DIGITAL MOUNTAIN®

SPRING 2021 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, and cybersecurity needs. For this E-Newsletter, we discuss mobile device trends for legal and security, including malware, authentication, and legislation around backdoors to end-to-end encryption.

Authentication and Mobile Devices

Mobile phones are technological miracles, in a way. In a short period of time, we advanced from the bag phone, limited in range and convenience, to carrying in our pockets a massive amount of data processing capability and data storage capacity in addition to a phone and internet access – and that is where the danger lies. For all their convenience, mobile devices, especially cell phones, represent an undeniable temptation to would-be thieves and scammers. We hear, read, and discover daily, how commonplace mobile phone compromise is becoming. We must face the fact that mobile authentication, while not foolproof, is still our best option.

Stick a PIN in It

Mobile authentication is the process by which a mobile device user's identity is confirmed. There are three commonly referenced methods: passwords and PINs, biometrics, and tokens. The first two, passwords and PINs and biometrics originate with the user. The user sets the password/PIN combination, and it is their fingerprint, facial scan, or ocular scan that unlocks the device. Tokens are external hardware that generate random codes to be used with authentication applications. The common element to these methods is that they keep devices reasonably secure from an external threat, i.e., someone breaking into your phone if its lost or stolen. Which is great…except, it's not foolproof. Brute-force attacks have successfully cracked password/PIN security without engaging automatic wiping protocols. Additionally, there are at least two well-documented methods by which biometric measures have been defeated: (1) with lifted fingerprints, including using gelatin-based substances (yes, the gummy bear "hack" happened); and (2) for certain ethnicities, cheap masks, even photographs, have tricked the facial scan thresholds.

More is Better

Conventional wisdom for mobile authentication is that Two-Factor Authentication ("2FA"), or

Multi-Factor Authentication ("MFA"), is better than the standard Single-Factor Authentication wherein just a password/PIN or biometric scan is needed. We tend to agree but acknowledge that some users just cannot be bothered with a PIN, a thumbprint, and then potentially another PIN or a token to unlock their phone and check their email. However, it's worth considering where you take your phone, what's on your phone, and what you have to lose.

No longer can iOS-platformed device users take comfort in the proprietary environment that Apple created and the stringent standards that app developers were required to meet to list their apps on Apple's App Store. iOS devices are vulnerable to attacks from within legitimate apps, such as mail apps, where users themselves open the door to black hat hackers through phishing emails and other ploys such as in-app malicious advertisements. Irrespective of platform, SIM swapping, where a scammer convinces a carrier to port SIM card data from the legitimate owner to a new SIM and thus take control of the mobile account to create a "clone" of the phone, has created a nightmare situation for those with a dangerous combination of too little security and healthy crypto wallets or other high value data on their cell phones.

Solutions: Mobile Device Management, Authentication Apps, and Tokens

If an organization is managing employees' mobile devices, they have an upper hand in securing the data on the devices. Organizations can employ Mobile Device Management ("MDM") software solutions, many of which are cloud-based, to handle updates, security protocols, reporting, and incident response, including wiping lost, stolen, or decommissioned devices. The downside of MDM appears to be that many solutions are still somewhat heavy handed when it comes to threat detection, often slowing down legitimate business functions on mobile devices in the name of security. Investing in training administrators to work with the MDM's gatekeeping functions, organizations can customize the solution to their specific needs.

Authentication apps are becoming increasingly popular, especially for use with banking apps, for adding a second layer of security. Many apps already employ a one-time code system which requires the user to enter a code in addition to a PIN, password, or biometric scan, especially for operations such as a password reset. However, many of those apps will allow SMS messaging apps to transmit the code to a device, which because SMS messaging lacks the end-to-end encryption of Apple's iMessage, can be vulnerable to man-in-the-middle attacks.

The most secure option is to add a token system which requires the key to be physically present. Developers are working on making tokens easier to use, including substituting a button push for code entry and a wireless dongle that makes physically connecting with the phone unnecessary (think remote engine start). While the upside of the token system is that a SIM swap is defeated because the physical token must also be present, the downside is that if the token is lost or damaged, the phone or selected apps are locked until the backup token or codes are located.

Many mobile device users dismiss the idea of increasing the security of their phones to Two-Factor or Multi-Factor Authentication because they don't believe that the assets accessible through their mobile devices are worth the effort for a black hat hacker. But considering that a single stolen credit card number sells for as little as $3.00 on the dark web, black hat hackers are looking for massive numbers of accounts to sell, irrespective of card limit. Every user is at risk, and every organization has data to secure. Two-Factor or Multi-Factor Authentication? That's still a hacker's biggest headache and a good investment of time and money.

Please direct questions and inquiries about electronic discovery, computer forensics, cybersecurity and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

DATA CONNECTORS CYBERSECURITY CONFERENCE
Seattle & Portland: March 31, 2021 - April 1, 2021

LEGALWEEK VIRTUAL SERIES 3
April 13, 2021

THE SEDONA CONFERENCE WORKING GROUP 11 ANNUAL MEETING 2021
April 14-15, 2021

IAPP GLOBAL PRIVACY SUMMIT 2021
April 27-28, 2021

THE SEDONA CONFERENCE WORKING GROUP 1 MIDYEAR MEETING 2021
April 28-29, 2021

Click here to see more upcoming events and links.

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com. In the short term, she is available for webinars and remote e-conferences.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: