

NOTICEBORED

*Security
awareness
seminar*

I & A

Identification and Authentication

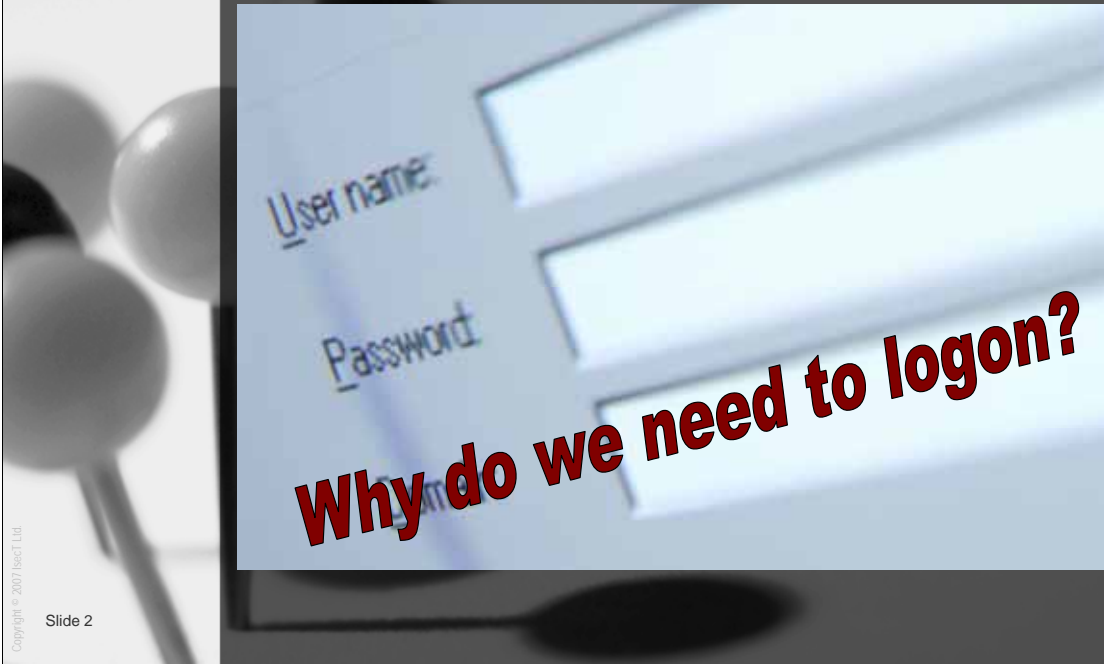
Copyright © 2007 Isect Ltd.

July 2007

These speaker notes expand upon the slides for the benefit of seminar leaders and participants. To print these notes and slides as handouts, select “Notes Pages” from the “Print what” drop-down on the print dialogue.

Copyright © 2007 Isect Ltd. This presentation is for use by NoticeBored customers according to the terms of the NoticeBored license agreement. Contact Isect Ltd. (info@isect.com) for further information.

Introduction



It's something we do just about every day: logon to the computer. But what does the logon process achieve? What's it for?

This seminar explains what happens when we logon, and why we have to do it.

Agenda

Identification

Authentication

User IDs
(usernames)

I&A

Passwords
& PIN codes

Security
tokens

Biometrics

The two areas we will cover are:

1. Identification – finding out who is using the computer
2. Authentication – confirming that they are who they say they are

NOTICEBORED

Identification

Access control

Accountability

Auditability

User IDs (usernames)

I&A

Identification

Copyright © 2007 Insect Ltd.

