

Customer Whitepaper

Motion™ Tablet PC Security Basics

Table of Contents

Whitepaper Goals and Intended Audience	2
Security for your Motion Tablet PC	2
Thinking about Security	2
Areas of Vulnerability	3
Layers of Security	5
Motion LE1600 Security Features	6
Motion LE1600 Encryption Tools	7
Motion LE1600 Add-on Security Features	8
Conclusion	9

Whitepaper Goals and Intended Audience

This paper will introduce basic concepts of security and different areas of vulnerability. It will then highlight the features of the Motion Tablet PC and discuss how those features can be used to provide a more secure computing environment. This paper is meant to be an overview only of the LE1600 security features for Motion customers or prospective customers. It is not meant to be a guide for implementing these features or for designing a corporate security policy.

Security for your Motion Tablet PC

Motion Computing has strongly embraced the need for enhanced platform-based security for its Tablet PCs. The result of that commitment has been to provide safe and effective computing environment out-of-the-box that enables strong security protection. That base level offering will serve as the foundation for complementary add-on security technologies that will allow you to maximize your security protection.

The Motion Computing security architecture is structured on integrating various hardware security technologies and software security applications to deliver customizable, uncompromising protection, and performance. This architecture is designed to provide an extensible security framework that enables a wide array of security features. The multi-layered approach addresses vulnerabilities in four protection classes labeled access control, application and data protection, platform protection, and network protection.

Ultimately it is the organization or the end users decision as to how much protection is needed. For some, security policies may identify data as the most important asset. They may choose to enable existing and add-on security technologies that will provide the highest level of protection for their data. For other users, the tablet pc may be the most important asset and they can choose to enable existing and add-on theft protection technologies to harden their platform.

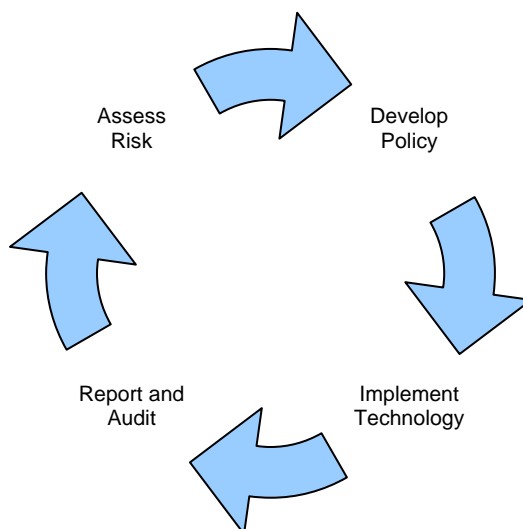
Thinking about Security

When developing a security strategy, it is important to do it top down. Good security practices require risk assessment, policy development, technology deployment, and follow-up reports and audits. The security technology and implemented policies will define the level of security achieved by a platform or organization.

Risk assessment is important for identifying areas of vulnerability and priorities. From this knowledge, security policies can be developed. Developing security policies involves a thorough analysis to reveal vulnerabilities and their potential harm and to identify possible control mechanisms and their associated costs. Once completed, a cost-benefit analysis should be performed to determine what controls and expenditures are appropriate for the given vulnerabilities. The result is a security plan and policies that describe what the security system will do. The next phase is to implement the policy along with the technology. It is also necessary to provide the end users with training to make sure they understand the security policies and how to use the technologies being implemented. Once the technologies and policies are implemented, it is important to do periodic audits to make sure the vulnerabilities have been addressed and any new ones are identified.

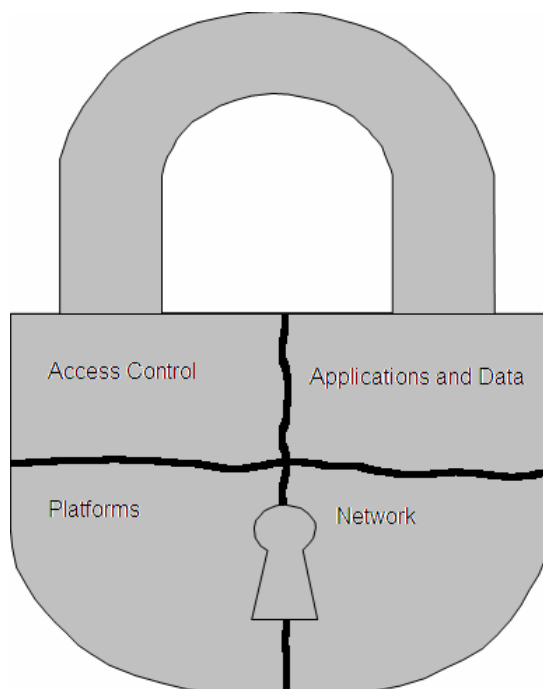
The security system assurance process will provide information describing how well the security system meets the security policies requirements. This provides a feedback mechanism back to

