REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05/15/2019	Conference Briefing	

4. TITLE AND SUBTITLE
Attacking VoIP and VTC Systems

5a. CONTRACT NUMBER
W56KGU-18-D-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
DeShazo, Patrick G.; Pfannenstiel, Zach; Crow, Brian P.

5d. PROJECT NUMBER
0719N802TE

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730

8. PERFORMING ORGANIZATION REPORT NUMBER
PRS-19-1392

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
United States Army (ACC-APG)

10. SPONSOR/MONITOR'S ACRONYM(S)
ACC-APG

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
Preprint to USAREUR Cyber Summit

14. ABSTRACT
Questions asked:
Does a DISA Command Cyber Readiness Inspection (CCRI) include components such as the call managers for VoIP phones? Or are these “orphan babies” to the process?
Are there Common Vulnerabilities and Exposures (CVEs™) for these systems?
Do open source toolkits exist to hack VoIP/VTC systems?
What precautions can/should be taken?

15. SUBJECT TERMS
Communications Services; Network Security; cybersecurity; data exfiltration; Video Teleconference; VoIP; Voice Over Internet Protocol; VTC

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		27	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

Attacking VoIP and VTC Systems

Patrick DeShazo

deshazo@mitre.org

+1.781.271.2350

Zach Pfannenstiel

Brian Crow

MITRE

Background

- **Asked to look at Voice over Internet Protocol (VoIP) and Video Teleconference (VTC) in a cross-domain environment**
  - Nominally US to non-US Voice and Video
  - All material open source – no classified sources
- **Questions asked:**
  - Does a DISA Command Cyber Readiness Inspection (CCRI) include components such as the call managers for VoIP phones? Or are these "orphan babies" to the process?
  - Are there Common Vulnerabilities and Exposures (CVEs™) for these systems?
  - Do open source toolkits exist to hack VoIP/VTC systems?
  - What precautions can/should be taken?
- **For the purposes of this presentation VoIP == VTC. On an IP network they are fundamentally the same; for VoIP the audio is digitized and put into packets and for VTC the audio and video are combined into packets to transit the IP network.**

