

# NOTICEBORED

## Management briefing on Authentication

### Summary

This paper covers the authentication of computer users and systems, plus related aspects such as validation and access control that are closely associated with authentication. Authentication is a critical part of information security. It reduces the risks of identity theft, fraud, hacking and random data errors, and helps maintain the integrity of our systems and data. Anyone who has bought poor quality counterfeit goods from the Far East, or suffered identity theft, should immediately appreciate the value of authentication.

### Introduction

We have all experienced authentication at some time or another – when we present our passport to an immigration officer or our password to login to the network, for instance, we are presenting credentials in order to be authenticated. Those credentials, in turn, are acceptable because we trust in the processes for checking us out and issuing them to us, and because they are difficult for someone else to steal or forge.

### What gets authenticated?

**Individuals** are authenticated to be sure they really are who they claim to be, and therefore to determine whether they are allowed to access our information assets. Authentication helps us spot forgers, imposters and fraudsters, and differentiate them from authentic, upstanding, trustworthy members of society.

Authentication of **computer systems, networks and programs** is also important, although this mostly happens 'behind-the-scenes'. When someone accesses a WiFi hotspot with a company laptop, for instance, it is important that they give their username and password to a legitimate access point, not a fake controlled by a nearby hacker. When a computer system sends important data across an interface to another system, it is important that it is not sending data to a bogus system. With no authentication, a malicious user (such as a computer hacker or fraudster) may send information intended to disrupt the network or penetrate the systems, or steal information.

**Data authentication** is essential at virtually all points of data entry, especially when people type values into our systems. People often make typing mistakes, some of which the computers can pick up before they do any damage. Hackers sometimes deliberately undermine system security, for instance by entering commands into databases instead of plain data – the systems must therefore be programmed to authenticate (validate) data.

### How does authentication take place?

Passwords are the main mechanism for authenticating users to systems – the crux is that passwords must remain secret, only known to the person we are authenticating. As far as the computer is concerned, if someone claiming to be John Doe logs in with John Doe's password, then they **MUST BE** John Doe. Passwords are **something only the user knows**.

Security tokens (such as SecureID) and smartcards add another level of checking. Tokens are **something only the user has**. Again it is important that tokens are not passed around.

Biometric checks (such as retina or fingerprint scans) are more difficult to fool than the others because these relate to **something only the user is**. These are not totally secure (nothing is) but are significantly better than the other authentication methods, albeit slower and more expensive.

Multi-factor authentication combines techniques from more than one of the above categories, such as passwords plus tokens or biometrics. If properly implemented, multi- is much stronger than single-factor authentication, making it much more difficult for fakers to present false credentials.

Why do we need to authenticate anyway?

We use authentication primarily because there *are* fakes, fraudsters and imposters who intend to mislead us. Authentication helps us differentiate authentic, trustworthy people, systems and programs from the fakes. It makes identity theft less likely. In the form of validation, it also helps us spot genuine mistakes such as typing errors or corrupted data arriving at a system interface.

Authenticated individuals can safely be given access to sensitive information resources for which they are authorized. Without authentication, unauthorized access would be a big problem and our risks would be greater.

Authentication is not just about preventing unauthorized access – it is also used to keep tabs on legitimate users, for instance by keeping secure system records to prove exactly what someone did on the system. If they later claim to have done something different, the audit trail may be checked to verify or refute their claim (technically, this is known as **nonrepudiation**). Take for example the situation where someone orders something from us but later claims it was not them who made the order, or claims they ordered something different. That would leave us with the cost of retrieving and restocking the item. From a contractual point of view, it may be vital that we can prove the order came from them and was not modified by us. Authentication using digital signatures and audit records could save the day.

Management responsibilities relating to authentication

- Be aware that when you sign an 'authorization for systems access' or 'new user' form for a member of your staff, you are granting the person access to valuable corporate information assets. Before you sign, think: are they sufficiently trustworthy? Do they know what they are doing? Especially if they will be able to access sensitive systems or if they will be using a privileged user ID, take a moment to impress upon them the responsibility that goes with IT systems access, and remind them that they are *personally accountable* for everything that happens under their user ID.
- Lead by example. **Never disclose your password to your secretary or another member of staff.** If anyone ever asks you for your password (even someone from IT), just say no. Remember, *you are personally accountable for everything* that happens under your user ID! As a manager, your user ID probably gives access to more sensitive information and functions than most and so deserves greater protection.
- Take time to review access rights every so often for computer systems used by your department. Auditors will quite rightly complain if they find active user IDs for staff who have long since left the company, or user IDs with inappropriate access rights. Keep an eye out for divisions of responsibility (such as a block on anyone's ability to both raise a purchase order and approve payment).
- Work with your staff and information security people to ensure that new computer systems have suitable authentication, access control, audit trails and other security functions built-in. It is much more cost effective in the long run to design and build-in solid security from the start than to suffer security failures later and have to modify the systems.

For more information

Please contact the CIO or Information Security Manager or visit Information Security's intranet website for further information and advice.