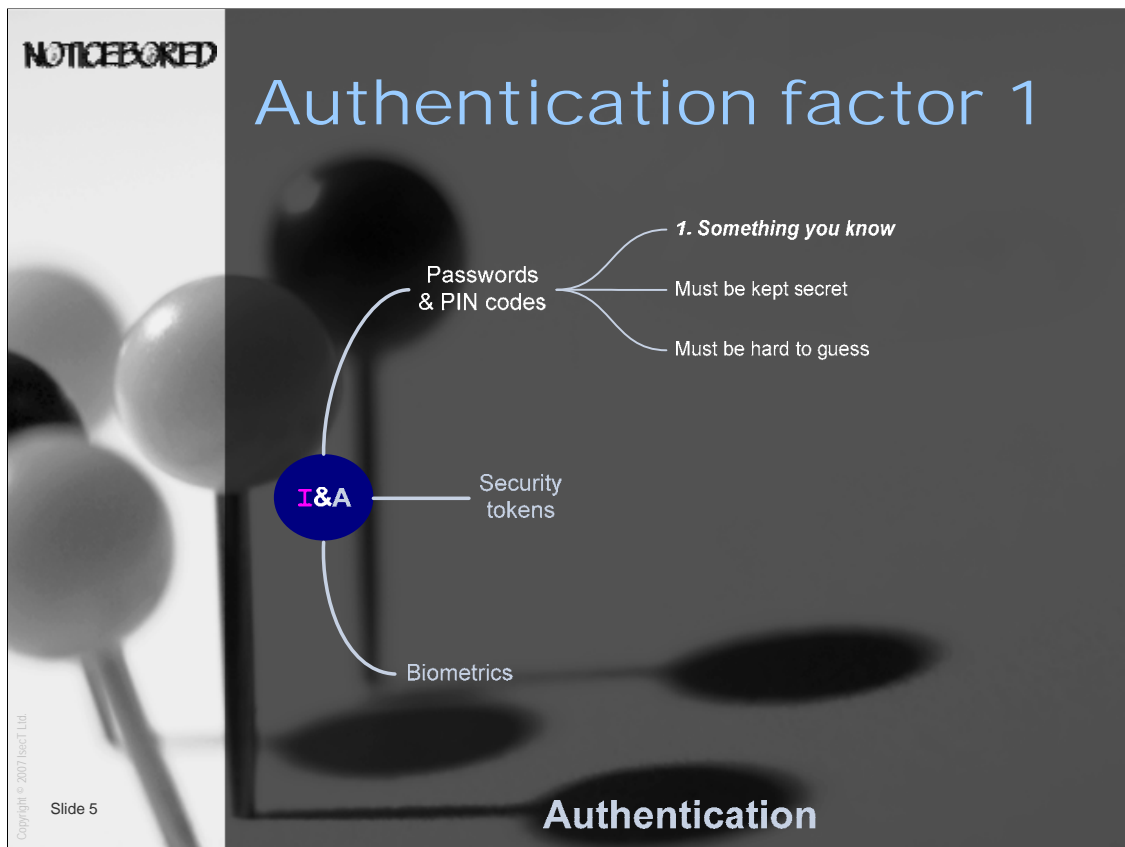
Slide 4

The first part of logging-on is to enter a username (also known as a user identity or user ID). **This is so that the computer ‘knows’ who we are.** The computer can’t see us and doesn’t just recognize us like a person would.

For obvious reasons, this step is known as **identification**.

Once we have successfully logged on, the computer will control our access to information and track what we do on the system. We will be held accountable for everything that happens under our user ID. Entries will be recorded in the system logs and audit trails.

If we *only* had to enter a username to logon, there would be nothing to stop someone putting someone else’s username in. The computer would accept the wrong identity without question. This is clearly not good for access control, accountability and auditability ... so something else is needed ...