MITRE

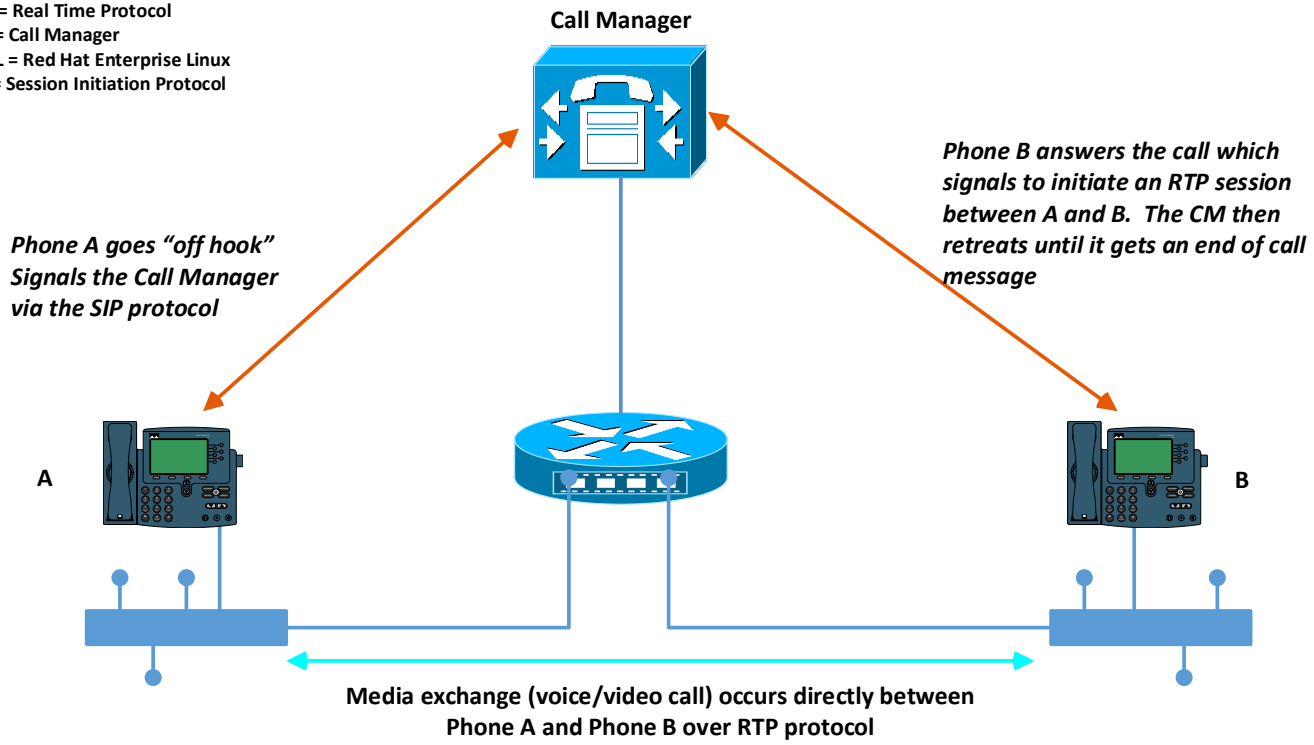
The Technology

MITRE

Call Initiation Process

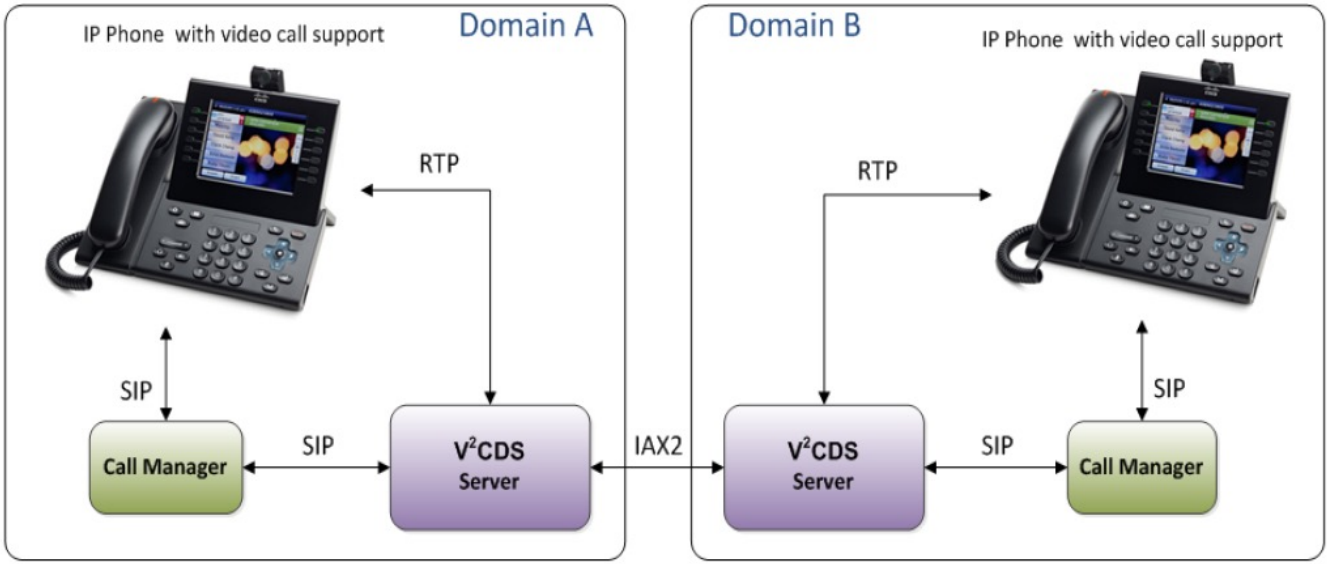
VoIP = Voice over Internet Protocol
RTP = Real Time Protocol
CM = Call Manager
RHEL = Red Hat Enterprise Linux
SIP = Session Initiation Protocol

Call Manager receives call request and using the SIP protocol sends a "ring" signal to Phone B



MITRE

VoIP in a Cross-Domain Environment [1]



IAX2 = Inter-Asterisk eXchange2
RTP = Real Time Protocol
SIP = Session Initiation Protocol
V2CDS = Voice and Video CDS

