

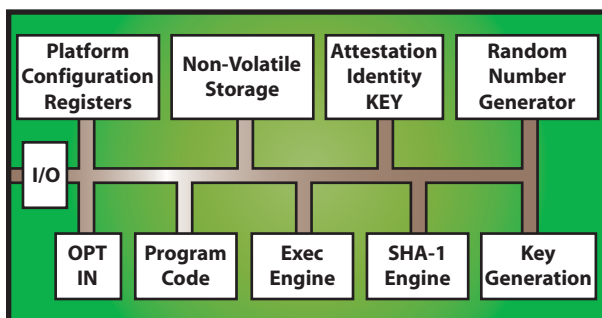
Trusted Computing

Taking the cost and complexity out of data & network security

Historically, significant revolutions in technology usage patterns take about twenty years.

- The steam engine took about twenty years before it was applied to transport;
- Telephones were used for about twenty years before inter-city calls could be made;
- The Internet was around about twenty years before the browser.

This is also the case for client security and the PC. The first PC was shipped in 1981. It took until 2003 before the major IC and PC manufacturers got together to implement a comprehensive yet affordable embedded hardware solution for data security, identity protection and network security. To complement this hardware revolution, Wave Systems offers software utilities and applications that accelerate the usage and adoption of this new security initiative.



Trusted Platform Management

In 2003, computer manufacturers started shipping PCs with a specialized security processor embedded on the motherboard. This specialized security processor is called the Trusted Platform Module (TPM). TPMs are independently manufactured by a number of leading semiconductor vendors. The TPM is a tamper-resistant device that provides a number of security functions:

- Random number generator
- RSA signatures, up to 2048 bits
- Secure non-volatile key storage
- PKI key pair generation
- Tamper-resistant packaging

Each TPM is shipped with a secret key stored in a non-volatile, non-readable register. All cryptographic operations involving this key are executed internally to the TPM. In this way, the root key cannot be stolen or copied. The reciprocal public key can be certified in a public credential. All transactions using this key pair are irrevocably bound to the PC containing the tamper-resistant TPM hardware. This is where the concept of platform trust is rooted.

The Practical Benefits of Hardware-Based Trust.

Client PCs have been a weak link in traditional security. Like a levee to retain water, enterprise security is only as strong as its weakest point. Client PCs present a number of security problems, including:

- Software-based keys and passwords can be stolen or compromised.
- Software-assigned IP addresses can be spoofed.
- PCs containing valuable data can be stolen.
- Lack of control over how people use valuable data stored on PCs.
- The ease with which valuable data can be transferred to removable media.
- Valuable data can be lost through P2P and other dark nets.
- Valuable data can be lost to spy bots and back-door viruses.

The flavor of attacks is changing from randomly distributed nuisance viruses to targeted criminal attacks. This shift is generating new security requirements. Encryption/protection is needed for data at rest inside the network and on mobile platforms. Strong network authentication and effective control over removable media and its duplication are also required. TPMs provide the root of trust to address each of these considerations. Software products from Wave harness the power of embedded TPMs to provide comprehensive security that is integrated and easy to use within a Windows environment. These include:

- **Data Protection**
 - File and folder encryption with hardware-protected keys
 - Secure sharing of sensitive data
 - Key management and access logging
 - Protected storage on removable media
 - Key archival and recovery
- **Identity Protection**
 - Hardware-protected storage for digital identities and passwords
 - Secure proxy server for digital identities and passwords
 - Application-aware management and indexing of strong passwords
 - Secure archival and recovery of digital identities and strong passwords
- **Network Protection**
 - Hardware-based multi-factor authentication, without external hardware
 - Combined authentication of user identity and of secure platform identity
 - Server-based biometric template matching
 - Centralized provisioning, management and enforcement of multi-factor policies
 - Fully integrated into Domain Controller, Active Directory and Microsoft Management Console

Software products from Wave Systems coupled with TPM-enabled PCs offer comprehensive security to a wide variety of users. The target users span from consumers to corporate users.

The Security Challenge

As business and commerce evolve to match consumer behavior, increased infrastructure is required. Business process outsourcing, external ISPs, mobile/remote workers and after-market customer access are universally used to lower costs and drive customer satisfaction. These trends demand more fluid and more porous network boundaries. This increases vulnerability.

On the other side of the vulnerability equation, the motivation for criminal activity has never been higher. The potential return on effort is very high. From a purely practical point of view, crime has become attractive. Cyber-criminals are not at risk of physical injury. Criminal identity can be obscured through IP reconfigurability and geographical independence. There also exists a wide variety of sophisticated tools and methods to assist the criminal intent.