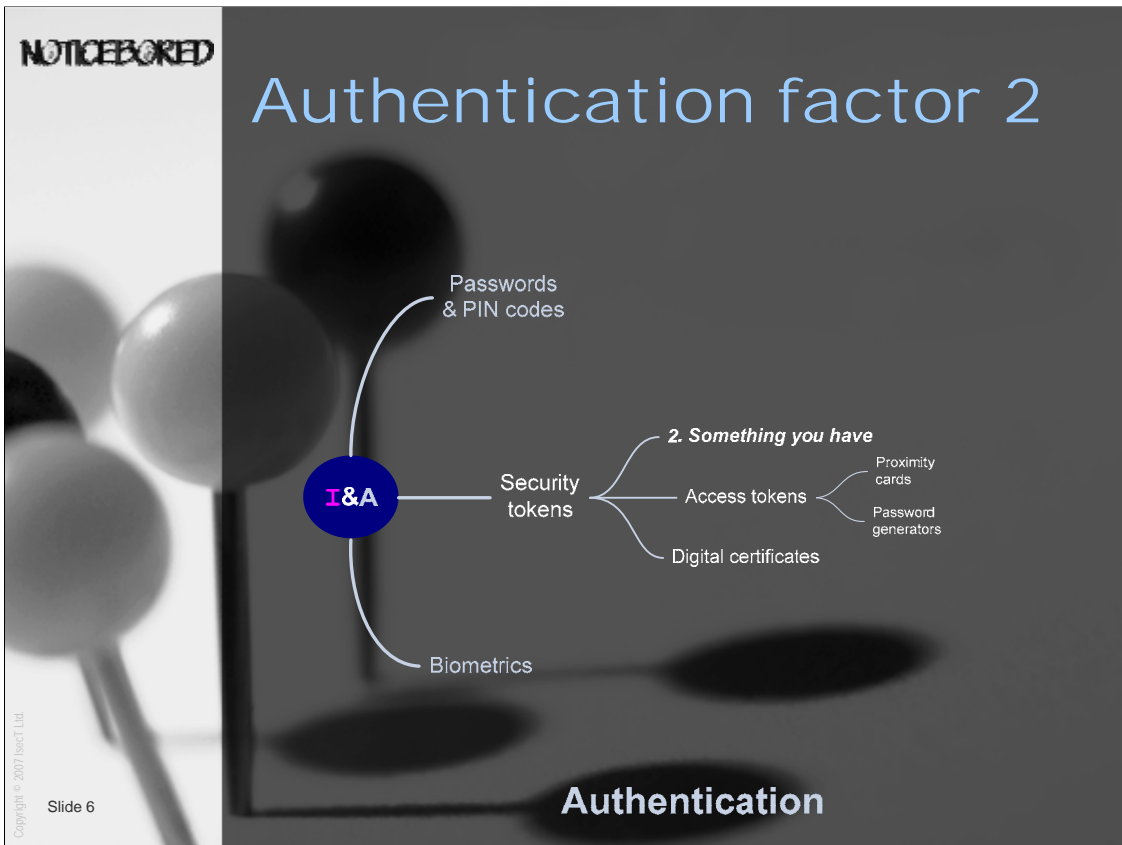


... that something else is **authentication**.

The first and most common way to authenticate someone is to ask them for a secret password or Personal Identification Number (PIN code), in other words **something that only that person should know**.

Passwords that are shared, given away, left on Post-It notes on the screen *etc.* are clearly not secret. *Anyone* who obtains the correct username and password can logon to the computer, and everything that happens will be logged against the true owner of that username.

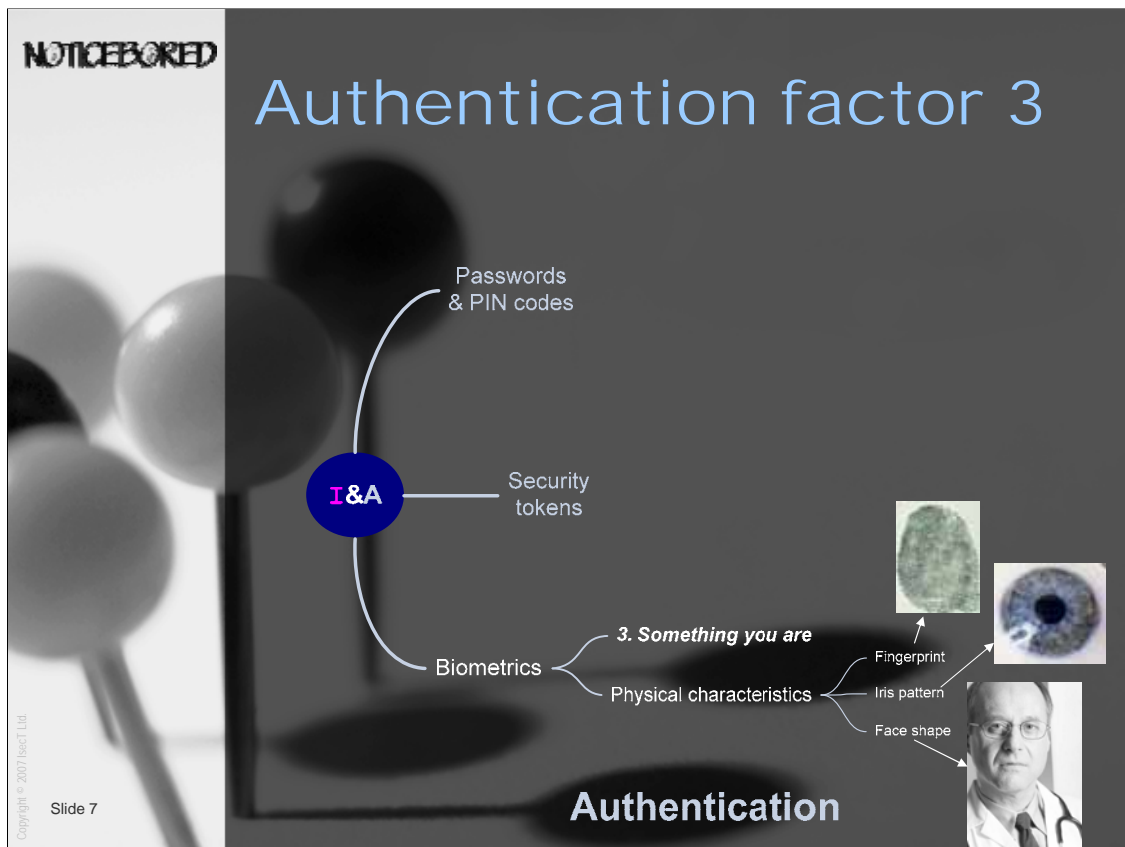
Passwords must also be difficult for someone to guess, meaning long and complex. We'll give you some hints on choosing hard-to-guess passwords at the end of this presentation.



