Analysis and Demonstration of a Cisco Call Manager 0-day

October 26/2012

Hugh Ellis, Andrey Markov

Outline

- Quick intro to VoIP
- IP Telephony: target rich
- Case studies of 3 zero-day exploits VoIPshield discovered
  - Application level DoS
  - System level DoS
  - Full system compromise
- Combining zero-days to create a worm
- Zero-day discovery methodology
- Conclusion

Introductions

- VoIPshield: Ottawa-based IP telephony security and fraud prevention specialists since 2005. Enterprise and telco clients.
- Hugh Ellis: Director of Professional Services
- Andrey Markov: Director of Research, Senior Developer, Exploit Development

Disclosure

- Vendor and product names are registered trademarks of their owners.
- Some of the zero day examples presented today were subsequently patched by the vendor; they are used as examples of the broad range of attacks still possible in current industry products.
  - However when made aware of zero day attacks, some of the many vendors we approached did not publish them as known vulnerabilities.

Simplified VoIP Deployment

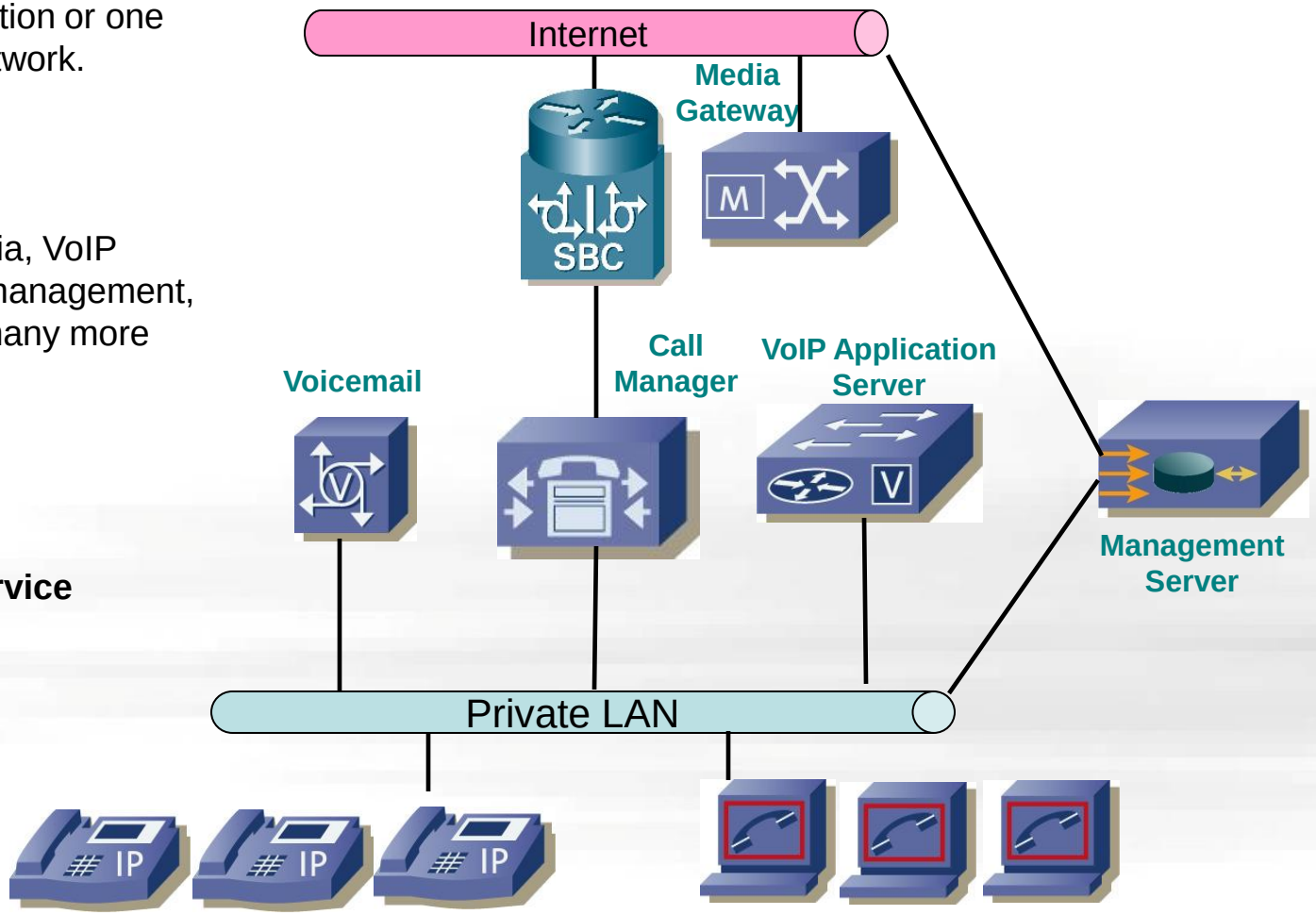
- **Complex** or **extremely complex**

  It is not one application or one system inside your network.

