Baseline security: Leading the industry toward a standard foundation for infrastructure security

by Mike Lee

Nortel was one of the first vendors to develop a consistent set of baseline security requirements and best practices. First used in its own product portfolios, these baseline requirements today form the foundation for the security baseline standards being defined by both national and international standards bodies, including the Alliance for Telecommunications Industry Solutions (ATIS) and the International Telecommunication Union (ITU-T). These standards are key to the creation of a more resilient, secure, and trusted network environment.

Several years ago, when service providers and enterprises began converging their networks onto single IP-based infrastructures, Nortel – from its vantage point as a pioneer and leader in building secure, reliable networks – foresaw the need for an industry-wide set of baseline security requirements. Anticipating the coming challenges for network security, Nortel set out to develop a common and consistent set of security features that would form the "must-have" suite of protective measures and best practices needed to provide a solid security foundation for future next-generation, converged networks.

Nortel began by developing a common baseline of security requirements for its own products, and then championed the adoption of these requirements by the industry, through industry forums, customer engagements, and standards development organizations. While the standards focus has been on public networks, the principles and techniques can also be applied to private or enterprise networks.

Nortel took the view that sharing its basic infrastructure security strategy with the industry made good business sense, for several reasons.

For one, a standardized security baseline addresses the network complexity that was developing as operators and enterprises responded to growing network security concerns with differing but related requirements. To illustrate, one request for proposal (RFP) issued not long ago by a major North American wireline service provider listed more than 2,000 security requirements – a significant change from what previously might have been a handful of items. Moreover, different operators were adopting different approaches to addressing various security issues. While similar in intent, their security choices differ vastly in implementation and have introduced a host of challenges for both providers and vendors.

Second, providers face significant cost and deployment challenges in having to integrate inconsistent and often incompatible security feature sets from multiple vendors, which ironically exposes customer networks to even greater security vulnerabilities. For example, if one piece of equipment uses IPsec (Internet Protocol Security) exclusively as its encryption protocol and another piece of equipment relies on the Transport Layer Security (TLS) protocol, the two boxes won't be able to "talk," and therefore would be unable to provide seamless encryption – even though the underlying encryption technologies used by both protocols are equally as strong. Similarly, two different authentication technologies, such as RADIUS and Kerberos, while equally good, are incompatible.

Third, a standardized security baseline would address the challenges that vendors face in having to "cover the waterfront" and support all customer requirements, which is difficult and costly to do because it requires manufacturers to develop a super-set of security technologies across all products, with the added burden of keeping up with the rapid pace of new attacks and security bulletins. Additionally, a security baseline would facilitate the generation of inter-carrier interconnection security agreements.

Nortel knew that a common set of security specifications would enable service providers to more easily procure and build secure infrastructures comprising multiple vendor platforms, while enabling vendors to lower the complexity and costs of development.

Different traffic plane requirements

As a starting point, Nortel defined a three-pronged approach to developing baseline security standards. First, it would tackle the new security needs of network management (management plane issues), followed by the needs of signaling (signaling plane issues), and then of user traffic (media plane issues).

Indeed, as networks have converged on IP-centric infrastructures, these three planes are no longer separated physically, as they were in traditional telecommunications networks.

In the past, protecting the overall network from intrusion by hackers and other threats was relatively straightforward, because purpose-specific traffic was separated onto different and isolated elements in the network. Operations, administration, and maintenance (OAM) traffic, for instance, traveled over a separate management plane in the network on point-to-point connections that could be accessed only by legitimate operators in the customers' network operations centers (NOCs). Similarly, signaling traffic took a separate communications path through the network via distinct signaling network elements, such as CCS7 (Common Channel Signaling System 7) elements. The general public, then, had access only to user traffic and was unable to penetrate either the management or signaling planes of the network (Figure 1).

On the whole, past telecommunications networks were considered relatively safe from widespread malicious activity. When the comparatively rare intrusion or malicious act did occur, it was often in the form of an error on the part of operators, or it was a typical type of fraudulent activity – such as an attempt to change service profiles or alter billing records – and was easily detected.

