

# The IP security

IP, THE ARRIVAL OF VOICE OVER IP, AND REAL-TIME SERVICES ARE ALL FORCING THE INDUSTRY TO REVISIT ITS NETWORK SECURITY SOLUTIONS. AND THERE ARE NO EASY ANSWERS, AS **CAROLINE CHAPPELL** REPORTS

---

**IP network** security has come a long way in the past 10 years. Tools that allow carriers to monitor and analyse traffic patterns in their networks are maturing, enabling operators to detect and deal with threats more quickly. Operators have built up a solid understanding of how to design and build security into IP networks, the policies and processes they need to have in place and the countermeasures they need to deploy.

What has also changed is the support that operators' security organisations are receiving from senior management. "Security groups have a much better chance of being heard than was the case five or six years ago," says Robert Temple, BT's chief security architect. "The incessant tempo of stories in the press means that people don't switch off the second you talk about network security." In fact, Temple suggests that the security community has become a victim of its own success: a whole raft of security-minded legislation, from Sarbanes-Oxley and Basel II, to new laws requiring publication of information security breaches, is piling on the pressure. "In 1999, you could go to the company secretary and tell him he risked receiving a stiff letter about breaching the Data Protection Act if a security measure wasn't put in place. Now if an investment goes wrong, it's 10 years in prison," Temple points out.

"We have better detection tools now than we did two years ago and we feel more prepared and secure," comments Daniel Sjoberg, head of strategy at Teliasonera International Carrier (TSIC). "But the people launching attacks are becoming much more skilled at the same time. We have to make sure we continue to have the mechanisms in place to protect the network." Like Global Crossing, TSIC separates best-effort and real-time traffic in its network so that even if denial of service attacks affect best-effort (public internet) traffic, critical voice services and data services in higher class of service categories remain unaffected.

## **SECURITY ARCHITECTURE**

"Physical separation of the public internet and the IP network used by enterprise customers for security purposes is increasingly the model for next-generation networks," points out Bob Hagen, Global Crossing's director of security architecture and engineering. Connections to each network are physically distinct at the edge – customers access each network via discrete edge devices – but are logically separated in the core using MPLS VPN technology. "From a carrier perspective, the design we have gives us a good compromise between security and cost, since two physically separate networks would not be cost effective. The greatest risk is configuration error, so when we provision customers onto the networks, we use automated tools to help. We do see customers trying to combine devices – if a customer has one egress router for both its inter-branch communications and internet connection and it isn't configured properly, inbound traffic can leak into its internal systems." The weakest link is always the customer premises but here, carriers see the opportunity to spin revenue out of their security capabilities by offering customers managed security services.

However, until very recently, IP networks only carried data traffic and any latency in packet delivery caused by security countermeasures – such as virus scanning, deep packet inspection, email quarantine – has been perfectly acceptable. The arrival of VoIP, at the vanguard of the expected explosion in next-generation real-time services, does change the security game. "Handling VoIP is very different from data," comments Stephen Sargood, VoIP security design architect, Nortel. "There is more



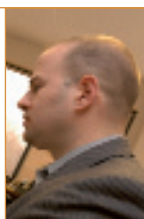
# minefield

complexity involved in the VoIP signalling path because the protocols have more to do and more ports are needed. A lot of intelligence is built into the softswitch which is not typically there in the data world." At the same time, operators can't – yet – put intrusion detection systems and firewalls in the way of VoIP communications because of the effect on latency. "We need to use different techniques," Sargood says. "We need to use network-based intrusion detection systems rather than host-based systems," although he admits that traffic samples will need to be taken off-stream for inspection, so by the time a VoIP-borne attack is detected, it might already have partially succeeded.

And as carriers move into a next-generation network world of multi-vendor equipment supporting multiple services delivered to multiple types of devices, the VoIP security threat will be compounded. "The paradox with next-generation services is that operators want to be the first to market to deliver IMS or

**"As broadly deployed as VoIP is, the industry hasn't figured out standards to protect signalling"**

**BOB HAGEN, DIRECTOR, SECURITY, GLOBAL CROSSING**



IPTV applications, but often the security associated with those solutions is only half-baked," Hagen points out. "As broadly deployed as VoIP is, the industry hasn't figured out standards for protecting signalling." Of course, carriers do use encryption mechanisms to secure the VoIP signalling plane, but these are typically proprietary and vendor-specific. To ensure the secure exchange of inter-carrier VoIP traffic, carriers' VoIP engineering teams have to work closely with one another.

Global Crossing further secures VoIP signalling by carrying it in a logically separate VPN from bearer traffic, but once the call disappears through an enterprise customer's IP PBX, "we lose control of it. We need to get to the point where we have defined standards to ensure security across heterogeneous, multi-vendor, multi-operator environments," Hagen says. "The greatest risks occur when VoIP end-points are accessible to the public internet, or calls are carried on the public internet. Large multinational customers are cognisant of the risks but smaller businesses may jump into VoIP to get the cost benefits without taking the necessary precautions."