MITRE

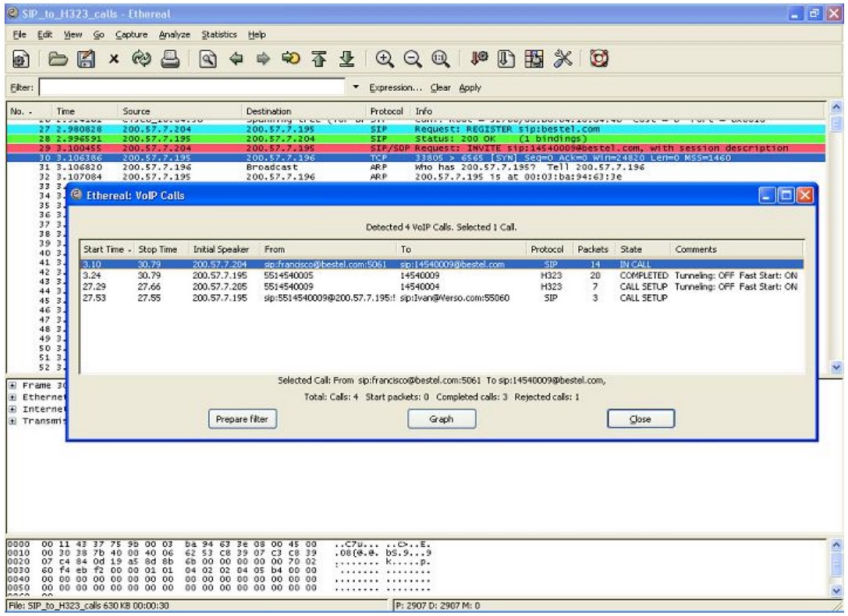
Are there open source Toolkits?

- **Mr.SIP is a tool developed to audit and simulate SIP-based attacks.**
  - Described in an academic journal paper titled "Novel SIP-based DDoS Attacks and Effective Defense Strategies" published in Computers & Security 63 (2016) 29-44 by Elsevier, Science Direct http://sciencedirect.com/science/article/pii/S0167404816300980 [2]
  - UDP is used widely in SIP systems as a transport protocol, so attacks on the target server are implemented by sending the generated attack messages in the network using UDP.
- **SIPRogue -** Allows the user to perform a variety of application level man-in-the-middle attacks.
- **enumiax** – IAX protocol username enumerator (IAX is used between the Asterix call managers) [In Kali Distributions]
- **IAXHangup -** injects a HANGUP control frame into the call
- **Wireshark** – to listen in and capture packets
- **… yes**

Wireshark Packet Example [3]

To try out this dialog, a small capture file containing a VoIP call can be found at SampleCaptures/rtp_example.raw.gz which contains an example H323 call including H225, H245, RTP and RTCP packets.

List VoIP calls



The VoIP calls list shows the following information per call:

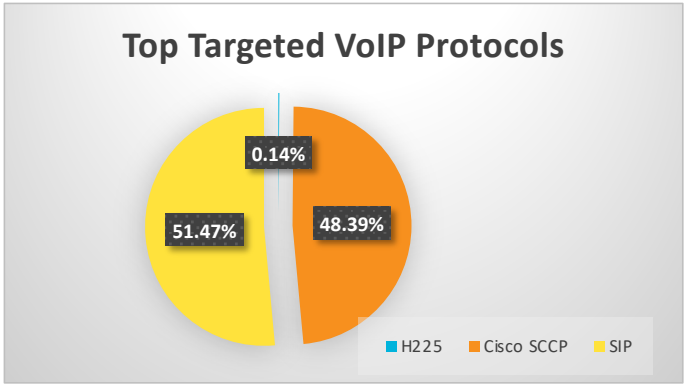
- Start Time: Start time of the call.
- Stop Time: Stop time of the call.
- Initial Speaker: The IP source of the packet that initiated the call.

