Network Security – How to Defend an Infinitely Expanding Frontier

Titu kumar , Rohit kumar jha, Sitanshu Mohan Ray

Corresponding author:-Mr Rohit Jha Institute of Engineering &Management Salt Lake, Electronics ComplexSector-v, Kolkata-700 091 INdia   Email: **jharohit999@gmail.com**

Abstract: *This paper is all about the network security, how to save your network from various type of attack. I am very thankful to all my friends and teacher who help me to write this kind of article*.

Key words: The Emerging Network Security Landscape, Trusted Platform Modules: Myths and Methods, Self Encrypting Drives: Securing Data at Rest, Restoring Centralized Network Management: Remote Management, Summary

Introduction

The increasing use of home offices and laptops has put an ever-expanding number of users, data, devices and applications beyond the security of the traditional enterprise network firewall. At the same time, organizations – and their IT administrators – are held to increasingly higher standards of accountability for breaches in data and network security. Unfortunately, the traditional tools for network security have not adapted well to the rapid decentralization of the enterprise network. Conventional security methodologies based on passwords and software fail to effectively authenticate users and machines on the network or secure data on lost or stolen laptops, or ensure compliance with laws that require disclosure of lost personal data. This paper will outline perhaps the most powerful, cost-effective and simple solution for bringing the scattered end-points of today's mobile networks back under the umbrella of a strong centralized network security architecture. It is built on three widely available, prove but poorly understood technologies: Trusted Platform Modules, Self-Encrypting Hard Drives and centralized (or remote) security management. This paper will not only help readers distinguish myth from fact about these technologies but will also build a strong case for how their combined application can re-establish network security as an enforceable corporate policy, rather than a strategy.

The Emerging Network Security Landscape

Few IT managers would argue that the task of information security has undergone a radical and irreversible expansion in the last decade. In addition to the conventional role of managing security on centralized networks, today's IT managers must also contend with an increasingly mobile work force that has moved more and more end-users, devices, computing applications and highly sensitive data beyond the safety of the enterprise firewall. In this new landscape, enforcing information security is comparable to defending an infinitely expanding frontier, and essentially protecting network elements "in the wild." As the exposures to risk have expanded, so has the price of failure. According to estimates by Gartner Research, the costs related to the loss of a single device or unauthorized access to a company's computer network1 may reach as high as $1.32 million dollars – even if the breach does not lead to any further security issues such as the misuse of the lost data. Much of the expense is driven by "Notice of Breach" laws adopted so far by 46 states and the District of Columbia. Such laws require companies to publicly report security breaches unless the company can guarantee the data is safe and cannot be misused by unauthorized persons.

Complicating the issue is the reality that conventional security measures for authentication and encryption have not adapted well as enterprise network users have become more mobile and scattered. Traditionally, limiting network access only to legitimate users has relied

on the use of passwords. While somewhat effective at authenticating users on a corporate terminal, however, passwords are easily forgotten by the user – especially if policy dictates passwords involve randomized and frequently updated sequences. More to the point, passwords can be easily compromised – providing minimal protection beyond the enterprise firewall.

As enterprise users and computers moved beyond the firewall, a number of authentication tools emerged, including digital certificates, biometrics, one-time password (OTP) tokens and smart cards. All these tools mark a definite improvement over passwords – especially tokens and smart cards, which provide a high level of trust for the road warrior class who rely heavily on laptops. But as use of laptops and work-at-home policies have expanded the number of telecommuters, so has the cost of acquiring, deploying and replacing tokens and smart cards, as well as their supporting software and hardware. Traditional data protection measures haven't kept pace to the new network environment
either. Again passwords, such as BIOS, OS and ATA passwords, provide minimal security against experienced hackers and offer no means of data encryption. A simple Google search of the phrase "unlock hard drive password" yields several options such as HDD Unlock and Password Crackers, which sell both standalone software products and services for less than $100.

Instead, the de facto standard for protecting laptop data has become software-based full disk encryption (FDE), which encrypts every bit of data that goes on a disk or disk volume, preventing unauthorized users from operating the machine.

