Client Security in the Enterprise Network: Dell's Perspective
February 2000

Client computer security is a broad subject that includes securing access to network resources, securing data transfers over private and public networks, and protecting client computers and local data from theft. Security is increasingly important as portable computers, vulnerable to theft, proliferate and the Internet revolutionizes communications and commerce. Applications such as e-commerce, remote access, e-mail, wireless and wireline intranets, Internet telephony, and media distribution all depend on robust security solutions.

Security is also a major contributor to the total cost of ownership of client computers. The cost to companies of security issues such as theft, support issues such as forgotten passwords, and virus infections are substantial.

This article reviews key security technologies, discusses several industry security initiatives, and presents Dell's security offerings for enterprise client systems.

Physical Theft Protection and Recovery

Theft is a growing problem with client computers, particularly portables. The problem is twofold: theft of the computer itself and the resulting loss of sensitive data stored on the hard-disk drive. The data loss is not only a security issue, but it is also a big contributor to the cost of ownership of portable systems. The lost data can be very expensive to rebuild or recover.

The most common theft protection devices in use today are locks and cables to deter system theft, and chassis intrusion sensors that trigger alerts over the LAN to system managers when a PC configuration is changed or a chassis is opened in an unauthorized manner. Finally, physical or electronic asset tags help to recover stolen systems.

Secure Access to Network Resources

An important component of client security is to protect network resources from unauthorized access and viruses. This aspect of client security—typically achieved through various authentication and data protection methods—can be organized into three levels as shown in Figure 1.

- Level 1 — This security level protects the client computer from unauthorized access. Preboot authentication occurs before the operating system boots and includes BIOS and hard-disk drive passwords. Operating system passwords provide further authentication. In addition to passwords, various biometric devices discussed later in this section can be used for preboot and operating system authentication.

- Level 2 — Network logon authentication is typically achieved through network passwords and various biometric devices. This security level protects the network from unauthorized access.

- Level 3 — Advanced data protection techniques protect the data stored on client and network hard-disk drives. The authentication methods used in levels 1 and 2 provide data protection by limiting access to the data. In addition, techniques such as encryption of data stored on hard-disk drives, regular use of antivirus software, and the use of firewalls protect data.
Figure 1. Three Levels of Securing Access to Network Resources

Authentication methods are commonly described as:

- “What you know” — requires the user to remember a password or personal identification number (PIN).
- “What you have” — requires the user to carry a token such as a smart card.
- “What you are” — identifies user based on fingerprint, iris scan, and so on.

Multifactor authentication combines more than one authentication method to provide increased security. Typical multifactor approaches combine “what you have” with “what you know” or “what you are.” For example, a token device such as a smart card (“what you have”) is usually combined with a user password or PIN (“what you know”). In this way, if the smart card is lost, it cannot be used without knowing the password.

Authentication verifies the identity of a user logging on to a network. The most common authentication method is the use of passwords to log on a corporate network or Internet resource, or passwords to log on to the operating system, BIOS, or hard-disk drives of individual client systems. The proliferation of passwords presents a significant systems management burden for most organizations. By some estimates, as much as 30 percent of internal help desk calls are related to forgotten passwords.
Authentication can also be achieved via devices such as token and biometric devices.

**Token Device**

A token is a security device given to an authorized user who keeps it in his possession. The best known token device is the smart card, a credit-card sized device with an integrated microprocessor and memory. The latest smart cards can be used to access buildings, computers, and networks, thus allowing users to carry only one identification card. Smart cards require smart card readers to interpret the information encoded in a smart card. Smart card readers for computers are available as PC Cards, external serial, parallel, or P/S2 port devices, or integrated in the keyboard.

Single-use Universal Serial Bus (USB) tokens provide an alternative to smart card PC authentication systems. They are key-sized hardware devices that use an electrically erasable programmable read-only memory (EEPROM) to store access settings, and they insert in a standard USB port instead of a card reader, so there are no infrastructure costs. USB tokens can provide security for:

- System logon
- Network administration
- Network access

**Biometric Authentication**

Biometric devices authenticate users based on identification of physical features such as fingerprints, voice, or facial features.

