globalscape™
securely connected

Whitepaper

Multifactor Authentication

"In 2164 separate incidents, over 822 million records were exposed, nearly doubling the previous highest year on record (2011). Four of those breaches made the all-time top ten and almost half involved the loss of password data."

- http://nakedsecurity.sophos.com/2014/02/19/2013-an-epic-year-for-data-breaches-with-over-800-million-records-lost/

Secure Login with Mobile-Based Authentication

The classic username+password authentication to an account is only as secure as the security and complexity of the password. Passwords can be stolen or forgotten, and can place an unnecessary burden on support departments to reset passwords or to delete and recreate accounts. People are notoriously terrible at remembering complex passwords, so we tend to make them easier to remember—and easier to guess. Then we make it worse by reusing the same passwords in multiple locations.

A lack of secure end-user passwords is the number one reason accounts are compromised. Weak or stolen user credentials are exploited in 76% of all network breaches.* For this reason, many organizations have instituted two-factor authentication using hardware tokens.

Hardware token technology, the first generation in user authentication, was introduced in the 80s and can't protect against modern cyber threats, such as Man-in-the-Middle (MiTM) attacks. Some hardware tokens generate an authentication code at fixed intervals (usually 60 seconds) using a built-in clock and the token's factory-encoded random key. Additionally, hardware tokens can be lost, stolen, damaged in the washing machine, forgotten in a hotel while out of town, or just have a dead battery, leaving you with no means to authenticate your credentials—not to mention the expense of replacing the token.

Allowing users to authenticate over the Internet leaves a system open to MiTM attacks against the TCP/IP network. In such an attack, an imposter intercepts information from the legitimate user and then uses it to authenticate on the system. Out-of-band authentication, such as sending a text message to a phone, provides another way to thwart MiTM.

With the widespread use of smart phones and the high cost of buying, maintaining, and replacing hardware tokens, many organizations are moving away from hardware tokens and searching for secure mobile device-based authentication options.

**http:// www.smspasscode.com/hacking*

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

globalscape™
securely connected

Whitepaper

Two-Factor Authentication

Two-factor authentication requires something the user **knows** (password, PIN, or pattern) and something the user **has** (token, magnetic stripe card, smartcard, one-time pad, or mobile phone). For example, when you are asked to enter your Zip code at the gas pump after swiping your credit card, or enter your PIN after swiping your ATM card, you are using two-factor authentication. In organizations, hardware tokens or magnetic swipe cards are most often the "something the user has."

Short Message Service (SMS) is used for text messages on mobile phones. Many banks and social media websites use SMS-based one-time password authentication that sends a passcode to a mobile phone via text message. Most people carry their phones with them everywhere they go, making the SMS passcode more convenient—and much less expensive—than a hardware token or key card.

New-user registration, identity verification, and fraud prevention are the main reasons IT administrators want to implement SMS-based authentication on their networks.

New-user registration, identity verification, and fraud prevention are the top reasons IT administrators implement SMS-based authentication on their networks. SMS codes are generated in real time, never stored, and can use IP address-based policies, and "geofencing" to identify the location of the login request.

SMS Authentication Security

Some SMS authentication software, such as SMS PASSCODE®, generate the codes in real time—codes are never stored—when the user enters a username and password, and then clicks "Log In." SMS authentication offers more protection than the username and password alone. In a text message, the amount of data being sent is very small and is sent quickly. Additionally, SMS PASSCODE locks the code to the specific login session, meaning that even if a hacker intercepts the code, he can't use it, because it is locked to the device.

Ideally, the passcode is associated with the session ID of the login attempt, and encrypted using FIPS-validated cryptographic modules with AES256-bit encryption. The SMS server can be in the "cloud," but many organizations opt for the more secure on-premises installation. SMS-authentication software can use IP address-based policies to allow or block certain IP addresses from logging in, and "geofencing" to identify the geographic location from which the user is attempting to log in.

Remember, each code can only be used once; the user must first authenticate with the username and password, then the SMS code is sent for the second authentication. Your mobile device can augment the security of your authentication system, provided that you:

- *Guard your mobile phone as you guard your wallet.* Leave your mobile device in your pocket or purse instead of on the bathroom counter or dining table in restaurants.
- *Create unique passwords for each account*, regularly change your passwords, and don't allow apps to remember the password.
- *Create unique usernames*; it is more secure than your email username or address. It's usually easy to guess a person's work email address.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

globalscape™
securely connected

Whitepaper

Globalscape® EFT™ Platform Introduces Mobile-Based Two-Factor Authentication

Globalscape® EFT™ Enterprise includes mobile-based two-factor authentication. On a Local or LDAP-authenticated site, the administrator can connect to an SMS authentication provider to deliver a passcode via text message to a user's smart phone as part of the login process for HTTP/S or SFTP transfers. With this configuration, users enter their username and password at a login prompt in a browser window, and if the username and password authenticate successfully on the server, they are then asked to enter a passcode. A passcode is delivered to the mobile phone via text message, and the user types that code into the login screen.

