SIM2K
Adapting Technology to Your Business Needs

2•21
*Information you can use*

SIMformation

# FIDO – For Security, not a Dog

The FIDO (fast identity online) Alliance aims to reduce reliance on passwords for security, complementing or replacing them with strong authentication based on public-key cryptography. To achieve that goal, the FIDO Alliance has developed a series of technical specifications that websites and other service providers can use to move away from password-based security. In particular, the FIDO specs allow service providers to take advantage of biometric and other hardware-based security measures, either from specialized hardware security gadgets or the biometric features built into most new smartphones and some PCs.

Why does the FIDO Alliance want to get rid of passwords? Even with strong encryption, any system that performs authentication by exchanging passwords between two different computers over the internet has vulnerabilities. Encryption isn't perfect so it is possible to intercept passwords in transit. And a password system requires that a service provider keep a list of user passwords on its servers; such a list should itself be encrypted, but that doesn't always happen, and that makes a tempting target for hackers.

The various FIDO specifications all address these fundamental weaknesses by shifting authentication entirely to the devices that are local to the user. These local devices then tell the service provider, via communications protected by public key encryption, that the user has been authenticated, without actually transmitting any sensitive information about the user.

The FIDO specifications are based on public key cryptography. In this form of cryptography, each party uses two "keys" – very large numbers – to encrypt messages via an encryption algorithm. Each party shares a public key that's used to encode a message, which can only be decoded by a private key, which is kept secret. The two keys are related by some mathematical operation that would be difficult or impossible to reverse – for instance, the private key might be two very long prime numbers and the public key would be the number you get by multiplying those two primes together.

The FIDO UAF standard (Universal Authentication Framework) focuses on users of devices like smartphones or tablets. To access a service under UAF, the user would register their account via their devices, which would then request that the user authenticate themselves using some security protocol the device supports, like biometrics (ie: fingerprints or Apple's FaceID.). Once this has occurred, cryptographic keys – but no other data like a password – is exchanged.

FIDO U2F (Universal Second Factor) focuses on using two-factor authentication. Specifically, U2F defines how to use a hardware device to make logins more secure; the private cryptographic key required for encrypted communication is stored on that device. While the standard supports a number of possible devices for this purpose, the most common implementation uses a dedicated hardware security key fob.

Here's an overview of how the authentication process flow works. First, is registration at a website or other service that uses WebAuthn* (Web Authentication):

1. You send a message asking to create an account.
2. The service provider requests a public key.
3. You authenticate yourself using some local method supported by the WebAuthn spec and accepted by the service provider.
4. Your local device generates a pair of cryptographic keys – one public, one private – associates them with your authentication data, and sends the public key to the service provider.
5. The service provider stores the public key and associates it with your new account.

*(*WebAuthn defines communications between the end user and the service provider via an open JavaScript API, so any device or PC that runs a browser that supports the standard can participate.)*

Once you've created that account, you would use the same authentication method to log in.

1. You send a login request to the service provider from your local device.
2. The service provider requests a digital signature, a piece of data establishing your identity that can only be created by a private key but can be read by the corresponding public key.
3. You authenticate yourself on your local device.
4. Your local device correlates your authenticated identity and the service you're trying to access in order to determine the appropriate key pair to use, creates a signature with your private key, and sends it to the service provider.
5. The service provider uses your public key to read the signature and confirm your identity, logging you in.

These specifications are open and can be implemented by any device manufacturers or software developers. It is appearing in more and more applications including Android and most browsers. The quest to find more secure ways of access without divulging information that hackers can use is ongoing in the tech industry, and FIDO is the latest tool being incorporated to add new security checkpoints.


**We have Moved!**
Our new address is:

6330 E 75th St., **Suite 214**
Indianapolis, IN 46250
*Phone number and e-mails remain the same!*

## Malwarebytes Hacked

US cyber-security firm Malwarebytes said it has been hacked by the same group which breached IT software company SolarWinds last year. Malwarebytes said its intrusion is not related to the SolarWinds supply chain incident since the company doesn't use any of SolarWinds software in its internal network.

Instead, the security firm said the hackers breached its internal systems by exploiting a dormant email protection product within its Office 365 tenant. Malwarebytes said it learned of the intrusion from the Microsoft Security Response Center (MSRC) on December 15, which detected suspicious activity coming from the dormant Office 365 security app. At the time, Microsoft was auditing its Office 365 and Azure infrastructures for signs of malicious apps created by the SolarWinds hackers, also known in cyber-security circles as UNC2452 or Dark Halo. Malwarebytes said that once it learned of the breach, it began an internal investigation to determine what hackers accessed. "After an extensive investigation, we determined the attacker only gained access to a limited subset of internal company emails," said the Malwarebytes CEO.