**Secure Communications Over Public and Private Networks**

Transporting data securely over public and private networks is an important enabler of applications such as e-commerce, remote access, e-mail, wireless LANs, Internet telephony, and media distribution. Three key technologies are Public Key Infrastructure (PKI), the Secure Sockets Layer (SSL) protocol, and Internet-based virtual private networks (VPNs).

**PKI**

PKI provides the infrastructure to exchange information securely over networks. PKI is a system of digital certificates issued by trusted third-party certificate authorities (CAs) such as VeriSign or Entrust that verify and authenticate the identity of each party conducting an Internet-based transaction. The CA issues digital certificates, the digital equivalent of an identification card used in conjunction with a public key encryption system. CAs guarantee the identity of the two parties exchanging information. The associated public/private key pairs enable the two parties to share encrypted data. PKI provides robust security that is used in e-commerce and VPN applications. All PKI exchanges are encrypted.

**SSL**

SSL is used extensively for e-commerce transactions. The SSL protocol is used to set up a secure session between a Web client and a server. SSL-enabled browsers and servers authenticate each other (using PKI or other methods) and transmit encrypted data. Software applications are required to enable the use of SSL and, when invoked, SSL encrypts all data exchanged between the client and the server. A possible successor to SSL is the emerging Transport Layer Security (TLS) protocol. TLS is currently a proposed Internet Engineering Task Force (IETF) standard.

**Internet VPNs**

A VPN is a logical connection that provides privacy on public networks such as the Internet using technology commonly referred to as "tunneling." The heart of a VPN is the tunneling protocol and associated security mechanisms used to create secure paths or tunnels over the Internet. Internet-based VPNs can use various established tunneling protocols such as the Point-to-Point
Tunneling Protocol (PPTP). Two emerging VPN standards promise to provide Internet VPNs with more robust security features: the Layer 2 Tunneling Protocol (L2TP) and the Internet Protocol Security (IPSec).

The IETF has extensive information on PKI, PPTP, L2TP, and IPSec.

**Recent Standards and Industry Initiatives**

Standardization is the key to making security a pervasive technology feature on PCs. Until recently, most company security solutions have been proprietary and customized to fit their specific needs. As a result, these solutions are very expensive. As the need for IT security has grown from supporting specific applications to that of protecting the complete corporate infrastructure, the industry has pushed for standardization to make security more affordable and widely available.

**TCPA**

Recognizing that e-commerce applications require a more secure PC platform, the Trusted Computing Platform Alliance (TCPA) is a new industry working group that will focus on improving “trust” on computing platforms. The group will focus on building standard security features into the base platform (hardware, BIOS, and the operating system). Dubbed the “Trusted PC,” the platform could include features such as nonvolatile storage of symmetric or asymmetric keys, certificates, or other confidential information; hardware generation of random numbers; digital signatures; and hash functions. The goal is for computer users to be confident that they know who and what they are talking to, that the communication is confidential, and that the information is transmitted accurately. The Trusted PC will complement other security technologies such as the X.509 digital certificate standard, IPSec, PKI, smart cards, biometric authentication devices, and SSL. Formed in November 1999, the TCPA is developing a specification for a standard that is currently scheduled for release in June 2000. TCPA members include Dell, Microsoft, Intel, and 3Com.

**Microsoft® Windows® 2000 Security Features**

The Windows 2000 operating system has significant security enhancements, including:

- **Integrated PKI** — This infrastructure extends the Windows-based public-key cryptographic services to provide integrated services and administrative tools for creating, deploying, and managing public key-based applications.

- **Support for smart cards** — Under Windows 2000, smart card capabilities are integrated into the operating system. This integration makes it easier to set up and use smart cards on a PC for client authentication, interactive logon, code signing, and secure e-mail.