By contrast, in next-generation converged networks, all packet types are sent over common network elements. Because different traffic types are no longer separated, such mechanisms as encryption are now needed to virtually separate and protect the traffic, in order to provide even the most basic security, which involves ensuring data confidentiality, integrity, authentication, authorization, and auditability – known in the industry by the mnemonic 'CIAAA.'

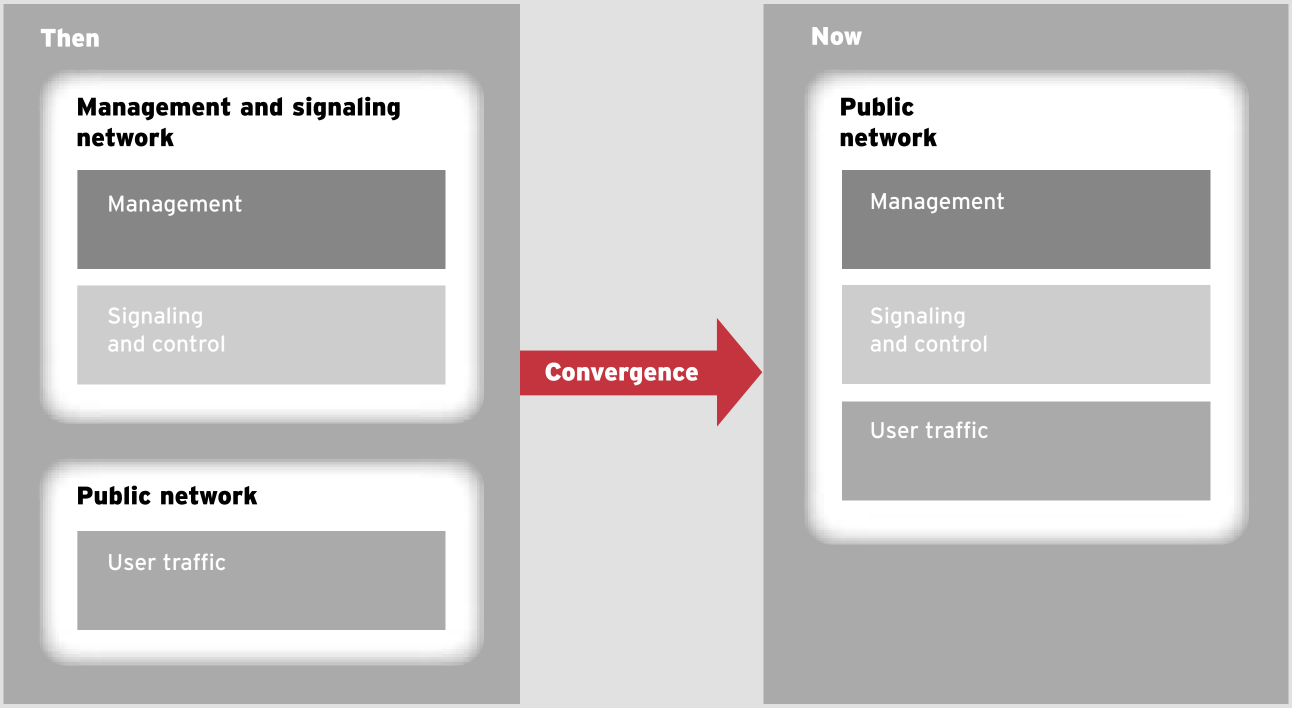
These CIAAA requirements were the starting point for the Nortel team, as it defined the "must-have" security needs for all three traffic planes.