More recently, Microsoft launched its own software FDE product, called Bitlocker, which is offered "free of charge" with select Windows VISTA and Win 7 operating systems. Coupled with other security tools (that we'll discuss presently), this signifies a compelling advance for securing mobile devices.

However, while software FDE delivers good protection, it remains quite vulnerable since encryption keys are accessible through "cold boot" and "evil maid" attacks. Plus, because software FDE relies on a laptop's memory and processing resources, it often causes a marked degradation in overall system performance — extending boot times and slowing overall productivity. Lastly, software FDE literally takes

hours to install and configure, further adding to the workload of an already overtaxed IT staff. In short, the use of authentication passwords and software-based encryption attempts to apply conventional measures to risks and challenges that are rapidly evolving past their scope. In addition to the limitations already listed, software-based security cannot guarantee the safety of data in the wake of a lost laptop or other security breach. Thus, the security in place does not comply with reporting requirements mandated by notice of breach laws, therefore failing to protect the enterprise against costly legal action. Put simply, a network that cannot guarantee the security of its end-points is not a secure network. Yet the basic tenets of information security still apply even as more data, devices, users and applications move beyond the firewall. In order to ensure the integrity of the enterprise network, IT managers still must:

1. Secure sensitive data, whether stored or transmitted
2. Ensure the identity of all devices and users accessing the network, and
3. Exercise centralized control over network security protocols, being able to prove compliance with security regulations
Most IT managers already know this. Although not commonly known, there are tools that can restore each of these tenets in the most mobile and fractured network, restoring them virtually overnight, with minimal cost. They include:

1. Trusted Platform Module (TPM) security chips to establish automatic and Transparent authentication of authorized network devices and users,

2. Self-encrypting hard drives (SEDs) to ensure unbreakable protection of data "in The wild," and

3. A software management platform that puts both encryption and device authentication at the fingertips of a centralized office, providing proof of compliance with data breach laws Of these three tools, the first two are already well-established, cost-effective and either installed on most enterprise-class laptops today or readily available as an option. Further, they are activated in a few simple steps. Most importantly, applied together, this trio of tools can restore the basic tenets of security on today's mobile network where it's most vulnerable – at every end-point.

Trusted Platform Modules: Myths and Methods

The term Trusted Platform Module (TPM) is not well-known to many IT professionals. Defined simply, it is a security chip attached to a computer's motherboard, thereby integrating security functionality directly into the device's hardware. Because the TPM chip is physically part of the device, it is uniquely suited for creating and verifying strong device identities and ensuring only authorized access to networks. Indeed, the business case for TPM is fundamentally the same case for strong, fully automated and transparent authentication of both devices and users on the enterprise network.

Unfortunately, IT managers who have looked into TPMs have probably encountered widespread misconceptions about the technology. Without exception, these perceptions arise either from a fundamental misunderstanding of what TPMs are, how they're meant to be applied or what the security needs of the modern enterprise network truly are. One of the most common myths presents TPMs as a bleeding-edge technology. In reality, they're probably already present in excess of 90% of an enterprise's total PC population. Leading vendors, such as Dell, Lenovo and HP, have been including TPMs as a standard component on all their business-class notebook and desktop computer lines for many years. And TPM-equipped laptops now comprise the vast majority of units in use. By the end of 2010, the percentage will approach 100%.

Another misperception cast onto TPMs is that hardware security is overkill when compared to "good enough" software solutions. Despite these lingering assertions, other hardware-based solutions, such as RSA SecurID® tokens, have enjoyed explosive growth over the past decade and are now in use by some 25,000 businesses who rely on them on a day to day basis. The extra degree of security that hardware tokens add over software helped justify their adoption – mostly to secure

remote user access. Ironically, however, this success has also exposed the downside of tokens, namely that their total cost of ownership increases in proportion to the number of employees using them. While a viable solution when used by an organization's small population of frequent flyers, tokens have become increasingly expensive to acquire, deploy and replace as enterprise laptop use has expanded. In addition, one-time password tokens are not natively supported by Windows, which imposes two separate pathways for users logging into the

