Authentication

To authenticate means to confirm that the request for access to corporate data or other resources is genuine, authentic or valid. Every time a hacker successfully phishes enterprise information, the ante is upped to find a more secure way to establish all network access points as valid.

The Myth of the "Strong" Password

Remember when there was so little valuable information stored outside the firewall that hackers didn't even bother stealing passwords? Those days are long gone, but end-users still cling to the familiarity of the password, whether using it to authenticate to their online banking site or the enterprise network. Despite the password's evolution into an alphanumeric, multi-character monster, however, it hasn't kept pace with the changes in the security landscape. Today, there is simply no such thing as a password strong enough to keep a diligent hacker out.

Passwords Are a Dangerous Attack Vector

With the advent of social media, there is so much information out there about each of us that crafting a credible phishing message that can fool even security professionals is entirely possible. From stealing an enterprise user's credentials, it is a short hop to hacking into the enterprise network and going after the crown jewels. Even if the enterprise enforces strict password protocol, there is always the risk that an employee will use the same password on an unsecured site, resulting in potentially compromised credentials. The stolen password can then be used to access sensitive data the employee keeps on other websites such as gmail or Dropbox, or even allow the hacker access back into the corporate network.

The proliferation of valuable information protected only by a password has improved the incentive for hackers. In fact, most current malware efforts are directed at obtaining access to user/password pairs or to information that can be used to craft additional credible phishing attacks against contacts of a subverted user's machine. That's a lot of pressure to put on a weak link. Brute force attacks are now capable of cracking the majority of passwords, even if hashed when stored, within a time frame of minutes to days—all without setting off enterprise alarms.

The only way to fix the password problem is to take them (and other human data) out of the equation as primary methods of authentication.

Additional Authentication Factors

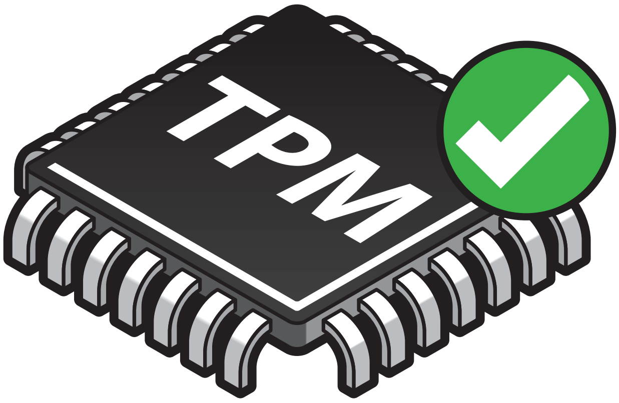
Despite security concerns, organizations still primarily control access to enterprise IT resources by checking usernames and passwords against an enterprise directory. But in cases demanding higher levels of assurance, additional authentication factors are often added – OTP (One-Time Password) tokens, smartcards, USB tokens, and biometrics.

These are stronger than passwords in part because they can't be guessed by knowing what street someone grew up on, but also because they represent a physical authentication which a remote user carries with them, making them much more difficult to hack.

- OTP tokens generate random passwords that can only be used once
- Smartcards (such as Common Access Cards, or CAC) look similar to a credit card and unlock access either by being held over the laptop (contactless) or inserted into the laptop (contacted)
- USB tokens are inserted into the machine to provide credentials
- Biometric readers verify the user's identity by scanning a physical attribute—fingerprints, for instance

Any one of these is more secure than a password. But no technology is unhackable. Remotely authenticating to the enterprise and accessing sensitive data often requires an increased level of

> "A good rule of thumb is to combine something you know, something you have, and something you are."



Solution Brief

wave®

assurance. To answer this challenge, the industry typically recommends adding another layer of authentication. A good rule of thumb is to combine something you know, something you have, and something you are.

Moving Beyond User Authentication

The right combination of these factors offers a high degree of assurance that network resources are secure. However, all these factors have one thing in common: their aim is to authenticate the user. But what device is being used to access these sensitive resources?

With the right tools, devices are actually easier to identify with a high degree of assurance than are users.

Wave's Solution: Start with the Device

TPMs (Trusted Platform Modules) are hardware security chips embedded into a computer's motherboard. Developed by the industry-standard Trusted Computing Group, TPMs ship on most business-class PCs today, and have for several years, with the result that more than 600 million devices worldwide are already equipped with TPMs. The TPM is the hardware root of trust that can be used to secure credentials and certificates, authenticating devices to networks with a high degree of assurance.

Wave can provide authentication through "something you have" without requiring employees to carry an additional device. This way, remote employees are still authenticating with a non-transferable, non-duplicable credential that greatly improves an organization's security by storing credentials inside the TPM.

Can Your Password Do This?

Using TPMs makes cloning of credentials highly impractical, because it requires physical access to the device. This not only prevents external attacks from hackers, but also greatly improves accountability and compliance as internal sharing of credentials is also made much more difficult. Because they are already included in many enterprise machines, TPMs make deploying a secure authentication solution easier and cheaper than deploying and maintaining an add-on solution like smartcards. IT can remotely provision and deploy TPMs already present in enterprise machines simply by rolling out a management solution such as Wave's EMBASSY Remote Administration Server (ERAS).

With authentication secured by ERAS-managed TPMs, the enterprise is able to secure each of the following, from one centralized console:

Secure WiFi

Instead of using a password to sign on to Windows and then another to sign on to WiFi, users can authenticate to their TPMs and their TPMs will automatically provide credentials to sign them on to the enterprise WiFi using 802.1x. This better secures enterprise wireless by requiring the stronger, hardware-based credentials of the device, but it also streamlines user experience, increasing employee productivity. By completely foregoing the SSID password, nobody can gain access to enterprise-wide WiFi by stealing a device and extracting the credentials.

Secure DirectAccess

Microsoft's DirectAccess provides password-free network connectivity without traditional VPN, and has the advantage of being integrated into the Windows platform. Using ERAS, enterprises can store DirectAccess credentials on the TPM and add hardware-strengthened security to their DirectAccess program, providing full access to any internal resource without interfering with a seamless user experience.

Secure VPN

ERAS can also secure traditional VPN, storing credentials in the TPM and allowing IT to secure network resources against unauthorized devices. By securing and automating VPN authentication this way, enterprises don't have to worry about token or smartcard deployment, and can immediately detect theft or loss.

Use Virtual Smart Cards

The hardware-secured credentials of the TPM can be used to replace deployments of smartcards. By using hardware embedded in the machine itself to authenticate to the network, the need to regularly re-deploy smartcards is eliminated, and users aren't required to carry another piece of technology.

Wave Systems EMEA

Northern Europe
50 Broadway
St James Park
London SW1H 0RG
United Kingdom
+44 1235 520956
emea@wave.com

Netherlands
Jan Pieterszoon
Coenstraat 7
2595 WP The Hague
Netherlands
+31 (0) 70 799 9326
emea@wave.com

Central/Eastern Europe
Excellent Business Center –
Westhafen Tower, Westhafenplatz 1
D-60327 Frankfurt am Main
Germany
+49 69 959 32 393
emea@wave.com

Southern Europe,
Africa & Middle East
La Grande Arche-Paroi Nord
92044 Paris La Defense
France
+33 1 40 90 33 44
emea@wave.com

Israel
32 Habarzel Street
Tel Aviv 69710
Israel
+972 3 6442662
emea@wave.com

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238, USA
+1-877-228-9283 · Fax +1-413-243-0045
www.wave.com