AUTHENTICATION

Rep. Mulin D., *ES - 52*

Authentication (from Greek: *αυθεντικός* ; real or genuine, from *authentes*; author) is the act of establishing or confirming something (or someone) as *authentic*, that is, that claims made by or about the subject are true. This might involve confirming the identity of a person, tracing the origins of an artifact, ensuring that a product is what its packaging and labeling claims to be, or assuring that a computer program is a trusted one.

There are two types of techniques for doing this.

The first is comparing the attributes of the object itself to what is known about objects of that origin. For example, an art expert might look for similarities in the style of painting, check the location and form of a signature, or compare the object to an old photograph.

The second type relies on documentation or other external affirmations. For example, the rules of evidence in criminal courts often require establishing the chain of custody of evidence presented. This can be accomplished through a written evidence log, or by testimony from the police detectives and forensics staff that handled it. Some antiques are accompanied by certificates attesting to their authenticity. External records have their own problems of forgery and perjury, and are also vulnerable to being separated from the artifact and lost.

The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication: something you know, something you have, or something you are. Each authentication factor covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.

Security research has determined that for a positive identification, elements from at least two, and preferably all three, factors be verified. The three factors (classes) and some of elements of each factor are:

- the **ownership factors**. Something the user has (e.g., wrist band, ID card, security token, software token, phone, or cell phone)

- the **knowledge factors**. Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN))

- the **inherence factors**. Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature, face, voice, unique bio-electric signals, or other biometric identifier).

When elements representing two factors are required for identification, the term *two-factor authentication* is applied, e.g. a bankcard (something the user has) and a PIN (something the user knows). Business networks may require users to provide a password (knowledge factor) and a random number from a security token (ownership factor). Access to a very high security system might require a mantrap screening of height, weight, facial, and fingerprint checks (several inherence factor elements) plus a PIN and a day code (knowledge factor elements), but this is still a two-factor authentication.

In a computer data context, cryptographic methods have been developed. Digital signature and challenge-response authentication are currently not spoofable if and only if the originator's key has not been compromised. That the originator (or anyone other than an attacker) knows (or doesn't know) about a compromise is irrelevant. It is not known whether these cryptographically based authentication methods are provably secure since unanticipated mathematical developments may make them vulnerable to attack in future. If that were to occur, it may call into question much of the authentication in the past. In particular, a digitally signed contract may be questioned when a new attack on the cryptography underlying the signature is discovered.

Security experts argue that it is impossible to prove the identity of a computer user with absolute certainty. It is only possible to apply one or more tests which, if passed, have been previously declared to be sufficient to proceed. The problem is to determine which tests are sufficient, and many such are inadequate. Any given test can be spoofed one way or another, with varying degrees of difficulty.

Supervisor Mulina N.I., *ELA*