



>THIS IS **THE WAY**

>THIS IS **NORTEL**<sup>TM</sup>

## CDMA End-to-End Security

Positioning Paper



**Computer viruses grew by 34% in 2004, with 28,327 to a total of 112,438. (Source: IBM)**

**Losses from insecure networks are expected to reach \$700K per day. (Source: IDC)**

With the advent of Wireless Broadband, wireless users are enjoying many rich application and services over the Internet virtually anywhere they go. Wireless Broadband services offer a new way of life where information is at our fingertips whenever it's needed reducing the stress of anticipation. Business transactions can be carried out in real-time, minimizing delay and maximizing productivity. These benefits outweigh some of the potential security concerns of doing business over the Internet.

Wireless Broadband service providers are facing public network risks such as viruses, worms, blended threats, and software vulnerabilities that can impact their infrastructure, service offering and their end user experiences. Security measures must be taken in order to minimize service disruptions, avoid loss of revenue from theft and maintain a high level of customer satisfaction.

A combination of deploying security solutions and putting the appropriate processes in place will help face these challenges and proactively protect Wireless Broadband service offering. Nortel offers a layered end-to-end network approach to security that not only ensures network security but overall network reliability and resiliency to allow business continuity.

Code Division Multiple Access (CDMA) technology originated from military applications and cryptography, and to date, do not have any report of high-jacking or eavesdropping on a CDMA call in a commercially deployed network.

## **The Inherent Security of the CDMA Air Interface**

CDMA air interface is inherently secure and is clearly superior to first-generation analog and Time Division Multiple Access (TDMA) systems. The inherent security of CDMA air interface comes from spread spectrum technology and the use of Walsh codes.

CDMA utilizes specific spreading sequences and pseudo-random codes for the forward link (i.e. the path from the base station to the mobile) and on the reverse link (i.e. the path from the mobile to the base station). These spreading techniques are used to form unique code channels for individual users in both directions of the communication channel. Because the signals of all calls in a coverage area are spread over the entire bandwidth, it creates a noise-like appearance to other mobiles or detectors in the network as a form of disguise, making the signal of any one call difficult to distinguish and decode.

CDMA also has a unique soft handoff capability that allows a mobile to connect to as many as six radios in the network, each with its own Walsh code. This means that someone attempting to eavesdrop on a subscriber's call has to have several devices connected at exactly the same time in an attempt to synchronize with the intended signal. In addition, CDMA employs a fast power control, 800 times per second, to maintain its radio link. It is difficult for a third party to have a stable link for interception of a CDMA voice channel, even with a full knowledge of a Walsh code. Synchronization is critical, as without this synchronization, the listener only hears noise.

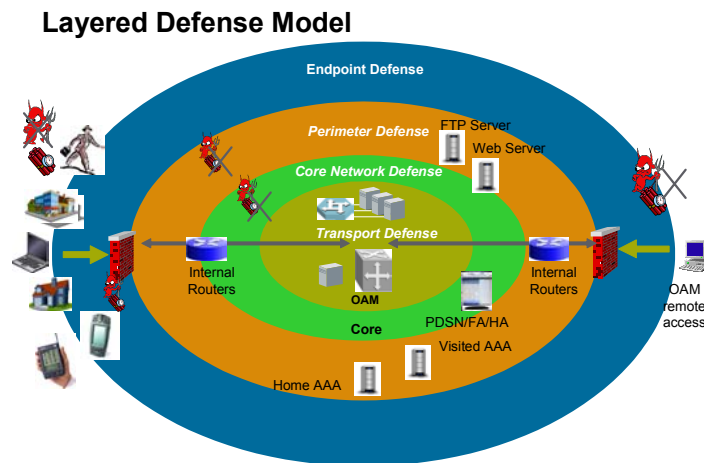
For CDMA 1xEV-DO, the high speed data technology, the forward link utilizes rate control instead of power control and time division multiplexing instead of spreading codes. However, it still has inherent security that protects the identity of users and makes interception very difficult. In addition, the Media Access Control



Identification (MACID) assigned to users is encrypted. User packets are assigned variable time slots and the data rate is controlled by the access terminal based on radio conditions. Packets are divided into sub-packets using Hybrid Automatic Repeat Request (HARQ) and early termination mechanisms. These attributes makes it virtually impossible to identify the user or correlate user packets. 1xEV-DO standard specification supports a security protocol layer ready for implementation of future security protocols.