MITRE

The Threats

MITRE

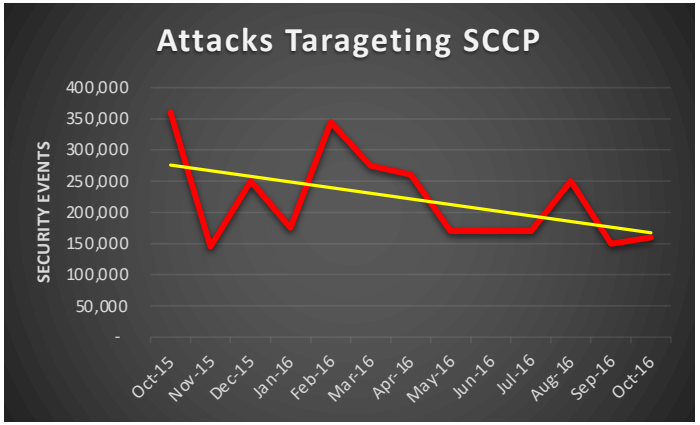
IBM Security Intelligence Statistics [4]

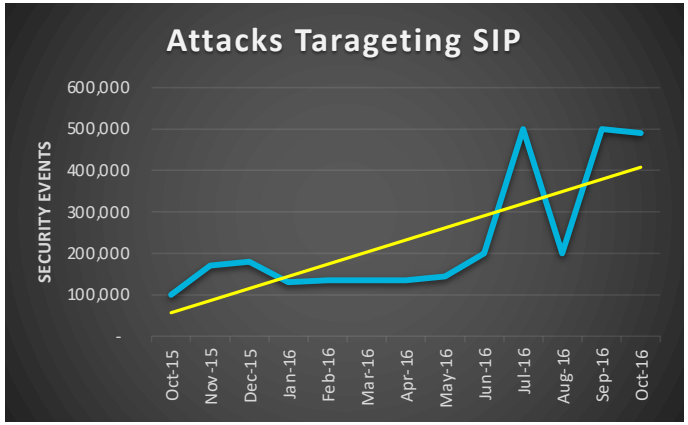


Research from IBM Security Intelligence shows a dramatic increase in attacks targeting the SIP protocol while millions of attacks occur every month on the SCCP protocol. Specially crafted SIP messages that are terminated incorrectly and include invalid characters cause servers to fail. The H225 protocol, which is part of the H.323 protocol suite, accounted for less than 1% of the activity.

(SCCP = Skinny Client Control Protocol; a Cisco protocol for call management)

Source: https://securityintelligence.com/hello-youve-been-compromised-upward-attack-trend-targeting-voip-protocol-sip





MITRE

Attacks are Real and They're Happening Now

- **Attacks coinciding with the meeting between President Donald Trump and North Korean President Kim Jong-Un in June 2018 targeted VoIP phones in Singapore.**
  - The single most attacked port was SIP 5060, receiving 25 times more attacks than the second most attacked port (port 23)
  - The primary attack on SIP originated in Brazil
  - 88% of attacks targeting Singapore on 12 June, 2018 originated from Russia

"Our assumption is that attackers were trying to gain access to insecure phones or perhaps the VoIP server."

-Sara Boddy, F5 Labs

Source: https://www.f5.com/labs/articles/threat-intelligence/russian-attacks-against-singapore-spike-during-trump-kim-summit

MITRE

Top 20 Attacked IoT Ports [5]

(source f5.com/labs [October 2018])

Service	Port	IoT Device Type
SSH	Port 22	*Includes IoT
HTTP	Port 80	Mainly web apps but includes common IoT devices, ICS and gaming consoles
Telnet	Port 23	ALL
SIP	Port 5060	ALL VoIP phones, video conferencing
HTTP_Alt	Port 8080	SOHO routers, smart sprinklers, ICS
TR069	Port 7547	SOHO routers, gateways, CCTV
Applications	Port 8291	SOHO routers
Telnet	Port 2323	ALL
HTTP	Port 81	*Can include IoT: Wificams
SMTP	Port 25	*Can include IoT: Wificams, Game consoles
Rockwell	Port 2222	ICS
HTTP_Alt	Port 8081	DVRs
WSP	Port 9200	WAPs
HTTP_Alt	Port 8090	WebCams
UPnP	Port 52869	Wireless chipsets
Applications	Port 37777	DVRs
UPnP	Port 37215	SOHO Routers
Applications	Port 2332	Cellular gateways
Rockwell	Port 2223	ICS
Secure SIP	Port 5061	VoIP phones, video conferencing