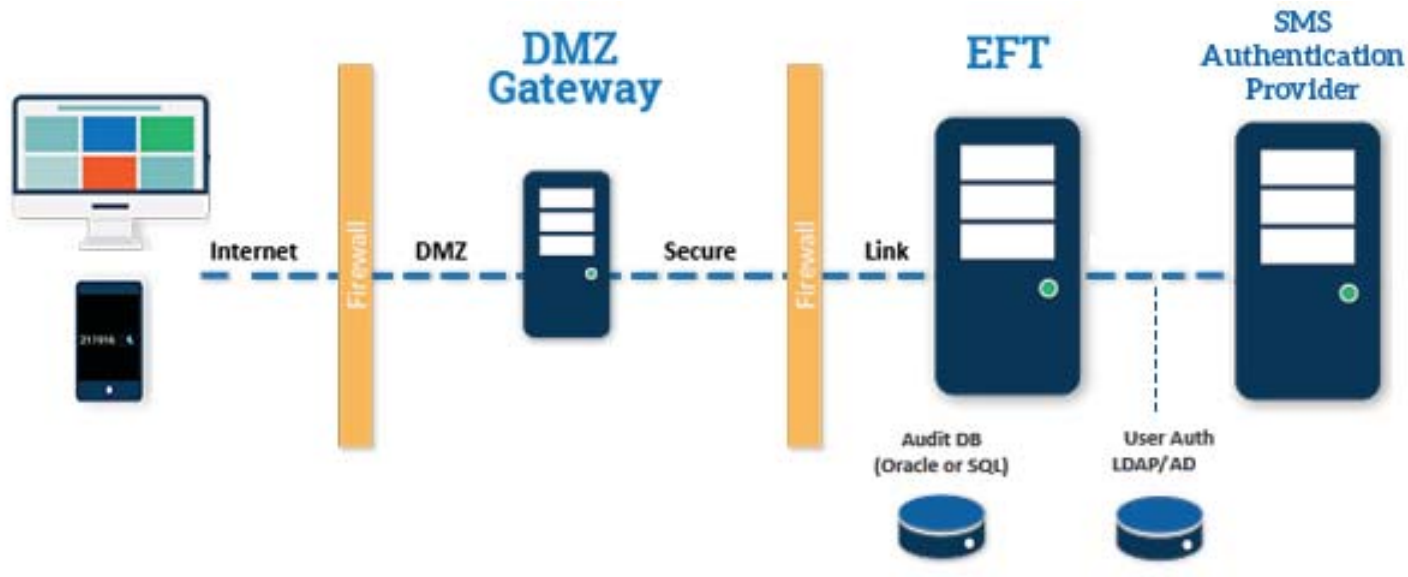
EFT and SMS PASSCODE integrate seamlessly with ActiveDirectory, where user accounts are already stored, making it easy and convenient to add protection to the accounts in a matter of minutes.

In a YouGov survey about SMS-based two-factor authentication, 72% of respondents in the US, 77% of respondents in the UK, and 78% of respondents in Brazil did not know what SMS or two-factor authentication is, even though it's offered as an option on social media sites like Facebook, Google, LinkedIn, and Twitter.

- http://www.theguardian.com/media-network/media-network-blog/2013/nov/22/two-factor-authentication-twitter-google

A built-in Windows feature "Microsoft Network Policy Server" (NPS) must be enabled, and an AD domain must be available. AD integration is configured to retrieve users from an AD group. The SMS provider is installed and configured in your network using basic policies and pointing to the AD server. The user account in AD must have the "mobile number" field configured to know where to send SMS messages.

The SMS authentication software is installed in the internal network behind the firewall. The DMZ Gateway® can be installed in the DMZ for a secure liaison between external connections and your internal network.



4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

Once SMS PASSCODE and EFT are configured, any user account configured to use SMS authentication must use SMS authentication to log in via HTTP, HTTPS, or SFTP. (FTP and FTPS are not supported.) When logging in via EFT's Web Transfer Client, a session cookie allows subsequent operations without further login prompts or SMS messages (until an idle timeout or the user logs out), thereby saving SMS costs and providing an easy-to-use file transfer experience.

Conclusion

Usernames and passwords alone do not secure your network assets, and expensive hardware tokens can be lost, stolen, or damaged. As authentication methods continue to evolve so, too, do cybercriminals' methods to exploit them. Biometric controls such as fingerprinting, and voice and retina scans will eventually become commonplace. Until then, SMS-based authentication combined with the hardened security of the EFT platform provides both ease of use and secure network access.

To learn more about Globalscape EFT or to request a free trial, visit http://www.globalscape.com/mft/.

About Globalscape

Globalscape ensures the reliability of mission-critical operations by securing sensitive data and intellectual property. Globalscape's suite of solutions features EFT Server, the industry-leading enterprise file transfer solution that delivers military-grade security and a customizable platform for achieving best in class control and visibility of data in motion or at rest, across multiple locations. Founded in 1996, Globalscape is a leading enterprise solution provider of secure information exchange software and services to thousands of customers, including global enterprises, governments and small businesses.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)