## ENTERPRISE VoIP

Temple agrees that while operators have invested in VoIP security, enterprise VoIP is a source of horror stories. However, carriers have only protected the signalling and management parts of their VoIP service, putting in strong authentication between all the network elements involved in hosting a VoIP call, for example, and preventing key participating elements – session border controllers or SIP gateways – from allowing unregistered end-points to join a call. The actual content of the call between two end-points, also referred to as the bearer plane, or media stream, is carried in the clear across their networks. On an IP network, the integrity



Covered regions:

- Russia
- C.I.S.
- East Europe
- Asia
- and other...

*International carrier of voice services*

Best solutions and newest technologies for a voice calls termination.

TDM or VoIP carrier-to-carrier interconnections.

E-mail: [info@camelottc.com](mailto:info@camelottc.com)  
Web: [www.camelottc.com](http://www.camelottc.com)

of the call may be more secure than it would be if it travelled over the public internet, but authentication and confidentiality could be compromised on either network. "Devices in the network are authenticated, not users," Sargood says. "There is a large debate going on in the industry at the moment around secure real time packets (RTP), the transport for voice content. We want to be able to authenticate the RTP (media) stream and

optionally encrypt it."

"Service providers are driving toward the encryption of VoIP signalling to prevent fraud, but individuals using a VoIP application will want to adopt end-point encryption to protect the privacy of their calls," Keith White, security services director, Asia Pacific Lucent, points out. While wholesale operators, such as TSIC, see voice content encryption as a retail customer problem, BT and Global Crossing are actively investigating encryption technologies, including public key infrastructure (PKI) technologies (p30) because they need to understand the impact of such countermeasures on the overall security of their VoIP services.

In the longer term, Graham Starkins, director of internet and security services,



## IP THREATS AND COUNTERMEASURES

**It is** inherently more difficult to attack a TDM network because the protocols are so obscure "and you have to be technically competent to commit toll fraud, for example, in TDM," points out Nortel's Sargood. "With IP, one person needs to be technically capable, but can post his threat on a web page and others can pick it up and launch attacks from anywhere in the world." Wholesale networks per se are not those under attack, according to Lucent's White, "It is the network elements at the end-points which suffer from threats such as denial of service (DoS) attacks and malicious code." The explosion in the number of network end-points, the different types of devices attached and the variety of applications means that "we keep finding new vulnerabilities," White says. "No network is 100% secure – it's a continual measures versus countermeasures battle."

So what are the main threats to IP networks at present? They include:

> **DoS attacks.** "The security issue we're asked to deal with most frequently is stopping traffic carrying out a DoS attack," says TSIC's Sjoberg. "We need to detect this traffic and use 'black hole' filtering to get rid of it." "We have a multinational IP abuse team that monitors and detects such attacks on behalf of our customers and responds to specific instances," says Verizon Business's Starkins. This includes dealing with incidents originating from a Verizon IP address range that has been resold. Automatic monitoring and detection tools are proving effective countermeasures, as well as policies for penalising and removing customers that allow attacks to be launched unchecked. According to Global Crossing's director of information security operations, Jim Lippard, responsible for day-to-day network security management: "We've been keeping statistics on DoS attacks across the public internet and we've seen the number of attacks drop by over 50%. We believe this is in part due to the steps we take to keep abusive customers off our network." However, Starkins says that DoS attacks are becoming more sophisticated as they move from the realm of the student hacker or individual with a grudge against an organisation to organised crime bent on extortion. "These types of attacks focus on removing a company's web presence, preventing online trade or theft of resources," Starkins explains. Since the success of such attacks often depends on weaknesses in the customer's infrastructure, carrier-managed security services can be the answer.

> Closely related to DoS attacks, are email **spam** and its telephony relative, **spit**. "When we emerged from Chapter 11, we had a goal of reducing spam operators on our networks by 75%," Lippard says. At the time, Global Crossing had 40 listings on spam-watching site, Spamhaus.com. Today, it has one. "Our goal this year is to get to zero and then to keep at under five forever," Lippard remarks. "We have seen the benefits of having the right controls built into our contracts and a strong use policy." Spit is likely to grow as a threat as VoIP takes hold. "There are already tools available that can be downloaded to bypass authentication and billing mechanisms in a standard VoIP infrastructure," White points out. The insertion of marketing messages and/or viruses into the VoIP media stream is only a step away. Encryption is a possible solution, but no one knows how it will work yet.

> **Botnets:** "These are collections of compromised machines often controlled by organised crime that launch identity theft, phishing and DoS attacks," Lippard explains. "The vast majority – over 90% – of bots are consumer end-points on DSL or cable modems and botnet controllers seem to be even more narrowly focussed on a small number of high-volume, low-cost web hosting companies. This helps us know what to monitor and what action to take when we find them and we are working on methods to deal with these much more rapidly."