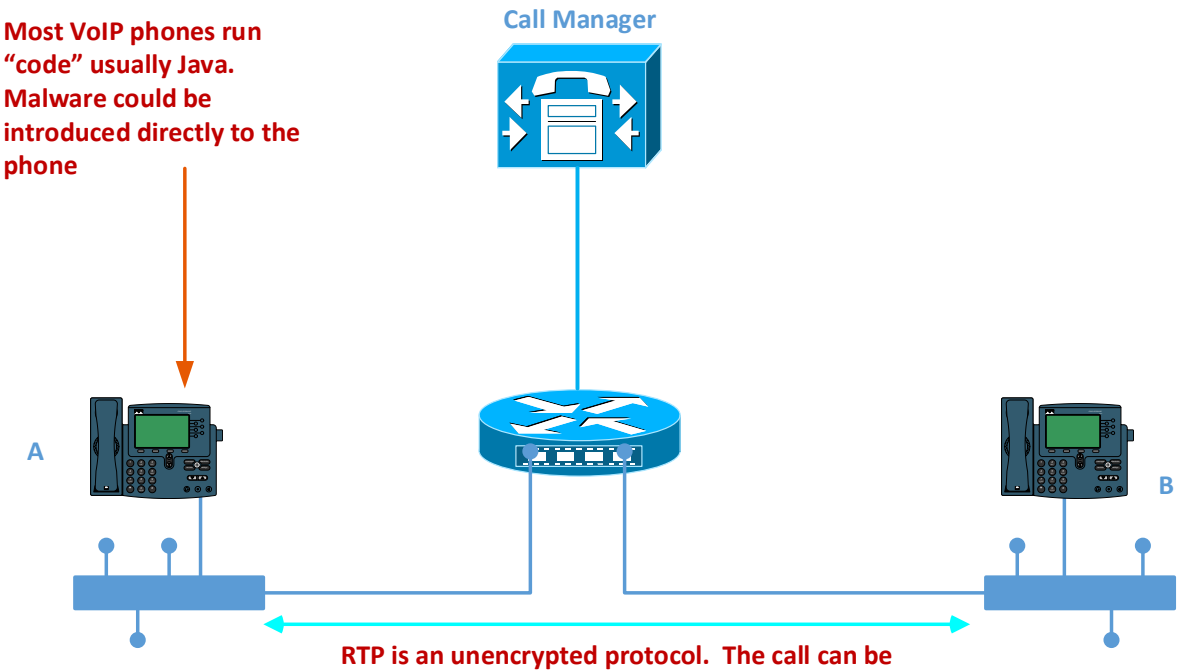
Attacks were collected from the top 20 services and ports commonly used by IoT devices to gain a big-picture view of IoT-targeted attacks around the world. (source f5.com/labs)

MITRE

Potential Attack Points

The CM is just a computer running an off-the-shelf operating system (OS) like RHEL or Windows Server, and is vulnerable to the same OS attacks

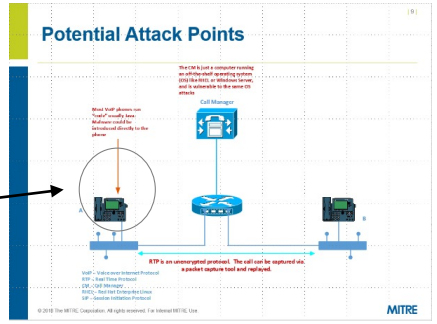
Most VoIP phones run "code" usually Java. Malware could be introduced directly to the phone



RTP is an unencrypted protocol. The call can be captured via a packet capture tool and replayed.

MITRE

Potential Attack – VoIP phone

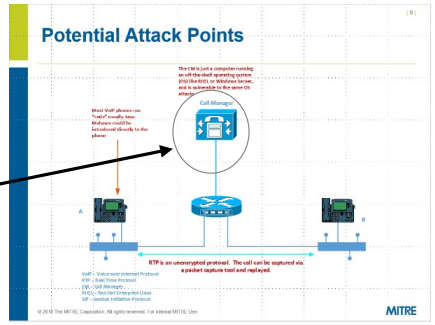


- Cisco patched a critical flaw. The flaw highlighted in https://nvd.nist.gov/vuln/detail/CVE-2018-0341 [6] would allow command injection and remote code execution on IP phones, including higher-end models that have HD video call functionality.

