User Authentication Methods

User authentication systems, such as through the use of a username and password, will log in the user to the system authorising them to access certain areas and perform certain functions.

The username is used to uniquely identify each user and is not kept secret. Usernames don't have any particular rules on complexity and are often simple words, however, it is still important in allowing us to ensure different users are given the correct access rights.

The password is used to authenticate the user as the person who should have those access rights. These passwords have to be kept private and secure to prevent attempts to gain unauthorised access, such as through brute-force attacks.

We'll now look at some methods that are used to ensure that user authentication is kept secure.

Strong Passwords

Weak passwords, such as ones made up of a simple word, are incredibly easy to crack by any hacker. Pretty much any simple word will be able to be cracked instantly. That's why strong passwords are required.

Strong passwords will:

- not contain a dictionary word
- have uppercase letters, lowercase letters, numbers & symbols
- be a minimum of 10 characters in length.

By following these rules, a password will be strong enough that it will be almost impossible to crack through brute force.

Graphical Passwords

Most passwords are text-based, however, graphical user authentication works by getting users to select images in specific order. This most commonly works by presenting the user with a screen full of images, and then the user will select the images (or a number of them) in a specific order.

As people usually remember images better than words, this can add greater security as people are more likely to set a complex password.

Biometric Authentication

This has become very popular in recent years with many smartphone devices have built-in fingerprint recognition and some offer facial recognition. These are the two most common forms of biometric authentication.

This information is very unique to each individual and difficult to fake. This makes it generally more secure than passwords, particularly the simple passwords that many users typically choose.

However, some biometric systems are fallible, particularly mobile phones which often have shaky hand pictures and complex backgrounds. Also, if our biometric data was compromised this would be serious as we can't change our biometric data.

Two-Step Verification

This is often used as an additional layer of security by asking a user to verify their identity more than once, one after the other.

This usually works by a user entering a password and then receiving a unique code by email or text, which they then must enter to gain access. There are also apps that can be used that will provide a time-based one-time password to enter as the secondary authentication.

However, any two authentication methods could be used together for two-step verification, such as fingerprint authentication, followed by a password.

This adds security as the attacker doesn't just need the password, but additionally access to a secondary system, such as the user's email, text or the password generating app.

Security Tokens

These are small hardware devices which the user carries around with them to authorise access to a network or area. Often this is a USB device you plug into your computer or a key fob that uses NFC to wirelessly authenticate.

This can be used on its own but is often used with an additional authentication method such as a password. The reason for it not being used on its own is that it is very vulnerable to loss, theft or even copying.

Knowledge-Based Authentication

This authenticates a user through the use of question and answers pairs. A user will be asked one or more questions which the user must answer correctly to authenticate themselves.

We most commonly see this in authenticating a user for a password reset, where the user has set a question and answer which they must get correct before being sent a password reset email.

It can however also be used in a two-step authentication process, but wouldn't be used on its own for access as these questions usually involve answers which are not difficult to discover and may even be common knowledge.

Kerberos Network Authentication

Kerberos is a computer network authentication protocol. This protocol involves a client first authenticating itself with a server called the "Domain Controller". Once authenticated the client will be able to request access to network resources from the domain controller for a period of time.

It does this through a ticketing system to authenticate users which is encrypted using different passwords for different resources. No password is ever transmitted though, including the user's password, which protects from a variety of threats.

It is considered a very secure protocol for accessing network resources and is used in most Windows networks.

Certificate-Based Authentication

This uses a digital certificate to identify a client on a network. In a business network, a user must be issued a certificate for their device which will be stored on it locally. This digital certificate is used to encrypt data (with the certificates key) that can be sent to the server and decrypted (using the servers private key) to authenticate the user. The user will then be authorised to access the resources.

This is usually used alongside a username and password system and adds far greater security to it by ensuring only authorised devices can access the network resources.

Further Thought

Where else are digital certificates used other than in certificate-based authentication?

Lesson Summary

- User authentication can be performed through a variety of techniques, but usually involves a user entering a username and password.
- It's important strong passwords are used as simple passwords can be cracked instantly.
- Graphical passwords ask users to select images in a set order from a page of images.
- Biometric authentication uses biological information like fingerprint or facial recognition to authenticate a user.
- Two-step verification asks a user to verify their identity more than once, one after the other using two different authentication methods.
- Security tokens such as a USB device or an NFC fob authenticates a user by connecting them to the device.
- Knowledge-based authentication asks questions to a user, usually requested personal information, in order to authenticate them.
- Kerberos is a computer network authentication protocol that uses a ticket system to authorise access to network resources.
- Certificate-based authentication uses a digital certificate to authenticate a device to access network resources.