- **Support for newer authentication protocols** — Windows 2000 supports the Extensible Authentication Protocol (EAP), a programming interface that allows third-party security protocols to be installed and used.

- **Support for Internet-based VPNs** — Windows 2000 adds support for the L2TP tunneling protocol and IPSec. The operating system also enables hardware acceleration of IPSec, a potentially CPU-intensive technology. This support is enabling a new generation of network interface controllers (NICs) that include IPSec hardware acceleration.

- **Encrypting file system (EFS)** — The Windows 2000 EFS encrypts each saved file with a randomly generated key. This feature helps to secure data stored on hard-disk drives.

- **Single sign-on** for Microsoft Windows networks.

- **Active directory** for organizing and maintaining the security associations for the system.

These Windows 2000 features will help to drive more widespread and pervasive security technologies.

**Intel® Initiatives**
Intel's Boot Integrity Services (BIS) address the need of system administrators to securely update client systems. In addition, a new Intel initiative, the Preoperating System Authentication Services (PAS) envisions a preoperating system authentication architecture.

**BIS**

Part of Intel's Wired for Management 2.0 specification, these services are designed to help network administrators securely download software images. BIS provides for a trusted Preboot eXecution Environment (PXE) boot. At boot-up, the client systems check with a server for pending updates such as BIOS, hard-disk drive image, or operating system driver updates. After the server updates the client system over the network, the boot-up process continues. If the client computer supports BIS, the server sends a digital signature with the file updates. In this way, the client computer knows that the network boot image arrived intact and came from a trusted server. BIS is an emerging standard and deployments are just beginning to appear.

**PAS**

This initiative provides a preoperating system user authentication architecture that is independent of the BIOS, device, or operating system. PAS is particularly useful for portable systems, because it allows a user to be "bound" to the portable computer so that it is completely unusable if it is stolen. Using PAS interfaces, a portable computer could be configured to require user authentication to boot the system or access the hard-disk drive. Currently, the specification is expected the second half of 2000 and implementations will follow in late 2000.

Dell and Intel are development partners and Dell plans to monitor BIS and PAS for feasibility and relevance to Dell™ customers.

**Security Efforts in Specific Industries**

In addition to industry-wide standardization efforts, specific industries and the federal government are addressing more narrow vertical security requirements. These efforts are accelerating the development of standards that will benefit the entire industry. For example, the banking industry has launched the Banking Industry Technology Secretariat (BITS). The goal of BITS is to enhance security, develop standardized payment systems, and increase consumer confidence using the Internet for banking transactions. Another example is the Presidential Decision Directive 63 (PDD 63), which requires government agencies to protect their critical information systems and infrastructures against "cyber attack."

**Dell's Security Offerings**

Client computer security is a major concern for Dell customers, but often is not adequately addressed until a theft of mission-critical data or physical property has occurred. Proper deployment of security measures requires advance planning and knowledge of emerging standards. Dell works with leading security vendors and standards organizations to ensure that new security products are standards-based and that they meet the needs of Dell's customers. Conformance to standards enables Dell hardware to integrate into diverse customer environments.

Dell offers a variety of standard security features on Dell client systems designed for enterprise network environments—OptiPlex™ desktop computers, Dell Precision™ WorkStations, and Latitude™ portable computers.

**Theft Protection**

Dell client systems can be equipped with a number of security features to help deter system and component theft and to track stolen systems.

**Locks**

Dell Latitude portables, Latitude C-Dock II docking stations, Latitude C-Port II port replicators, OptiPlex desktop computers, and Precision WorkStations are equipped with standardized cable slots for security cable locks (such as Kensington locks) or padlocks to lock the entire system to a
desktop. In addition, OptiPlex and Precision systems have a chassis ring to allow the chassis cover to be locked, preventing the theft of valuable internal components.