- **Multiple protocols**

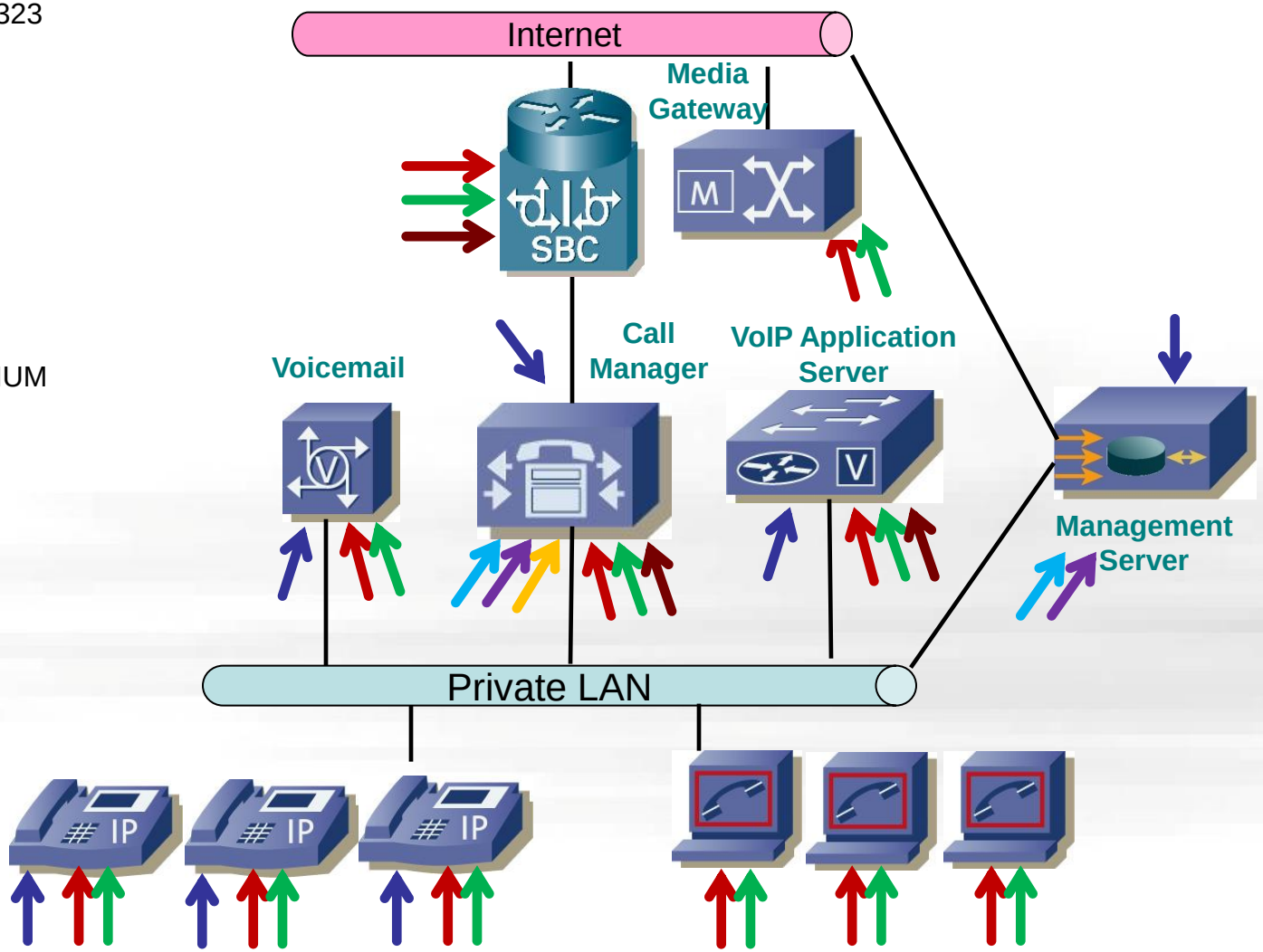
  VoIP signaling, media, VoIP supporting, updates, management, synchronization and many more

- **Dynamic ports**
- **Delays are critical**
- **Mission-critical service**
- **Trusted!**



Attack vectors

- signaling SIP/Skinny/H323
- Media RTP/RTCP
- management HTTP
- supporting FTP
- monitoring
- recovery
- VoIP support STUN/ENUM



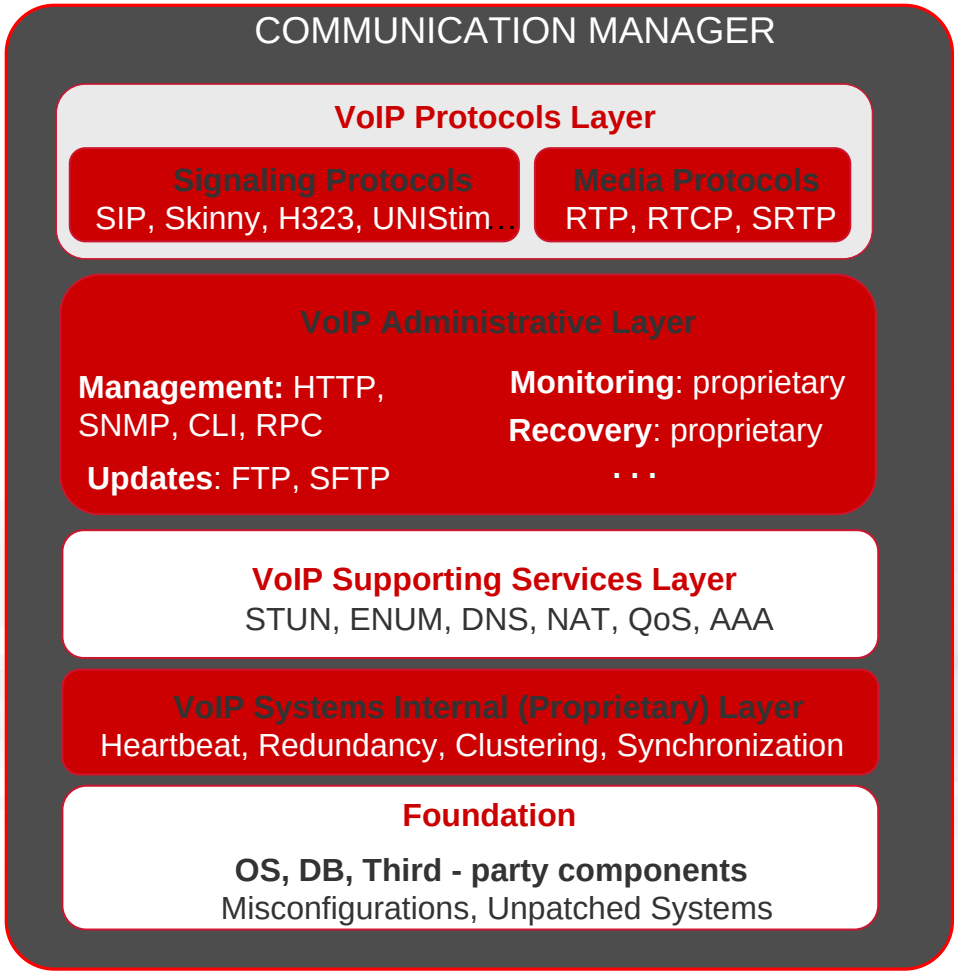
Application/Device Level Attack Vectors

- Tens of networking applications are running on single box representing potential attack vectors

Example:

Cisco Communication Manager has about 30 ports open in default configuration!

