VoIP Cell Phones : Security concerns and Countermeasures

Saurabh R Kulkarni Chinmay Khasnis

Abstract— This paper deals with modern cellular phones that operate on Voice over Internet Protocol, their current development, several Information security risks associated with them and various countermeasures that can be undertaken to prevent data theft/misuse. VoIP is vulnerable to well known traditional modes of attack such as Denial of Service (DoS),Man in the middle (MiTM) etc but also introduces new ones like Toll frauds and 'Vishing'. Having said that, once we understand the associated risks, with proper planning and checks in place, we can utilize the VoIP network without compromising its security or Quality of Service(QoS).

Index Terms— Voice over Internet Protocol (VoIP),SIP, RTP, Mobile Voice over Internet Protocol (mVoIP), Distributed Systems, Network Security, InformationSecurity

1 VOIP AND MVOIP

VoIP stands for Voice over Internet Protocol. VoIP consists of set of standards that have been adopted to facilitate the transfer of voice over the internet. Broadly, VoIP includes several hosts of applications like Instant Messaging,P2P clients, conventional hardphones, softphones etc. Most notable application that utilizes VoIP is Skype. VoIP is primarily based on:

1.1 SIP

Session Initiation Protocol is a text-based protocol that allows two user agents to set up, modify and end a phone call between them. Like HTTP in many regards, it also relies on specific requests and responses for its function.

1.2 RTP

Real Time Protocol is an IETF standard, documented in RFC 3550.RTP provides payload type verification, sequence numbering (a vulnerability for Man in the Middle attack, described later in the paper), time stamping and delivery monitoring features. It generally resides on top of UDP.

mVoIP or mobile VoIP is a relatively new version of the conventional VoIP. mVoIP is specifically designed for VoIP applications over a cell phone. There are several ways a cell phone can be integrated into a VoIP network viz.

1.A mobile device can be converted into a standard SIP client. This then can use mobile's data network to send/receive SIP messages and to manage RTP for the voice part. A pre-requisite for such a device, at minimum, is high speed IP communication. Here VoIP protocols can be used over any high-speed broadband IP capable wireless network such as EVDO rev A, HSDPA, Wi-fi or WiMAX. Such a device is also called as a Wi-fi phone. It's coverage, however, is restricted to the boundaries of adequate Wi-fi signal reception.

2.A mobile device can act as an mVoIP device whenever there is a presence of supported WLAN and as a regular cellular phone when its not. It basically uses a softswitch like gateway to bridge SIP and RTP into the mobile network's SS7 infrastructure .Such a phone can perform dually. It runs on Unlicensed Mobile Access (UMA) that is a kind of generic access network designed to allow VoIP to run over a GSM cell backbone.

Security Vulnerabilities in mVoIP devices can be found in four basic areas:

1.IP infrastructure: This deals with security risks of the non VoIP systems like the WLAN used for IP communication.

2.Underlying Operating System: VoIP endpoints can be infected with VoIP device or Protocol specific viruses.

Certain OSes like WinCE, Symbian OS etc vulnerable in this regard as they are less robust and typically don't run anti-virus software.

3.Configuration: mVoIP device configurations are set by the manufacturer are rarely changed. This can be taken an advantage of by the attacker, who can guess the default parameters, passwords etc set and thereby cause buffer overflows and Denial of Service (DoS) attacks.

4.Applications: Loopholes in various applications can be used by the attacker to eavesdrop, record or modify VoIP calls.

2 SECURITY VULNERABILITIES

Converging voice and data on the same wire introduces a host of security risks. Technically, a VoIP call can be compromised in three basic ways: The call can be eavesdropped on as soon as it leaves the handset, the mVoIP device can be rendered useless by a third party as a DoS attack or the handset itself can be hijacked. Some of the typical attacks are showcased as below:

2. 1 Denial of Service(DoS) attack

DoS poses a greatest risk to any mVoIP server. VoIP applications provide an excellent cover for launching such attacks. This is a way to disrupt or deny a particular service to legitimate users. If a VCP or any IP phone is bombarded with UDP packets of more than 65,534 bytes, the device ceases to work. This type of flooding is pretty easy for an attacker since UDP source addresses can be spoofed easily by employing one of the many such tools found freely on the internet. Similarly ,a large number of TCP SYN floods or ICMP smurf floods can cause equivalent damage. SIP Inviteflood is one type of attack which consumes a lot of system resources and causes outages. The inviteflood tool is one tool that can execute this kind of SIP inviteflood. It generates semi-valid invite messages that are continuously transmitted at a high rate. This can cause dropped calls and several SIP exceptions in the target. Many a softphone has showcased its vulnerability against it. DoS can be also done by means of 'botnets' or a kind of PC's 'zombie army' wherein scores of legitimate machines are employed by the attacker to target one victim. It can be done against a whole WLAN too, where large amount of 802.11 or 802.1x frames are transmitted which can cause a network disconnection thereby compromising all the devices that use that network.

2.2 MiTM attacks

Man in The Middle attacks are caused when an attacker gains an access to the packets sent and received by both the calling parties. Here, an attacker can either passively monitor the chat or can also modify the packets sent or received and undermining their integrity. MiTM is caused when an attacker intercepts RTP messages of the victim. The attacker can conveniently modify the timestamps and sequence numbering so that this interception goes undetected. This sort of attack is usually observed in a poorly secured wireless medium wherein anybody having an access to the WLAN can sniff out packets sent or received by someone using the same WLAN. A good Wi-Fi network is the fundamental pre-requisite of an mVoIP device. Generally wireless LANs employ 802.11b/g protocols with WEP or WPA/WPA2. WEP (Wired Equivalent Privacy) is vulnerable because of relatively short IVs(Initialization vectors) and a key that remains static. Even if WEP is enabled, an attacker can easily sniff and spoof MAC addresses because they appear in a clear text format.WPA on other hand relies on hashing passwords(RC4) which can be brute-forced. Free tools such as Wireshark can be employed to sniff VoIP conversations of the target.