corporate network: Logging on via a virtual private network (VPNs) requires users to have an OTP token, but, when users log on within the firewall (wired or wireless), they must provide a different credential, such as a password or smart card. In general, enterprises prefer to adopt a common user authentication experience to cut down on confusion, lost productivity and associated IT maintenance and help desk costs.Unlike OTP tokens, which only verify users, TPMs automatically authenticate devices trying to access the network. They are, in effect, built-in hardware tokens. Often pre-installed on a new laptop, they impose no incremental acquisition costs, and eliminate the "hard" deployment expenses that tokens incur. Thus, TPMs lower the total cost of ownership. More importantly, they are transparent to the end-user who then needn't keep track of additional hardware. For IT staff, that translates as reduced costs and fewer help desk calls stemming from lost or forgotten tokens. Further fallacies about TPMs stem from concerns over privacy, since they potentially provide a remote source with insight into how a laptop is being used. These concerns, however, confuse standards for consumer-level privacy with the more rigorous demands of protecting an enterprise network. Of necessity, corporations must place a higher priority on network integrity and compliance than on user privacy. Indeed, many corporations are required by law to ensure hackers cannot access the private client and customer information stored on their networks. That requires IT staff to be able to strictly manage PC usage and access, and mitigate and report data leakage.

In this context, the absence of TPM functionality on the enterprise network increases the threat to privacy. Most enterprise network end-users grasp this reality and readily accept security solutions built into their devices to ensure security policy compliance — from Web filtering, to policies about opening email attachments. Requiring an employee to access critical network resources using a company-authenticated machine with a TPM institutes an automated level of security that does not rely on the user's habits. As we debunk these myths, a picture evolves of what a TPM is not. But perhaps the biggest issue that TPMs struggle against is the general lack of understanding about what, exactly, they are, and what they enable in the modern enterprise network. By way of illustration, consider the design of mobile, cable and satellite networks – among the fastest growing and most secure networks today. All of them establish the identity of the endpoint device as the primary basis for

network security. More recently, the Apple® iPod, iPhone and iPad networks have also placed device identity as the key element for network access and delivery of services. In each of these cases, the network design principle is simple: Only "known" devices are allowed to access sensitive network resources. Another key design element is that the device identity is stored in, and protected by, hardware, not software. It therefore provides a permanent, protected identity for the device. In similar fashion, TPMs are hardware specifically designed to report on the state of a PC to ensure both the security and privacy of the user, while also protecting the integrity of the network. Hence, authentication is generally the first and most intuitive application of the TPM with an enormous impact upon end-point security. The vast majority of today's enterprises can activate TPMs already embedded in their current laptop fleet to strengthen security for VPNs and for wireless access. Also, as more users work remotely or access data and services online, TPMs can help "lock down" access to data to ensure only known devices are downloading email, financial documents, intellectual property and other sensitive information. While just one use of the TPM, this application has tremendous impact upon securing the cyber infrastructure. The TPM also holds great promise with the rise of Cloud Computing — an emerging Application platform that truly begs multiple questions: Who has access to the service? What data is being accessed, copied and distributed? Can organizations use Cloud services and remain in compliance with data protection laws?

A TPM does not inhibit access to Web services and content through traditional security Methods. It does, however, offer a hardware-based trusted connection where both the PC and the server can exchange information under the strictest confidence, verifying that the opposite party really is who they claim to be. The TPM is a hardware token — only enhanced and embedded into the motherboard of the PC.

Self Encrypting Drives: Securing Data at Rest

Establishing strong device authentication to prevent unauthorized access to your network is only one layer of an information security strategy suitable for today's landscape. The second is establishing impenetrable data security on the enterprise's mobile devices. As stated earlier, data need only be potentially compromised to impose significant costs to the enterprise. According to a recent study from the Ponemon Institute2, a security breach resulting from an errant laptop can cost the enterprise around $200 per record stored on that laptop. The study further observed that the average organizational cost of a data breach in 2008 was about $6.5 million dollars, depending on the public profile of the breach and the regulations that apply.