In doing so, Nortel has adhered to several key security principles. Specifically, that:

• customers expect the network elements and products to be inherently secure at manufacture;

• a layered defense (also known as defense in depth) security process should be applied to ensure network safety,

Figure 1. Convergence of network traffic types



In telecommunications networks of the past, public traffic and network management and signaling traffic were sent on separate networks. In this way, the management and signaling networks were relatively easy to secure and isolate from malicious activity. Today, by contrast, management, signaling, and user traffic are sent on the same "pipe," and threats that were once confined to user traffic are now threats to all traffic planes. The Nortel-defined set of baseline security requirements provides the higher levels of security now required for all planes.

through multiple layered security mechanisms with no single point of failure;
- security capabilities should be integrated into network products at the design stage;
- a common infrastructure security strategy is needed across all product lines to ensure interoperability; and
- standard protocols should be used to help ensure interoperability with third-party products.

Securing the management plane

Guided by these principles, Nortel targeted the management plane as the first priority, since it was here that attackers could most easily cause large-scale network disruption. For instance, an attacker – whether a disgruntled insider or a hacker from the general public – could reconfigure network equipment, cause denial of service (DoS) and network outages, destroy critical data, or perpetrate fraud through stealing or manipulating service or billing records.

Nortel's CTO Office led a cross-corporate security team with representatives across the product groups. This team examined the requirements and potential vulnerabilities of the management plane, sifted through the merits of the many existing technologies, solutions, and best practices, and identified those that would best meet the needs of an end-to-end network.

Indeed, an unsecured management plane has many vulnerabilities that can be exploited. These vulnerabilities include:
- use of unsecured protocols for network management, such as SNMPv1&2, FTP, Telnet, TFTP, and HTTP;
- use of weak, locally managed static passwords for operator authentication (an example of a weak password is "admin" for an administration password, or a three- or four-letter dictionary word, such as "cat" or "dog");
- lack of access control (or authorization) mechanisms to define network access permissions for different levels of administrators;
- security information, such as secret keys and passwords, that are transmitted in the clear or stored in plaintext;
- backdoor programs left in network management systems; and
- unnecessary functions, such as a Telnet administration function that has been left on, running on the operating systems of management devices and presenting targets for attack.

To protect the network against these vulnerabilities, the team identified several key requirements for management plane security, several of which are considered mandatory – including operating system hardening, virus-free software, cryptographic protection, secure remote access, operator authentication and access control, standardized security logs, and vulnerability assessment – as well as two best-practice recommendations (intrusion prevention/detection and firewall protection) that are considered optional, depending on individual customer needs (Figure 2). While many of these requirements need to be built in at the design stage, some – such as operating system hardening and anti-virus protection – also require ongoing monitoring to ensure that the latest patches are incorporated.

Operating system hardening: Computers and network elements are vulnerable to any number of attacks, including backdoor programs, password grabber and cracking tools, exploitation of defects in operating system services, and DoS attacks. Once a system has been compromised, an intruder can modify or destroy information, disclose sensitive information, install malicious code to gather information, or use the compromised server to attack other systems.

A key measure to counter these attacks is to harden commercial operating systems using procedures such as turning off unused services, ensuring removal of default passwords, and ensuring that security patches are up to date. Such services are essentially sound practices followed during installation and configuration of operating systems. The management plane security baseline requires that all operating systems used for management purposes undergo operating system hardening.

Virus-free software: "Virus" is a term used to categorize several types of malicious software programs, or malware, including viruses, worms, and trojan horse programs. Securing the management plane, then, requires that all network software be scanned using anti-virus software to ensure that it is virus-free to the maximum reasonable extent possible before installation. All software used in Nortel products, whether developed in-house or sourced from a third-party, is checked for viruses using a Nortel-developed virus-detection process before being incorporated into product.

Cryptographic protection: Encryption of data provides a high degree of protection against malicious insiders, while allowing legitimate operators access via encryption keys. The management plane security baseline requires encryption and authentication for all management traffic to ensure data confidentiality and integrity. Since different customers prefer different security protocols for cryptographic services, the baseline standard accommodates several, including IPsec, Secure Shell (SSH), Secure Socket Layer/Transport Layer Security (SSL/TLS), and Simple Network Management Protocol Version 3 (SNMPv3), all of which can provide data integrity and confidentiality for network management traffic.

