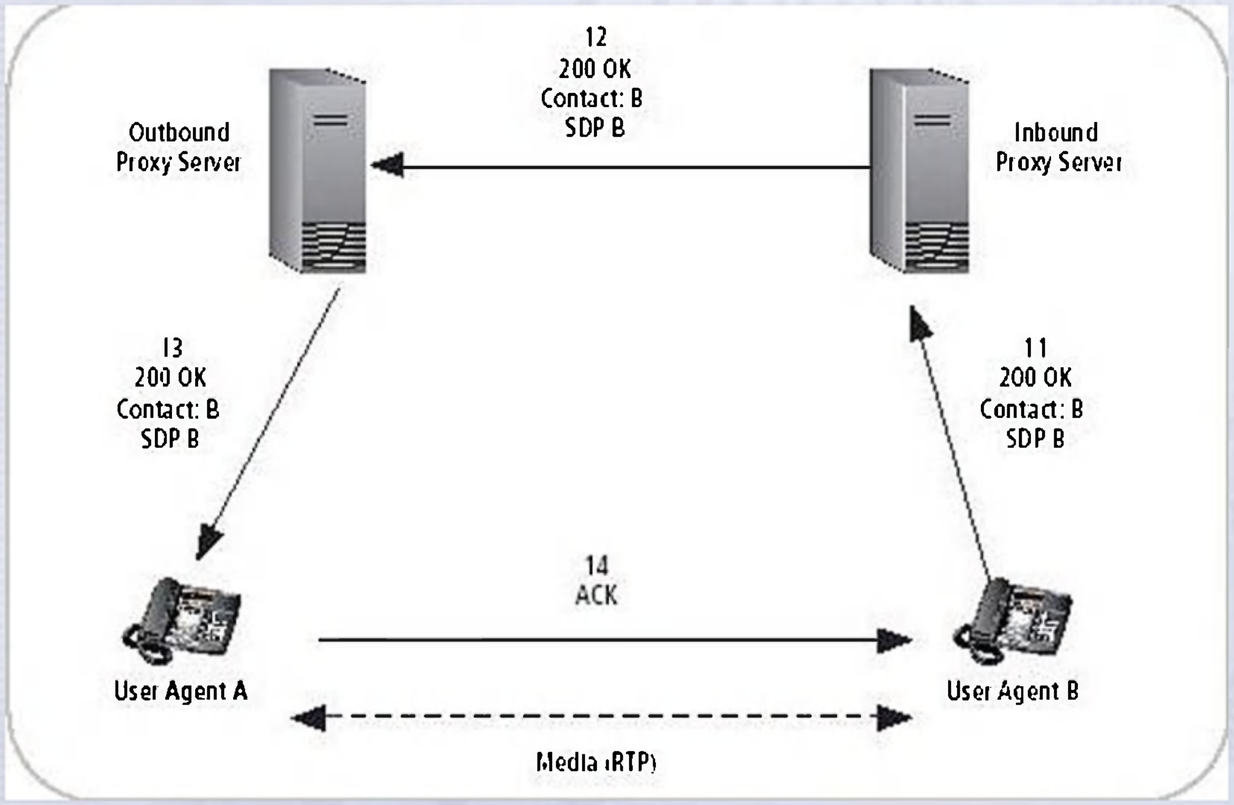
March 2009

Protocols

- Signaling/setup/control
  - SIP (Session Initiation Protocol)
  - H323
  - Skinny
  - Clarent
  - Yahoo proprietary
- Data - voice, fax, video
  - RTP (Real-time Transport Protocol)

The Problem

- Setup and data may take different routes
- Different routes may be collected at different sites
- Routes may change



XKS Solution

1. Local site XKS identifies VOIP setup involving a tasked target
2. Local XKS queries itself for corresponding RTP data
3. If the local query fails, it is passed back to HQS for a cross-site query across the entire XKS network
4. Forward hits to NUCLEON and generate summary reports

XKS Solution

If we find the RTP locally, forward it back across all servers

VoIP box

If we found the RTP locally, forward it back.

XKEYSCORE web Server

Forward back results

F6 HQS

FORNSAT site

SSO site

F6 Site 1

F6 Site 2

queries itself for the RTP on a hit

VOIP Hits

Use this to find data for which…

- There was a dictionary hit on the VOIP signaling (TRAFFICTHIEF, CADENCE, OCTAVE, MARINA, UTT)

  … AND …

- We were able to find the RTP corresponding to the signaling information

VOIP Hits

XKEYSCORE Welcome: oper switch users

Home | Admin | Users | Workflow Central | Search | Results | Statistics | Preferences | Help

Navigation Menu

- Search
  - Classic
  - Common
  - Dictionary Hits
  - File Transfer
  - MultiSearch
  - Network Management
  - Search Wizard
  - UserActivity
  - VoIP
    - Hits
    - Sigdev
  - Wireless

Search: Voip

Query Name:	oper_0
Justification:	
Additional Justification:	
Miranda Number:	
Datetime:	1 Day Start: 2009-03-04 00:00 Stop:
Email:	From
Email:	To
Name:	From
Name:	To
Phone Number:	From
Phone Number:	To
Country Phone Number:	From
Country Phone Number:	To
Tasking Type:	
Tasking Value:	
Dictionary:	
Category:	
Priority:	
Target:	
Description:	
Contacts:	