While the cost of a full disk encryption solution may vary, on average they cost around $100 per seat in volume.

As we established earlier, encryption software has not adapted well to the needs of today's increasingly mobile network. By comparison, self-encrypting hard drives (SEDs) offer protection that is always on; the keys never leave the drive, while assuring compliance with data protection regulations. How self-encrypting drives work is simple: Incorporating a closed and independent architecture, they include their own processor, memory and RAM, and impose very strict limits on the code that can run within their architecture. Encryption and decryption of data occurs in the drive controller itself, rather than relying on the PC's host CPU.

Every SED reserves a small block of internal memory isolated from the rest of the drive. These "protected partitions" securely house encryption keys and user access credentials. Once the drive is unlocked, data will flow normally in and out of the Drive. If you are an authorized user, you can access the data. If you are not, the drive will not grant access and the data cannot be obtained by any other means, such as traditional software-based attacks via malware and rootkits. Since the encryption key is created onboard the drive during manufacture and never leaves the drive's protected hardware boundary, it is impossible to steal and it is immune to traditional software attacks. No software – malicious or otherwise – can run on the machine until the drive is unlocked and the OS is booted. The "baked in" encryption of data also provides logistical and cost of ownership benefits over software solutions. Because encryption keys never leave the hard drive, there is no need for IT staff to spend time or money managing keys, or building key escrow and backup programs. Finally, SEDs do not draw on a machine's memory or processing resources, thus avoiding the marked degradation that software solutions often impose on system performance. A study by Trusted Strategies LLC showed a commercially available SED performed as well as a standard drive and handled large-file operations nearly twice as fast as three drives equipped with active software-based encryption.3

Like TPMs, SEDs are often regarded as an emerging technology that is not yet widely available. Again, however, the opposite is true. Leading hard-drive manufacturers including Hitachi, Samsung, Seagate and Toshiba all offer commercial SEDs. Further, these manufacturers are building SEDs that conform to the Trusted Computing Group's Opal standard – the industry benchmark for interoperability and reliability. In addition, PC vendors like Dell and Hewlett-Packard offer SEDs as a basic storage option. And, on average, specifying an SED from Dell costs about tens of dollars more than a comparable non-encrypting drive. Other leading computer manufacturers like Lenovo and Panasonic also offer SEDs on select machines.

SEDs are also supremely easy to implement. In the study cited earlier by Trusted Strategies4, software encryption tools took anywhere from 3½ to 24 hours to fully encrypt a hard drive. In contrast, a corporate IT department can phase SEDs in with the purchase of each new machine. Since the drive comes built-in and with encryption on, there is virtually no IT overhead or machine downtime required to turn on data protection.

SEDs are a natural complement to TPMs. Both technologies shift fundamental device security functions to a hardware environment. This not only extends the strongest security possible to the network's end-points, it also lowers the cost of ownership for laptops equipped with hardware-based protection. Plus, SEDs and TPMs both help circumvent software's intrinsic logistical, system performance and compliance issues.

Restoring Centralized Network Management: Remote Management

TPMs and SEDs help restore a high level of confidence to the end-points of the enterprise network. They ensure that data stored on mobile devices will remain secure even if the device is lost or stolen. And they guarantee that all devices and users trying to gain access are authorized to do so.

Another element of modern information security ties these two elements together and returns full management and accountability for all network end-points to a centralized corporate authority. More importantly, this third element is the one that restores the corporate enterprise's ability to define its information security as an enforceable policy rather than a strategy. The phrase "central

