TELEGRID

6 Two-Factor Authentication Pitfalls

TELEGRID

The following describes 6 potential pitfalls an organization can encounter when setting up Two-Factor Authentication (2FA). These pitfalls are not exclusive to a specific 2FA solution (e.g., One Time Password (OTP), Out Of Band (OOB), SMS, Hard Tokens, etc.) or an implementation (e.g., on-premise, cloud, etc.). This paper concludes with a discussion of TELEGRID's SMRTe which ensures secure implementation of 2FA within an organization.

TURNING 2FA INTO 1FA

2FA requires two of "something you know", "something you have" or "something you are". Too often programmers take the something you know (i.e., password) for granted because it is used in conjunction with something you have (e.g., hard tokens) or something you are (e.g., retinal scanners). The purpose of 2FA is to have two equally secure forms of authentication, not just one. If you installed a home alarm system would you stop locking your door?

2FA enabled network devices and applications should require the storage of passwords and PINs in a secure central database and password validation over secure TLS. However, there exists several 2FA solutions which put the onus of securing initial username+password authentication on the programmer. TELEGRID has seen many cases where programmers perform local username+password authentication against unencrypted databases. This invalidates the first form of authentication, in effect leaving the front door unlocked.

WEB SERVER AUTHENTICATION

2FA solutions must be integrated directly into web server authentication as the primary means of authentication or else gaps will develop which can be hacked. TELEGRID has seen instances where a user was authenticated by a web server, failed the second factor

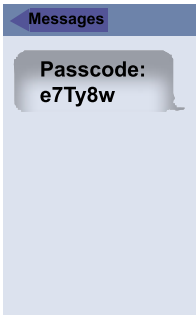
of authentication and could still gain access to an application. While the user might be shown a fault screen, because they failed the second factor of authentication, they can still access the application, for instance, by typing the address into the web page. Since the session has been authenticated by the web server, and there is no communication with the 2FA solution, the user is able to access the application.

WHEN CONVENIENCE TRUMPS SECURITY

Beware of "out of the box" settings and how they expose your network devices and applications to simple hacks. One particularly worrisome setting is the addition of users in some 2FA systems. This setting automatically adds users if they pass initial username+password authentication. It is done to simplify user provisioning so that administrators do not need to spend time uploading user lists to a secondary 2FA system. Rather, the 2FA system assumes that if the user is in an Active Directory or local database, and has therefore passed username+password authentication, then they should automatically be added to the 2FA system and receive a token.

While the thought process is sound it becomes an issue if the initial username+ password authentication uses one of the faulty techniques described above. In that case a hacker can get a username+password and then quickly add themselves to the 2FA system.

GETTING STUCK IN OLD TECHNOLOGY



It is important to have the network allow selection of different 2FA solutions in case the current 2FA method is found to be non-secure. For instance, SMS based 2FA is set to be deprecated in the upcoming NIST Special Publication 800-63B. If network devices and applications were hard coded with SMS based 2FA, it would cost an organization a lot of time and money to change.

THE "US" IN RADIUS

The risks surrounding local authentication are well known but employing centralized authentication is only half the battle. For instance, RADIUS must be encrypted and sent over a secure channel in order to avoid eavesdropping.

TELEGRID

Additionally, RADIUS encryption requires a shared password between the client and the server. Do your non-secure and secure applications use the same RADIUS shared password? How often do you change your RADIUS shared passwords?

ALL OR NOTHING

Deploying 2FA across an organization only works if it is "deployed across an organization." While this seems intuitive, the truth is that cost considerations often force system administrators to pick and choose which network devices and applications to secure. This attitude causes us to ignore so-called non-critical devices and applications. It is often the non-critical devices and applications that are the easiest to compromise and offer the most potential for network-wide attack. To learn more see TELEGRID's paper 3 Attacks from "Non-Critical" Apps.

SMRTe

TELEGRID's SMRTe sits seamlessly between users employing a 2FA solution (e.g., RSA SecurID, Smartcard, etc.) and network devices or applications. Its design resolves the concerns surrounding local authentication or the use of non-secure central authentication protocols. The SMRTe promotes industry best practices by requiring network devices and applications to utilize secure authentication with a centralized AAA server (e.g., Active Directory or RADIUS).

TELEGRID's patent pending technology provides secure authentication without the use of a firewall or reverse proxy. After a user is authenticated and authorized by the SMRTe, they access the network device or application directly thereby removing any bottlenecks or latency. Even though devices and applications do not "sit behind" the SMRTe, its revolutionary design ensures that hackers cannot perform a brute force password attack thereby eliminating the need for password vaults.

TELEGRID Technologies Inc.
23 Vreeland Road
Florham Park, NJ 07039
973-994-4440
sales@telegrid.com
www.telegrid.com