the security policies step so that improvements and changes can be made as attacks and vulnerabilities change.



Areas of Vulnerability

When assessing an organization's or platform's risk, there are four areas of vulnerability. These areas are access control, application and data protection, client hardware protection, and network protection. Security mechanisms are the techniques and technologies that can be deployed within each area to achieve the security policy objectives. The security policies will dictate the level of protection and security mechanisms implemented within each area.



Access Control

Access control is the process by which users are identified and granted privileges to information, systems or resources. Controlling how privileges are granted and how resources are accessed is critical to protecting private and confidential information from unauthorized users. Access control technologies properly identify people and verify their identity through an authentication process so they can be held accountable for their actions. The access control system should record and timestamp all communications and transactions so that they can be audited for security breaches and misuse.

There are two general types of access control, discretionary and mandatory. Discretionary access control allows the owner of the information or resource to decide how to manage it. They determine read and write privileges, and if the requestor can execute a particular file or service. Mandatory access control systems do not allow the creator of the information to determine who can access it or modify data. System administrators predetermine who can access and modify data, systems, and resources. Mandatory access control systems are commonly used in high security environments or where government regulations require privacy protection of data (e.g. HIPAA requirements regarding electronic medical records).

Some of the mechanisms available to address access control include unique user names and passwords, smart cards, TPMs and digital certificates.

Application and Data Protection

Application and data protection involves addressing security concerns associated with the operating system, the application programs and the data. The goal is to enable better application and data availability, reduce exposure to data loss and to maintain integrity of the applications and data.

Some of the mechanisms available to address these vulnerabilities include solid system and application configuration and patch management schemes, anti-virus, anti-spam, and anti-spyware applications, data encryption and signing and application hashing techniques.

Platforms Protection

Platform protection is primarily focused on addressing physical attacks on the client hardware. The threats include hardware theft, tampering, or destruction, and data disclosure, tampering or destruction. Some of the threats can be as simple as illicit copying of files from an unattended tablet PC. This is very dangerous because the loss of data can go completely unnoticed.

Some of the mechanisms available to address these vulnerabilities include never leaving the tablet PC unattended or in an operational mode when it's not being used, or using a cable lock or software-based tracking/recovery application to protect the hardware when it is left alone.

Network Protection

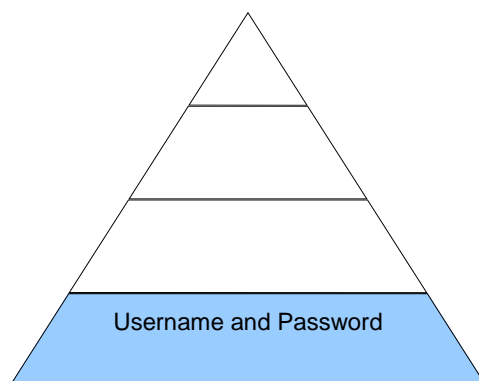
Network-based protection is implemented to address both "attacks attempted across a network" as well as "attacks against the networking protocols". Network-based attacks attempt to compromise a system through flaws in the internet protocol standard. These attacks are typically used to gain access to systems, applications and data. These attacks can also be used to cause a "denial of service" failure that would prevent users for accessing network resources. The network attack is usually the entry point for the next level of attack on the client and/or network.

Some of the mechanisms available to address these vulnerabilities include identifying and authenticating users, programs and systems, as well as restricting and monitoring activities to those whom have been authorized. Encryption and other methods should be utilized to provide confidentiality and integrity protection for data transmitted over the networks.