management of end-point security" covers a lot of territory, and it doesn't help to narrow the definition by explaining that the enabling technology takes the form of software and remote servers. Perhaps the best way to define what the term means is to describe the three basic key capabilities that any solution should provide: policy-based access controls, centralized administration and proof of compliance. Despite all the challenges posed by an increasingly mobile and remote workforce, today's corporate IT managers are still expected to centrally provision security policies to end-points across the enterprise, limit access of encrypted information to authorized individuals and remotely manage user credentials. Plus, most importantly, they must demonstrate their organization was, and is, compliant with regulations in the wake of a security breach. Establishing a data security policy isn't enough; IT managers must be able to prove provide proof that their policy was implemented and enforced. Not surprisingly, client application software has evolved in support of hardware-based security solutions. These solutions go beyond software FDE products that have been "modified" to support self-encrypting drives. Instead, they were designed from the ground up with only hardware security in mind. This means that there are no back doors and no security vulnerabilities that might have been introduced in "adapting" the code to support hardware. Such applications, available from Wave Systems, are designed to support all the on-board security features of TPMs and encrypting drives. For example, Wave Systems' EMBASSY® software is the only ISV that verifies pre-boot user credentials in the "secure partitions" of self-encrypting drives – thus enforcing policy-based access controls whenever a mobile device is powered on. It also supports a secondary external (USB) self-encrypting drive, as well. An additional feature is the support of Windows® single sign-on, which minimizes the number of passwords that users need to remember (and the frequency of help desk calls). Additionally, integration with Windows password update allows the drive access policies to be automatically updated with the OS, ensuring compliance with company password policies. Wave software also helps maximize TPM security features, such as the ability to move software-based digital certificates to the TPM environment, effectively converting them to hardware certificates. On a broader scale, this allows enterprises to set up hardware based PKI environments. IT administrators can direct their enterprise VPN servers to only authenticate machines with

hardware-based certificates, thus prohibiting users unable to verify credentials to their local hardware from logging onto the domain or network. For enterprise-wide deployments of TPMs and/or SEDs, Wave's EMBASSY Remote Administration Server (ERAS) provides robust policy management of users, credentials and access rights from one central location. Through native integration with existing directory structures and policy distribution mechanisms, assigning users and associated policies can be performed within the directory framework – dramatically simplifying deployment.

Today's data protection regulations demand that organizations can prove that adequate protection measures were in place, should a breach occur. Hence remote administration servers should deliver security logs and robust reporting capabilities to ensure compliance verification.

ERAS also provides support for ALL commercially available TPMs, including Intel® vPro. Instead of enabling TPMs machine by machine, such infrastructure tools help IT staff to activate, take ownership of and manage TPM policy over the entire enterprise from a central location. Once TPMs are available on the network, an enterprise can use any standard certificate authority and Wave's EMBASSY software to create hardware-based digital certificates for its VPN, wireless or other PKI enabled application – providing high security of the private key functions and the capability to assure device identity.

Summary

As the enterprise workforce continues to expand beyond the corporate firewall, the fundamental goal of IT administrators remains the same: To protect the integrity of the network by ensuring the security of all data, users, devices and applications – from the network's central servers all the way out to every scattered end-point. Most companies rely on a small arsenal of solutions to address this increasingly complicated landscape. Hardware-based security is not only the most powerful solution, it is also the simplest. IT organizations that care about which PCs they allow on corporate networks have found that the first step is to leverage the TPM for machine authentication. We've seen organizations turn their TPMs on to strengthen security for VPNs and for wireless access. And, as more users work remotely, and access data and services online, it becomes even more critical to manage their access to ensure only known devices with known

security profiles are downloading email, financial documents, intellectual property and other sensitive information.

Meanwhile, the need to secure data "in the wild" and prove compliance with notice of breach regulations has distinguished SEDs as the best-in-class option for data encryption. Designed, from the ground up, with their own secure environment, these self-contained devices offer the most secure and best-performing full disk encryption solution commercially available.

Finally, in today's connected world, a complete data protection solution requires more than solid authentication and encryption. Policy-based access controls, centralized administration and proof of compliance are all "must haves." Organizations need to be able to centrally provision security polices across the enterprise, limit access of information to only authorized individuals and, perhaps, most importantly, today's IT administrators must prove that security was in place in the event of a data breach. Wave's EMBASSY software, expressly designed to support SEDs and TPMs, provides all of the above mentioned capabilities and more.