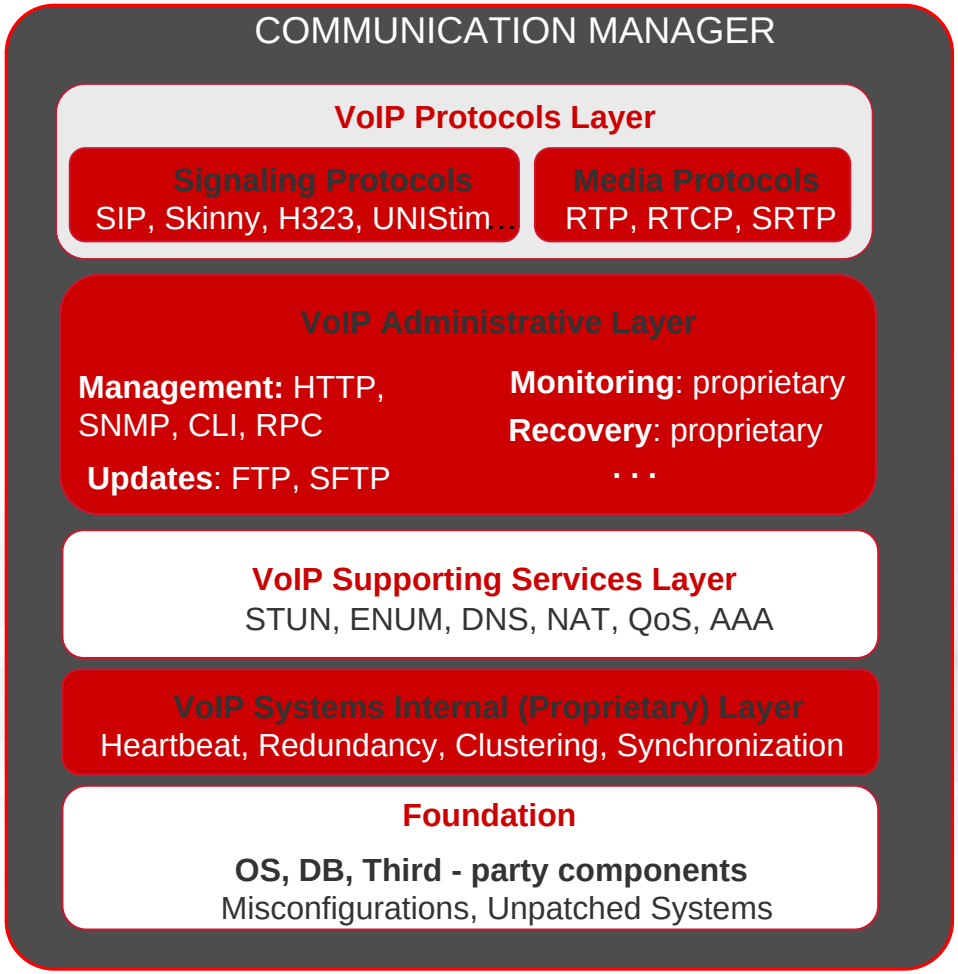
- There is no application without bugs
- It is even more true for delay sensitive applications implemented using lower level languages



Application/Device Level Problems

- buffer overflows
- integer overflows
- command injections
- lack of authorization
- hardcoded passwords
- SQL injections

Any one could provide FULL access to the system or data and remember there are 30 protocols to try!



Cisco Communication Manager Services

Command: netstat – lnp

tcp	0 0.0.0.0:8001	3693/dbmon
tcp	0 192.168.3.81:8002	4517/ccm
tcp	0 192.168.3.81:8003	4522/CTIManager
tcp	0 0.0.0.0:5060	4517/ccm
tcp	0 192.168.3.81:5061	4517/ccm
tcp	**0 0.0.0.0:4040**	**4275/CiscoDRFMaster**
tcp	0 0.0.0.0:32778	3657/java
tcp	0 0.0.0.0:1099	4443/amc
tcp	0 192.168.3.81:1515	3286/python
tcp	0 0.0.0.0:33132	5228/TAPS
tcp	0 0.0.0.0:2444	4526/CTLProvider
tcp	0 192.168.3.81:6060	4247/enStart
tcp	0 0.0.0.0:1101	4523/acserver
tcp	0 0.0.0.0:1102	4523/acserver
tcp	0 0.0.0.0:32879	4352/tracecollectio
tcp	0 0.0.0.0:5007	3657/java
tcp	0 0.0.0.0:111	1299/portmap
tcp	0 192.168.3.81:2000	4517/ccm
tcp	0 0.0.0.0:8080	3657/java
tcp	0 0.0.0.0:32883	4443/amc
tcp	0 0.0.0.0:5555	4248/CiscoLicenseMg
tcp	0 0.0.0.0:22	1366/sshd
tcp	0 192.168.3.81:2551	4524/cef
tcp	0 0.0.0.0:1720	4517/ccm
tcp	0 192.168.3.81:2552	4524/cef
tcp	0 0.0.0.0:7000	4352/tracecollectio
tcp	0 0.0.0.0:9050	5228/TAPS
tcp	0 0.0.0.0:6970	4519/ctftp
tcp	0 192.168.3.81:2555	4442/RisDC
tcp	0 0.0.0.0:8443	3657/java
tcp	0 192.168.3.81:2428	4517/ccm
tcp	0 192.168.3.81:2556	4442/RisDC
tcp	0 0.0.0.0:2748	4522/CTIManager
tcp	0 0.0.0.0:3804	4527/capf
tcp	0 192.168.3.81:1500	3061/oninit
tcp	0 0.0.0.0:7070	4316/certM
udp	0 0.0.0.0:61441	5111/ccmAgt
udp	0 0.0.0.0:32769	4316/certM
udp	0 0.0.0.0:514	1198/syslogd
udp	0 0.0.0.0:32773	4523/acserver
udp	0 0.0.0.0:32774	4523/acserver
udp	0 192.168.3.81:32775	4523/acserver
udp	0 0.0.0.0:32777	4517/ccm
udp	0 0.0.0.0:6162	3678/snmpdm
udp	0 0.0.0.0:3223	4517/ccm
udp	0 0.0.0.0:3224	4523/acserver
udp	0 0.0.0.0:161	3678/snmpdm
udp	0 0.0.0.0:8500	2130/ipsec_mgr
udp	0 0.0.0.0:6969	4519/ctftp
udp	0 192.168.3.81:5060	4517/ccm
udp	0 0.0.0.0:111	1299/portmap
udp	0 192.168.3.81:500	2127/racoon
udp	0 192.168.3.81:2427	4517/ccm
udp	0 192.168.3.81:123	2851/ntpd
udp	0 0.0.0.0:123	2851/ntpd