## Layered Defense Approach to Secure Management, User and Control Planes

With wireless air interface secured, focus can now be placed on other areas of the User, Control and Management planes to ensure they are secured. The User plane consists of all user data/voice traffic from the air interface. The Control plane consists of signaling messages, session management & setup and subscriber/device authentication. The Management plane consists of OA&M platform, interfaces, access control and remote access.



All three planes are composed of multiple platforms and interface connections that require a holistic approach to protect from external and internal threats. Nortel has devised a unique layered defense model to network security such that solutions can be placed across the network to complement CDMA security standards.

## Core Network Security

### Management Security

Securing the management plane is a critical part of an end-to-end security solution. Network management nodes contain management policies and databases that are critical to the operation of the network. To ensure robustness of the management plane, security must address platform, internal and external threats.

Nortel CDMA Network Manager (CNM) provides consolidated Operations, Administration, and Maintenance (OA&M). CNM integrates Fault, Configuration, Performance and Security management for up to 6 circuit or packet switches, and associated PDSN/FA/HA, onto a single OA&M server. The CNM support a number of security features such as OS hardening, user access and operation audit, privilege-based user groups, centralized authentication, user profile and group management, customer plug-ins for authentication and secure remote access with IP Security Protocol (IPSec) and other capabilities in subsequent releases.



## Provisioning

Older cellular technology transmits subscriber identity information over the air interface during registration and call set-up in a format that can be easily detected and read by radio scanner devices, making it susceptible to fraudulent activities such as cloning and tumbling. CDMA avoids these issues by using a 64-bit authentication key (A-key) and the Electronic Serial Number (ESN) of the mobile. The A-key is used to generate sub-keys that provide voice privacy and message encryption. CDMA allows several distribution methods of A-keys to valid users for acquiring subscription-related information to communicate with the network providing service.

For all distribution methods, security data is provided electronically in an encrypted format. The most secured distribution method uses handsets that are pre-programmed with the A-key and ESN by the mobile vendor, and then the wireless provider or dealer assigns ESN with Mobile Identification Number (MIN). This approach ensures that neither the equipment manufacturer nor the dealer has all three pieces of security information.

## Subscriber Authentication

Subscriber authentication is a key control mechanism to protect the infrastructure and to prevent unauthorized access to network resources. CDMA 1X access authentication is accomplished by means of an 18-bit authentication signature that is verified by the network's databases of user information, the Home Location Register and Authentication Center. 1xEV-DO also uses the same 512-bit algorithm in OTASP to exchange keys between the mobile device and the Access Node-Authentication Authorization Accounting (AN-AAA) server. Both technologies utilize strong authentication key exchange protocols to ensure identity.

For CDMA2000 1X data sessions and EV-DO, users are authenticated using the Challenge Handshake Authentication Protocol (CHAP) by the Packet Data Serving Node-Authentication Authorization Accounting (PDSN-AAA) server. CHAP is a proven Internet authentication protocol that is leveraged in the wireless network to verify identity.

## Packet Core

In CDMA2000 architecture, the wireless packet core network is leveraged for both 1X and 1xEV-DO. The wireless packet core is the ideal place for applying IP services -- especially security services, common across the CDMA2000 access network. Nortel Packet Data Network supports :

- Subscriber stateful firewall – protects both subscriber and/or operator's infrastructure traffic
- Ingress Anti-spoofing – Prevents subscribers from launching attacks based on forged source IP addresses
- Traffic Steering to off-board services such as content filters or virus protection servers.
- Deep packet filtering & inspection from TCP/IP layer to Application Layer
- On-board Lawful intercept meeting regulatory security requirements

Mobile IP Foreign Agent (FA) to Home Agent (HA) and HA outbound connections must also be protected. These connections can be protected via IP Security (IPSec) encrypted Virtual Private Routed Network (VPRN) capabilities on FAs and HAs.