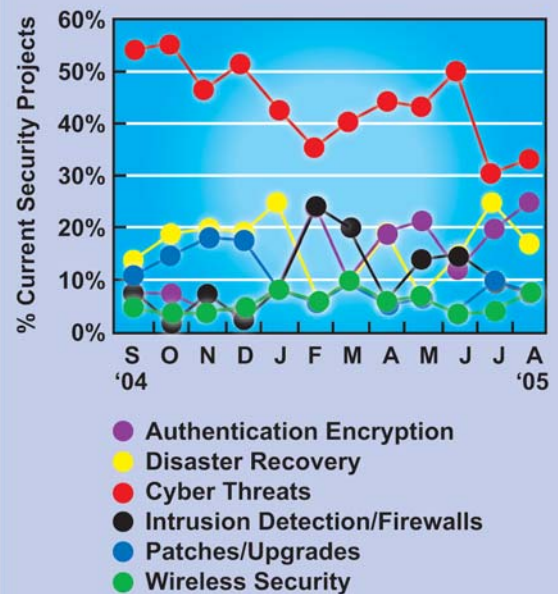
The nature of security threats is changing. The impact/risk of targeted criminal attacks is growing faster than the nuisance of cyber-hooliganism. Identity theft, theft of valuable data and targeted e-commerce attacks are far more dangerous than viruses, worms and spam.

Increasingly, traditional crime entities are focusing on the career and the business opportunities offered by networked commerce. The result is a greater diversity in attack mechanisms, including: network attack, physical theft and insider theft. It really does not matter how strong the firewall or the VPN is, criminals have social methods to circumvent standard HTTP filtering and TCP/IP analysis tools.

Unlike spam generators and virus creators who seek notoriety, perpetrators of targeted attacks seek to avoid detection. As can be seen in the graph (see right), the focus of IT spending is changing to reflect the increased targeted attack threat.

An integrated solution to protect data "at rest" and data "in transit" is required. Since the IT market is mature, business constraints exist on all sides: cost, ease-of-use, compatibility and interoperability. Wave Systems' products are based on the distributed power of TPM-enabled clients. This enables organizations to construct a robust "bottom-up" security solution. Traditional "top-down" approaches are prone to over-provisioning, feature bloat and complexity.

Quiet summer for virus outbreaks reflected in shift toward other security concerns



Source: Data Point Research: 8/9/2005

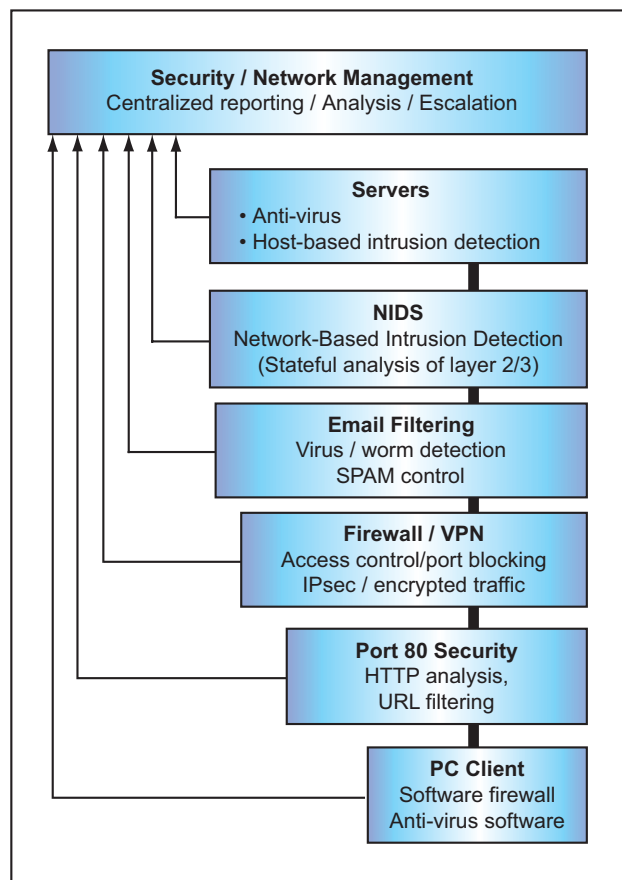
Traditional Multi-Layer Security

Information security and network security is big business. The total market was in excess of \$10 billion in 2004. Much of today's security products are based on the traditional "moat and drawbridge" approach. A myriad of appliances monitor access, filter content and analyze transactions.

The cost and complexity of acquiring, integrating and managing all these appliances is a large drag on the evolution of networked intelligence and networked commerce. The irony is that even those corporations that can afford the latest and greatest equipment, and a army of PhDs, still fail to provide effective security. The resulting lack of confidence is a threat to future growth.

We hear about the security breaches, which corporations are mandated by law to disclose. It is realistic to assume that many breaches go undetected and/or unreported. Existing domain centric security products and strategies are not sufficient.

Trusted computing enables a more complete solution, it enables an integrated data centric and domain centric approach. TPM-enabled clients and associated server products protect data at all stages of deployment, while also providing network security and identity protection. Software products from Wave Systems are compatible with TPM implementations from all IC vendors and PC providers. Server products from Wave provide centralized management, auditing and disaster contingencies. Wave server products integrate transparently and are fully interoperable with standard Microsoft management utilities.



