Virtual Smart Card 2.0 from Wave

Cyber-threats are everywhere, but with Wave **Virtual Smart Card 2.0** (Wave VSC 2.0) enterprises have a hardware-based, tokenless, two-factor authentication security solution with the security of a hardware token solution and the convenience and cost savings of a software token solution.

Wave VSC 2.0 delivers strong two-factor authentication using the Trusted Platform Module (TPM), the embedded security chip built into enterprise PCs. Wave empowers IT with management of the TPM and VSC 2.0. Companies successfully use Wave VSC 2.0 to secure VPN access, web applications and other certificate-based applications, like Wi-Fi with 802.1x, remote desktop, or Windows-user login. Use the security that's already been deployed and save money with Wave VSC 2.0.

Every month we see headlines highlighting mammoth breaches (i.e. EBay, JP Morgan Chase, Sony, Target, etc…). In each case, millions of records were stolen, corporate images were tarnished, and enormous costs were incurred as a result. And equally disturbing, more often than not the attacks go undetected and as a result important information is stolen.

wave®

Access control best practices and regulations recommend two-factor authentication (2FA).[1] Token solutions are the most common 2FA solutions. Yet, hardware tokens are expensive, easily misplaced, and unwieldy to use. Software tokens are subject to a variety of attacks creating a false sense of security.

This begs the question: what should security-conscious companies do? TPMs have been installed in all enterprise-class PCs and laptops since Windows Vista. Wave VSC 2.0 leverages the TPM to create an embedded hardware root-of-trust to secure credentials and certificates. The result is a device with the security of a hardware-based solution with the convenience and cost savings of a soft token solution – the best of both worlds.

Common Approaches to Two-Factor Authentication

Hardware tokens like the RSA SecurID and smart cards have been successful for 2FA, but in some cases their infrastructures have rendered them vulnerable. RSA SecurID tokens use a proprietary symmetric algorithm. The symmetric key has to be stored both in the token and on a server. If a hacker, for example, can get the key list they have full access rights of the valid user. In March of 2011, RSA was hacked and it appeared as though the hackers gained access to the symmetric seed keys.[2] Following that attack, Northrop Grumman and Lockheed Martin, which used RSA SecurID, were attacked. It is suspected the attacks were related to the RSA attack.[3] Smart card systems have been deployed at most federal government agencies, but report a total cost of more than $200 per employee.

An often unanticipated and expensive added cost of hardware tokens is replacement. An informal survey of five companies indicated on average 25% of the hardware tokens in an organization had to be replaced each year because many were lost or damaged. When companies tallied up the overall cost of hardware tokens alone it was substantial – an average annual cost of $32.91 per user.[4]

[1] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf
[2] http://www.cnet.com/news/rsa-cyberattack-could-put-customers-at-risk/
[3] http://www.scmagazineuk.com/study-states-benefits-of-smart-tokens-over-hard-and-soft-options/article/248836/

Software Tokens have emerged as a less expensive alternative to hardware tokens. There are multiple methods used by competitive companies, which deploy soft token systems. In general regardless of the soft tokens method, they create a false sense of security due to their ability to be hacked. It's like installing a door lock that opens if you simply twist hard – you feel safe but you're not. Examine the following attack scenarios for soft tokens:

- **Software Tokens on a PC**

  Two examples of soft tokens are the RSA SecurID Software Token and the Vasco Software DIGIPASS. When the soft tokens are implemented on the same platform that is being used to request access to a resource, malware on that platform has a much higher chance of successful theft of the token credentials and secrets that can then be used to bypass user authentication. Local OTP generation requires secure storage of a secret key/seed, access to current time and/or counters, and isolated execution. Secure storage and isolated execution are extremely difficult to obtain on standard platforms when a token is implemented in software. Without secure storage and isolated execution, the token can be copied to another platform or subverted and used by malware.

  In May 2012, Behrang Fouladi, a researcher at SensePost, devised a method that attackers with control over a victim's computer can use to clone the software token that RSA's SecurID uses to generate one-time passwords. Fouladi noted that both RSA and its customers have been targeted by highly motivated hackers, so attack scenarios in which PCs are infected or stolen aren't unrealistic. He suggested the sensitive data should be managed by an industry-wide specification known as the TPM, or trusted platform module.[5]

[4] http://arstechnica.com/security/2012/05/rsa-securid-software-token-cloning-attack/

Software Token on a Smartphone

Software tokens on a smart phone have some limited protections against physical attack, but they are significantly less robust than physical tokens. It is now common to acquire malware on a smart phone, but very uncommon on a hardware token.