Nortel includes all of these security protocols across its product lines, and the CTO team provides consultation to individual product groups on a network or product basis, to not only help guide implementation of the protocol that will work best for a specific customer but also to ensure end-to-end encryption solutions.

Secure remote access for operators: A particular security concern in the management plane is to ensure that network management data and processes are accessible over the public Internet only by legitimate operators, who often need to administer the network from a remote location. In this case, strong security is needed to authenticate these remote operators, as well as protect the confidentiality and integrity of all data both to and from them.

To provide this level of security, the management plane baseline requires the use of secure virtual private networks (VPNs) based on IPsec. IPsec VPNs, such as Nortel's VPN Router portfolio (formerly known as Contivity), provide secure encrypted tunnels for data traffic to and from all remote operators.

Centralized network operator authentication/access control: "Authentication" refers to proof of identity of the party accessing the network, and Nortel's customers require strong authentication of all network operators. Moreover, once an operator has been allowed onto the network, access control policies limit the network resources that network operators can administer.

The management plane security baseline requires a centralized authentication/authorization system with enforcement of strong passwords for all Nortel products. To achieve this level of protection, Nortel uses a system based on RADIUS/LDAP (Lightweight Directory Access Protocol) to automate centralized authentication within Nortel solutions. The use of Pluggable Authentication Mechanism (PAM) is also recommended to allow other customer-specified authentication mechanisms, such as Kerberos, to be incorporated more easily.

Figure 2. Baseline security at a glance

Mandatory baseline security features

- Operating system hardening
- Virus-free software
- Encryption of network management traffic
- Secure remote access
- Operator authentication and access control
- Standardized security logs
- Vulnerability assessment

Optional baseline security features

- Intrusion prevention/detection
- Firewall protection

The Nortel-developed baseline security requirements for the management plane have been used to form the foundation for industry-wide security baseline standards – a common and consistent set of security requirements that form the "must-have" suite of protective measures for basic security. These requirements include several that are considered mandatory, as well as two best-practice recommendations (intrusion prevention/detection and firewall protection) that are considered optional, depending on individual customer needs. Nortel has also defined requirements for the signaling and media planes, and is sharing these recommendations and best practices with the industry at large through key standards bodies.

Security audit logs maintain an audit trail of operator activities and events, and provide a basis for accountability, reconstruction of security incidents, problem analysis, and long-term trend analysis. (The raw data collected is called the "audit log," and the verifiable path of events through the audit logs is referred to as the "audit trail.")

Audit log information helps to identify the root cause of a security problem and prevent future incidents. For instance, audit logs can be used to reconstruct the sequence of events that led up to a problem, such as an intruder gaining unauthorized access to system resources, or a system malfunction caused by an incorrect configuration or faulty implementation.

To be effective, logs must contain enough security information to conduct an after-the-fact investigation or analysis of security incidents. As well, to be useful across end-to-end network solutions, logs need to be in the same format.

Nortel's management plane baseline calls for a common log format to be used across its product portfolio, along with a common comprehensive log content specification detailing the security events that need to be logged (e.g., administrator log-in and configuration changes). Syslog is the recommended logging mechanism for storage and transfer of logs, because it is a common mechanism compatible with all third-party log analyzer systems.

Vulnerability assessment of products is used to discover security weaknesses and areas of risk before a product is deployed. While product verification testing focuses on ensuring that systems pass defined test scenarios, vulnerability testing is designed to try to make the system fail by circumventing security controls, capturing confidential data, obtaining unauthorized access, and performing other attacks.

The management plane baseline requires that vulnerability assessment be conducted routinely in order to identify and better understand threats and vulnerabilities, to determine an acceptable level of risk, and to mitigate identified issues. In this effort, Nortel created a comprehensive company-wide program that includes training for all product groups on how to perform this assessment and resolve issues.