**Asset Tags**

Asset tags enable customers to track systems. Dell OptiPlex, Latitude, and Precision systems are equipped with an asset tag utility that allows a user to enter the system's asset tag number. This number is retained as part of the BIOS settings on the system. In addition, DellPlus™, Dell's custom integration services, offers customized asset tags affixed to the outside of the system chassis.

**Toll-Free Theft Tracking Service**

According to the Federal Bureau of Investigation, over 90 percent of all stolen computers are never recovered. This low recovery rate exists, in part, because buyers of second-hand computers and hardware are often not aware that they are purchasing stolen equipment. Available in the United States and Canada, Dell's toll-free theft tracking number (1-877-DELLTHEFT) provides a way for customers who lose a Dell computer or who are victims of theft to seek recovery of their equipment. When a customer reports a lost or stolen Dell computer through 1-877-DELLTHEFT, it is logged in Dell's database of stolen equipment. If someone calls Dell to request service or support for a computer that is logged as stolen, service is denied and the call is routed to Dell's Global Security group for follow-up with the appropriate law enforcement agency.

**Phone-Home Capabilities**

Through DellPlus, Latitude portables can be configured with Absolute Software Corporation's CompuTrace software. CompuTrace is a fully Internet-enabled PC security and recovery solution for tracking and recovering lost or stolen computers. When connected via modem to a telephone line or the Internet, a "Tracking Agent" installed on the Latitude portable automatically and silently calls into the CompuTrace Monitoring Center at regular intervals to report the number it is calling from and its unique electronic serial number. If the portable is reported as lost or stolen, CompuTrace can report the system's location.

**Security Alerts**

Dell OptiPlex and Precision WorkStation systems are instrumented to generate a chassis intrusion alert to the local user the next time the system is booted after the chassis has been opened. These systems are also equipped with integrated 10/100 Ethernet NICs that enable alerts to be generated when the operating system is not running. These alerts can be sent over the LAN to system administrators when the chassis is opened or when an invalid BIOS password is entered. Recent OptiPlex systems are also instrumented to generate configuration change alerts over the LAN to a management console. The same capability is being implemented on Precision Workstations.

**Secure Access to Network Resources**

Dell offers factory installation of antivirus software on all Dell systems, and all Dell systems have standard password authentication capabilities, supporting BIOS and operating system password authentication. In addition, Latitude systems are equipped with hard-disk drive passwords.

Dell also offers smart card authentication devices factory installed through DellPlus, or nonfactory installed through DellWare™. For example, Dell provides a smart card solution for OptiPlex and Precision WorkStation systems through DellPlus. Dell plans to offer PC Card-based smart card readers for Latitude portable computers. These readers will work with industry-leading smart card solutions. Dell is also investigating fully integrated smart card solutions, as well as biometric authentication devices, for future Latitude systems.

In addition, Dell offers third-party file encryption software for Windows 95 and Windows 98 through DellWare. This software allows computer users to encrypt files that are saved to local hard-disk drives. This measure protects sensitive data if a system is lost or stolen. Dell systems running Windows 2000 include EFS.
Secure Communications Over Public and Private Networks

Dell currently offers VPN solutions through DellWare. And, Dell client systems running Windows 2000 support established VPN protocols, as well as the L2TP and IPsec protocols. An encrypting NIC with hardware support for IPsec encryption is currently available on Dell PowerEdge servers, and Dell plans to offer the NIC on OptiPlex systems later in the year.

Dell systems can be configured to work with any current PKI infrastructure, and systems running the Windows 2000 operating system will include native support for Microsoft's PKI infrastructure.

Conclusion

Dell will continue to incorporate security features into corporate desktop and portable systems. These features will address traditional security concerns such as system theft and data protection, as well as new customer usage models such as business-to-business e-commerce and VPNs. Dell will focus in particular on standard security technologies or technologies that are maturing through de facto support. The result will be more secure Dell client computers which, when combined with the new security features in Windows 2000, will help customers address their security challenges.