VoIP Security, an overview of the Threat Landscape

Peter Cox
CTO Borderware Technologies
peter@borderware.com

Abstract

Voice over IP (VoIP) services are, as the name suggests a method of running Voice Telephony over IP networks. The protocols used for VoIP and specifically the Session Initiation Protocol (SIP) also provide a number of other real-time communication services including Video Conferencing, Instant Messaging and Presence services. The latter provide intelligent call routing ensuring improving communications services.

VoIP offers many business benefits, but in the rush to realise these benefits it is easy to forget that VoIP is an IP service and is subject to all the IP network level vulnerabilities and threats that other IP applications such as web and email have faced for the past 10 years or more. In addition, the real-time requirements of VoIP and Video Conferencing and the position of these services as a key-stone in business communication makes VoIP applications uniquely vulnerable to application and content vulnerabilities.

This paper reviews the VoIP threat landscape, highlighting the risks posed by these threats and outlining the security requirements for an effective and robust VoIP implementation.

VoIP Services

Voice-over-IP (VoIP) services continue to attract attention with most enterprise users exploring the benefits of VoIP while both carriers and service providers are starting to offer VoIP based services.

The term VoIP covers a wide range of service offerings including business grade services and peer-to-peer services aimed at consumers and end-users. For businesses, VoIP offers efficiencies and enhanced services by linking voice and data applications and delivering converged communication applications that integrate email, Instant Messaging and telephony. Further integration couples these converged communication applications with back-office database systems making VoIP services a favourite of call centres but equally applicable in other industry sectors.

The benefits of VoIP are obvious and have been extensively documented, but an equally important aspect that receives a lot less attention is security. It is easy to forget that, as its name suggests, VoIP is an IP service and as such is open to all of the security threats that affect services such as web and email. There are also a range of application specific threats that stem from the design of the VoIP protocols and the nature of the application itself. Security is often overlooked because users consider their VoIP systems to be restricted to internal use and therefore isolated from other network and because they see little evidence of threats.

The reality is that a completely isolated VoIP system is a rarity. Any level of voice/data integration and any use of softphones on laptops or PDAs links the VoIP system and the data network where emails and web downloads require external links. There are also pressures for more direct links including the use of trunking services, disaster recovery requirements, the need to extend the VoIP network to roaming users or home workers or simply to be able to make VoIP calls to other organisations. Any of these connections brings VoIP into contact with the hostile world of the Internet.

Unless steps are taken to protect the VoIP infrastructure, it is vulnerable to external threats and attacks that could seriously disrupt the service or lead to complete failure. At very least these threats have the potential to negate the benefits of installing VoIP, but the risks extend to loss of control over the system, loss of call confidentiality and integrity or complete service failure.

The Threat Landscape

The standard phone system has a history extending back more than 100 years. For most of this period the phone system has delivered a relatively secure and mostly trust-worthy service. The phone networks are operated by the various national telecommunications corporations or by large companies who carefully control access to those networks. Issues of the security of these networks and specifically the risk of attack by 3rd parties are rarely considered. For these reasons, the Telecommunications sector has not spawned an

independent security speciality and has nothing like the range of security products and technologies we see in the IP networking sector.

VoIP changes all this by moving telecommunications services to the IP networking realm. The threat landscape in the IP world is radically different. The Internet is the wild-west compared to the sedate and controlled world of telecommunications. While is it not impossible to run a successful VoIP service on a public IP network, we do need to be aware of the threats and to ensure that the appropriate security controls are in place. Moving telephony services from the relatively safety of the telco networks to the challenging world of IP networking requires a different mind-set and a much greater awareness of the risks.

The security threats facing VoIP networks and systems can be categorised in three areas; IP network level threats, application and protocol specific threats and content related threats.

IP Network Level Threats

IP network level threats are faced by all IP applications. For the last 10 or more years the IP security industry has been building Firewalls to protect web, email and other application servers from flooding attacks, malformed packet attacks and a variety of denial-of-service threats. No one would contemplate running a web or email server without adequate security. A VoIP system merits the same level of protection. IP network level threats have the same impact on VoIP systems as on any other IP service ranging from service degradation to loss of service and including the risk of loss of control of the system. In the VoIP world loss of control means someone else getting your calls.

