GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

SANS GIAC Training and Certification: Security Essentials (LevelOne) Practical
Robert Owens
October 31, 2000

One-Time Passwords: Functionality and Analysis

The use of passwords remains a highly recommended solution for securing access to confidential information systems. However, the use of static passwords, passwords that do not change from session to session, has come under increased scrutiny because of their susceptibility to hacker attacks, cracker applications, and other attempts to gain unauthorized access to private networks. To counter the inherent weaknesses of static passwords, security professionals are recommending the use of one-time passwords (OTPs).

A one-time password (OTP) is one "that exists only for the length of the current session and that has no currency outside that session…" Input Research Bulletin. "One-Time Passwords Address a Growing Problem." URL: http://www.input.com/bulletins/eirb_0297.htm (18 October 2000). OTP solutions include both hardware components and software applications, and can be divided into three categories of functionality: asynchronous (challenge/response) authenticators, synchronous (time-dependent) authenticators, and synchronous (time-independent) authenticators. Bosen, Bob. "When Passwords are Not Enough." Secure Computing Corporation. URL: http://www.safeword.com/wpanel.htm. (31 October 2000).

With asynchronous authenticators, authenticators generate numeric challenges to the user or their client machines and allow access to the system if they must receive the correct response. Bosen, Bob. "When Passwords are Not Enough." Secure Computing Corporation. URL: http://www.safeword.com/wpanel.htm. (31 October 2000). For example in a manual asynchronous authentication environment, a user enters their id name and receives a randomly generated "challenge" number from the authenticator. The user must then inputs the appropriate encrypted response, and send that response back to the authenticator. If the response matches the challenge, the user is allowed access to the system.

Automated asynchronous authenticators include Belcore's S/key OTP system. The S/key process begins when a user enters their secret pass-phrase into the system. The OTP system generator then "passes the user's secret pass-phrase, along with a seed received from the server as part of the challenge, through multiple iterations of a secure hash function to produce a one-time password." N. Haller and C. Metz. "A One-Time Password System." Network Working Group. May 1996. URL: http://www.cis.ohio-state.edu/htbin/rfc/rfc1938.html (19 October 2000). The hash function creates a unique password by reducing the number of iterations that the pass-phrase cycles through by one each time login is requested. The client then receives the challenge, and responds according to the S/KEY parameters established in the challenge. Finally, the server verifies the password by sending it back through a secure hash function and compares it against the preceding password. N. Haller. "The S/KEY One-Time Password System." Network Working Group. February 1995. URL: http://www.cis.ohio-state.edu/htbin/rfc/rfc1760.html (19 October 2000).

Time-dependent authenticators base their OTP generation on time intervals. Thus, a numeric password will only be valid for a given amount of time, such as one minute or thirty seconds.

© SANS Institute 2000 - 2005 Author retains full rights.

Due to the fact that a unique number is generated based on the time of the logon and the number is only applicable for that specific login attempt, it cannot be used at a later time to compromise the system.

Hardware components implement synchronous authentication through the use of small key cards with digital displays. The key card displays a unique numeric combination that has been randomly generated by the hardware token on the server. Thus when users attempt to logon, they simply enter their personal PIN numbers, followed by the current OTP displayed on their key card. SercuriTeam.com. "One-Time Passwords." 29 September 2000. URL: http://www.securiteam.com/securityreviews/One-Time_Passwords.html (20 October 2000). Vendors of hardware solutions include Security Dynamics and CRYPTOCard, Inc. Input Research Bulletin. "One-Time Passwords Address a Growing Problem." URL: http://www.input.com/bulletins/eirb_0297.htm (18 October 2000).

The third category of OTP password systems, time-independent synchronous authenticators, function in much the same way as time-dependent authenticators. However, time-independent authenticators generate the production of OTPs randomly rather then relying on the time interval during which the user attempts to logon. Bosen, Bob. "When Passwords are Not Enough." Secure Computing Corporation. URL: http://www.safeword.com/wpanel.htm. (31 October 2000). Examples of time-independent synchronous authenticators are Safeword Authentication cards, which allow users to activate the password generator by entering a PIN. The generator then provides the user with a randomly generated OTP, that the user then inputs to logon to the system. Secure Computing. "Data Sheet." Secure Computing. URL: http://www.securecomputing.com/index.cfm?sKey=507. (31 October 2000).

