



Protecting Network Access in the Wild

Today's IT managers must 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. This, coupled with the rising tide of regulations that require organizations to comply with increasingly higher standards of accountability for data security, has led to an explosive need for ensuring that only authorized entities get access to sensitive information. In this new landscape, enforcing information security is comparable to defending an infinitely expanding frontier, and essentially protecting network elements "in the wild."

User Authentication Falls Short

As enterprise users and computers have 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 are a definite improvement over passwords — especially tokens and smart cards. One example of this can be seen with RSA SecurID® tokens, which have enjoyed impressive growth over the past decade. The extra degree of security that hardware adds 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 they have become increasingly expensive to acquire, deploy and replace, as the number of telecommuters continues to grow, and corresponding enterprise laptop use explodes. In addition, one-time password tokens are not natively supported by Microsoft® Windows®, which imposes two separate pathways for users logging into the corporate

network: The use of OTP tokens for virtual private network (VPNs) access and the use of passwords inside the firewall. In general, enterprises prefer a common user authentication experience to cut down on confusion, associated IT maintenance and help desk costs.

Regardless of whichever authentication technology you are currently using, one thing is clear: Identity theft continues to rise at an alarming rate. Javelin Research found that in 2009 over 11 million U.S. adults became victims of identity fraud, a 12% increase over 2008, and a 37% rise since 2007. Therefore, how can the network and its associated data be secured if the only thing being verified are users' identities? Further, while using a token might protect access to data, it does nothing to ensure that, once available, the data can only be stored on authorized systems.

Can your current authentication solution do this?

- ✓ Strongly authenticate both the device and its user
- ✓ Provide 2-factor authentication without any incremental hardware acquisition, deployment or maintenance costs
- ✓ Be fully activated and operational in a matter of minutes
- ✓ Seamlessly integrate with your existing VPN and wireless infrastructure
- ✓ Present a common user experience both outside and inside the firewall

TPM: The Next Authentication Token

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. Because the TPM chip is physically part of the device, it is uniquely suited for creating and verifying strong device identities, thus ensuring only authorized access to networks. Indeed, the business case for TPM is fundamentally the same case for strong and transparent authentication of both devices and users on the enterprise network.

The TPM is a standards-based technology that is present on most corporate laptop and desktop computers. In fact, companies like Dell, HP and Lenovo have included TPMs as part of their standard hardware configurations on hundreds of millions of systems over the past several years. The TPM can securely generate cryptographic keys and can attest to the state of a PC — providing the basis for trust in a networked computing environment.

What does a built-in security chip have to do with securing network access? 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 end-point 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.

In similar fashion, TPMs are hardware specifically designed to report on the state of a PC ensuring 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. The vast majority of today's enterprises can activate TPMs already embedded in their current computer fleet to strengthen security for VPNs, as well as 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.



Scalable Enterprise Management

Wave's EMBASSY® software also helps maximize TPM security features, such as the ability to create hardware-based digital certificates. IT administrators can direct their enterprise VPN servers to only authenticate machines with these TPM-protected certificates, thus prohibiting users unable to verify credentials to their local hardware from logging onto the domain or network.

Wave's software 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.

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. A managed TPM solution is not only the most powerful authentication solution, it is also the simplest.