Digest Authentication

January 1998 / Web Project / HTTP Authentication / Digest Authentication

Digest authentication (see http://www.w3.org/Protocols/rfc2069/rfc2069) will occupy a middle ground between basic authentication, which is very weak, and client authentication, which is very strong. You can use client authentication today (see "Digital IDs," http://www.byte.com/art/9703/sec8/art1.htm). But the administrative burden of client certificates and the overhead of the required Secure Sockets Layer (SSL) transport weigh against this option.

In digest authentication, as in NT LAN Manager (NTLM) authentication, the server sends the client a special value (nonce) that the client uses to encrypt the password. When it receives the encrypted password, the server applies the same operation to its own copy of the user's password and checks for a match. As a result, the password need not be sent in the clear.

The protocol uses several techniques to restrict the scope of a transaction. First, the specification recommends that the nonce should include the client's IP address and a time stamp. The IP address helps prevent a man-in-the-middle attack by forcing an attacker to spoof the IP address of the original client. The time stamp limits the period during which such an attack might be tried. Second, the digest that the client sends back to the server is based in part on the URL it originally requested. If an interloper alters that URL, the digest computed by the server won't match the one computed by the client.

Couldn't a rogue server use a constant challenge, as with NTLM authentication, to mount a dictionary attack? Yes. The digest method is inherently better than the NTLM method, because it seeks to limit the scope of transactions and it doesn't permit the invisible handshake that Internet Information Server (IIS)and Internet Explorer currently perform. But the authors of RFC2069 are candid about the uses and limitations of digest authentication:

"Users and implementers should be aware that this protocol is not as secure as Kerberos and not as secure as any client-side private-key scheme. But it is better than nothing, better than what is commonly used with telnet and FTP, and better than basic authentication."

You Must Authenticate to Pass the Box

screen_link (15 Kbytes) 

The familiar user/password dialog box.