DOING THE SECURITY TWO-STEP: WHY AUTHENTICATION SHOULD BE BUILT INTO HARDWARE

To be truly effective, multifactor authentication (MFA) methods need to be grounded in hardware, not reliant on software alone.

> "WE'RE GIVING THE USER THE CONVENIENCE OF A SOFT TOKEN WITH THE SECURITY AND HARDENING OF A HARDWARE TOKEN."
>
> —Yasser Rasheed
> Director of Business Client Security, Intel

You know by now that password-only authentication is no match for today's sophisticated cybercriminals. Passwords are being acquired by hackers at record rates, usually by Trojan-horse-style traps, which have increased by 55 percent in recent years[1].

And stolen credentials are a pervasive and costly problem for today's enterprises—they accounted for 81 percent of all data breaches last year[2], and it's predicted that $6 trillion in cybercrime damages will be incurred by 2021[3].

Hackers are learning the two-step, but they struggle to crack hardware

Many enterprises have already transitioned to a two-step authentication process in response to this growing issue. That's certainly a smart move, but even the best two-step authentication protocols can be vulnerable when they rely on software alone. Software is inherently hackable, and if intruders can break through the code of one authentication factor, they can probably crack through a second. And if not, they change the IT policy or circumvent the token representing the authentication decision.

Some businesses are now relying on key fobs or other physical tokens as a secondary form of authentication to overcome the weaknesses of software-only security. While this is more secure, it's also cumbersome, as these tokens can be lost, broken, or stolen. A better solution is one that incorporates authentication into the hardware itself.

True multifactor authentication (MFA) needs to be built into the hardware to effectively combat breaches. Grounding security in the silicon processes of the hardware provides a hardened layer of protection that's much more difficult to hack than software alone—and does so without the added burden of requiring employees to carry physical tokens. Fortunately for today's enterprises, 7th Gen Intel® Core™ vPro™ processor-based devices feature this kind of hardware-enhanced security right out of the box.

With the built-in Intel® Authenticate solution, these devices are designed to prevent intrusions thanks to MFA that's rooted in the hardware. And with a wide variety of authentication factors and security options to choose from, businesses can tailor their solution to specific needs with greater precision.

"The Intel Authenticate solution gives businesses the flexibility to choose type of factors, when to apply location, apply per groups, per user, per device, per

situation, and change protocols when something goes wrong," said Yasser Rasheed, director of business client security at Intel. "And on top of that, they have the ability to control all of this remotely."

New factors = better security

Malware is evolving quickly, but so is factor diversity. The Intel Authenticate solution supports the ability to combine a breadth of authentication factors, including fingerprints, Bluetooth* proximity, protected PIN, and device location.

"With Intel Authenticate, we're giving the user the convenience of a soft token with the security and hardening of a hardware token," said Rasheed.

Through integration with software and hardware leaders across the ecosystem, the Intel Authenticate solution's range of factors continues to grow and provide more choices and policy flexibility.

As software security partners such as Microsoft*, Citrix*, Cisco*, and RSA* build additional capabilities on top of the Intel Authenticate solution to take advantage of its factor innovation and hardware strength, the Intel vPro platform provides a solid foundation.

Hardened security that doesn't hinder productivity

Not only is it impossible for employees to forget the unique ridges of their fingerprints or distinguishable facial peaks, but biometric-based factors are also harder for hackers to impersonate. Bluetooth phone proximity or new devices themselves can also confirm an identity based on logical location when Intel® Active Management Technology (Intel AMT) is activated with the Intel Authenticate solution.

With new devices, authentication can now verify the fingerprints and facial features that make every employee unique, and the physical devices that have become an extension of them. Using these types of passive, personalized factors keeps the authentication process easy for users, allowing them to log in quickly and having little to no effect on their productivity.

"Combining one interactive, active factor with one or more of the passive factors makes it super convenient for the user," said Rasheed. "It's actually a lot more convenient than using a password."

Preparing for new standards

Security compliance standards are becoming ever more stringent. New requirements like those in the General Data Protection Regulation (GDPR) are compelling organizations to continue to improve their security posture and be prepared for audits. Deploying hardware-based security technology like the Intel Authenticate solution and Intel® Data Guard data encryption will help organizations prepare for these new rules, increasing their ability to meet compliance deadlines while diminishing the likelihood of financial penalties.

IT'S PREDICTED THAT $6 TRILLION IN CYBERCRIME DAMAGES WILL BE INCURRED BY 2021[3]

Putting security into the silicon

Grounding authentication into the silicon of the hardware itself renders most Trojan-horse attacks ineffective, as stealing a user's password or breaking through the security software won't be enough for a hacker to enter the system. Comprehensive authentication needs to be anchored in processing—farther from sight, further from reach—below the software layer, where code is too easily manipulated. This process includes securing in hardware the moment when the user is authenticated and granted access to network services and data. While no security setup is wholly foolproof, adding MFA hardware layers such as those provided with the Intel Authenticate solution makes intrusions far less likely to succeed.

"The beauty of multifactor done in the hardware is that you have the best of both worlds: convenience for users and flexibility and control for IT," said Rasheed.

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[2] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
[3] http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

0725/CC/DOR/PDF