Sorry I was wrong, it is not 30 it is 55 listening services

Case Studies

- Application level DoS by single RTCP
- System DoS by RTP packet
- Full system compromise by single RTP packet
- VoIP worm

Case studies: RTCP integer overflow

Vendor: Microsoft

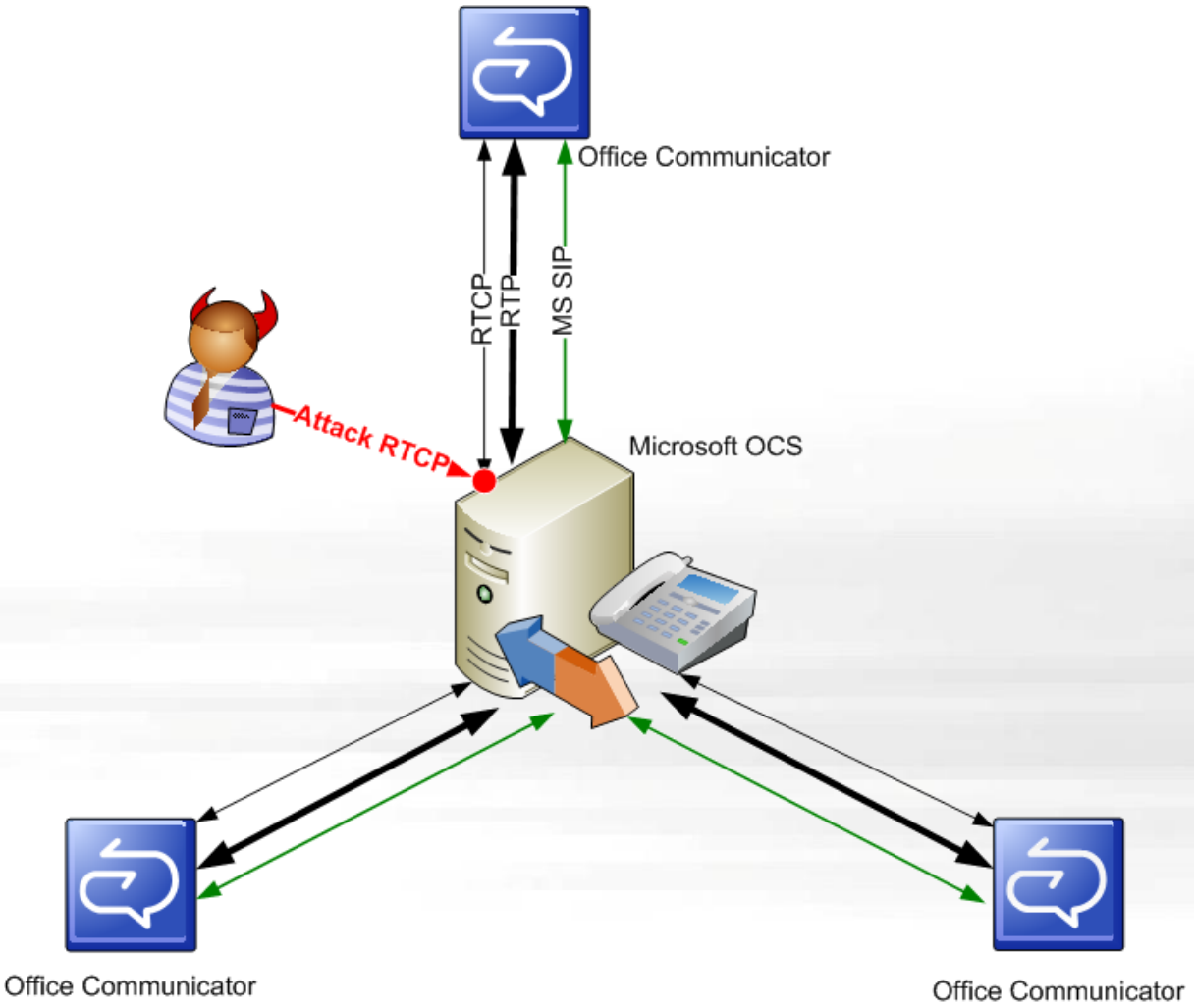
Product: Microsoft OCS, Microsoft Office Communicator

Description: Using a specially crafted RTCP receiver report packet it is possible cause a Denial of Service (DoS) against Microsoft Communicator, Office Communications Server (OCS) and Windows Live Messenger