Traditional Layered Security Model

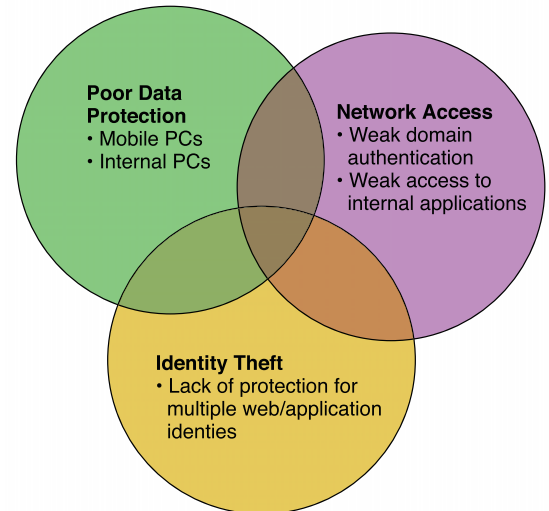
The Roots of Vulnerability

Metcalfe's law states that the value of the web increases to the cube of the number of connected entities. There should be a similar law that links criminal motivation to the cube of the aggregate value of all transactions conducted over the web. As business and commerce increasingly migrate to networked transactions, criminal attention increases. This is the "Sutton effect." When questioned by police on why he robbed banks, infamous bank robber Willie Sutton declared "Because that's where the money is."

The main vulnerabilities targeted in criminal attacks can be grouped into three categories. These are identity theft, data theft and network penetration.

TPM-based security products from Wave Systems cover all three bases with one unified suite of intelligent utilities.

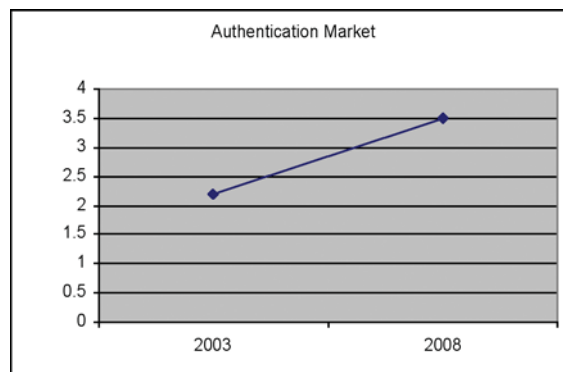
Wave Systems is dedicated to providing secure applications. Wave products transparently extend the TPM-anchored chain-of-trust and seamlessly integrate with existing Windows applications.



Elements of Vulnerability

Authentication – The Achilles Heel

Authentication is long recognized as a weak spot: a dizzying array of available products address the need for strong authentication. IDC predicts that the identity and access control market will grow to \$3.5 billion by 2008. The estimate is that 80% of this will be hardware; such as, USB keys, biometrics, etc.



Growth of Authentication Market
Source: IDC

According to analysts, the forces driving market trends are in a state of transition.

- Currently: Regulations (HIPPA / SOX) are driving authentication decisions
- Ultimately: Federated identity and service-oriented architectures (SOA) will drive authentication decisions

TPM-enabled PCs, in concert with products from Wave Systems, uniquely address the needs of two groups located at either end of the authentication market spectrum. These two target groups are:

- Users with high security requirements: At the high end of the market, users need strong multi-factor authentication. For this group, Wave client/server products provide:
 - PKI-based client platform authentication that is irrevocable.
 - Centralized management of policies for PKI, Biometrics and TPM credentials.
 - Policy granularity to provision-specific multi-factor combinations to match role-based security requirements.
 - Heterogeneous biometric capability: Wave “authentication server” products provide server-based biometric template-matching. The Wave architecture can be extended to accommodate different matching engines to manage vendor-specific templates.
 - The Wave “key server” is the anchor that balances distributed autonomy of TPM-enabled clients. Wave key server products provide centralized secure management and backup of TPM-secured keys. This provides secure insurance against disaster or malfeasance.

For these customers, products from Wave enable platform authentication and provide centralized management and management of multi-factor policies.

- Users with standard security requirements: At the lower end of the market, there are customers who wish to augment password authentication for regulatory compliance.
 - Wave Systems Corp. provides an integrated comprehensive solution that meets their needs and avoids the cost and complexity of external card readers and external biometric sensors.
 - Wave provides a cost-effective solution to leverage the secure PKI capabilities on TPM-enabled client PCs.

TPM-based trusted computing is uniquely suited to meet the evolving security requirements of many groups, including the needs of SOA and federated security. TPM-enabled hosts and clients are capable of autonomously negotiating trust. This low-touch, autonomous security is well-suited for business process flexibility, enabled by SOA and federated security.

Conclusion

In nature, distributed autonomy is the key to evolutionary success. In a similar fashion, trusted computing provides distributed security intelligence embedded in each client.

Networks of TPM-enabled clients provide a fabric of distributed hardware-anchored security. Networks of TPM-enabled clients provide the optimal security cost/benefit curve for organizations of any size. The client-based “bottom-up” approach yields robust security and efficient use of resources.

Security products from Wave Systems integrate TPM-based security intelligence with user applications. Wave products are transparent by design: this yields direct integration with standard Microsoft utilities and also enables interoperability with traditional and legacy security products.

The call to action for security-conscious PC buyers is to ensure that all future PC purchases contain an embedded TPM.