2.3 Toll Frauds and 'Vishing'

Toll frauds are caused when an attacker 'piggybacks' the victim's VoIP connection to make free calls anywhere in the world and bill is traced to the victim. This can happen in a variety of ways. SIP registration hijacking is one of them. SIP consists of a Registrar server ,which processes REGISTER requests from the user and maps his SIP URI to his current location. In this, the attacker intercepts the victim's IP address in this request with his own, thereby gaining an illegal access to his connection. 'Vishing' or 'Phreaking' is a VoIP term for Phishing. In this, a victim can receive a pre-recorded or an IVR message asking for his bank/credit card details. The call is then redirected to the attacker who in turn can gain access to the victim's personal details. This however is not a specific vulnerability of mVoIP but a part of the social engineering attacks.

2.4 Handset Vulnerabilities

mVoIP handset itself can be vulnerable to many security risks. IM applications could be a convenient medium to transfer viruses, worms and other malware onto the instrument. Some older mobile OSes being incapable of handling them may fall prey .A phone can be used by an attacker as a part of a 'botnet' , as described earlier, and be used to carry out illegal activities without the knowledge of the victim. Spamming over Internet telephony or SPIT too works in a similar way. Moreover, traditional Bluetooth attacks like Bluejacking, Blue Snarfing etc. too pose a significant risk.

3 COUNTERMEASURES

3.1 Anti-DoS solutions such as SYN rate limiting, ingress/egress filtering should be implemented. Any VoIP system can be targeted for DoS attack. Stronger authentication policy and removing unwanted network services helps. Although a mass DDoS cannot be completely thwarted, this might give a mVoIP system a fighting chance. Call log monitors should be installed to check SIP Registration hijacking. This again, might not prevent this attack but one can be able to check out its occurrence and possibly trace the attacker.

3.2 VoIP traffic must be totally encrypted. Even though we can't maintain 100% security of traffic on the internet, we can implement a harder encryption algorithm so that even if the data ends up in wrong hands, it is rendered unusable e.g. Skype uses a 256 bit AES encryption when it tries to establish connection with the client server. It then uses two central server key pairs for security of 1536 and 2048 bits respectively. Moreover, all sessions are encrypted by XORing of plaintext and key streams generated by the AES.

3.3 Wi-Fi must be secured by adopting a suitable strategy for MAC address filtering. Firewalling or combination of protocol based measures can also be used to secure a wireless network.

3.4 WLAN typically behaves like a hub-based wired network which enables broadcasts of data thus subsequently, it must be monitored by a security team regularly to check network sniffing, ARP spoofing etc.

3.5 Phone OS must be updated regularly and relevant security patches must be installed. Bluetooth must be switched on only when needed and must be monitored to ensure the connection only with the legitimate party.

3.6 Trusted WLANs should be used. While trying to connect one should make sure that the beaconed SSID is genuine and not the one belonging to a rogue access point. Its recommended to use a VPN application in any case.

3.7 Default configurations provided by the manufacturer can be easily guessed. Hence they must be replaced at the earliest. User login passwords, AMI manager passwords (in case of Asterisk SIP server) must be long and difficult to guess. It is recommended to have an alpha-numeric password with a mixture of special characters in it. This makes brute-forcing difficult.

3.8 Credit card/Bank account details must never be confided in to anyone on the IVR , internet or otherwise.

3.9 mVoIP system must be adequately stress-tested. Fuzzing might be used to check buffer overflows and other such vulnerabilities.

3.10 Strict laws must be enforced on those who indulge in VoIP attacks.

4 THE FUTURE

mVoIP is the future of cellular telephony. Use of VoIP in place of current PSTN and cellular network will greatly reduce the cost and also increase the speed and the quality of service. Despite having some glitches, with proper security implementations in place, an mVoIP network proves out to be a much difficult network to attack as compared to PSTN. Mobile phone companies like T-Mobile in the USA have already begun the manufacture of mVoIP cell phones. It's just a matter of time before mVoIP takes the world by a storm, all the more reason for us to be better prepared for it.

REFERENCES

[1]Mills-Tettey, G.A, 'Mobile Voice Over IP (MVOIP): an application-level protocol for call hand-off in real time applications' in the proceedings of Performance, Computing, and Communications Conference, 2002. 21st IEEE International.

[2] Elleuch, W, 'Sip-Based Protocol for P2P Large-Scale Multiparty VoIP (MVoIP) Conference Support' in the proceedings of Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE

[3]Thomas Porter et al. "Practical VoIP Security" , SPD

[4]David Endler and Mark Collier ,"Hacking Exposed: VoIP", Tata McGraw Hill.

[5]Allen Harper, Jonathan Ness et al. "Gray Hat Hacking",3rd Edition Tata McGraw Hill

[6]Nadeem Unuth, http://voip.about.com/od/security/a/SecuThreats.htm (URL)

[7] AZIZ AHMED, http://aperfectchaos.blogspot.com/2011/03/voip-phone-service-taking-over-cell.html (URL: 2011)

[8] http://en.wikipedia.org/wiki/Mobile_VoIP (URL)

[7]Peter Thermos, http://news.support.veritas.com/connect/de/articles/two-attacks-against-voip (URL)