Actionable Business Insights

Mi6Research Note

IT Infrastructure - Security

1/20/2016

Review of Intel Gen 6 vPro Authenticate

Intel’s New 4-factor authentication in hardware – Is it A Game Changer?

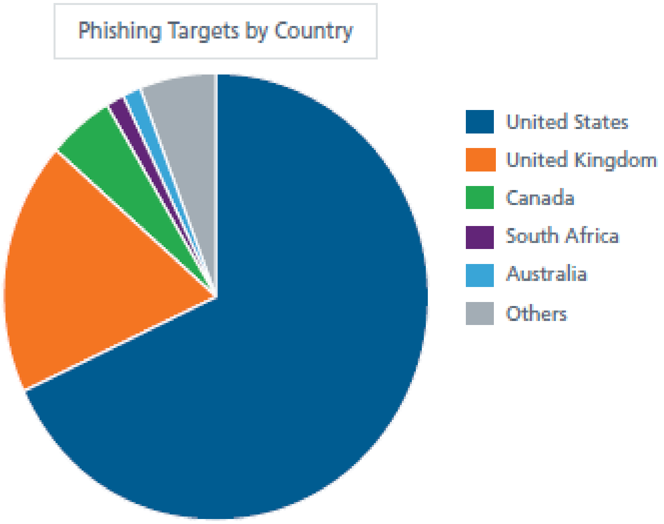
Summary:

6th Generation Intel Core vPro processors now feature Intel® Authenticate Solution, a hardware-enhanced multifactor authentication solution that strengthens identity protection. Intel is previewing the new security innovation Intel® Authenticate for businesses to begin internally testing and qualifying. Intel Authenticate is a hardware-enhanced, multifactor authentication solution that strengthens identity protection on the PC, making it less vulnerable to identity and security credential attacks.

Analysis:

The Problem

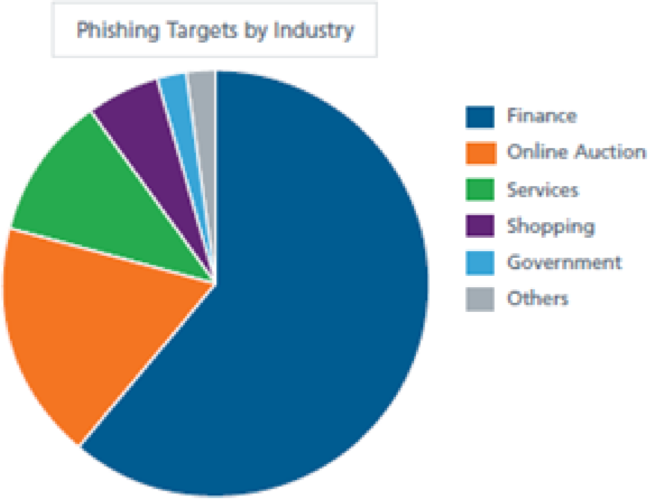
Hackers just keep getting more inventive and dangerous. It is estimated that phishing, which is tricking people out of usernames, passwords and other sensitive information with phony emails, is a growing threat both to governments and businesses.



According to Verizon’s 2015 Data Breach Investigations Report, nearly 50 percent of victims open phishing emails and click on the link within the first hour of receiving them. The Monthly Online Fraud Report – January 2015 found that there were 46,747 phishing attacks worldwide in December United States regional banks were targeted by a quarter of all phishing attacks in December while US nationwide banks experienced an increase in phishing volumes from 50 per cent in November to 58 per cent in December.

And of course now there's spear phishing where the spear phisher does his research on you and knows your name, email address and other details that make the spear phishing email seem relevant, real and worthy of a response because it appears to be from an individual or business that you know and trust. Beware - it's not. The email will make reference to a known entity, like a mutual friend or to a bank or ecommerce site you belong to, possibly asking for urgent action, tempting you into acting before thinking. I've seen spear phishing attacks claiming to be PayPal and eBay to name a few.