Some systems require “tokens” or credentials for users to logon. Examples are the magnetic proximity cards used to access secure buildings, and password generator key fobs such as “secureID” which display a new sequence every minute or so. Tokens are **something that the person must have** – physical possession of the token is necessary to logon.

Security tokens are often combined with a password or PIN code (the first authentication factor) in order to prevent someone simply stealing the token and using it to logon. They also need the password or PIN code.

Digital certificates are another example of a security token. Certificates may be stored on a smart card or PC, and again may be locked with a password.



High-security systems are starting to use **biometric authentication**, usually in addition to passwords/PIN codes and perhaps tokens.

Biometrics involves the system checking the person's unique physical characteristics such as their fingerprint, iris pattern, face shape, hand shape, vein pattern *etc.*

Biometric authentication is the strongest available form of personal authentication but it is relatively slow and expensive. It is also subject to errors (for example if you have been doing some building work over the weekend, the ridges on your fingertips may have worn down so your fingerprints might not be recognized).

Biometric devices (usually fingerprint scanners) are gradually being introduced into consumer electronics such as mobile phones and laptop PCs.

When the controls fail ...

Hackers Exploit Well-Known Security Weaknesses

“The hackers generally gained access to the DOD computer systems by travelling through several networks and computer systems. Using commercial long-distance services, such as Tymnet, the hackers weaved their way on the Internet through university, government, and commercial systems, often using these sites as platforms to enter military sites. The hackers then exploited various security weaknesses to gain access into military sites. The most common weaknesses included (1) **accounts with easily guessed passwords or no passwords**, (2) well-known security holes in computer operating systems, and (3) vendor-supplied accounts--privileged accounts with **well-known passwords or no passwords** at all that are used for system operation and maintenance.”

Copyright © 2007 Insect Ltd.