- No exploits have yet been seen in the wild and the requirement for an attacker to be logged into the user interface in order to launch an attack somewhat mitigates the severity of the issue.

MITRE

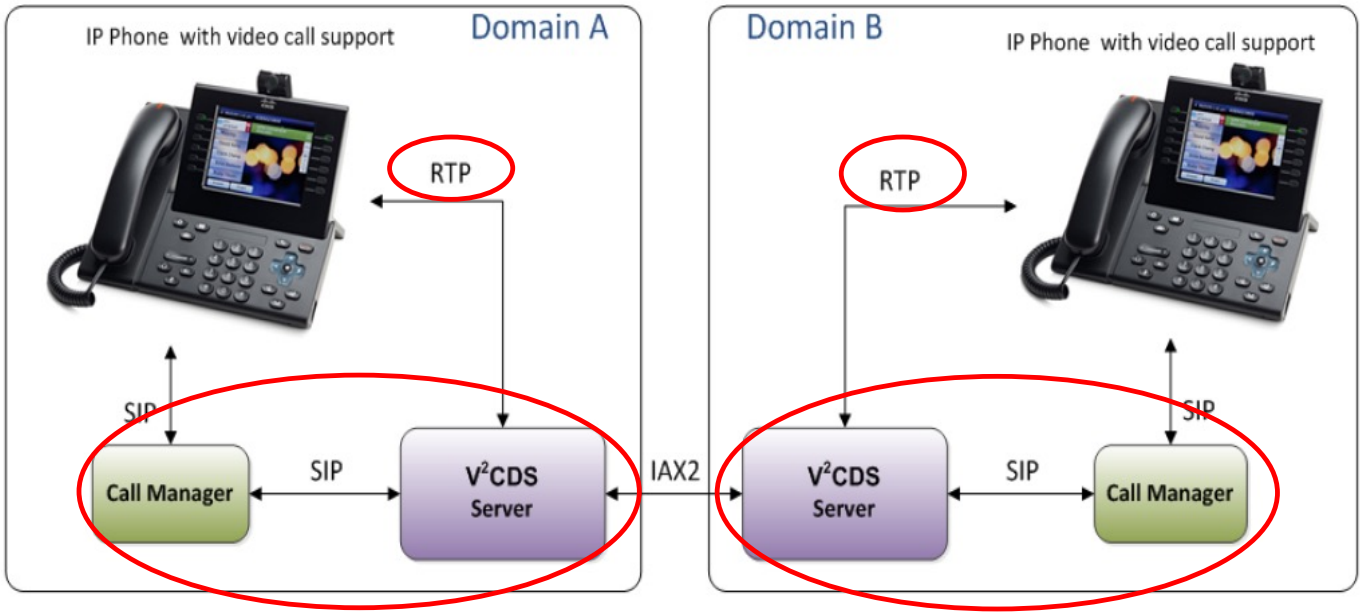
Potential Attack – RHEL



- **RHEL is the OS for many of the industry's call managers**
- **Potential for Remote Root Access**
  - CVE-2016-9604 [7] It was discovered in the Linux kernel before 4.11-rc8 that root can gain direct access to an internal keyring

MITRE

Attack Surface for VoIP in a Cross Domain Environment

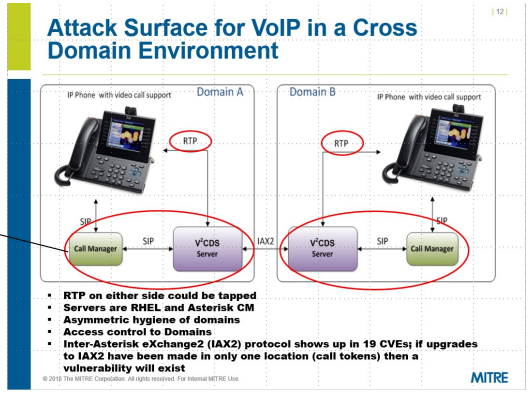


- **RTP on either side could be tapped**
- **CM Servers are RHEL and Asterisk**
- **Asymmetric hygiene of domains**
- **Access control to Domains**
- **Inter-Asterisk eXchange2 (IAX2) protocol shows up in 19 CVEs; if upgrades to IAX2 (call tokens) have not been made in all domains, then a vulnerability will exist. (IAX2 is the protocol between the V2CDS servers in each domain)**