Application and Protocol Specific Threats

The application and protocol specific threat category covers the set of threats that are specific to VoIP applications and to the protocols used to drive these applications. The standard protocol defined by the Internet Engineering Task Force for VoIP and other real-time communication applications is the Session Initiation Protocol (SIP). SIP is implemented either as a primary protocol or as an option in the majority of VoIP systems. Inherent in the design of SIP are a number of potential vulnerabilities that have been demonstrated in many real-world products. These include flooding attacks that flood a VoIP server with registration requests or with bogus calls.

Registration requests are sent whenever a SIP based end-point such as a hardware phone or a soft-phone is powered on or started. The request tells the VoIP application server or IP-PBX that the device is active and ready to receive calls. In most cases the VoIP application server requires that the registering device provides authentication details. A of flood registration requests can swamp a VoIP. Malicious floods can send as many as 30,000 to 40,000 requests per second. Receiving and checking these requests is time consuming and can take up so much system resource that the server that it is

unable to process new calls. The author has tested at least one commercial system that was affected to the point where not only did new calls fail, but existing calls were dropped.

A call flood is a slightly more subtle attack. A call flood rings phones and either plays a short message when the phone is answered or simply hangs up, immediately ringing the same phone again. Both registration floods and call floods are very effective denial of service attacks which are very easy to run on an IP network.

Application specific threats are not limited to denial-of-service attacks. The VoIP protocols can be manipulated to disrupt calls, for example by terminating calls or transferring them. These attacks would be serious for any organisation, but potentially devastating for an industry with a heavy reliance on a reliable phone service such as a call centre.

Content Related Threats

Content related threats target calls directly. Threats in this category include call monitoring and eavesdropping as well as VoIP Spam. The concept of call monitoring is familiar from the PSTN world, but the reality is that it is limited to spy movies and, in most countries, law enforcement authorities backed by appropriate legal authority. It is next to impossible for a malicious attacker or criminal to wire-tap an organisation's phone lines. Moving voice calls to an IP network moves them to an environment where not only is wire-tapping relatively easy, but where there are freely downloadable tools to help you do it.

We are all familiar with email spam, which has grown to a level that threatens the usability of email. In Western Europe and North America at least, the problem of unwanted calls on the regular phone system is also well understood. VoIP means that the technologies used to generate the huge volumes of email spam can be applied to the phone system. We are in the fortunate position that VoIP spam is not a huge problem yet. This is because the number of VoIP endpoints, at least those reachable from the Internet, is still significantly smaller that the number of email boxes. However this number is growing and will soon reach the point where unless pre-emptive action to control the problem, VoIP systems become just as much of a target for spammers as email systems.

Addressing the Threats

VoIP is a specialist application and requires specialist security technologies. Standard firewalls, that are used for protect web and email servers do not offer a complete solution for VoIP. Even so-called *SIP Aware* firewalls offer only a partial solution. While firewalls can address the IP network level threats they are less effective at protecting against application and protocol specific threats and offer no protection against content related threats.

VoIP is a real-time application, packets carrying fragments of conversation must be delivered in near real-time. Any of the attacks outlined above can

seriously disrupt this delivery. These means that the attacks do not even need to succeed in their original aim in order to impact the performance and usability of a VoIP system.

Although one of the benefits of VoIP is that shares a common network transport with email, web, Instant Messaging and a wide range of other applications there are important differences between VoIP and more traditional IP applications. Effective VoIP security requires purposed designed security solutions.

Is this all Hype?

Vendors of security technologies are often accused of over-hyping the threats. This is particularly true in the VoIP sector where critics point to the lack of reports of VoIP security incidents in as evidence of hype. This response is wrong on several levels. Firstly the various VoIP security web sites and mailing lists continue to report both potential security threats and actual examples of successful exploits. Secondly affected organisations are just as reluctant to publicly admit problems with their VoIP network and they are with their email system and web site. Thirdly, ignoring security warnings just because it hasn't happed yet is very much a head in the sand approach. The Internet community learnt this lesson, somewhat painfully, over the last 10 or more years, the VoIP world can avoid this pain by taking the issue of security seriously.

All of the threats outlined in this article are real and in most cases are very easy to demonstrate. A series of white papers available from Borderware Technologies provides more details on each of these threats and discusses the technology response needed to address them.

Peter Cox
CTO International
Borderware Technologies
peter@borderware.com
24th May 2007