In addition to these seven measures that Nortel defined as mandatory, the team also identified two best practices – intrusion prevention/detection and firewall protection – that, while considered optional with respect to the baseline requirements defined by Nortel and being formally standardized, are considered important by many customers. **Intrusion prevention/detection systems (IPS/IDS)** can be incorporated in a network solution to provide even stronger defense. For example, Nortel's Threat Protection System (TPS) (page 35) can be used to warn network administrators of the possibility of a security incident, such as a compromised server or DoS attack.

IPS/IDS can be broadly categorized according to the following criteria:

- *Incident prevention/detection timeframe:* real-time or off-line, depending on whether system logs and network traffic are analyzed as events take place or in batch mode during off hours;
- *Type of installation:* network-based or host-based. A network-based IPS/IDS typically involves multiple monitors (often pre-configured appliances) installed at choke points in the network (where all traffic between two points can be monitored). A host-based IPS/IDS requires that software that monitors network connections and user activity on servers that need to be protected be installed directly on those servers; and
- *Type of reaction to incidents:* whether the IPS/IDS actively intervenes to head off attacks (such as by modifying firewall rules or router filters), or simply notifies staff or other network systems of

Table. Summary of baseline requirements to mitigate against common infrastructure vulnerabilities

Network security threat	Nortel-recommended mitigation measures
Masquerade	• Use of RADIUS for centralized password management ensures strong authentication of operators. • Encryption of management traffic prevents snooping of administrator passwords.
Denial of service (DoS)	• Addition of firewalls provides first stage of defense-in-depth strategy to prevent DoS attacks. • Nortel standard security logs provide strong traceability for forensic analysis.
Hacking	• Use of RADIUS for centralized password management ensures strong authentication of operators. • Encryption of management traffic prevents control or modification of network resources by hackers.
Sabotage	• Use of RADIUS for centralized password management ensures only legitimate operators have access to the system. • Encryption of management traffic prevents control or modification of network resources by attackers. • Nortel standard security logs provide strong traceability for forensic analysis.
Intrusion	• Use of RADIUS for centralized password management ensures only legitimate operators have access to the system. • Encrypted management traffic ensures attackers cannot control network elements. • Nortel standard security logs enable intrusion analysis and incident recovery. • Use of intrusion prevention/detection systems.
Backdoor programs	• Operating system hardening ensures backdoor programs are removed or disabled. • Encryption of management traffic and RADIUS authentication limit access to equipment to only legitimate operators. • Nortel standard security logs provide strong traceability for forensic analysis.
Disgruntled employees	• Encryption of management traffic allows only authorized insiders to view network data and/or modify network element operation. • RADIUS authentication ensures that only legitimate operators can access/modify equipment. • Nortel standard security logs provide strong traceability for forensic analysis. • Firewall placement provides segmentation between network zones and limits scope of any attack.

the problem.

For proper intrusion prevention/detection measures on the network management plane, Nortel recommends that both network and host-based IPS/IDS be implemented in the network solution.

Firewall protection: A firewall is a set of safeguards that enforce a security policy between two networks. Firewalls are sometimes called "policy enforcement points" that implement an organization's corporate security policy, which is typically expressed as a rule set in the configuration language of the particular firewall.

Traditionally, firewalls were used to isolate private networks (intranets) from public networks (the Internet). Nortel recommends the use of firewalls in all network solutions in order to segment the management, signaling, and user traffic into different security domains. In this role, the firewall controls the type of traffic that transits the boundary between different security domains. Depending on the type of firewall (application versus packet filtering), this control can also be extended to include filtering of the application content of the data flow. Typically, firewall placement, type, and filtering rules are designed for a particular network implementation.

Management plane baseline standardization

These nine network safeguards constitute Nortel's management plane baseline security requirements, which were formally documented in the company's systems requirements document (SRD) and are being implemented across all product portfolios. (The table on page 24 summarizes the recommended measures to mitigate against key network infrastructure vulnerabilities.)