Since the same threat actor breached SolarWinds and then moved to poison the company's software by inserting the Sunburst malware into some updates for the SolarWinds Orion app, Malwarebytes said it also performed a very thorough audit of all its products and their source code, searching for any signs of a similar compromise or past supply chain attack. "Our internal systems showed no evidence of unauthorized access or compromise in any on-premises and production environments. Our software remains safe to use," the company says.

With this disclosure, Malwarebytes becomes the fourth major security vendor targeted by the UNC2452/Dark Halo threat actor, which US officials have linked to a Russian government cyber-espionage operation. Previously targeted companies include FireEye, Microsoft and CrowdStrike, with successful intrusions being reported at FireEye and Microsoft.

FireEye investigated how its own systems were infiltrated in the same campaign. Officials from FireEye's incident response division, known as Mandiant, confirmed that its teams were first to raise the alarm to SolarWinds and U.S. law enforcement after discovering the far-reaching security compromise. "We looked through 50,000 lines of source code, which we were able to determine there was a backdoor within SolarWinds," said a Mandiant spokesman. "If this actor didn't hit FireEye, there is a chance that this campaign could have gone on for much, much longer. One silver lining is that we learned so much about how this threat actor works and shared it with our [partners]," the company said.

The fallout from the cyber-intrusion is that a slew of powerful agencies had possibly been hit, including the Department of Homeland Security (DHS), the State Department, Commerce, Treasury and the Pentagon. This malware attack continues to grow in scope as more and more companies have detected the intrusion. SIM2K will continue to monitor and report.

## Windows 10X vs. Chrome?

Demand for laptops soared to record levels in 2020, driven by the work-at-home and school-at-home requirements brought on by the COVID-19 pandemic. Notebook sales exceeded 200 million, a record 22.5% year-to-year increase.

Microsoft should be celebrating. But look closely and there is a disturbing trend for the company: Chromebook sales went sky-high last year, with nearly 30 million purchased. That represents 74% year-over-year growth and comprises 15% of notebook market share and dropped Microsoft below 80% for the first time ever." It is predicted that Chromebook sales will continue to grow at a faster rate than Windows notebooks, with Microsoft's market share dropping to perhaps 70%, and Chromebook's rising to 20%. (The remainder will go to Apple laptops.)

To counter Chromebooks, Microsoft is releasing Windows 10X, a Chrome-like operating system that Microsoft is betting will be a Chromebook killer. It is a simplified version of Windows 10, with just a basic Start menu with icons representing apps, but no live tiles or other add-ons. The Taskbar is streamlined too, and there are no notifications icons and no ability to right-click to customize. The streamlining extends to the operating system. It won't run legacy Windows applications — in other words, the apps you normally run from the desktop like Office. There's no true file manager, just an extremely limited file browser built for OneDrive.

In short, everything about Windows 10X has been built for the cloud, just like Chromebooks. You'll mainly run web apps on it, just as you do on Chromebooks. And you'll run them on the Chromium-based Edge browser, which should mean that any web app and browser extension that runs on a Chromebook will be able to be run on a Windows 10X notebook. Windows 10X, however, will also run Windows apps, the apps built into the full-blown version of Windows 10, such as Mail, Weather, Calendar, and so on.

At some point, Microsoft is expected to let Windows 10X run traditional desktop apps in containers. But why bother? They'll likely run painfully slow on the kind of low-end hardware Windows 10X notebooks will have to be if they're going to compete with Chromebooks. And that gets to the crux of the choices Microsoft and its hardware partners will have to make with Windows 10X devices. Are they willing to compete on cost, selling them for as little as $300 or even less? Or will they build the devices with more powerful hardware and charge a premium? If they go only the premium route, Windows 10X devices should make little to no headway against Chromebooks. Chromebooks are ubiquitous in education, and few, if any, school systems will be willing to pay several hundred dollars more for a Windows 10X device than for a Chromebook. If Microsoft and its partners decide to stuff Windows 10X devices with higher-end hardware and enough RAM to run desktop Windows 10 applications, it's hard to imagine many people will buy them.

*SIMformation* is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

## Work from Home — Work from Anywhere

The importance of flex work became well established in the past five years. LinkedIn found a 78% increase in job posts referencing flexible work between 2016 and 2018. But when the pandemic hit, what had been a slow trend became an overnight one. And large-scale remote work appears to be here to stay, and may lead to employees wishing to work from anywhere – not just within a "still drive to the office" distance. What if that "home office" was a condo in Florida? Would that employee still be part of your team?