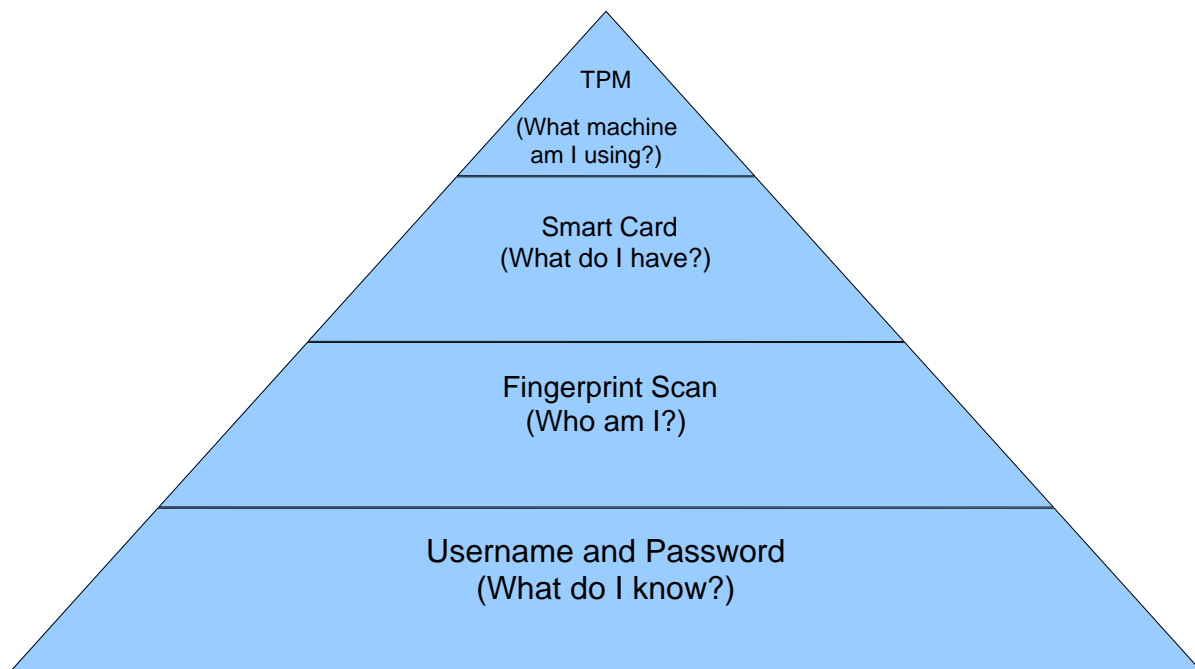
Layers of Security

Within each of the areas of vulnerability there are several security technologies and techniques available to harden the system. No technology by itself will completely protect a client or an organization. Instead, multiple technologies should be used together to increase the protection of a system. The individual layers combine to strengthen or harden a system.

Example: Single Factor Authentication



Example: Multi-factor Authentication



Motion LE1600 Security Features

The Motion Tablet PC has several security mechanisms built-in and ready to go for out-of-the-box protection. They can be enabled using the pre-installed software applications, by developing or using your own applications, or by installing a third-party application. Most of the built-in security technologies have software development kits available for custom development. Motion's technology partners also have business relationships with many third-party software vendors that have already developed or qualified the Motion Tablet PC for use with their applications.

Fingerprint Reader

The Motion Tablet PC includes a built-in fingerprint reader. Biometric authentication has two primary advantages over usernames and passwords. First, it is more difficult to hack a fingerprint than a password. Second, users don't have to worry about forgetting passwords and calling the IT department. Using passwords and biometric authentication together is more powerful than using either option by itself.

With the fingerprint reader you can securely and conveniently identify yourself with your fingerprint to applications requesting user authentication. The Motion OmniPass software application enables you to use the fingerprint for Windows logon, VPN authentication, file and folder encryption, and various web-based authentication requests.

Trusted Platform Module (TPM)

Motion's tablets also include a built-in Trusted Computing Group 1.1b compliant TPM. The TPM is a self-contained, secure micro-controller that is attached to the tablet PC motherboard. When enabled and configured, it provides the core level of trust for the platform security. It does this by storing sensitive data within the chip, instead of in the more vulnerable hard drive, providing authentication for the platform, protecting cryptographic functions, and communicating the attestable trust state of the platform. For example, an organization's security policy may require all machines that access the network to have a registered TPM. This prevents unknown machines from accessing the network and sensitive data. If you use a digital certificate to sign and encrypt email, you can store the keys for the certificate in the TPM.