## Transport Security – protecting traffic in transit

Protecting mobile user or management information is an important role of the layered security defense. Prevailing VPN protocols – IPSec and Secure Socket Layer (SSL) – are complementary. IPSec VPN provides encryption, authentication protection at the IP layer thus protecting all IP application traffic. SSL VPN provides secure



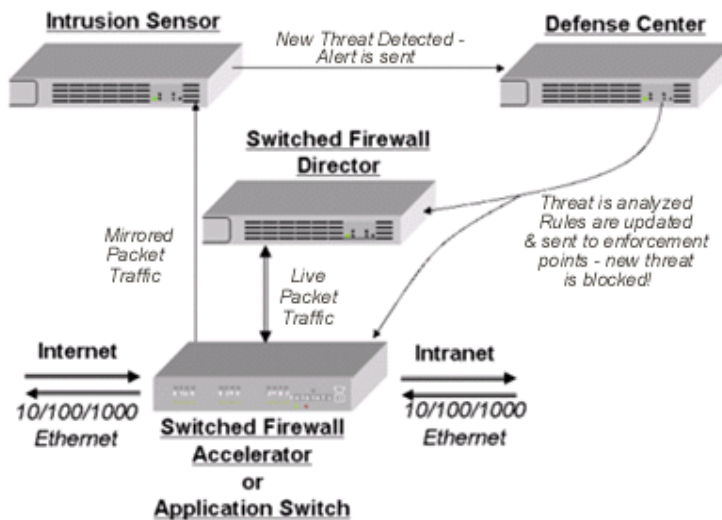
communications for the web application. Nortel is the first vendor to offer support for both VPN technologies in a single platform.

Nortel Secure VPN router is proven and widely used. More than 60 million clients have been deployed in F500 corporations. The client software establishes a secured, encrypted connection between itself and the server, thereby shielding all traffic between the client and server from other routing domains. IPSec is usually best for remote access that requires full use of network resources from laptops. Support for telecommuters and branch sites where multiple applications will be used, for example, are ideal applications for IPSec.

SSL VPNs are easy to deploy because no client is required on the mobile device. Using the Web browser as a universal client makes it easy to upgrade from legacy application interfaces to a Web interface. SSL VPNs provide security above the TCP/IP layer, thus ensuring compatibility with existing Network Address Translation (NAT) services, firewall configurations and proxy settings. SSL VPNs are good options for securing applications or services for an enterprise partner access to a single or limited set of applications, online customer access to services or mobile employee on-demand access to e-mail from any Web browser while at airport or on the road.

## Perimeter Security

Perimeter security has been around for some time and is generally referred to as firewall. With the continuous increase in Internet viruses and worms, the complexity of updating firewall rules and ensuring detection/prevention of unknown threats can be a burdensome task. Nortel introduced Threat Protection System (TPS) using Snort-based™ intrusion detection method that is easy to use with outstanding support for rules maintenance and report generation.



The TPS Intrusion Sensor uses a rule-based, deep-packet inspection method to examine protocol fields on mirrored packet traffic for attacks. The sensors detects anomalies such as port scan, IP stack fingerprinting, Denial of Service attack and Address Resolution Protocol (ARP) spoofing. Threats are analyzed at the Defense Center and automatically update rules and sent to firewalls in real-time to block the detected threat. Policy management and control along with threat analysis, reports, trap and trace capabilities, and event database for analysis are provided by the Defense Center which supports a hierarchical grouping of sensors for centralized management.



Nortel Switched Firewall portfolio complements the TPS by load-balancing and active policy enforcement. Nortel Switched Firewall is based on a next-generation security architecture called the Nortel Open Security Architecture

(OSA). OSA is a new paradigm for very high-throughput security with unmatched scalability and flexibility. The Switched Firewall Director handles the control functions of policy management, session acceptance and management etc.

## **End Point Compliance**

Mobile enterprise users using laptop or smart devices are increasingly taking advantage of the speed and services of EV-DO. End points, either mobile devices or management consoles, can be potential sources of threats. These devices may be infected with viruses or worms which if allowed to connect to the wireless network, may become the source of an attack. Unprotected end points can carry Distributed Denial of Service (DDOS) attack handler which launches attack to service provider resources such as Web, email or Domain Name System (DNS) servers.

Nortel VPN Tunnel Guard provides a security solution capable of enforcing best practices on both managed (IPSec/SSL) and unmanaged SSL endpoints. Tunnel Guard helps to prevent the end-user PC from becoming a vehicle for viruses or other unwanted intrusions into the wireless network. Tunnel Guard enables the VPN administrator to define endpoint security policy on the VPN gateway itself and ensure all user laptops/devices connecting to the gateway are inspected for compliance to the policy throughout the life of the VPN session. Tunnel Guard is completely open while flexible and can interrogate the security status of the end point, including the status of its operating system, service packs and patches, personal firewall, anti-virus software versions and definitions before granting network access.