Impact: permanent DoS of all VoIP deployment

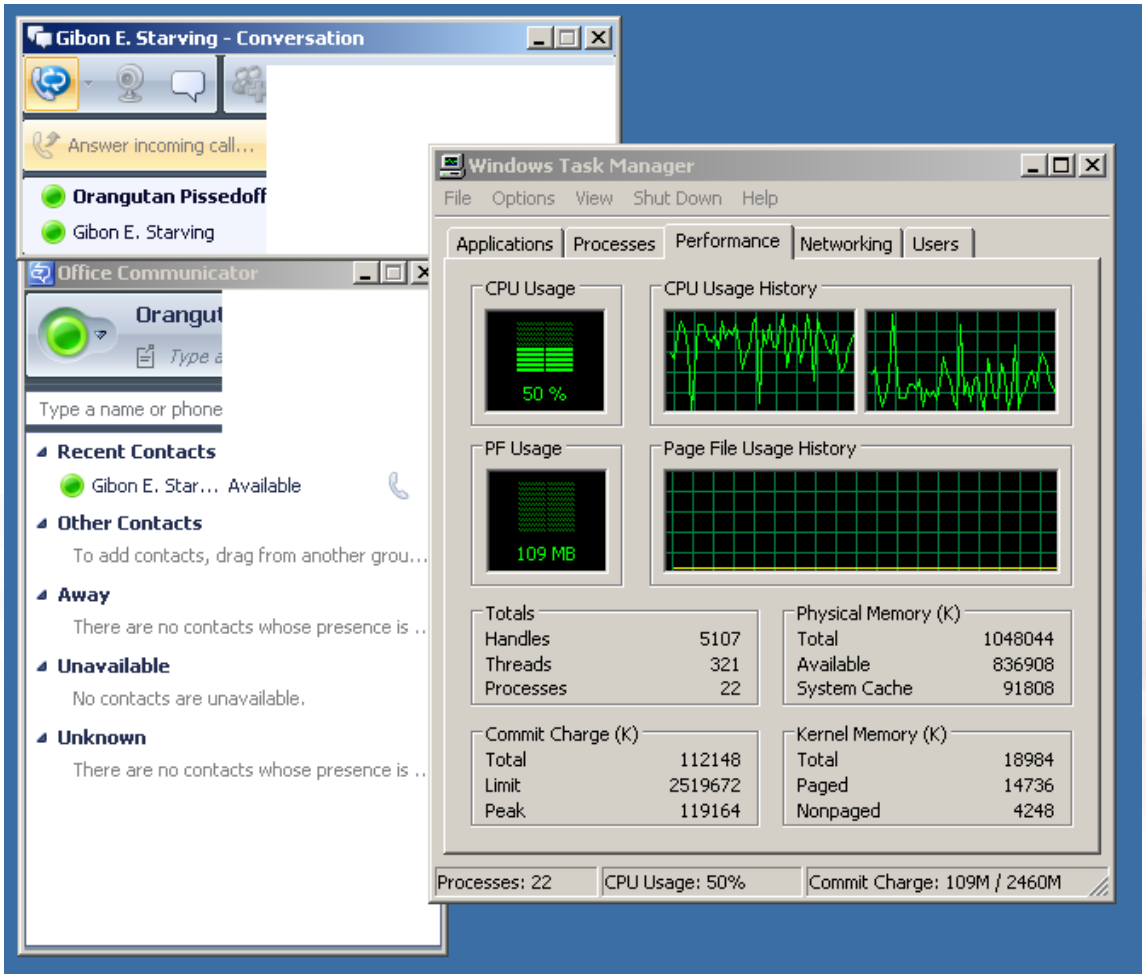
Severity: High

Case studies: RTCP integer overflow



Case studies: RTCP integer overflow

Screen capture below shows what happens to a two core system after single crafted RTCP packet was injected. It was not possible to make a snapshot on single core system because it completely freezes until computer is restarted.



