EDUCAUSE INTERNET2 HIGHER EDUCATION INFORMATION SECURITY COUNCIL

Two-Factor Authentication

Important Note!
Please visit the 2014 version of the **Information Security Guide** for the most current information and resources.

What Is Two-Factor Authentication?

It is the use of two independent means of evidence (factors) to assert the identity of a user requesting access to some application or service to the organization that provides the application or service. The objective of two-factor authentication, as a method of electronic computer authentication, is to decrease the probability that the requestor is not who he/she claims to be (i.e., providing false evidence of his/her identity.) Two-factor authentication is achieved by a combination of any two of the three “Somethings” below:

Something you know

- Personal Identification Number (PIN)
- Password

Something you have

- Smartphone
- Token
- ID Badge / Smart card

Something you are

- Fingerprint
- Retinal Scan
- Voice Pattern
- Typing Cadence

Note that the use of a password in combination with a PIN, for example, is NOT considered two-factor authentication because both pieces of information involve a single factor - something you know.

The use of two-factor authentication has been pervasive and ubiquitous for quite a long time already. Any person who has used an ATM machine to withdraw cash for a bank account has used two factor authentication – you had to provide something you had (a card) and had to provide something you know (a PIN) in order to complete the transaction.

What Is The Difference Between Two-Factor and Multi-Factor Authentication?

The subtle difference is that, while two-factor authentication uses exactly two factors to assert the identity of a user, multi-factor authentication uses two or more factors to assert identity. In essence, two-factor authentication is a subset of multi-factor authentication. An example of multi-factor authentication would be the requirement to insert a smart-card (something you have) into a smart-card reader, enter a PIN (something you know), and provide a valid fingerprint (something you are) provided via a biometric fingerprint reader. This example uses three factors to assert the identity of a user.

What are the Business Reasons to Consider Two-Factor Authentication?

Privacy, and the threat of identity theft, is increasingly a concern as more of personal information finds its way to online applications. In addition, passwords alone can frequently be easily guessed or compromised through phishing or hacking, consequently, no longer providing adequate protection for mission-critical information system and applications containing Personally Identifiable Inforrmation (PII), Personal Health Information (PHI), and other confidential information. Some specific concerns:

- As passwords become easier to guess or compromise, password complexity requirements are quickly coming to exceed what users can reasonably remember.
- Password proliferation has increased the time and effort spent on user support because of forgotten passwords and the need to reset them.
- Many password reset mechanisms are insecure, even if the passwords themselves are not.
- The increased use of single sign on increases the value of passwords and the number of ways by which those passwords can be potentially attacked.
- Passwords are all-too-often cached in applications (e.g., email clients or web browsers), stored off site (e.g., POP/IMAP consolidation of email from multiple accounts), and reused for multiple services, some highly sensitive.

See Passwords, a presentation at the NWACC Security Conference 2009, for a in-depth review of all the reasons why it makes good business sense to consider two-factor authentication as alternative to traditional passwords.

Compliance is also driving adoption of two-factor authentication in other areas – three examples:

- The Federal Information Security Management Act (FISMA) applies to grantees (e.g., institutions of higher education) when they collect, store, process, transmit or use information on behalf of the United States Department of Health and Human Services (HHS) or any of its component organizations. In other words, Federal security requirements apply and the institution of higher education is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III and NIST SP 800-63 Electronic Authentication Guideline).
- The Health Insurance Portability and Accountability Act (HIPAA), where the most important concern is the confidentiality of patient records and protected health information, does not explicitly require two-factor authentication but clearly makes an appeal to the use of industry best standards.
- The Payment Card Industry Data Security Standard (PCI DSS), where the most important concern is the confidentiality of