Digital signatures 1: certificates and certification authorities

PB/INFO/002 (06/06)

In many ways the Internet is parallel to the real world. In the Internet there are usernames and URLs, in the real world there are people and organisations. For many applications, especially those involving money or personal information, we need to link the two worlds. It is reasonable to seek assurance that a web site belongs to a particular, trusted, organisation before sending it our credit card details, or to confirm the identity of a student before revealing exam scores. Domain names alone give no such assurance: www.whs.com [1] is not the well-known British high street stationers.

Certificates provide the necessary link between objects in the electronic world and real people or organisations. In its simplest form a certificate may assert, for example, "this is the Janet web server". On its own such an assertion has little value: it only becomes useful when an independent person or organisation signs it to indicate that it believes the assertion to be true. If a customer or service trusts the signer, and believes that they have good procedures for verifying the assertions they sign, they may decide that it is safe to believe the statement made by the certificate owner. A service may allow a user to access particular information; a user may decide to trust a server with a secret such as a credit card number. To be effective, a signer should be chosen who is more trusted, or at least more widely known, than the certificate owner.

Signers may in some cases be individual people, but they may also be companies or organisations. A college might sign a certificate for each student to indicate their status in the institution, though this certificate would have to be revoked when the student leaves. There are also companies whose sole function is to issue signed certificates, usually certifying the identity of a person or organisation. Such a company is known as a certification authority, often abbreviated to CA. A CA should publish, and may also include in the certificate, the procedure it follows to confirm the identity of the certificate owner. Standards of proof range from "the e-mail address is deliverable" to checking legal documentation; knowing the procedure used, the recipient of a signature can make an informed decision on how far to trust the signed statement.

Certificates may be issued with a fixed duration; after a scheduled expiry date such certificates become invalid and their assertions should be re-confirmed. This may be useful when the assertion itself has a fixed lifetime – for example the "I am a student" certificate above – or to limit the effect of certificate theft. Some CAs themselves use fixed duration certificates which cause all customer certificates to become invalid when the CA master certificate expires. This may cause previously encrypted web connections to become insecure, among other undesirable results. If the CA issues a replacement certificate then users should be especially careful to check the validity of the replacement, since this is an

ideal opportunity for a fraudster to distribute a forged certificate.

There are a number of applications where certificates may be useful. Since these involve different combinations of users, services and software, different considerations and, in some cases, different types of certificate may apply.

Applications Web Server Certificates

A web server can use a digital certificate to establish an encrypted channel to protect the privacy of communication between browser and server. Most web browsers will also accept certificates provided by servers as evidence of the server's identity. However, as noted above, a certificate needs to have a trusted signature to have any value as proof of identity. Popular browsers come pre-configured with a list of trusted signers, usually large commercial Certification Agencies: a server offering a certificate signed by one of these CAs will be indicated, for example by displaying a closed padlock icon, to the user. While it is possible to add new trusted signers manually, few users do this without instruction. Except, perhaps, within a closed user community a server that tells its readers to add a new CA to authenticate its certificate should probably not gain any trust by doing so. A server that needs to prove its identity to the general public should therefore have its certificate signed by one of the standard pre-installed Certification Agencies.

One other issue is common to all uses of "organisation" certificates. Before using a certificate to assert that a service belongs to a particular organisation it is important to determine who is authorised to make such a statement, both under internal rules and by law. Even if no legal liability is incurred, a service with a certificate is likely to be perceived as "official" so particular care will be needed to avoid inappropriate conduct or content.

Web Client Certificates

Certificates may also be offered by web clients to servers as proof of the identity of the user. In theory this could be used to replace password-protected web pages. however there is much less built-in support for these client certificates in current browsers and servers, and manual configuration is likely to be needed at both client and server ends. This situation has changed little in the past two years: server vendors see no benefit in supporting certificates until users possess them while users are unlikely to spend money on certificates which are of little use. User certificates may have current applications within closed, technology-literate communities but their general use will require promotion by both Certification Agencies and on-line services. Finally, user certificates need to be installed into browsers and kept secure; for mobile users who do not have their own dedicated workstation it is not clear how this can be achieved.

Signed Programs

When downloading a program from the Internet a signed certificate asserting its origin may give confidence in the safety of running the program. Both Sun's Java system and Microsoft's ActiveX can be configured to give signed programs greater access to the host computer's disk or network. In particular a signed Java applet or ActiveX control may run without displaying the normal warning alert box. This idea has not been an unqualified success. Neither company has been prepared to accept liability for the actions of signed code, signing certificates have been issued to the wrong people, and hostile controls have used forged

signatures. Users should remain wary of any program obtained from the Internet, even if it carries a signature; program writers should beware of any implicit liability if they sign their own code.

Management

In any application involving certificates or keys, management problems are likely to predominate. A successful deployment must have procedures for issuing, storing and cancelling certificates. In particular:

- deciding what a certificate will assert, identifying the appropriate holders and ensuring correct
- finding an appropriate form for the owner to hold and use the certificate and keeping secure backups if required;
- ensuring that old certificates are revoked to prevent use which is no longer authorised.

- use;

Meeting these requirements without increasing the cost of ownership beyond the perceived benefit may be the greatest challenge – see, for example, Bruce Schneier's article at:

http://www.schneier.com/paper-pki.html [2]

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/digital-signatures-1-certificates-and-certification-authorities

Links
[1] http://www.whs.com
[2] http://www.schneier.com/paper-pki.html