A LinkedIn report in February found that 98% of those surveyed would prefer to work remotely, and 29% would quit if they had to return to the office. It's time for businesses of all sizes to understand the consequences of remote work. Companies facing the new world of remote work should not assume that it's just like the old but with "people out of the office." Here are some issues to be faced in a world of work from anywhere:

**Vastly more complex HR**. An employee working full time from home already adds complexity when you consider that you have to comply with the tax, employment, and leave requirements – including meal breaks, overtime, vacation pay, and other issues – where each employee is based, not just where the company is based. If you have employees in 3 states, you have to comply with the law in those 3 states.

**New pay issues.** Companies differ on whether to change the pay of employees who transition to remote work. The idea goes that a salary often takes into consideration the high cost of living in an expensive or premium area, but if people move to a place with a lower cost of living, they don't need the same compensation. Employees may not see it that way.

**New legal issues**. When employees move to remote work status, or when remote workers are out of state, the legal complexities can add up. For starters, most employment laws still apply to remote workers: workers' compensation, discrimination, wage law, overtime issues – these don't change when employees are working remotely. On top of what stays the same, a host of legal issues arise for remote workers. If employees are working in other cities or states, the laws in their locations normally have to be adhered to as well. Some large cities have unique legal requirements for hiring, leave, and other issues.

**Significant tax implications.** Employing workers in different states require state tax withholdings in those states.

**Security**. Remote employee security is a much bigger deal when more people are working from home. Left on their own, employees may abandon best security practices. Physical security to company computers and data can't be assumed. Cybercriminals are actively targeting the new opportunity of the mass migration to remote work.

**Communication.** Some of the biggest challenges with remote work are team bonding, collaboration, and work oversight. Casual conversations may appear needless and frivolous but in fact help employees bond, make work more enjoyable, and lead to valuable work ideas. It is not sustainable to keep employees on video calls for hours each day. And the perception of isolation for an at-home worker may present issues with work satisfaction.

Allowing employees to work remotely used to be optional. Now, it's far less so for many companies. The pandemic is showing the need for companies to embrace remote work. Now is the time to be sure your company is prepared to support these workers. SIM2K can help with data security, VPNs and other tools to help keep these remote workers connected and protected against malware and cybercriminals.

## "Random Tid-Bytes"

### New Chrome Browser Features

Google has released Chrome 88, adding capabilities to the browser's password manager; streamlining permission requests from sites that asked, say, to switch on the microphone; and for enterprises, ending support for an add-on that called up Microsoft's Internet Explorer (IE) to render old intranet websites and legacy apps. In Chrome 88, the integrated password manager — reached by clicking the key-like icon after clicking the user account in the upper right — boasts an in-browser password checker that quickly identifies weak passwords and/or those which probably have been revealed in past data breaches. (This service, dubbed "Safety Check," debuted in May 2020; Google claimed that since then, it's seen a 37% reduction in compromised credentials stored in its browser.) Depending on the result of the check, one or more of the stored-in-Chrome passwords may be labeled "Change password." Because Chrome updates in the background, most users can finish a refresh by relaunching the browser. To manually update, select "About Google Chrome" from the **Help** menu under the vertical ellipsis at the upper right; the resulting tab shows that the browser has been updated or displays the download process before presenting a "Relaunch" button.

### 10 Overused Terms in the Tech Industry

Recently, CIO magazine released a list of the 10 most overused buzzwords that the tech industry uses on a regular basis:

- Digital Transformation
- Change Management
- Agile
- DevOps
- Minimal Viable Product
- Artificial Intelligence
- Machine Learning
- 5G
- Extended Reality ("XR")
- Disruptive Technology

Reasonable minds can differ on what constitutes legitimate or sketchy applications of terminology. Sometimes 5G really means 5G. XR can include a legitimate application of virtual reality. Buzzwords have a place, but in the end, for example, it's acceptable to use digital transformation as shorthand to describe how you successfully altered the business through people, process and technology. But substituting "digital transformation" for plain speak before you've executed the strategy sets a high bar that often does not hold up well in decision-making rooms. Here at SIMformation, we try to stay clear of these buzzwords unless we are specifically discussing that technology.

### Improvements to Firefox

Mozilla has upgraded Firefox, adding to its emphasis on privacy by isolating supercookies that some sites rely on to track users' movements on the web. Supercookies store user identifiers in "obscure parts of the browser," as Mozilla puts it, including caches and various types of connections and sessions. Tracking entities have gone to great lengths to hide their trackers as browser makers have blocked more obvious avenues, such as traditional cookies. Called "Network Partitioning," Firefox now isolates multiple caches used by the browser to boost performance and restricts content for each particular site, rather than sharing content where tracking information may be hidden and thus reducing chances of monitoring your browsing activity.