Case studies: RTP Blue Screen of Death

Vendor: Cisco

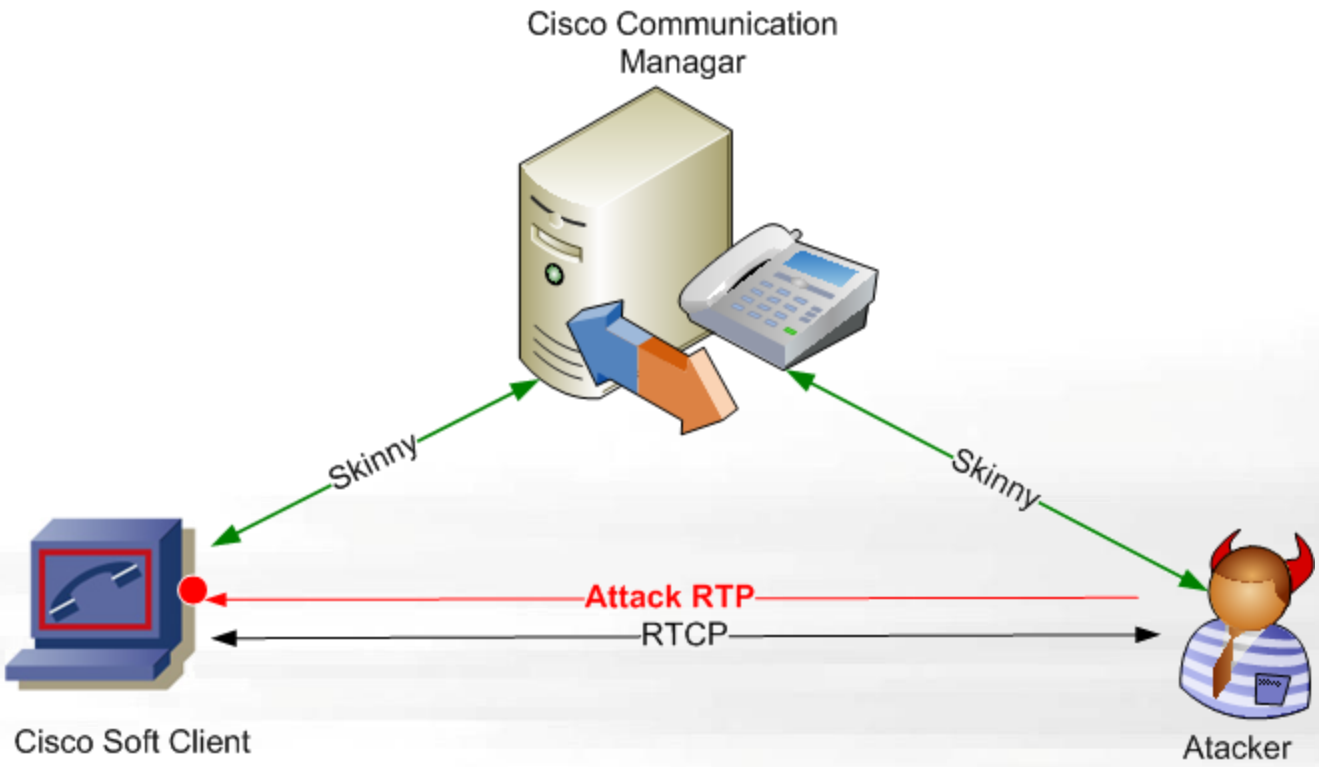
Product: Cisco IP Communicator

Description: Using a specially crafted RTP packet it is possible to cause system permanent DoS by “Windows Blue Screen of Death”

Impact: client system DoS

Severity: High

Case studies: RTP Blue Screen of Death



Case studies: RTP Blue Screen of Death

- O-day

Case studies: remote control by RTP packet

Vendor: Nortel

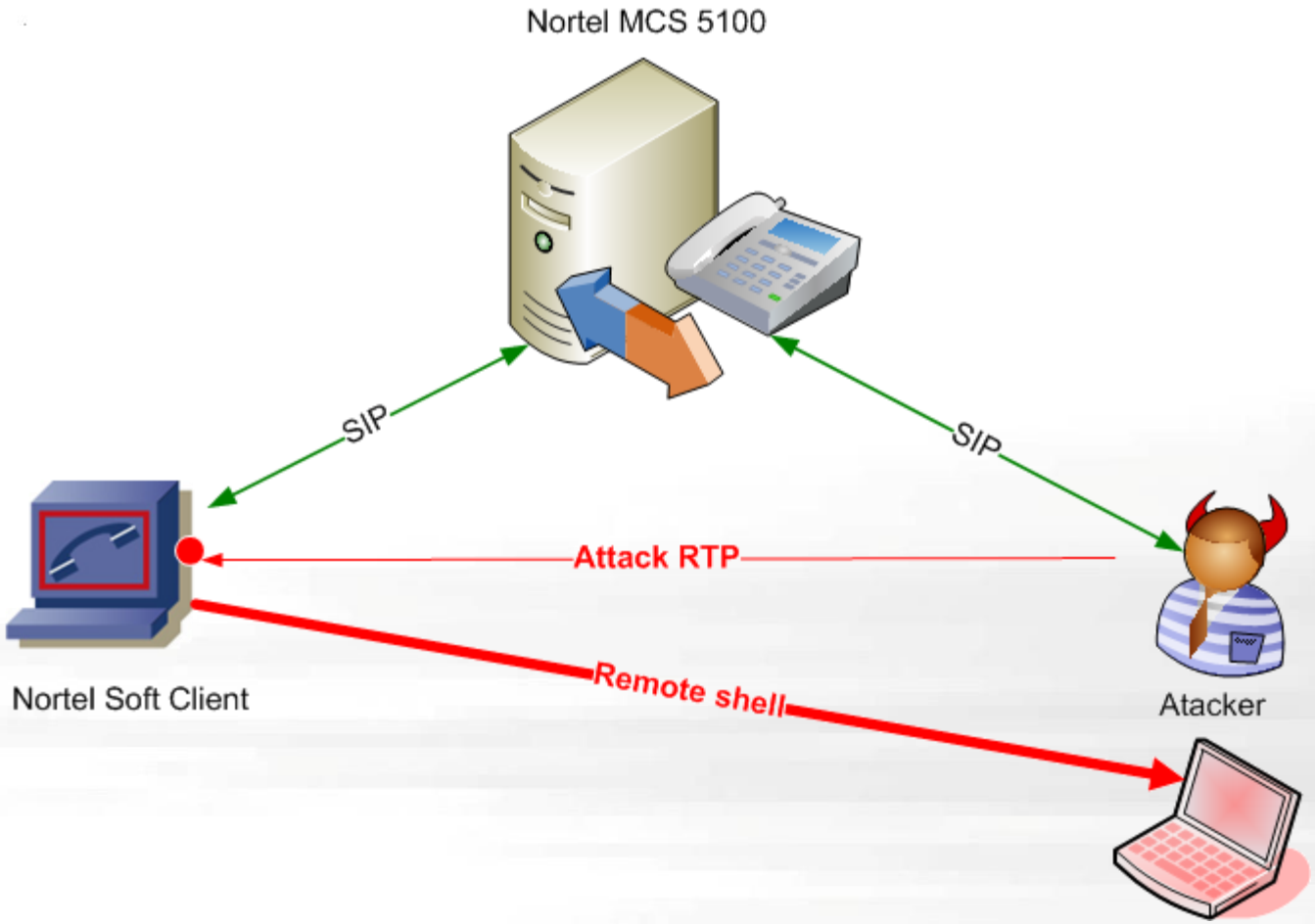
Product: Nortel MCS 5100

Description: Using a specially crafted RTP packet it is possible to cause application buffer overflow with possibility of arbitrary code execution

