July 30, 2018

Optimizing your two-factor authentication security

CYBERSECURITY
BY SCHNEIDER DOWNS PROFESSIONAL

Often when discussing cybersecurity threats like phishing and initial points of compromise with clients, we'll hear something along the lines of, "That looks great, but we have two-factor authentication enabled on that login." But while enabling two-factor authentication (2FA) is a step in the right direction – Schneider Downs recommends it everywhere – it isn't foolproof. Traditional two-factor does add an extra layer of protection on top of your accounts, deterring lazy malicious actors, but will not stop attackers dedicated to breaching your organization. What traditional forms of 2FA (SMS, push code) really do is limit attackers to a single login session per compromised account.

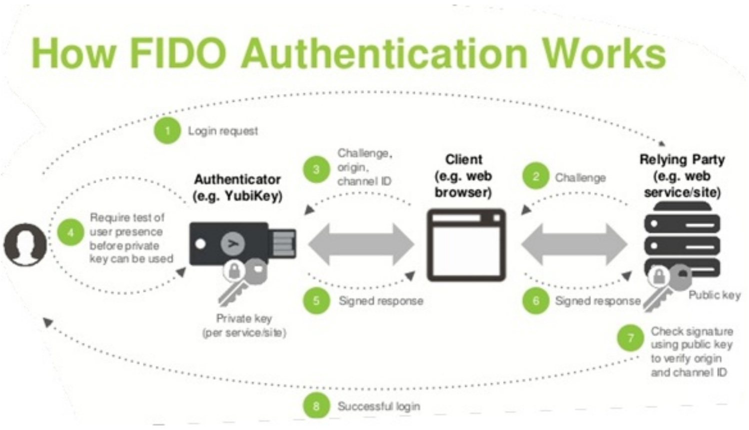
How? Because traditional 2FA requires you to type in a code, it can be phished just like usernames and passwords. If an attacker tricks a user into entering credentials on a fake login site (www.schn3iderdowns.com, for example), they can programmatically submit those credentials to the real site (www.schneiderdowns.com), triggering the SMS token or notification, which the user may also then enter on the fake site. These 2FA methods still rely on users to notice red flags like a slightly different domain, URL or sender, which phishing has proven users are susceptible to overlooking.

Enter Universal 2nd Factor (U2F), created by the FIDO alliance, a form of two-factor using public key encryption and involving a small USB device on which the private key is stored. It gets plugged into an open USB port and is able to communicate directly with your web browser, meaning no additional drivers or software needs to be locally installed.

When you login to a site with U2F enabled, the site sends your device an encrypted challenge, which includes the URL of the website asking for the information. If the user has the USB plugged in and approves authentication, the challenge is signed and sent back. Since the exchange included the URL of the inquiring site, the authentication token is only good for that site. This means that an attacker who tricks a user into entering and approving authentication for www.schn3iderdowns.com cannot successfully relay that authentication to www.schneiderdowns.com.

Methods to attack U2F security will likely become a hot topic in the future, but right now, enabling it on a supported service drastically reduces the success rate of attacks that rely on phishing techniques or keyloggers as a means of breaching that service.

U2F authentication deployment is still in early stages, but may be quite common soon. Chrome, Firefox and Opera are the only browsers that currently support it, but some large services like Google, Dropbox, Facebook, Twitter and GitHub have already adopted U2F support. You can find a list of sites and whether they support U2F at https://www.dongleauth.info/#.


How FIDO Authentication Works
1 Login request
Authenticator (e.g. YubiKey)
3 Challenge, origin, channel ID
Client (e.g. web browser)
2 Challenge
Relying Party (e.g. web service/site)
4 Require test of user presence before private key can be used
5 Signed response
6 Signed response
Public key
Private key (per service/site)
7 Check signature using public key to verify origin and channel ID
8 Successful login

You've heard our thoughts… We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.

Material discussed is meant for informational purposes only, and it is not to be construed as investment, tax, or legal advice. Please note that individual situations can vary. Therefore, this information should be relied upon when coordinated with individual professional advice.