The TPM can integrate with most secure applications that use Public Key Infrastructure (PKI) solutions through the Microsoft CryptoAPI or PKCS#11 interface. It uses 2048 bit RSA encryption to protect keys and secrets.

With the Motion OmniPass software application, you can use the TPM to enable strong encryption algorithms as well as for user and platform authentication. The Infineon TPM software application provides a personal encrypted hard drive partition and various maintenance functions. Some other applications that are also strengthened by the TPM include Check Point VPN/FW, Entrust Enterprise PKI Solution, Internet Explorer, Adobe Acrobat, Verisign PKI, RADIUS EAP, Netscape, NS Messenger Sun ONE PKI, and PGP.

Data Execution Prevention (DEP) and Execute Disable

DEP, a built-in OS level software technology, and Execute-Disable, a CPU hardware feature, enables stronger memory-protection policies to help prevent malicious code from executing in the data page segment of memory. The technology can help prevent block viruses and malicious code from taking advantage of exception-handling mechanisms in Windows. The Intel chipset combined with Windows XP Tablet PC Edition 2005 makes this technology available to every customer.

BIOS Level Security

The Motion tablet PC BIOS has several security features. The BIOS is built-in software that is separate from the operating system. It controls the keyboard, display screen, disk drives, as well as communication devices. If the operating system is damaged, the computer will still be able to

boot, allowing the user to repair the software installation by restoring or reinstalling the operating system.

Inside of the BIOS you can configure the system networking resources at the hardware level. For example, the Bluetooth and 802.11 radios can be disabled so that they do not appear present to the operating system. Supervisor passwords can then be set within the BIOS to prevent users from changing the configuration. The BIOS hard drive password prevents the system from being booted without entering a password. This can be used to prevent theft of information stored on the hard drive.

Security Lock Slot

All Motion tablet PCs are equipped with a built-in security lock slot to support security hardware such as lockable steel cables. The cables can be attached to tablet and/or docking station chassis to prevent theft. The hardware cable locks are widely available from manufacturers such as Kensington and Targus.



LE1600 Security Lock Slot

Motion Security Center

The Motion Security Center is a launch pad for the different security applications preinstalled on the Motion Tablet PC. Users can access the different security applications, find information on what each application is for, as well as answers to frequently asked questions.

Motion LE1600 Encryption Tools

Encryption is used to prevent any non-authorized exposure of data and information. The level of protection provided is determined by what encryption algorithm selected. Security policies often determine the level of protection needed and will dictate the encryption algorithm to be used. The Motion tablet PC ships with three encryption applications that can be enabled to meet your needs: Motion OmniPass, Infineon Personal Secure Drive, and Windows Encrypting File System.

Motion OmniPass

With the Motion OmniPass software application you can securely lock files or entire folders on your tablet PC. Files can be encrypted with any algorithm you require. The application enables the basic and enhanced Microsoft encryption engines called Cryptographic Service Provider (CSP). Once encrypted, the files can only be unlocked or decrypted by the owner. The owner is required to authenticate every time a file is decrypted. The owner can authenticate with any combination of the following methods, using password, the fingerprint reader, TPM, or digital certificates in a smart card.

Infineon Personal Secure Drive

The Infineon Personal Secure Drive (PSD) provides protected storage for your sensitive data using the TPM. The software creates a virtual drive that is only visible and accessible by the user. Data contained in the PSD is automatically encrypted using the 192 bit Advanced Encryption System (AES) algorithm. When a file is opened or moved from the PSD it is automatically decrypted once the user has authenticated with the TPM. The PSD can be designated as your temporary drive and folder to be used as an application “scratch pad” which

will ensure that all data (temporary and logs) is also protected. Each user can configure a PSD up to 200 Mb.