## **Nortel on Nortel**

Nortel's own network, one of the largest and most technically advanced enterprise networks in the world, connecting more than 280 locations across 6 continents, runs on products from Nortel's own portfolio. That's about 33 million minutes of voice calls, 1.1 petabytes of data traffic (including 19 million e-mails), and 100 live web casts in a typical month – all on Nortel products. Leveraging the latest security available in Nortel's portfolio, Nortel's IS can use the Internet as a transport to reduce the costs and complexities associated with multiple network topologies and access methods while still protecting these critical network resources. Currently, as an example of a layered defense approach, among its many solutions, Nortel IS uses the Nortel Switched Firewall for its deep packet inspection, having prevented over 133 worms in the first month in the network, and with minimal latency, to protect our network IP Telephony applications. Nortel Application Switches are used to provide redundancy to Session Initiation Protocol (SIP) servers to ensure high availability of our SIP applications and bandwidth management of Peer-to-Peer network applications. The Application Switches provide global multi-site and local redundancy of key server, flexible packet inspection with packet offset, and pattern matching for User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), TCP/IP traffic, and to auto-learn and auto-update the latest attack signatures. Secure VPN Routers are used to provide mobile employees with secured communications with the added protections of stateful firewall inspection. Using best-of-breed security technologies available through Nortel's vendor partnerships, and security best practices including a strongly enforced and well-understood security policy, Nortel's IS enjoys a true end-to-end layered approach to security.



## **Nortel Security Professional Services**

Nortel offers Security Professional Services to complement the security built into Nortel's infrastructure products and architectures, and Nortel's award-winning portfolio of security products. Security Professional Services work closely with Nortel R&D and Engineering on layered defense strategies, understanding areas of vulnerability, and working across the corporation to develop solutions.

In depth security requires more than just a secure infrastructure. Nortel's Security Professional Services offer customers a lifecycle oriented portfolio which includes plan and build the infrastructure, develop security policies and procedures around the operations of the network, perform security assessments, and even setup and run Security Operations Centers.

## **Summary**

There are many existing security threats to Wireless Broadband networks with new threats appearing everyday and continue to be on the rise. A wireless broadband network requires a holistic end-to-end approach in order to secure the various nodes and signaling links within the network. In other words, it is not just about "securing the box"; it's about securing the entire network through a layered defense approach. CDMA air interface technology is inherently secure for protection of signaling and bearer traffic with excellent security in service provisioning for handset and parameter distribution. In addition, Nortel Switched Firewall, Threat Protection Systems and Application Switch can be utilized in the future to quickly protect the network from new threats when they are introduced. Today's service providers realize the importance of implementing security policy enforcement measure through software control for network elements, processes, best practices and physical control to allow subscribers peace of mind while fully benefiting from the Wireless Broadband Services. Nortel's layered security architecture and strong portfolio of security product protects your network, your subscribers, and your business.



**In the United States:**

Nortel Networks  
35 Davis Drive, Research Triangle Park, NC 27709, USA

**In Canada:**

Nortel Networks  
8200 Dixie Road, Suite 100, Brampton, Ontario L6T 5P6, Canada

**In Caribbean and Latin America:**

Nortel Networks  
1500 Concorde Terrace, Sunrise, FL 33323, USA

**In Europe:**

Nortel Networks  
Maidenhead Office Park, Westacott Way, Maidenhead Berkshire SL6 3QH, UK

**In Asia Pacific:**

Nortel Networks  
1 Innovation Road, Macquarie University Research Park, Macquarie Park NSW 2109, Australia  
Tel: (61)2 8870 5000

**In Greater China:**

Nortel Networks  
Nortel Networks Tower, Sun Dong An Plaza, 138 Wang Fu Jing Street, Beijing 100006, China  
Tel: (86) 10 6528 8877

Nortel Networks is an industry leader and innovator focused on transforming how the world communicates and exchanges information. The company is supplying its service provider and enterprise customers with communications technology and infrastructure to enable value-added IP data, voice and multimedia services spanning Wireless Networks, Wireline Networks, Enterprise Networks, and Optical Networks. As a global company, Nortel Networks does business in more than 150 countries. More information about Nortel Networks can be found on the Web at: [www.nortel.com](http://www.nortel.com)

For more information, contact your Nortel Networks representative, or  
Call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

\*Nortel Networks, the Nortel Networks logo, the globemark design, and Business without Boundaries are Trademarks of Nortel Networks. All other trademarks are the property of their owners

Copyright © 2005 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.

NN107760-091504