ATM SECURITY

LOGICAL SECURITY PROTECTION FROM THE INSIDE OUT

Self-Service Trusted Computing delivers enhanced protection against logical security attacks

Threats at the self-service channel come in many forms and are constantly increasing in frequency and sophistication. A single breach at the ATM can devastate an institution's brand and has been estimated to cost up to $150,000 per incident for card reissuance and reimbursement.

To assist FIs in implementing a high level of multilayered protection that incorporates some of the industry's most sophisticated defenses against automated teller machine (ATM) fraud, Diebold developed its comprehensive suite of ATM security solutions. The suite offers protection packages for each major security threat category—card and currency, physical and logical.

Often the most difficult attacks to detect, logical attacks target an ATM's software, operating system and communications systems. Logical attacks can be some of the most damaging in terms of the quantity of consumer data compromised. Logical fraud, which includes malware/hacking (violates the confidentiality, integrity or authenticity of transaction-related data) and malicious software such as viruses, worms, Trojans and rootkits, poses an ever-increasing threat to the security of ATM networks. To combat these threats, Diebold has developed its logical security offering to stay ahead of logical attacks at the self-service terminal.

Engineered to withstand logical attack vectors and hard drive removal, alternate system start-up, unauthorized basic input-output system (BIOS) or BIOS setting changes, and unauthorized boot sector or operating system boot loader changes, Diebold's Self-Service Trusted Computing offering delivers peace of mind for FIs and their brand.

Self-Service Trusted Computing

Encrypting hard drive
Diebold's Self-Service Trusted Computing offering features an Opal-Compliant Self-Encrypting Hard Drive. All data is encrypted and the hard drive is locked (not accessible), unless an unlock procedure involving the specific ATM the hardware was originally installed in or the use of ValiTech™ or the eToken supplied with the hard drive is used. In addition, the software on the ATM's hard drive cannot be modified for malware installation prior to reinstalling it into the ATM.

DIEBOLD
INNOVATION DELIVERED®

And, Self-Service Trusted Computing encrypts and locks the hard drive if the ATM boots from an alternate source other than the hard drive, such as an external CD/DVD drive, thumb/USB drive or external hard drive. In the event that the ATM boots from any of these sources, the hard drive becomes inaccessible.

Trusted boot
Diebold's Self-Service Trusted Computing delivers system software that identifies changes in the operating environment by verifying the integrity of the BIOS, boot section and operating system, and selected configuration information to assure that no unauthorized change has occurred.

Self-Service Trusted Computing examines the BIOS, BIOS settings, boot sector and operating system boot loader every time the system is started to ensure that a rootkit type of attack has not occurred. If unauthorized changes are detected, the ATM can be configured by the customer to:

- Halt the boot process (default setting)
- Continue the boot process and log the event to the hard drive

Administrative token
Diebold's Self-Service Trusted Computing offering features a Logical Administrative Key intended for service technicians from Diebold or non-Diebold Opteva® service organizations that need to access the administrative functions specific to Self-Service Trusted Computing. The administrative token provides two-factor authentication and a means to securely separate the administrative password from the SED.

In today's climate of increasingly sophisticated attacks against the self-service network, Diebold's ATM security suite for Opteva offers enhanced protection. Integrating cutting-edge hardware, software and award-winning services, Diebold's layered approach to ATM security casts a broad net of protection to help financial institutions deploy a level of technology that helps protect their customers, their assets and their brand.

Contact Information:
Diebold, Incorporated
P.O. Box 3077
Dept. 9-B-16
North Canton, Ohio
44720-8077

800.999.3600 USA
330.490.4000 International
email: productinfo@diebold.com
www.diebold.com

DIEBOLD
INNOVATION DELIVERED®