MITRE

Potential Attack – Asterisk

- **Asterisk is the call management software used in Voice and Video Cross Domain Solution (V2CDS)**
- **Asterisk using the default configuration could allow RTP packets to be injected into an ongoing conversation or an adversary to listen to a conversation**
  - If the vulnerability exists on the Asterisk server, the bad guy sends an RTP packet to the server port the real recipient is using and the server will redirect the traffic to the faux recipient
  - This happens because of RTP proxies and the fact that there is no end to end authentication of the traffic
  - CVE-2017-1409 Unauthorized data disclosure (media takeover in the RTP stack) is possible with careful timing by an attacker. The "strictrtp" option in rtp.conf enables a feature of the RTP stack that learns the source address of media for a session and drops any packets that do not originate from the expected address. This option is enabled by default in Asterisk 11 and above. The "nat" and "rtp_symmetric" options (for chan_sip and chan_pjsip, respectively) enable symmetric RTP support in the RTP stack. This uses the source address of incoming media as the target address of any sent media. This option is not enabled by default, but is commonly enabled to handle devices behind NAT. .



MITRE

Asterisk Details (concluded)

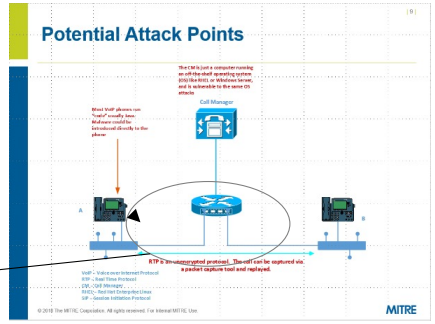
- **For Asterisk, the bug is triggered when the system "is configured with the nat=yes and strictrtp=yes" – and because NAT is pretty much ubiquitous, those are default settings.**
- **What's special about this bug is that the attacker doesn't need to be between the two ends of the conversation: a system with a vulnerable RTP implementation can be persuaded to reflect media streams towards the attacker.**
  - To exploit this issue, an attacker needs to send RTP packets to the Asterisk server on one of the ports allocated to receive RTP. When the target is vulnerable, the RTP proxy responds back to the attacker with RTP packets relayed from the other party. The payload of the RTP packets can then be decoded into audio.
- **Tapping the RTP is the same either side of V2CDS (Eavesdropping)**
  - Like tapping a phone line, you get to hear the whole conversation

The Good News?

- **Access is the attacker's biggest issue**
  - However, US only controls ½ of the connection when talking to a coalition partner

MITRE

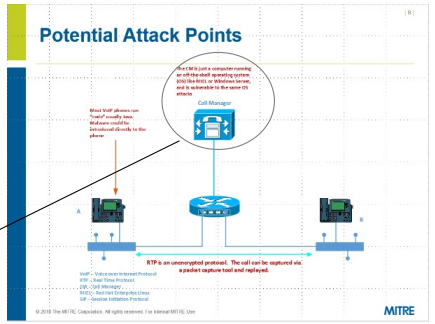
Primary Attacks to VoIP/VTC



- **Denial of Service/Distributed Denial of Service (DoS/DDoS)**
  - A Denial of Service attack is a hacking technique to take down a site or server.
- **Eavesdropping (Passive Attack)**
  - Unlike other attacks which are active in nature, using a passive attack, a hacker just monitors the computer systems and networks to gain some information.
- **SIP Scan and Bruteforce**
  - SIP Scan and Bruteforce breaches occur when SIP-enabled targets are barraged with INVITE, REGISTER and OPTIONS messages. Valid SIP credentials are harvested from the responses to these messages and then used to hijack the device.