Nortel then initiated an activity at the U.S. National Security Telecommunications Advisory

Table continued

Network security threat	**Nortel-recommended mitigation measures**
Snooping	• Encryption of management traffic prevents snooping. • Nortel standard security logs provide strong traceability. • Use of firewalls limits scope of any attack.
Modification of data	• Encryption of management traffic prevents modification of management data by attackers. • Nortel standard security logs provide strong traceability. • Use of firewalls limits scope of any attack.
Proliferation of unsecured protocols (unsecured protocols include ICMP, Telnet, SNMPv1&2, DHCP, TFTP, NTP, DNS, and HTTP)	• Replacement of unsecured protocols with secure, encrypted protocols. • Telnet, FTP are replaced by SSH or IPsec. • IPsec used to encapsulate other unsecured protocols. • Use of TLS for HTTP traffic. • Use of SNMPv3 for SNMP traffic.
Use of weak, locally managed, static passwords	• Use of centralized RADIUS server enforces strong, centrally managed passwords, as per Nortel standard password guidelines.
Unprotected security information (e.g., unencrypted password files, passwords sent in the clear, firewall rule sets, and cryptographic keys)	• RADIUS protocol transmits passwords across network and stores passwords in a hashed format. • Encryption of management traffic ensures critical data is sent securely across network.
Non-hardened network elements and operating systems	• Operating system hardening.
Management ports and interfaces unnecessarily exposed to the public network	• Encryption of management traffic. • Firewall segmentation of network.
Industrial espionage	• Encryption of management traffic and strong authentication of operators via RADIUS prevents unauthorized access to equipment.

Committee (NSTAC) to standardize these requirements and drive them into the industry at large.

Early activity at NSTAC was so successful that Nortel was asked to act as a technical editor on a new U.S. standard for management plane security being implemented through the U.S. Alliance for Telecommunications Industry Solutions (ATIS). Working with a large government and industry team at ATIS – a team that included members from the U.S. Department of Defense, as well as from Verizon, Sprint, MCI, BT, and others – Nortel drove the baseline requirements into the American National Standards Institute (ANSI) T1.276-2003 *A Baseline of Security Requirements for the Telecommunications Industry.*

Following this effort, Nortel then worked to drive the management plane baseline requirements into international standards bodies, including the 3GPP (Third Generation Partnership Project) TS 32.371 Security Concepts and Requirements, and the International Telecommunication Union (ITU-T) M.3016.x series of standards. Nortel was also the editor of the Security Requirements for NGN Release 1, produced within the ITU-T SG13 Focus Group on NGN.

In addition, Nortel has driven the management plane baseline best practices into the U.S. Network Reliability and Interoperability Council (NRIC), where they have been accepted as formal NRIC best-practice recommendations.

Securing the signaling/control plane

With standardization of management plane security well under way, Nortel then focused its attention on determining the fundamental requirements for securing communication between signaling elements in multimedia networks – e.g., those that use H.323 and Session Initiation Protocol (SIP) protocols.

Following an approach similar to the one it used for the management plane, the Nortel team identified several key security requirements and associated technologies to address the requirements for the signaling/control plane. These include:

Data confidentiality and integrity: The signaling/control plane baseline requires the use of IPsec or TLS protocols to provide data confidentiality and integrity – that is, to protect all SIP signaling messages from unauthorized reception and modification.

Authentication: Authentication verifies the identities of those involved in a communications exchange. The signaling/control plane baseline requires the enforcement of bidirectional authentication based on X.509 certificates through IPsec or TLS protocols for all machine-to-machine SIP signaling exchanges. For SIP user agents (SIP soft clients, SIP phones, and SIP integrated access devices), the signaling/control plane baseline requires authentication based on HTTP digest over a secure protocol, and recommends the use of X.509 certificates.

Access control (authorization): Access control is based on lists of known IP addresses with which a network element or server will allow communication. The signaling/control plane baseline recommends the use of access control lists for SIP client and server applications, enforced by packet filtering software.

Audit logs: Security audit logs maintain an audit trail of network element and server events, and are used to identify causes of security problems, prevent future incidents, and provide information for evidence. The signaling/control plane baseline provides a list of SIP signaling and control events to be logged.

