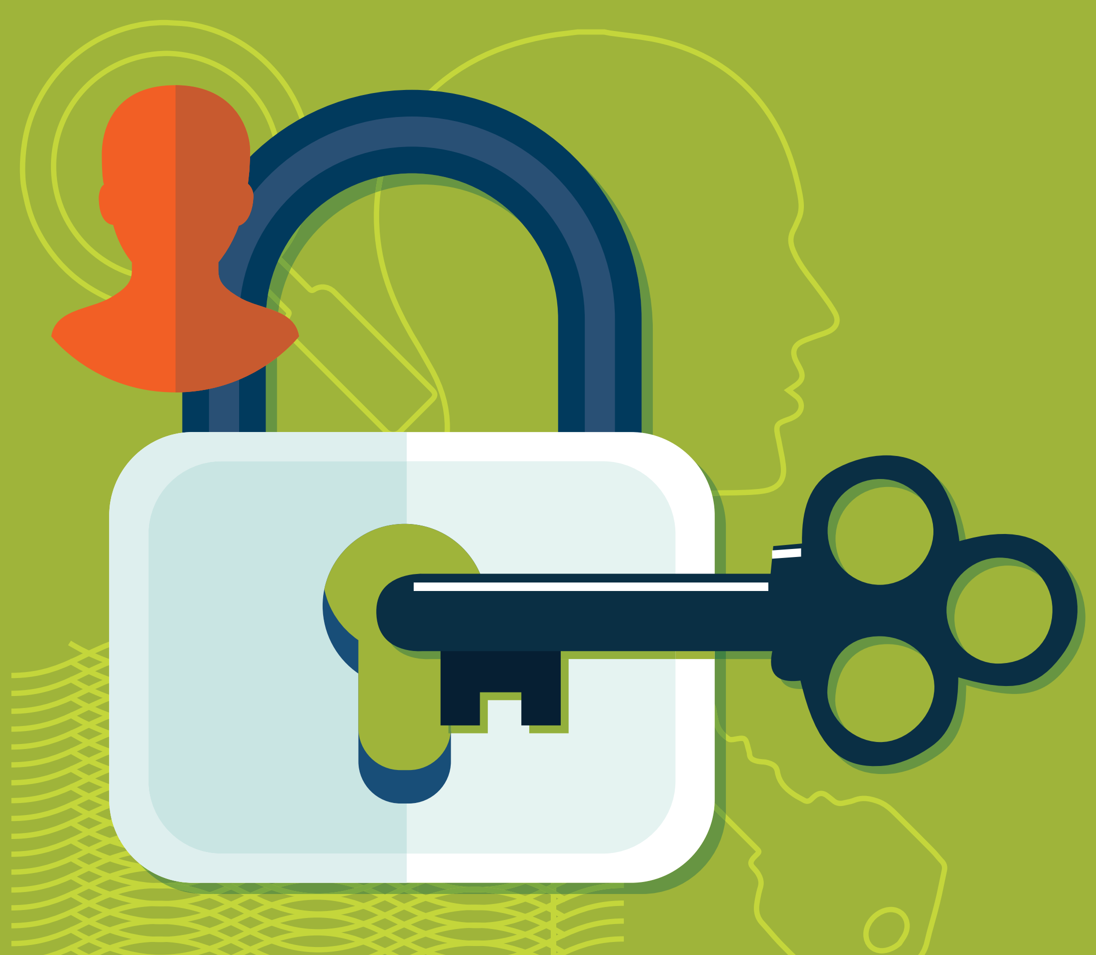
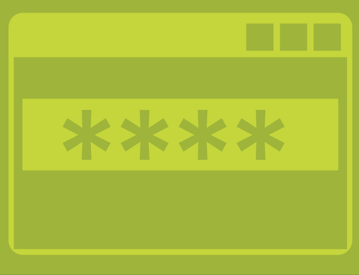
FOUR AUTHENTICATION DEFINITIONS EVERY IT SECURITY PRO SHOULD KNOW

How does enterprise IT ensure users are who they say they are?

SOMETHING **YOU KNOW**

I.E. **passwords, PINs, patterns, passcodes,** and any other verification based on information only the user should know. Passwords have been the primary means of verifying user identity since the need to protect data emerged.





PROS

Users are accustomed to them; there is no special hardware required; and almost all applications accept them.

CONS

Easily hacked via social engineering, phishing, poor password hygiene, and brute force attacks. Also require users to remember and properly guard multiple unique, complex passwords; and IT management to reset when forgotten.

SOMETHING **YOU HAVE**

I.E. a smart card, token, virtual smart card – a physical item carried by the user that is unique to them and is presented during the authentication process.

PROS

Usually requires physical access to the smart card or token in order to be hacked. If authenticating based on PKI, there is no password or PIN transmitted over the network. Smart card technology has been in use for over a decade and is a proven and understood strategy.

CONS

Requires users to keep track of additional, unique pieces of hardware for various services. Requires IT to replace hardware when lost. Additional costs associated with acquisition and replacement.

VIRTUAL SMART CARD: a subset of "something you have," a virtual smart card functions like a traditional token or smart card, but is embedded into the PC, laptop, tablet or phone.

PROS

Nothing extra to be carried, reducing management costs significantly. Based on an industry-standard piece of hardware already included in most enterprise devices, thus eliminating hardware acquisition costs for smart cards and smart card readers.

CONS

The virtual smart card is fixed to a specific device, and can only be used to authenticate from one endpoint.

SOMETHING **YOU ARE**

I.E. a biometric. A user authenticates based on a fingerprint check, voice print, retinal scan, or other unique physical attribute.

PROS

Convenience – nothing to carry or remember.

CONS

Can be spoofed and may give false positives/negatives. Not as widely standarized as other solutions. Require additional readers, scanners, and support. High acquisition and maintenance costs. Impossible to revoke without revoking the user's biometrics.

TWO-FACTOR **AUTHENTICATION**

is the practice of combining any two of these three types of authentication: something you know, something you have, and something you are. Two-factor authentication is a recommended best-practice for protecting sensitive data and resources, and is required by law when handling some types of information.

PROS

Hackers have two layers of protection to crack, greatly decreasing the chance for a successful attack. Reduces dependence on passwords, improving user experience and ultimately lessening cost.

CONS

Cost and complexity – organizations have to deploy and manage more than one form of authentication. The exception is virtual smart cards, which incorporate a password and therefore only require one deployment to achieve two-factor authentication.

wave®

Copyright © 2014 Wave Systems Corp. All rights reserved.