Phishing attacks use social engineering techniques mixed with technical tricks to fool the user and steal sensitive information and banking account credentials. Social engineering schemes are typically based on spoofed emails to lead users to visit infected websites designed to appear as legitimate ones. The websites are designed to lead customers to divulge financial data, such as account usernames, credit card numbers, passwords, and social security numbers.



Spear Phishing attacks have been associated with high-profile data breaches, such as those experienced by Target, Sony and the Pentagon. Spear phishing attacks can quickly yield valuable information such as user credentials to corporate or personal accounts, which attackers can leverage to gain additional insight into the target organization or individual, and to launch additional attacks that seek access to additional systems and services. It is also feared that breaches like the recent one of Ashley Madison provides a real treasure trove of personal details, emails, usernames and the like for spear phishers

The US hosted 48 per cent of phishing attacks in December, followed by the United Kingdom

(7 per cent), Germany (5 per cent) and China (3 per cent).

The Current Solution

Securing computers has become very challenging and one of the pain points has become the need for super complex passwords. You know the ones. It must include a capital letter, numbers but no repeat numbers, a special character and be at least 8 alphanumeric characters. Random numbers and letters work best and please…change them frequently and never use the same or similar password on multiple applications.

And BTW, good luck remembering your passwords.

Then there is the issue of sharing passwords and the consequent leakage to third parties who can enter the system and steal, corrupt or sabotage data!

Multi-factor Authentication

Multifactor authentication is the method of using more than one method for identifying a user. For example, if I used your fingerprint and a password or a PIN, I would be using two-factor authentication.

If I used a password (something you know), your phone (something you possess) and your iris scan or fingerprint (something you are) then I am using a very powerful three factor authentication method that is much harder to defeat than most of the authentication we use normally.

Enter Intel…

"6th Generation Intel Core vPro processors now feature Intel® Authenticate Solution, a hardware-enhanced multifactor authentication solution that strengthens identity protection."

Intel just announced Intel Authenticate that will become part of all enterprise PC processors. It will give IT managers the choice of several authentication methods they would like to use to safeguard users. And because it is hardware based authentication which is part of the Intel chip, it is much more difficult to hack. Based on the IT security policy and procedures for its company, IT will be able to choose from multiple methods of authentication that once configured, are captured, encrypted, matched, and securely stored in hardware.

Intel is tackling the challenge of securing computers, and the need for complex passwords. Passwords are a big pain point in the enterprise because people don't like to make difficult passwords, and sharing passwords can be a big problem. Social engineering and more complex attack vectors can render passwords the easiest way to get into a company's data.

Intel's new security system on a chip goes into test mode as of January 18th, 2016 and is targeting production in the next few months. It is similar to Windows Hello, but potentially better, as it allows for the use of more authentication factors and the authentication is done in 'tamperproof' hardware, within the CPU, providing stronger security.

So what's the big deal?

Intel's new business processors will verify an employee's identity with a personal identification number, proximity of the employee's mobile phone or badge, biometrics like a fingerprint, and location of the employee, i.e. building, site or office location.

So it could be really strong, and I mean super strength authentication based on who you are, what you know, where you are, and what you have.

But let us note that in practice today, the end user would not be using a single, albeit complex password. They are already using biometric scanners in conjunction with strong passwords in some cases, when accessing their PCs.

What Intel has done with Intel Authenticate is made the authentication multi-factor and integrated it at the chip level to produce much stronger PC login authentication. So now, depending on the configuration, the end user may need to also look at their PC (iris scan or facial recognition), or touch their thumb, have their smartphone or their company ID badge near them or be using their PC at a known/verified location like the workplace or home.

The PC login becomes much more secure, but what about other apps and mobile devices?

This solution focuses on the PC and its login. But as we know, the problem of enterprise authentication is much broader. For instance, many users use their mobile devices to access work email accounts or other SaaS applications. Intel Authenticate would need to be in these devices to broadly deploy a truly strong hardware based authentication solution, enterprise wide.

Plus there is still the issue of application authentication. Though Intel Authenticate ensures the right person is logging in to use their PC or laptop, when I am using my PayPal account, how does the app ensure it is really me? Back to using the strong passwords. At most, some apps offer a two factor authentication using your mobile phone but it is inconvenient and cumbersome to get into your apps that way.