Signaling/control plane baseline standardization

As part of its overall baseline security strategy, Nortel is taking these signaling/control plane specifications to the industry for standardization. The first focus for standardization of signaling security standards was within the ATIS Packet Technologies and Systems Committee (PTSC). Within PTSC, Nortel holds a vice-chair position and also chairs the PTSC Security Subcommittee where this standardization is occurring.

The PTSC committee is establishing a family of five signaling and control plane security standards, with Nortel acting as a technical editor for two of these. This activity is under way and the first of the five proposed standards – the Generic Signaling and Control Plane Security Requirements for Multimedia Networks – is currently being validated by ATIS members. The expectation is that these ATIS-produced standards will be fed into the ITU-T, for adoption into ITU-T Recommendations.

Securing the media plane

Nortel as well as others in the industry are also working to define baseline requirements for the media plane, which carries user traffic. When defined, the media plane security baseline will focus on security requirements for real-time user traffic on multimedia networks that use H.323 and SIP protocols.

Before these requirements can be formalized, however, several challenges need to be addressed. Chief among these is the current industry discussion about how much security is actually needed on the media plane for real-time voice and multimedia, which traditionally in public applications was not secured except in special environments, such as military applications. This debate centers on whether user traffic encryption is necessary: because user traffic forms the bulk of all network traffic, the added digital signal processing steps needed to encrypt all user data could potentially impact circuit performance and introduce new overhead in the network and in the endpoints, which could potentially require additional hardware (such as a dedicated encryption chip) in the endpoint devices and lead to increased costs.

Nortel believes that encrypting user traffic is important, not only because it will protect users from such attacks as eavesdropping, but also because it will be key to creating trusted, secure end-to-end networks in the future, as well as help to enable such enhanced capabilities as network-wide identity management (see page 65).

To secure real-time traffic, Nortel recommends the use of Secure Real-time Transport Protocol (SRTP), a protocol defined by the Internet Engineering Task Force (IETF) that operates on top of IP. When implemented properly, encryption can be supported while keeping delays to a minimum. Nortel is currently applying its significant heritage and leadership in understanding the requirements of real-time networking to several technology innovations in this area.

A second challenge with encrypting user traffic is the need for greater processing power at the network endpoints – a challenge that Nortel is also working to address. Potential solutions, among others, could include encryption chips embedded directly into the end devices, or suitable high-speed signal processors that boost processing power.

At the same time, though, Nortel recognizes that user traffic encryption solutions must be sensitive to law enforcement needs. Indeed, another challenge is the need to comply with the legal intercept requirements of some governments to enable law enforcement to access public user voice traffic under court order. If this traffic is encrypted by the carrier, there is an expectation that the network must also have the ability to decrypt it when required for the customer and authorized law enforcement agencies. To do this, the system must be able to store, track, and secure the encryption keys needed to decipher the code. Here, Nortel is exploring such potential solutions as key-sharing mechanisms.

Media plane standardization

As it did with both the management and signaling plane security baselines, Nortel is taking its media plane security recommendations to the industry at large. The first focus for standardization is within the ATIS Performance, Reliability and QoS Technical Committee (PRQC). The PRQC is establishing a family of media plane security standards, and Nortel is acting as a technical editor. These media plane standards will specify appropriate levels of protection, such as endpoint authentication, the use of SRTP, key exchange mechanisms, and other security measures such as the use of firewalls designed specifically for handling multimedia traffic. Activity at the PRQC is currently under way, with the first standardization expected in the 2006 timeframe.

By establishing and implementing baseline infrastructure security requirements for the network management, signaling/control, and media planes, and driving the industry toward standardized adoption of these baselines, Nortel is demonstrating its significant leadership in shaping next-generation networks and enabling the secure, trusted networks of the future. ■

Mike Lee *is Senior Security Architect in the CTO Office, and is contributor and technical editor on the baseline security standards in the ATIS, 3GPP, and ITU-T standards bodies.*