The ability of OTPs to eliminate a number of system vulnerabilities, such as password cracking, password sniffing, brute force attacks, and social engineering are obvious. However, installing an OTP system does not eliminate all password system vulnerabilities, nor does it eliminate the need for other network security applications.

The most common weakness of OTP systems that utilize hardware key cards, as with time-independent and dependent synchronous authenticators, is that users are required to use their keys every time they login. Thus, users who have forgotten, lost, or had their keys stolen will not be able to logon to the system, and there is also the threat of unauthorized access by attackers utilizing lost or stolen cards before they are made inoperative. Smith, Danny. "2.4.3. One Time Passwords." Selected Aspects of Computer Security in Open Systems. 8 November 1993. URL: http://www.auscert.org.au/Information/Auscert_info/Papers/Selected_Aspects_of_Computer_Security_in_Open_Systems.html (25 October 2000). Another availability problem can occur with time-dependent OTP systems that base their random password generation on time intervals. In these situations, clock synchronization problems across the network, due to either clock slippage or hacker attacks, will not allow users to logon to the server. Smith, Danny. "2.4.3. One Time Passwords." Selected Aspects of Computer Security in Open Systems. 8 November 1993. URL: http://www.auscert.org.au/Information/Auscert_info/Papers/Selected_Aspects_of_Computer_Security_in_Open_Systems.html (25 October 2000). A third vulnerability is specific to the UNIX environment. In

© SANS Institute 2000 - 2005 Author retains full rights.

situations in which S/KEY file permission are set to world readable, attackers that compromise the system could access the "skeykeys" files and launch a dictionary attack on these files. Mudge. "Vulnerabilities in the S/KEY one time password system." L0pht Heavy Industries. URL: http://www.mono.org/~arny/junk/skeyflaws.html (24 October 2000). Finally, many networks are not designed to handle OTP systems. Therefore, although OTP software may be distributed free of charge, a company may face a considerable expense implementing an OTP system. Security Solutions. "Effective Password Protection Techniques." A VaultBase White Paper. URL: http://www.vaultbase.com/page/Sec-Password.htm (25 October 2000).

In conclusion, OTPs decrease a network's susceptibility to unwanted access by eliminating the susceptibilities of reusable passwords. However, it is important to remember that OTP systems do not eliminate all system vulnerabilities, but are simply an added barricade in an overall security policy.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Works Cited:

1. Bosen, Bob. "When Passwords are Not Enough." Secure Computing Corporation. URL: http://www.safeword.com/wpanel.htm. (31 October 2000).

2. Input Research Bulletin. "One-Time Passwords Address a Growing Problem." URL: http://www.input.com/bulletins/eirb_0297.htm (18 October 2000).

3. Mudge. "Vulnerabilities in the S/KEY one time password system." L0pht Heavy Industries. URL: http://www.mono.org/~arny/junk/skeyflaws.html (24 October 2000).

4. N. Haller. "The S/KEY One-Time Password System." Network Working Group. February 1995. URL: http://www.cis.ohio-state.edu/htbin/rfc/rfc1760.html (19 October 2000).

5. N. Haller and C. Metz. "A One-Time Password System." Network Working Group. May 1996. URL: http://www.cis.ohio-state.edu/htbin/rfc/rfc1938.html (19 October 2000).

6. Secure Computing. "Data Sheet." Secure Computing. URL: http://www.securecomputing.com/index.cfm?sKey=507. (31 October 2000).

7. SercuriTeam.com. "One-Time Passwords." 29 September 2000. URL: http://www.securiteam.com/securityreviews/One-Time_Passwords.html (20 October 2000).

8. Security Solutions. "Effective Password Protection Techniques." A VaultBase White Paper. URL: http://www.vaultbase.com/page/Sec-Password.htm (25 October 2000).

9. Smith, Danny. "2.4.3. One Time Passwords." Selected Aspects of Computer Security in Open Systems. 8 November 1993. URL: http://www.auscert.org.au/Information/Auscert_info/Papers/Selected_Aspects_of_Computer_Security_in_Open_Systems.html (25 October 2000).

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.