Guard against identity theft with secure and transparent device authentication – the foundation for network security and personal privacy.

Ensuring Identities in a Digital World

Javelin Research recently reported that in the past year the number of identity fraud victims in the United Sates increased 22% to almost 10 million people — that's about one new victim every three seconds. So how are sites like Salesforce and Google verifying that Jane is really Jane? Or, how does "corporate America" know it's actually Bob who is accessing the quarterly sales numbers from the network?

Whether you're logging into Google® Apps or onto your company's Microsoft® Windows® domain, it is likely that you are using a password. While passwords provide a level of familiarity to consumers, they pose an increasing number of security problems for online service providers — as they are easily phished or pharmed. Similarly, for businesses, passwords provide only a weak level of security as they are easily guessed or "shoulder surfed." Many organizations have attempted to bolster password security by instituting Draconian policies mandating that passwords be changed routinely, contain upper- and lowercase letters, numbers and special characters. This complexity, however, comes at a substantial cost in the form of help desk calls and lost productivity. In the end, these practices actually weaken the security of the network as users must write down passwords on sticky notes and white boards simply to remember them.

Breaking the Password Problem

Why haven't widely available solutions such as transaction profiling or one-time password tokens done more to prevent identity theft? Over the past few years, online service providers such as banks have initiated transactional "monitoring" programs that watch for strange consumer behavior and adapt service-level permissions accordingly. However, while this might limit fraudulent transactions, it doesn't prevent one's identity from being compromised in the first place. And while two-factor token solutions have been used for decades to secure virtual private networks, they are only cost effective for a small percentage of employees.

Protecting confidential information is a top concern for organizations and consumers alike. What can be done to reduce the number of identities compromised each year and, in turn, increase the security of both public and private networks? Consider this: an identity solution that is factory-installed, uses standards-based technologies, can uniquely verify a PC, cannot be compromised and is already deployed in the hundreds of millions.

Be Confident on the Internet

As web-based applications and services increase in both number and importance, knowing who is on the other side of the cloud is increasingly vital. However, the proliferation of "on demand" communications has resulted in an enormous amount of sensitive information stored within the cloud. That fact is not lost on criminals — who live in a society where information is king.

Wave's online identity service allows you to create a single, secure, user-friendly token that is accepted at thousands of websites including Facebook, Google and Salesforce, eliminating the burden of trying to remember a list of countless passwords.

A standard protocol called OpenID makes web single-sign-on possible. Create an account with an OpenID provider such as Wave with simply a username and email address. Wave's identity service uses this information to create a token that can be used at any site that accepts OpenID logins. What makes Wave's identity service unique is that it takes the single-sign-on convenience of OpenID and combines that with the hardware security built into your computer. Now, your favorite websites can verify access without you having to reveal any personally identifiable information — much like your cable or satellite TV box verifies whether or not you have subscribed to HBO®. No more worrying about hackers — they cannot pretend to be you without your computer.

The United States government is leading the way for identity services based on OpenID and Information Card protocols by adopting them for their open government initiative. This open identity program is a key step in President Obama's memorandum to make it easy for individuals to register and participate in government websites — without having to create new usernames and passwords.

What do PCs and Cell Phones have in Common?

As the mobile workforce continues to expand, IT departments continue to grapple with making information readily accessible to employees while keeping the bad guys out. Whether directed by government regulations or motivated to safeguard your brand, protecting sensitive information is no longer optional.

Years ago mobile phone carriers had a major problem with cloned phones — resulting in unauthorized users on their wireless networks. This potentially serious issue was averted when mobile phones began to incorporate SIM cards for authentication. Now only Verizon phones can access the Verizon network — because of hardware-based device security.

Today, virtually every business class PC comes with an embedded security chip called a Trusted Platform Module (TPM), an industry-standard security chip that can be used for authentication and encryption. There are hundreds of millions of PCs worldwide containing TPM chips. Since TPMs are physically part of the PC, they are uniquely suited for creating and verifying strong machine identities used for network access — similar to how SIM cards are utilized for mobile phone networks.

Wave's EMBASSY® Security Center is a client application that enables TPM security by providing the low-level hooks required to communicate with the hardware, as well as the higher order logic needed to integrate with applications. Since TPMs and Wave software ship factory-installed from leading PC vendors, businesses can easily add hardware-based device authentication to their networks, providing a high level of security and transparency without breaking the bank.

Device Authentication Benefits:

World Wide Web:

- *Simplifies web sign-on: single, secure, user-friendly token accepted at thousands of websites*
- *Provides two-factor authentication for a higher level of trust*
- *Creates tamper-resistant device identity for authentication and RISK scoring*
- *Eliminates hardware security deployment costs — hundreds of millions installed and growing*
- *Reduces the threats from phishing and pharming attacks — cutting down on fraudulent transactions*
- *Limits exposure of personally identifiable information (PII)*

Corporate Network:

- *Increases network security and integrity — only authorized devices on your network*
- *Prevents the introduction of viruses and malicious software by "unknown" machines*
- *Limits possible attack scenarios — only authorized machines can access network resources*
- *Strengthens user authentication — reducing the threat associated with identity theft*
- *Reduces data breach exposure when coupled with self-encrypting drives*
- *Lowers costs associated with virus and data breach recovery*

03-000250/version 1.03

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE • fax (413) 243-0045
www.wave.com

wave®
Simplifying Encryption and Authentication