Implementations that generate OTP values in mobile phone applications also require secure storage and strongly isolated execution. Malware has been identified that can access secure storage and keys of OTP applications by reading the database in application directories. In addition, other malware can acquire OTP values from applications and forward or use them before the valid user can enter the value.[6]

High-end smart phones have some limited protections against physical attack, but they are significantly less robust than physical tokens. It is now common to acquire malware on a smart phone, but very uncommon on a hardware token.

Even when malware has only infected one platform, it can spread from a PC to a mobile phone, or vice versa, when the devices are tethered or when the devices share the same LAN/WAN. Subsequently, the malware can launch Man-In-The-Middle attacks.[7]

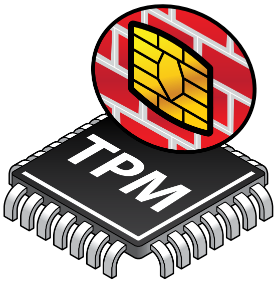
Remotely Generated Code to Smartphone (SMS)

Transmission of OTP values by SMS is an inexpensive solution that is easy to implement. However, SMS transmission has long been known to be susceptible to a number of attacks:

- Local capture of the SMS transmission
- Social engineering attacks such as convincing the service provider to forward calls and messages to a new number, modify the telephone number on the SIM card of the attacker's handset to copy the victim's number, and a number of recovery attacks due to supposed lose or stolen devices

[5] http://blogs.gartner.com/mark-diodati/2012/06/27/rsa-securid-crypto-and-satans-computer/

In addition, researchers recently identified 207 samples of Android malware capable of stealing SMS messages.[8] Malware on the smartphone can intercept the SMS, hide it from the user, and then forward it to another device for use with a stolen PIN/password from the associated user – something that is increasingly common today.



Wave VSC 2.0 is relatively new, but the supporting hardware, the TPM, has been shipped on enterprise class PCs and laptops since Windows Vista. The TPM is an industry standard chip (Trusted Computing Group and International Standards Organization) on the motherboard designed to deliver hardware-based security. The TPM stores non-exportable private keys, performing asymmetric cryptographic calculations within the chip, never revealing the secrets and making them virtually impenetrable to attacks or corruption.

Wave VSC 2.0 leverages the TPM to create an embedded hardware root-of-trust to secure credentials and certificates. The user experience with a VSC is simple: he or she logs in with a PIN or passphrase (authentication factor number one). The TPM (authentication factor number two) then transparently authenticates the user and the device to the network and connects the user to all the authorized services. Wave VSC 2.0 seamlessly works with Windows 7, 8, 8.1 and Windows 10 supporting enterprises as they migrate to newer Windows versions. Better yet, the Wave VSC 2.0 solution works virtually everywhere a standard smart card can be used – a few examples being Windows login, 802.1x, VPNs, and even virtual desktop applications.

We know hardware tokens offer the best security, but software is the lowest cost and easiest to implement. Wave VSC 2.0 delivers hardware security at cost similar to software tokens. Utilizing the TPM, which is already purchased and deployed in the enterprise, Wave VSC 2.0 uses security designed in, not patched on.

[6] http://fc14.ifca.ai/papers/fc14_submission_127.pdf

Most IT departments have heard of TPMs but don’t realize their machines already have them. Wave VSC 2.0 software empowers IT departments to remotely turn on and manage the TPM through the entire VSC lifecycle.

Method	Cost	Ease of Use	Security	Easy to Lose	Extra Device
Hardware Token	High	Easy	High	Yes	Yes
Software Token	Modest	Reasonable	Poor	No	No
Wave VSC 2.0	Modest	Easy	High	No	No

Conclusion

When evaluating two -factor authentication solutions, consider the facts; hardware token systems are expensive legacy solutions and are becoming a thing of the past. Software tokens – sometimes deployed on mobile phones – are taking up some of the slack, but the usability and security are serious impediments.

Wave VSC 2.0 is built on secure integrated circuits already in the hands of users (in their PCs). There are no tokens to lose. It is easy for users to use – just enter the PIN. Both the user and the device are authenticated to the network. Wave VSC 2.0 total cost of ownership is comparable to software tokens with much higher security.

About Wave
Wave Systems Corp. reduces the complexity, cost and uncertainty of data protection by starting with the device. Wave leverages the hardware security capabilities built directly into endpoint computing platforms themselves. Wave has been among the foremost experts on this growing trend, leading the way with first-to-market solutions and helping shape standards.

03-000432/ version 1.00

Copyright © 2017 Wave Systems Corp. All rights reserved. Wave logo is trademark of Wave Systems Corp. All other brands are the property of their respective owners. Distributed by Wave Systems Corp. Specifications are subject to change without notice.

Wave Systems
401 Congress Avenue
Suite 2650
Austin, TX 78701
sales@wavesys.com

(413)243-0045
www.wavesys.com