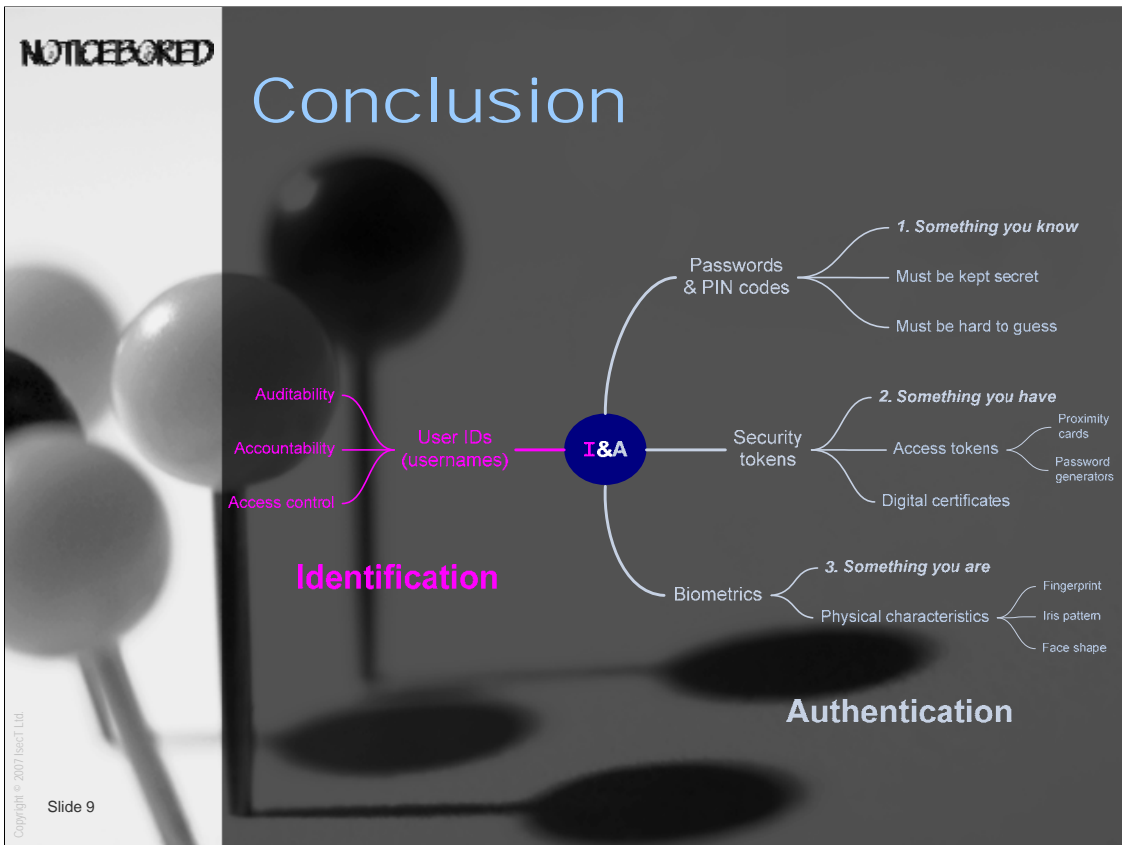
Slide 8

Jack L Brock Jr. testimony before the US Senate Subcommittee on Government Information and Regulation, US General Accounting Office, 1991

This is clearly an old, old problem! A more modern version of this issue is **“identity theft”**.

The quotation above is taken from a GAO Report “Hackers Penetrate DOD Computer Systems” documenting the testimony of Jack L. Brock, Jr. Director Government Information and Financial Management Information Management and Technology Division before the US Senate Subcommittee on Government Information and Regulation, Committee on Governmental Affairs.

URL: <http://wiretap.area.com/Gopher/Gov/GAO-Tech/REPORT10>



Copyright © 2007 Insect Ltd.

Slide 9

We have explained the typical computer logon process – the username for identification and password for authentication. This is known as Single-Factor Authentication.

We have also discussed security tokens and biometrics that are gradually being introduced to strengthen security. When combined with passwords, this is Multi-Factor Authentication (MFA).

MFA improves security but is costly and annoying for users. In the main, we still rely heavily on usernames and passwords.

Take home messages

- Choose long, strong passwords
- Use unique passwords on important systems
- Beware "shoulder surfers"
- Log off before you walk off

And most of all:

- Never, *ever* tell anyone your password

Tokens and biometrics are being introduced gradually on systems that need the additional security. Meanwhile, passwords are far and away the most prevalent means of authenticating users.

The five tips on this slide have been drawn from **Ten Top Tips on Logging-on and Logging-off the Computer** – a security awareness paper available from the Information Security Manager.



NOTICEBORED

Further information

Speak to your manager, call the IT Help/Service desk or contact the Information Security Manager for more information and advice.

Awareness briefings and other resources are available from Information Security's intranet website.

Copyright © 2007 Isact Ltd.
Slide 11

Additional web sites on this topic are listed in the NoticeBored links collection at

<http://www.noticebored.com/html/login.html>

and

http://www.noticebored.com/html/ID_theft.html