VOIP Hits - Search Form

- User/target information
  - Email
  - Name
  - Phone number
  - IP address
  - Country code
- Content information
  - Content type (audio, video, image)
  - Control type (SIP, H323, skinny, clarent)
  - Fingerprints - may indicate specific VOIP devices

VOIP Hits - Results

ID	Datetime	Datetime End	Content	From Email	From Name	From Phone#	From Country#	To Email
91	2009-03-03 05:05:28	2009-03-03 05:08:42		d @yahoo	"d "			h @yah
92	2009-03-03 06:41:22	2009-03-03 06:42:33		a @yahoo	"a "			s @yahoo
93	2009-03-03 09:39:09	2009-03-03 09:48:05		b @yahoo	h			s @yahoo
94	2009-03-03 09:36:01	2009-03-03 09:37:09		b @yahoo	h			s @yahoo
95	2009-03-03 10:02:31	2009-03-03 10:02:52		b @yahoo	h			s @yahoo
96	2009-03-03 12:57:27	2009-03-03 12:57:41		o @yahoo	"o "			g @yah
97	2009-03-03 05:05:28	2009-03-03 05:08:42		d @yahoo	"d "			h @ya
98	2009-03-03 06:41:22	2009-03-03 06:42:33		a @yahoo	"a "			s @yahoo
99	2009-03-03 07:50:18	2009-03-03 07:50:18		0092 @ .23		9234	pakistan	6661 @
100	2009-03-03 07:50:18	2009-03-03 08:04:15		0092 @ .23		9234	pakistan	6661 @

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

VOIP Hits - RTP Viewer

tions ▾ Reports ▾ View ▾

State	ID	Datetime	Datetime End	Content	From Er
	91	2009-03-03 05:05:28	2009-03-03 05:08:42		d
	[illegible]	2009-03-03 06:41:22	2009-03-03 06:42:33		a
	93	2009-03-03 09:39:09	2009-03-03 09:48:05		b
	94	2009-03-03 09:36:01	2009-03-03 09:37:09		b
	95	2009-03-03 10:02:31	2009-03-03 10:02:52		b

X-KEYSCORE C2C Session Viewer

Session 1 of 160

Datetime	Case Notation	From IP	To IP	From Port	To Port	Pro
2009-03-03 05:05:28	0000000	.61.149	.11.214	10122	8052	UD

Session | Header (3) | Meta (4)

formatter: AUTO | Send to: Download Session ▾ | Mode: Snippet | Options ▾ | Search Content: Enter text to search

Quick Clicks

- Session
- One-Click Searches
  - Find opposite side of sess
    - .61.149:10122 - .11.214:80
  - Find traffic on
    - .11.214
    - .61.149
  - Find application
    - multimedia/rtp/g729
  - Find fingerprint
    - region/

AUTO FORMATTER: app_id= **multimedia/rtp/g729** Viewer= **RTP** formatter. Info=

Extracting RTP data...

ssrc	# packets	% packets	# bytes	% bytes	min ts	max ts	min seq	max seq
39c4	9733	100.0%	194650	100.0%	1895262977	1896820097	0	65535

payload	# packets	% packets	# bytes	% bytes	min ts	max ts	min seq	max seq
g729	9733	100.0%	194650	100.0%	1895262977	1896820097	0	65535

Number of bad sequence numbers=2

Decoding media...

39c4 g729: raw decoded wav decoded au [194.7 sec] audio processing
combined g729: raw decoded wav decoded au [9.3 sec] audio processing
00000000 g729: raw decoded wav decoded au [0.0 sec] audio processing

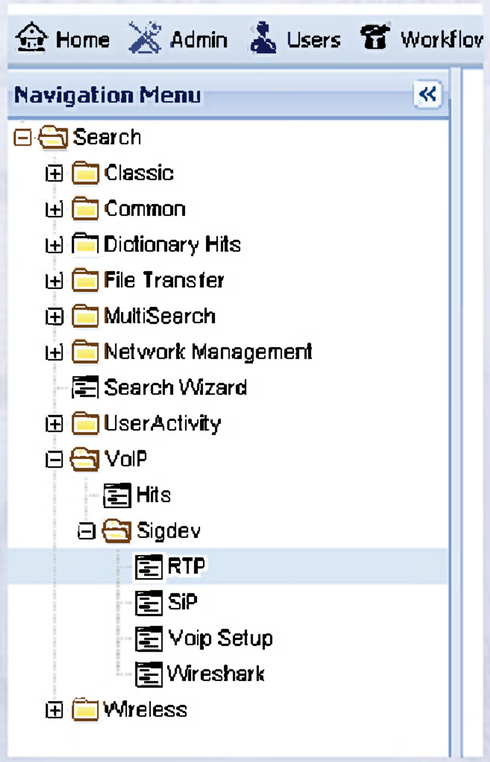
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

VOIP Hits - audio

VOIP Sigdev

Use these search forms to find other VOIP not included in the VOIP Hits

- RTP
- SIP
- VOIP Setup
- Wireshark



Questions?

- Contact the team:
  - xkeyscore@nsa.ic.gov
  - http://xkeyscore.[redacted] (go xkeyscore)

- Primary POCs for VOIP:
  - [redacted]@nsa.ic.gov
  - [redacted]@nsa.ic.gov