When a hacker breaks into your application account, let's say PayPal, they will have done so after successfully perpetrating a Phishing attack on the end user. Intel's solution does not prevent Phishing. The hacker will be able to enter your application with the app's password and continue to wreak havoc. '

One solution to this would be PayPal using network based authentication that checks the location from where the end user is logging in. If a location is suspected to be unusual, the app could lock out the user. This approach is already in use by a number of companies now, especially in the most vulnerable and highly attacked financial arena: Online banking, such as at Wells Fargo and Credit card account access such as at Barclaycard.

So even though this is a step in the right direction and better protects your PC login for work, there is a long way to go to give protection to important applications, mobile devices and from concerted phishing attempts.

However, imagine if location (where you are) and the Intel Authenticate (what you have) could be transparently added to all applications? Now that would be powerful. This would need a software enhancement in the app whereby the app gets the OK from Intel authenticate to confirm the presence of the PC you normally use and then the app uses IP address or maybe on a mobile phone it could also use GPS to confirm the location.

It remains to be seen how successful Intel's new Authenticate will be in practice and what the feedback will say once it has been tested broadly. Some of the factors that will determine its success will be:

- Ease of integration within the IT infrastructure
- Ease of use and implementation by IT staff
- Transparency and ease of use for the end users
- Security effectiveness of multifactor authentication in practice
- Reliability in practice. The absence of false positives.

The final verdict will come later in 2016, after the production rollout and IT managers give it a whirl and see how easy it is to rollout and how much additional protection it provides in day to day operations.

Intel's solution may be able to enhance application security further if applications chose to integrate with it in the future but this would require a retroactive integration effort which is unlikely to be undertaken by existing application providers without easy software oriented plug-ins and a marketing program that makes it painless and inexpensive for the thousands of enterprise applications and their mobile variants.

One other benefit for enterprises from Intel's innovation may be to encourage the development of strong (hardware based) authentication broadly within the mobile processor ecosystem.

So for now, it's a welcome enhancement and its real world results and consequences remain to be seen.

Bottom Line

Intel's vPro enhancement with multi-factor authentication provides much stronger protection for enterprise users when logging into their PCs. The flexibility of the solution is good, allowing for 1, 2, 3, or even 4 factor authentication, as per the security policy of the enterprise. This protection only applies to the PC login itself. It doesn't and cannot apply to other applications and therefore would still allow phishing attacks to succeed

The challenge of enterprise authentication is much broader than Intel's solution provides. There are mobile devices being used by many end users to access work apps and the problem of application level strong authentication persists. So for example, Intel Authenticate ensures the right person is using their PC or laptop, but when I'm using my smartphone to access my work email, or someone else is using my PayPal account, or my Amazon login, it is less relevant (for now).

With the current focus being on the enterprise PC, some of the factors that will determine success include ease of integration and implementation by IT, the transparency, speed and ease of use for end users and its proven security and ultimate reliability in day to day operations.

Intel Authenticate is a step in the right direction for enterprise PC login security. It remains to be seen, possibly as soon as late 2016, how successful Intel Authenticate will be in practice.

Relevant links:

http://newsroom.intel.com/community/intel_newsroom/blog/2016/01/19/intel-transforms-the-workplace-with-latest-6th-generation-intel-core-vpro-processors

Mi6Research provides market research and business insights to help decision makers in information technology, business, and marketing and investment functions. For more information visit www.Mi6Research.com or contact us at info@Mi6Research.com.

IMPORTANT NOTICE: Our information is based on sources believed to be reliable and information up to date and correct to the best of our knowledge at the time of preparation. The opinions reflect judgment at the time and are subject to change. Mi6Research disclaims all warranties as to the completeness, adequacy or accuracy of such information and shall have no liability for errors, omissions or inadequacy in such information. You assume responsibility for all interpretations of, use of all information in this report and Mi6Research is not liable for any interpretations or decisions made by you.

Copyright © Mi6Research 2015. All rights reserved. **Unauthorized reproduction is strictly forbidden.**