> **Skype:** "Skype looks for sufficient users online to act as softswitches and route calls," says White. "Anyone logged into Skype becomes a supernode and acts as a softswitch, effectively using the resources of his computer or network to switch other third-party calls." Tools exist to spot "parasitic" Skype supernodes and many corporate customers are banning Skype from their organisations. Ironically, voice content carried between Skype end-points is already encrypted and therefore more secure than the in-the-clear media streams transported by carrier VoIP services. ■

Verizon Business, believes it will be possible for operators to screen VoIP content on the fly. "All we need is a clever algorithm and the computing power. I see no reason why, within five years, such algorithms can't sit in backbone network devices. Already today, routers are powerful processing devices taking real-time decisions about packets. Adding virus-scanning capabilities here would not involve much effort. The piece that does need to be addressed is the dynamic updating of algorithms to cope with Day Zero viruses. In the case of emails, we can wait for a day while a virus signature is produced and the email disinfected and released from quarantine, but this would be a problem with voice. There need to be other mechanisms, but we are talking about the bleeding edge of development here."

### MULTI-PURPOSE APPLIANCES

Also on operators' security wishlists is a multi-purpose security appliance. "Vendors

## "It's tempting to buy the latest boxes ... but there's no substitute for the traditional approach"

ROBERT TEMPLE  
CHIEF SECURITY ARCHITECT, BT

want you to have boxes for QoS, bandwidth shaping, deep packet inspection, firewalls and intrusion detection," Temple points out. "Apart from the fact that we don't have an unlimited budget, there is the physical footprint of these devices and finding room for them in our racks. Also, if you have five different appliances, you have the nightmare of five different management systems. We would like to have an industry standard chassis into which we can bolt everyone's best of breed blade, but how close we are to this is anyone's guess." BT has more market clout than many operators and it is pushing suppliers in this direction. However, Temple also stresses that IP security is not all about technology. "Sometimes it's tempting to buy the latest boxes and plug them in but it can be like applying sticking plasters. There's no substitute for the traditional approach of carrying out a risk analysis, identifying threats and building a business case to address them through countermeasures. Good design, architecture, planning and processes are key to the security of data services or real-time services such as VoIP." ■

## PUBLIC KEY INFRASTRUCTURE: IS VoIP THE PROBLEM IT WAS LOOKING FOR?

**Around 10** years ago, small technology start-ups began to promote a cryptographic solution based on public key algorithms that split cryptographic keys into two parts, one of which is held privately and the other is made public. Only by putting the two halves together can a message be decoded and authentication is based on the fact that only the owner of a particular private key could possibly have encrypted a message which its matching public key unlocks. At one point, at the height of the dot com boom, one of these start-ups, Baltimore, gained a market capitalisation that catapulted it into the FTSE 100. However, the public key approach never fulfilled its early promise as an e-business security mechanism. Not only were there performance overheads in using it, but it relied on an infrastructure – the public key infrastructure (PKI) – which itself was based on a new model of trust. Trusted bodies were needed to generate keys (realised as ISO X.509 certificates), to securely deliver them, manage them throughout their lifecycle and revoke them. This trust infrastructure never materialised and still today, the management of public keys – which would run into many millions in a carrier environment – is the large headache facing any organisation that wants to adopt the technology.

Nevertheless, operators are looking again at PKI, and particularly at its applicability to next generation services such as VoIP. "PKI was a technology looking for a solution: VoIP may well be the problem it was looking to solve," comments White. "BT has two main drivers for 21CN: to reduce cost by collapsing networks and to offer new services. The latter is absolutely dependent on the ability to mass customise services. This sets up a requirement for authentication, and for the re-use of authentication across services. Since our customers are likely to have a basket of credentials, we want to be able to accept as many as possible and this is where PKI and federated identity models, like the one promoted by the Liberty Alliance comes in," Temple explains.

"The management of keys that would encrypt [voice content in] the bearer plane would be very complex, but this requirement might grow PKI adoption," Hagen concedes. "The problem would be how to manage keys across carriers. A private PKI for calls within a carrier organisation is one thing, but what happens when we need to peer across other carriers, or in a resale environment where there are multiple tiers of operators? However, we do see encryption as a key enabler for VoIP – otherwise, no matter how intelligent the infrastructure, there is always a possibility of interception."

There are ramifications of voice content encryption for law enforcement and, Starkins points out, for a carrier's ability to check for malicious content, such as viruses or spam. "Personally, I think biometrics is a better way of ensuring authentication," Starkins says. "Clearly, service providers are actively looking at media encryption, but at this point, the cost-benefit isn't there," Sargood says, adding that media encryption is on Nortel's roadmap for 2007. In the meantime, PGP creator, Phil Zimmerman, has come up with Zfone, a cryptographic algorithm for VoIP that requires key exchange between two known users. "It's been generating a lot of interest recently, but we're not sure how it fits into the carrier space," Lippard comments. ■