Statement by Ms. Dubhe Beinhorn
Vice President, Juniper Federal Systems
Before the Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
June 2, 2004

Mr. Chairman, Members of the Subcommittee, it is my pleasure to appear before you today to discuss the growing challenge of vulnerability management in information technology systems. You and the Subcommittee have been leaders in raising awareness of the importance of network security in the public and private sector. Your work with the Corporate Information Security Working Group is an important example of your commitment to ensuring a true public-private partnership for solving the very difficult challenge of cybersecurity. At Juniper Networks we take our participation extremely seriously as we do our commitment to you Mr. Chairman in fully supporting active participation by CEO's, working groups and other forums all with an end goal of joint solution determination.

The Challenge

The threats to today's networks continue to grow. Attacks continue to evolve and move from the network to the application level. They are more sophisticated, using new origination points, and come from known and unknown sources. The problem is made worse because of the inability of much of the existing internet infrastructure to identify and then block threats that emerge.

More vulnerabilities are discovered every day, the time from discovery to exploit continues to shrink, and the pressure placed on network administrators to remediate these vulnerabilities in a timely fashion continue to grow. Much like bailing water out of a boat that continues to spring leaks, patch management is only a short term fix and does nothing to solve the root cause of network insecurity.

Part of the challenge is the simple fact that the internet is not just one network; it is multiple networks connected together. As such, it was never designed with security in mind. Its greatest strength – widespread connectivity as low cost – is also one of its greatest weaknesses. With low cost comes diminished value, unreliability and a lack of security. Each network has its own security policy and, as we all know, network security is only as strong as the weakest link. At the moment only isolated networks can guarantee infrastructure and data security from outside attacks. However isolated networks work against net-centric Enterprise Services. Additionally, isolated networks do not address the problem of insider attacks and are cost-prohibitive for many government and enterprise networks.

Most people are focused on securing the enterprise. There is, however, another critical element, securing the fabric of cyberspace beyond the enterprise firewalls, the space between the enterprises. President Bush in his National Strategy to Secure Cyberspace called for "securing the mechanisms of the internet."   Right now all packets travel over the same public internet, with the same priority and the same security. So, part of the challenge is recognition that “all packets are not created equal” and we must devise a security approach that assigns the right level of security for each packet that flows from its originator through the public network and to its destination.   This is the challenge.

The Near Term Response - Strategies

First and foremost, Service providers and networking companies (of both private and public infrastructure) play a critical role in alleviating the problem. All companies should be encouraged by congressional leaders to share information. Specifically, public and private industry forums should focus on pre and post attack vulnerabilities as well as real time attack isolation and prevention. All internet stakeholders need to develop a set of industry best practices based on the information communicated by all forums. As an example such collaboration may yield mechanisms, to prevent users masquerading as other users and denying access in the first place. Techniques for securing the network control plane so that false routes may not be hijacked or injected thus preventing man in the middle attacks. And finally use of automated tools to conduct assessments and on-going security audits to help identify vulnerabilities on the network and unusual activity. These tools can also be part of a larger effort aimed at creating a culture within companies as well as government agencies of security awareness and responsibility.

These industry best practices allow for malicious traffic to be identified, blocked and prevented from spreading. They give us the ability to quickly identify and "quarantine" hot spots and reduce the spread of viruses and the rising cost to businesses and consumers from such attacks.

The public network, cannot stand alone in the protection of businesses, institutions and citizens, security must also be established at multiple levels including application , device, the department levels. And these security measures must be able to communicate with each other, and with the network, to form a level of protection that is greater than the sum of its parts.

Networks must intelligently interact with the user and the application so that the level of trust can be established at the beginning of each network transaction. Much work has been done by companies participating in the Web Services movement and standards development effort. Local and wide area networks must leverage this work to extend the concept of trust agents and user federations to the network itself.

The work is underway, Juniper Networks and 18 other industry leaders are working together to build on these standards to create networks that can deliver a specified level of security, performance and reliability. The group calls itself the Infranet Industry Council. It seeks to put existing technologies and standards to work, building on them when necessary, to form an underlying communications infrastructure that provides the best attributes of public and private networks. An Infranet is a *selectively-open* network that combines the reach and positive economics of the public network with the assured performance and security of a private network, enabling a packet infrastructure to support all communications. Infranets can be built and operated by service providers, agencies and businesses….and can be securely interconnected with each other…..for the purpose of giving users an on-demand network appropriately tuned to their unique security and quality requirements. At the appropriate time we would welcome the opportunity to explain this initiative further.

Over the longer term, vulnerability management must be addressed by all internet community members to design more secure systems and networks with a “zero trust tolerance” approach. What that means is there should be absolute distrust of outsiders and insiders. We should recognize both as equal threats and not give greater weight to one over the other. Building networks that trust no one is a far better approach to managing the threats and will ensure a higher level of security.

Conclusion

Mr. Chairman, Juniper Network's approach to network security is based on ensuring reliability, security and quality throughout a network.   This commitment and our activities with public infrastructure providers, with the defense and intelligence community, enables us to do our part to better secure our critical networks and play an active role as a member in the Cyber Security Industry Alliance. In today's world it is no longer about competing it's about collaborating. With your help Mr. Chairman, the government initiatives to guide industry, vendors and all stakeholders will succeed in true joint development of a worldwide internet capable of meeting its mission regardless of malicious intent, unforeseen failure or mis-adventure. On behalf of Juniper Networks and our CEO, Scott Kriens, thank you for the opportunity to speak before you today. I look forward to answering your questions.