Impact: client system compromise

Severity: High

Case studies: remote control by RTP packet



Case studies: remote control by RTP packet

- O-day

Case studies: VoIP worm

Vendor: Cisco

Products: Cisco Communication Manager and Cisco IP communicator

Description: combination of several vulnerabilities presented on Cisco Communication Manager and Cisco IP communicator allows worm propagation over VoIP networks

Impact: complete deployment compromise

Severity: High

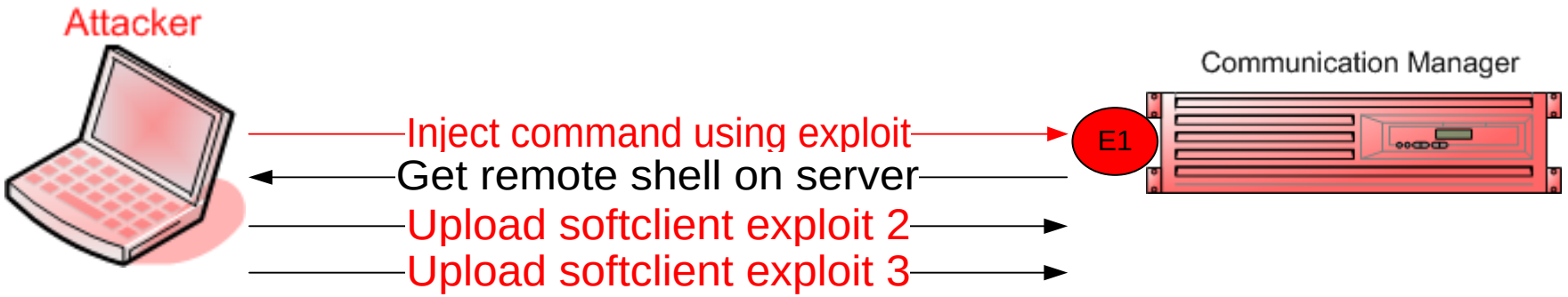
Attack anatomy: attack CM

Soft client

Attack anatomy: attack CM

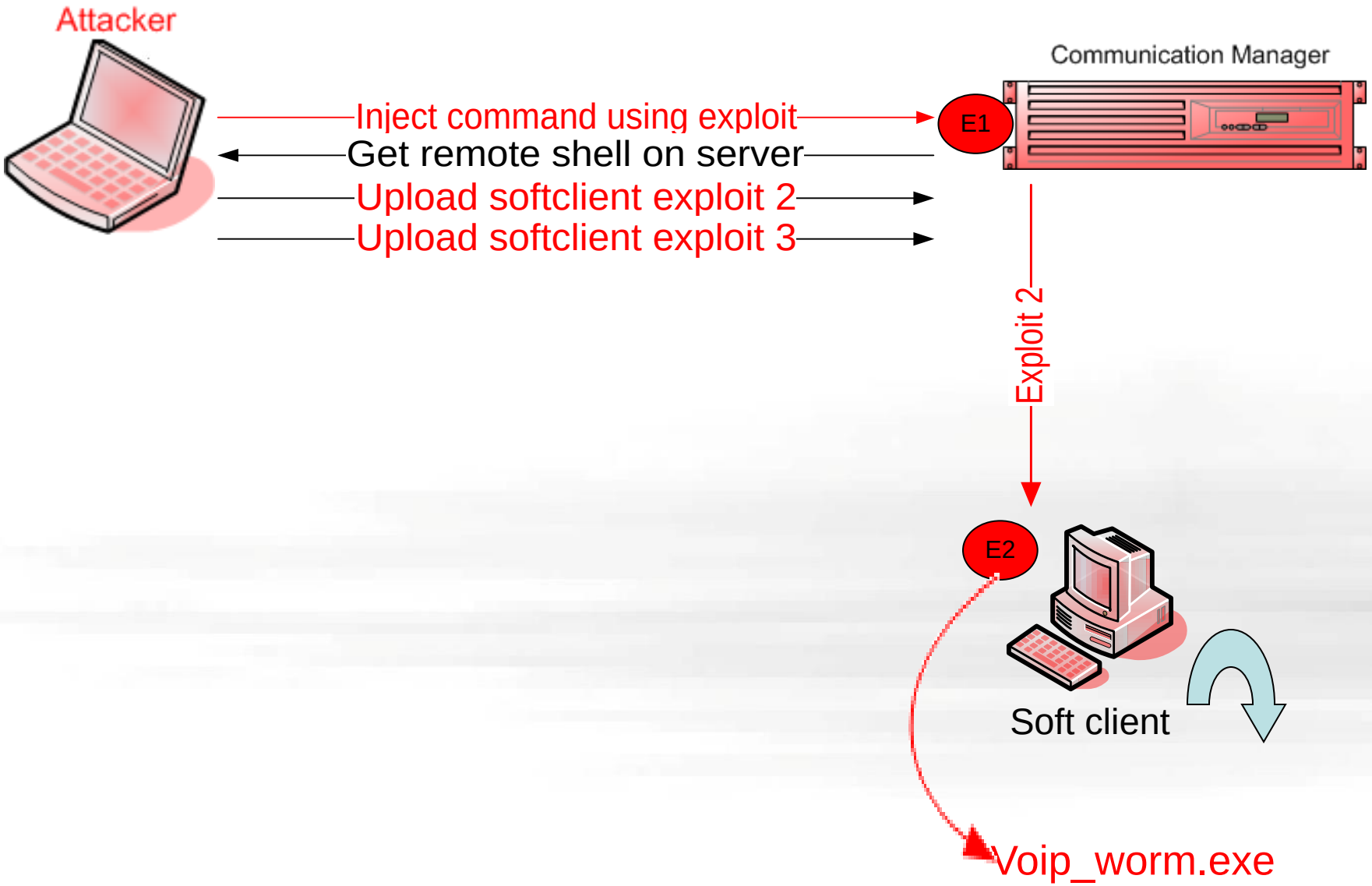
Soft client

Attack anatomy: upload payloads

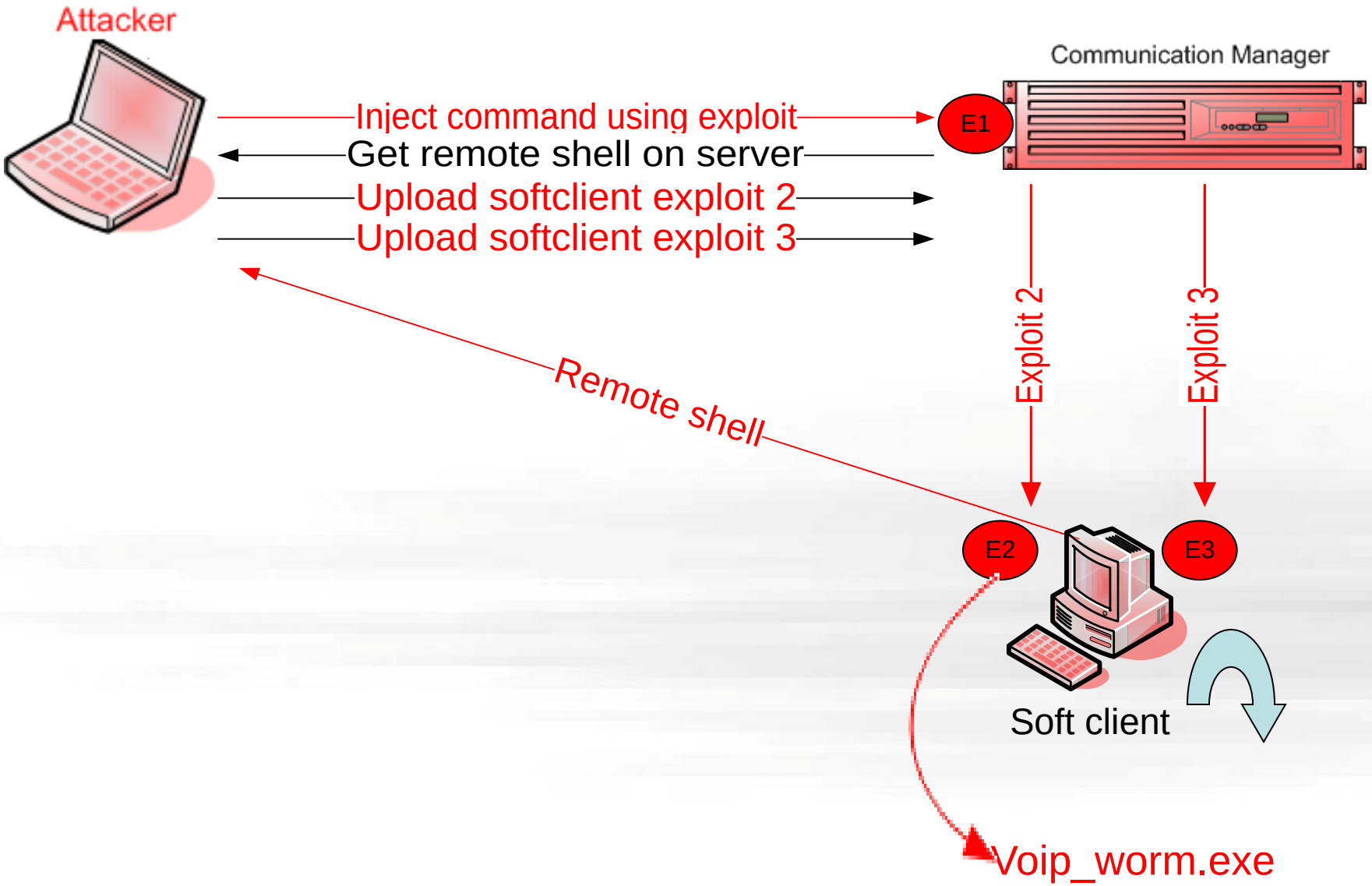


Soft client

Attack anatomy: attack client



Attack anatomy: client remote shell



Attack anatomy: worm spreading

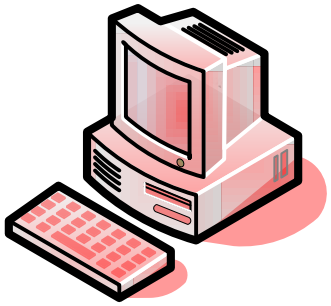
Attacker

=

Soft client

Voip_worm.exe

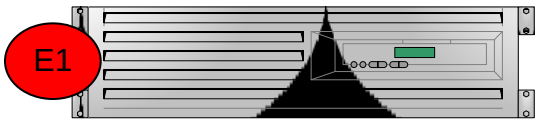
Attack anatomy: worm spreading



Soft client

Inject command using exploit

Communication Manager



Soft client

Case studies: VoIP worm

Hacker-Flash.exe

is 5 minutes recording of how an attacker could penetrate Cisco Communication manager, then launch worm distribution that would use IP Communicator vulnerabilities and finally obtain full control over every VOIP client computer on the LAN.

Vulnerability discovery process

10 minutes live presentation of vulnerability discovery process.

1. Obtain system root access in the lab

2. Select “victim” service

3. Identify service environment

4. Deeper service analysis:

a. Find message handling function

b. Analyze message handler

c. Build exploit

Conclusion

- 31% of installed business lines in North America are VoIP-based - expected to increase to 66.5% by 2015
- IP Telephony soft clients/end-points and infrastructure are target-rich environments; it only takes one …
- Exploits can be combined to compound the damage.
- *Damage is not limited to IP Telephony service*
- Best practices:
  - VA/PenTest/hardening of all components
  - IP Telephony-aware gateways are necessary but not necessarily sufficient to protect VoIP deployments

QUESTIONS