# The Dark Web Poses Threat to Security

Lately, dark web actors have one more worry: getting caught by law enforcement. Tracking dark web illegal activities has been a cat-and-mouse game for authorities, but in the end, they often catch their adversaries and seize the dodgy money. On the night of the 2020 presidential election, for example, US government officials managed to empty a $1 billion Bitcoin wallet, recovering funds linked to Silk Road, seven years after the market's closure. Silk Road was a popular underground marketplace dealing in illegal goods and services, such as narcotics, hacking for hire and contract killing.

Events like these have compelled cybercriminals to plot new strategies, which sometimes involves closing shop and cashing out before they get on the feds' radar. In October 2020, the Maze ransomware group shut itself down stating they had retired their activities. However, experts believe they have merely joined another group to continue operations under a new banner.

"In recent years, the dark net has dramatically changed, quite organically, due to increased organized criminal organizations' use of anonymous forums and marketplaces, the increased presence of young YouTube inspired 'criminal wannabes,' and naturally, the subsequent increased presence of law enforcement and their attempts to infiltrate, de-anonymize, and take down such groups and hidden services," said one security expert. His belief is that the dark web has evolved into an intermediary ground where cybercriminals minimally interact to recruit new members for their group. They then move to private, encrypted channels to plan their next actions. By switching patrons over to legitimate end-to-end encrypted messaging services, cybercriminals leverage the reliable distributed infrastructure of these platforms while remaining discreet and avoiding the scrutiny of law enforcement.

The dark web of today represents a wide variety of goods and services. Although traditionally concentrated in forums, dark web communications and transactions have moved to different mediums including IM platforms, automated shops, and closed communities. Threat actors are sharing covert intelligence on compromised networks, stolen data, leaked databases and other monetizable cybercrime products through these mediums.

"The market shifts are focused on automation and servitization [subscription models], aimed at aiding the cybercrime business to grow at scale," says another security expert. "As can be witnessed by the exponential rise of ransomware attacks leveraging the underground financial ecosystem, the cybercriminal-to-cybercriminal markets allow actors to seamlessly create a supply chain that supports decentralized and effective cybercrime intrusions—giving attackers an inherent edge."

On the plus side, security professionals and threat analysts can tap into this intel to identify and patch system weaknesses before threat actors can exploit them. Defenders can exploit these robust and dynamic ecosystems by gaining visibility into the inner workings of the underground ecosystem—allowing them to trace the same vulnerabilities, exposures, and compromises that would be leveraged by threat actors and remediate them before they get exploited.

This is done by monitoring forums and darknet sites where threat actors are most likely to lurk, discuss upcoming threats, and put exploits up for sale. A hacker recently posted exploits for over 49,000 vulnerable Fortinet VPNs on a forum, some of which were prominent telcoms, banks and government organizations. This was followed by a second forum post where plaintext credentials for all the VPN devices were posted, allowing anyone to exploit these channels. Thousands of corporate VPNs present on the list remain vulnerable. But, tapping into such forums and monitoring for such intel can give heads up to security teams at organizations to do their due diligence in where adversaries may be headed next.

Advanced persistent threat groups are now using the dark web to gather knowledge of their targets, then use legitimate network protocols and programs for covert data exfiltration. It used to be organizations tended to be concerned about their own data appearing on the dark web, and it would only be alarming if significant data was located. Now, many of the Chinese and Russian nation-state backed threat groups are using the dark net to probe for possible vulnerabilities then moving forward with an attack.

Since the start of 2020, the use of SSH by these APT groups has increased by over 200%. SSH, or Secure Shell Home, is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, login, and remote command execution, but any network service can be secured with SSH. Research indicated that APT groups are using SSH to infiltrate organizations unnoticed and, once inside, are using poorly monitored and maintained systems—especially industrial control systems—to steal significant amounts of data. Several recent attacks are alleged to have stolen over 1 terabyte of data from individual businesses, a huge amount that organizations are failing to spot because they are unable to monitor effectively for dark net connections.

This point has been substantiated by the discovery last month of the massive SolarWinds attack attributed to a Russian espionage group. by exploiting trust within a legitimate program like SolarWinds Orion and its secure update channels, sophisticated attackers managed to silently breach more than 18,000 of the 300,000 SolarWinds customers and remain undetected for months. This is different from cases where threat actors make noise on public or dark web forums when leaking data dumps.

So, monitoring the dark web alone for signs of data exfiltration isn't enough. Threat analysts and security researchers are therefore encouraged to reevaluate their monitoring strategies. Rather than focusing solely on detecting anomalies within corporate networks, such as foreign IPs and odd port numbers, or waiting for proprietary data to appear on the dark web, it is worth monitoring trustworthy programs and services, including their security updates, and your organization's software supply chains where threat actors could be hiding unnoticed.

Security of data continues to be paramount in the IT industry, and SIM2K is constantly evaluating our security offerings to have the best tools available for your network. Call us for more information on security and how we can work with you to protect your company information.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com