MITRE

Primary Attacks to VoIP/VTC



- **Trivial File Transfer Protocol (TFTP) attacks**
  - TFTP is an Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It lacks user authentication.
  - Like the name implies it lacks much in the way of security, however, the VoIP infrastructure systems **rely on TFTP to load configurations into the phones**. Most of the phones have web servers enabled and are programmed in Java—a compromise to the server that loads the configuration file could lead to a VoIP devices' boot files being corrupted.

MITRE

Data Exfiltration via Video

- **Data exfiltration has been seen in the wild using video uploaded to cloud services as a way to move data out of compromised networks without detection. The technique utilizes steganography where encrypted data is encoded into video files and uploaded to untrusted or unmonitored video sharing services.**
  - Technique could be modified to move data from one VTC system's host network to the network of another VTC system.
  - Attackers with access to the data split the data into compressed files of identical sizes, similar to how the RAR archive format transforms a single large archive into several smaller segments. Next, they encrypt this data and embed each compressed file within a video file. In doing so, they make the original data unreadable and further obscure it by hiding it inside a file format that typically has large file sizes; the video files containing stolen data will play normally.
  - In 2014, a Fortune 500 company was hit by an exploit and had sensitive data exfiltrated from their network. The data exfiltration went undetected by perimeter defenses and intrusion detection systems until the company received an alert that revealed multiple duplicate video files had been uploaded from their network to a video sharing website. [8]

While we are on the topic…

- **Multiple vulnerabilities in Cisco WebEx Network Recording Player for Advanced Recording Format Files could allow for arbitrary code execution.**
  - Multiple vulnerabilities in the Cisco WebEx Network Recording Player for Advanced Recording Format (ARF) files could allow an unauthenticated, remote attacker to execute arbitrary code on the system of a targeted user. The WebEx meeting service is a hosted multimedia conferencing solution that is managed and maintained by Cisco WebEx.
  - **WebEx**® for **Government**, is a FedRAMP[SM] Authorized service.

The Mitigations

Mitigations

- **Eavesdropping of the audio/video is the most significant issue primarily because the RTP sessions are not encrypted**
  - **Recommendation:** Put the RTP session in an encrypted tunnel (e.g. IPSEC Tunnel) between the VoIP/VTC system and the V2CDS. This prevents eavesdropping at points between the VTC system and the V2CDS because the RTP traffic would be unrecognizable to the packet sniffing software
- **Video**
  - **Recommendation:** If possible, keep VTC systems off your operational networks.

Hygiene

- **Your network is susceptible to the maladies of whatever it connects to:**
  - We can control our side of the boundary
  - We can (and do) a good job at overall hygiene of the network and servers (CM included)
  - We properly vet the people using our networks and systems
  - We control access to the network physical infrastructure
- **The question to ask yourself is "Do our partners take the same care we do?"**
- **Remember just because the sign says it – how do you know for sure without testing?**

Hygiene is the best mitigation to prevent Call Manager attack

MITRE

Conclusions

- **Questions asked (answered):**
  - Does a DISA Command Cyber Readiness Inspection (CCRI) include components such as the call managers for VoIP phones? Or are these "orphan babies" to the process?
    - **Yes included – not orphans**
  - Are there Common Vulnerabilities and Exposures (CVEs) for these systems?
    - **Yes**
  - Do open source toolkits exist to hack VoIP/VTC systems?
    - **Yes**
  - What precautions can/should be taken?
    - **Hygiene**
    - **Encrypted tunnels between VoIP/VTC systems and the V2CDS**
    - **Keep all VoIP/VTC systems off your operational networks**

References

- **[1]** Retrieved from https://www.tridsys.com/images
- **[2]** Retrieved from http://sciencedirect.com/science/article/pii/S0167404816300980
- **[3]** Retrieved from https://wiki.wireshark.org/VoIP_calls
- **[4]** Https://securityintelligence.com/hello-youve-been-compromised-upward-attack-trend-targeting-voip-protocol-sip.
- **[5]** Retrieved from f5.com/labs
- **[6]** Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2018-0341
- **[7]** Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2016-9604
- **[8]** (2014, November). Retrieved from https://www.tripwire.com/state-of-security/incident-detection/hackers-exfiltrating-data-with-video-steganography-via-cloud-video-services/

MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org