Are IPv4 Systems Safe from IPv6 Security Threats?

IPv6 is more ubiquitous than we think. It is enabled by default on operating systems and gadgets such as Windows 7, Linux, Android phones and iPhones. In Singapore, businesses are still in the nascent stage of embracing IPv6. This is evidenced by the modest showing when speakers at the 'Future-Proof and Enhance Your Business with IPv6' conference polled the 200-strong audience about adoption rates. The conference, organised by Infocomm Development Authority of Singapore (IDA), was held on 14 March 2014 at Mapletree Business City.

Early adopters of IPv6 include Microsoft: the corporation has been utilising the communications protocol since 2001. Senior Consultant at Microsoft Switzerland Mr Thomas Detzner shared that there was limited support from vendors back in the early days. "IPv6 was deployed using experimental '6bone' address space," he said. Due to poor performance on routing platforms, the protocol was deployed only on dedicated devices.

Over the course of a decade, the capabilities of IPv6 have improved significantly. Today, where Microsoft's infrastructure is concerned, 100% of its WAN and backbone are IPv6-enabled.

IPv6 in Today's World

As Chief Technologist of Hewlett-Packard Network Services Ms Yanick Pouffary put it, the world is already at the dawn of the Internet of Things (IoT). This is a term describing the phenomenon where things are connected to the internet. IoT applications include QR codes and sensors for monitoring air and noise pollution. With the advent of nanosensors, massive amounts of data are collected every day. Oil rigs, for example, collect up to 10 GB of data every 30 minutes.

A unique IP address is assigned to these things so that information can be transferred over networks. With the proliferation of mobile and sensor technologies, the number of available IPv4 addresses has dwindled. Thus, the world enters the age of IPv6.

IPv6 is more than just a solution that promises unlimited address space, said Ms Pouffary. Its operational advantages are many; for one, it enables service automation and frees manpower from ordinary tasks. The potential of IPv6 is also manifold and it can be used in 4G/LTE mobile networks, cloud computing, bring-your-own-device (BYOD) and mobile enterprises.

One novel application, as cited by Distinguished Services Engineer of Cisco Systems Mr Jeff Apcar, is IPv6-based streetlight and traffic signal management. A practical benefit of this technology is that dispatched ambulances now have the ability to turn traffic signals to green as they approach the traffic junction.

Circa 2011, hype surrounding software-defined networking (SDN) started to crank up. This is a trend that Mr Eric Choi, Head of Product Management at Brocade, shared with the audience. SDN is a new approach to networking, in which the network's control is detached from the hardware and then assigned a software application called a controller. Doing so allows administrators to manage components separately and hence more easily. In turn they can cater to changing business requirements in a more timely and efficient fashion.

A question then arises: is SDN IPv6 ready? Mr Choi shared that SDN protocols are still in the midst of development. However, OpenFlow —an enabler of SDN— has released its 1.3 version of the OpenFlow Switch protocol. OFS1.3 does support IPv6 but it is not being deployed yet.

Evidently, IPv6 is used in myriad disciplines and across many industries. The information transmitted to the internet can be sensitive data. Yet, as Executive Vice President of Silver Spring Networks Mr Eric Dresselhuys pointed out, we live in a world where physical security for critical infrastructures does not exist. How then do we ensure that millions of applications, from birth certificates to drivers' licenses, are protected from malicious attacks?

Security Threats Taking on a New Look

Where attacks are concerned, there has been a shift, shared Mr Apcar. In the past, attacks were launched with the sole motive of getting information. In a world that is increasingly powered by technology, hackers are now interested in actuating. They want to manipulate sensors so that they can open doors to key installations.

As technology gets more sophisticated, so do the hackers, an observation Mr Chong Rong Hwa, Senior Malware Researcher at FireEye, shared with the audience. It was not too long ago when malware took the form of executable files and they were usually sent by questionable sources.

These days, hackers use a recognised email account in one's address book to send out viruses. The malware can masquerade as an important PDF needed for a meeting. Hackers are also able to mastermind zero-day attacks, exploiting previously unknown vulnerabilities in a computer application. Even when attacked, antivirus programmes do not raise a red flag as their signatures do not recognise the malware.

Using IPv6 to Target IPv4 Applications

"IPv6 is not a concern as my infrastructure is IPv4-enabled" —this notion, as DBS Bank's Executive Director of Enterprise Architecture, Solution and Engineering Services Mr Tan Choon Boon opined, could not be any further from the truth. "IPv6 is not 'too new' to be attacked nor is it more —or less— secure than IPv4," he shared. Unless a system is explicitly IPv6-disabled, it is still susceptible to IPv6 security threats.

Already, legitimate tools such as Relay6 and 6tunnel allow hackers to use IPv6 systems to send malware to IPv4 systems. As the firewalls in the latter are not configured to recognise IPv6 traffic, the attack goes undetected.

Through a live demo, Mr Matthias Chin, Founder and Director of Banff Cyber Technologies, illustrated in real time how penetration testing (pentest) with IPv6 can lead to a serious security breach if an IPv4 system is unable to detect such an attack.

Using the story of a disgruntled employee, he led the crowd through the thought process of a hacker who wanted to leak customers' contact details and credit card numbers. Only her boss had access to this database. As the attack was an inside job, the hacker was privy to the fact that the security devices were configured to trace only IPv4-related threats.

1) Using a pentest tool for IPv6 network reconnaissance, she was able to derive her boss's IPv6 address, which was a link-local address.
2) A vulnerability scan showed that there was a programme that had yet to be patched.
3) From there, she was able to exploit the vulnerability using the IPv6 address and gain access to the boss's computer, and subsequently, the customer database.
4) After establishing an IPv6 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunneling across the IPv4 network, she was able to upload the sensitive information using FTP.
5) The information went live on an IPv6 internet server.

Best Practices to Preempt IPv6 Security Threats

Through the scenario, the audience saw the importance of proofing IPv4 systems with IPv6 security capabilities. Mr Chin shared the following best practices for businesses to follow: Ensure IPv6 is explicitly disabled on devices that do not require the protocol. This is done via AD GPO or manual DOS commands; Even if IPv6 is not utilised in the organisation, patches must be updated with IPv6-related fixes; Firewalls and intrusion-detection systems must support IPv6 and be enabled to detect any IPv6 activity; IPv6 first-hop security mechanisms on switches must be activated; and IPv6 tunnelling must be disallowed across firewalls.

###