Windows Encrypting File System

Windows Encrypting File System (EFS) is a Microsoft XP NTFS-based technology that enables a user to encrypt the contents of a folder or a file with a private key code known by the user who encrypted it. EFS uses the Data Encryption System (DES) algorithm to encrypt files and folders. Windows EFS can use any of the Windows Cryptographic Service Providers (CSPs) available on the system. Those CSPs enable encryption algorithms with keys lengths from 40 – 128 bits.

Motion LE1600 Add-on Security Features

There are several add on security features available for the Motion Tablet PC.

Raak Technologies Smart Cards

Smart cards are used by organizations to authenticate employees and/or as a tamper-proof storage device for user and account identities. A smart card is a plastic card with an embedded micro-chip that securely stores data and runs applications. Smart cards support security applications like secure logon and authentication of users to PC and networks, storage of digital certificates, passwords and credentials, encryption of sensitive data, and wireless communication subscriber authentication. Web browsers also can use smart card technology to supplement Secure Sockets Layer (SSL) for improved security of Internet transactions. Further, smart cards can be used within Motion OmniPass as an authentication device to support the multi-factor authentication feature.

Raak Technologies is a HID vendor and CheckPoint OPSEC certified. The Raak smart card and Motion OmniPass solution is Control Break International's SafeBoot capable. Learn more > <http://www.raaktechnologies.com/>

OmniPass Enterprise Edition

For enterprises with IT departments managing many tablets, OmniPass Enterprise Edition is helpful for administrating the built-in security features of the Motion Tablet PC. OmniPass Enterprise Edition can support multi-device and multi-factor authentication, file and folder encryption with seamless file sharing, and server storage and backup of fingerprint data. Storing fingerprint data on a central server enables users to login to any tablet. If the fingerprint data is stored locally, users must first enroll in the machine before they can authenticate with the fingerprint reader. Learn more > <http://www.softexinc.com/>

Sunbelt CounterSpy

CounterSpy is an anti-spyware application. Spyware is a growing threat to computer security today. Legitimate spyware is used by different companies for market research and to improve a user's experience at their website. Cybercriminals use spyware to scan your hard drive for credit card numbers, bank account data, and other personal information. CounterSpy monitors different areas of vulnerability on your computer for Spyware and then quarantines or removes it. CounterSpy is also offered in an enterprise edition for easy administration and maintenance in organizations. Learn more > <http://www.sunbelt-software.com/index.cfm>

Transaction Security, Inc.

Crypto-Sign™ is a non-invasive biometric technology, based upon electronic sign verification and signature capture. It combines the benefits (and eliminates the disadvantages) of the Password/PIN and traditional biometric signature verification systems as a means of remote user authentication. In application the technology requires the submission of a secret sign (no display

or inking) on a PDA or digitizer, which is statistically compared to a previously established template for the sign. Learn more > <http://www.crypto-sign.com/>

IdentityMine, Inc.

IdentityMine is a professional services organization specializing in delivering business value through the strategic use of information technology. IdentityMine's Tablet PC solutions include a Windows-powered SmartClient application for the insurance industry, among other solutions developed for Microsoft, Hewlett-Packard, Google, and Accede Networks. Our high tech expertise and wealth of experience leveraging industry standards with service oriented architectures, federated identity, and xml-based web integration make us a vendor of choice for custom solutions. Learn more > <http://www.identitymine.com/>

SOFTPRO Professional GmbH & Co. KG

SOFTPRO is the leading vendor of systems for the verification of handwritten signatures, worldwide. The company's portfolio contains solutions for authentication processes and documents. Therefore static and dynamic (biometric) characteristics of signatures are extracted and evaluated. Learn more > <http://www.signplus.com/en/>

Square One

SquareOne is a full-service consulting firm that specializes in Security and Microsoft Business Solutions. SquareOne also does custom software development for mobile solutions based on MS technologies. Learn more > <http://www.squareone.com/>

Conclusion

Developing and managing a security policy for an organization can be time consuming and daunting, but is well worth the effort. The Motion Tablet PC has many integrated components that can help make this easier and provide a solid foundation to build on. Whether you are using the TPM to control and verify enterprise resources or using the built-in fingerprint reader to encrypt a roadmap presentation, the Motion Tablet PC provides the fundamental security components needed to support a strong security policy. If you would like to learn more about the Motion Tablet PC and its security features, please call 1 866 MTABLET.