The escalation in password theft makes it clear that simple username and password combinations are poor protection against the methods that sophisticated cybercriminals use. Research released by Experian CreditExpert* and market research agency Opinion Matters concluded that 12 million pieces of personal information—90 percent consisting of username/password combinations—were stolen and sold during the first four months of 2012, a 300-percent increase over the same period last year.

In another risk assessment survey, the "McAfee Threats Report: Second Quarter 2012" noted that there has been a sharp rise in password-stealing Trojans.

“The reason password and login combinations make up nine out of ten illegally traded pieces of data is because they give access to a huge amount of other valuable information, such as address books and related accounts,” said Peter Turner, managing director at Experian Consumer Services.

As the frequency, severity, and ingenuity of cybercriminal attacks have increased, IT professionals, chief technology officers, and chief information officers are seeking stronger techniques to protect the integrity of online business and financial transactions.

Intel® Identity Protection Technology (Intel® IPT) can provide a deeper level of security, using one-time passwords generated in hardware to authenticate a user’s identity with websites enabled for this technology. Even if a username and password are stolen, a cybercriminal is highly unlikely able to log on to a participating site because the user’s identity is bound to security mechanisms embedded within the laptop itself.

Countering the Costs of Identity Theft

Citing data from several sources, an article on Mashable.com, “How Much Does Identity Theft Cost,” tagged the worldwide business costs of identity theft at USD 221 billion. As many as 10 percent of Americans have been victims of identity theft, resulting in average costs to each of about USD 5000.

Instead of letting businesses and computer users become victims, Intel IPT enables a proactive approach, minimizing the ability of a cybercriminal to mimic a user’s identity with a stolen username and password. If the cybercriminal cannot send the six-digit code generated by Intel IPT within the Ultrabook™ device or PC, access to the account on the website is effectively blocked.

Intel® Identity Protection Technology Capabilities

Through the use of two-factor authentication that relies on a tamper-resistant area within a PC’s hardware, Intel IPT delivers stronger security than software-only solutions. This technology is built into all Ultrabook devices and all computers based on 4th generation Intel® Core™ processors. Intel IPT is also available in the latest Intel® Core™ vPro™ processors and select previous generations of Intel Core processors. The capabilities of the latest version of Intel IPT include a number of security-strengthening features.

One-Time Password (OTP) Authentication

Two-factor authentication using an OTP combines something the user knows (a username and password) and something the user has (typically a token or key fob that produces a six-digit number—valid for only a short period of time—on demand). In the case of Intel IPT, that six-digit number is generated from an embedded processor, the Manageability Engine (ME), on the computer motherboard. The ME is tamper-resistant and operates separately from the operating system for added security. Algorithms developed by third-party security solution providers run in the ME, performing the operations that link Intel IPT-enabled PCs to a validated site and ensure strong authentication.

Embedded Public Key Infrastructure (PKI)

Intel IPT with PKI is found on the latest PCs with Intel Core vPro processors and offers a mechanism for authentication based on certificates that are stored and managed in a protected area in hardware, as are the encryption keys. Because the keys are stored in hardware, they are never exposed to software being run by the processor and they are permanently tied to the PC hardware. Intel IPT with PKI software allows interactions with the Microsoft CryptoAPI software layer, simplifying secure interactions with Microsoft Internet Explorer®, AnyConnect®, Microsoft Outlook®, and other security-aware applications.

Technology Brief

Intel® Identity Protection Technology

Safeguard Sensitive Information with Intel® Identity Protection Technology
Protected Transaction Display

Protected Transaction Display can display information to the user and receive input from the user using a separate embedded processor. Information displayed using PTD is designed to only be visible to a user physically present in front of the device. Therefore, meaningful user interaction with such information helps indicate user presence.

This powerful capability helps mitigate against malware such as screen scrapers, keystroke loggers, bots, and man-in-the-middle (MitM) or man-in-the-browser (MitB) and can be deployed in usages such as financial transaction verification, authentication with a PIN Pad or CAPTCHAs.

Near-Field Communication

Near-field communication (NFC) is a short-range wireless communication technology that describes a protocol for handling peer-to-peer data exchanges between a pair of end points. To facilitate easy and more secure sales transactions over the Internet using an Intel IPT-equipped device, the NFC feature, when used with an IPT-NFC-enabled cloud payment wallet, lets users connect to a merchant site, pay for a product by tapping their NFC-enabled credit card against an NFC sensor in the device, and complete the transaction with positive identity confirmation by means of cryptographic binding with Intel IPT.

Embedded Tokens Secured within the PC

Intel IPT works in combination with established authentication mechanisms developed by leading security companies. A key difference of this technology, however, is that it replaces the customary USB or phone token with an embedded token. When a user with an IPT-enabled device visits a website that uses IPT, the first time the website asks them to opt-in to activate IPT to provide them with stronger 2nd factor authentication. If a user opts-in then the website generates a unique “seed”, keeps a copy of the seed on the website and stores another copy on the user’s device. When the user revisits that website in the future, the website asks the user’s device to provide a password for that user. Embedded IPT token on that device then uses the seed to generate a password for that user and send to the website. The website also generates a password using its own copy of the same seed. If the two match, the user is allowed to log-in.

Unlike the normal Username/Password, this password can be used only once and is valid for only 30 seconds. That’s why it is known as a dynamic One-Time Password (OTP). Even if malware steals this password, it cannot be used for log-in at a later time. OTPs can be 6-digits or even much longer to increase their security.

Websites can implement IPT OTP such that it is automatically exchanged between the website and the user’s device. This way the user does not have to run any OTP software on their device and cut-paste the password into the website. This makes IPT OTP more user friendly than hardware tokens or phone tokens, where the user has to take their phones and generate a password. IPT OTP is also substantially cheaper for websites to deploy because they do not have to pay to manufacture a hardware token and ship it to their users, or pay for each SMS message, which can add up to millions of dollars over large number of users.

IPT OTP meant to be used in conjunction with Username/Password as 2nd factor authentication. For users who use multiple devices, some of which may not have Intel IPT technology, they can continue to use any existing authentication mechanisms e.g., Username/Password-alone, or SMS OTP, to log-in as they do today. But on Intel IPT enabled devices, they can benefit from stronger yet seamless security. Protected Transaction Display can be combined with OTP to further enhance security and ease of use against malware.

Requirements for Using Intel® IPT

For customers, clients, or employees to use this security technology, the following conditions must be met:

- Users must be on any 3rd generation Intel Core processor based device. To see if your device supports Intel Identity Protection Technology, please visit http://iptprd.odce.intel.net/iptdoor3.html
- The website or network being accessed must be Intel IPT-enabled. Users must actively opt-in to their Intel IPT-enabled PC to the website and their accounts.

Visit the Intel Identity Protection Technology website, iipt.intel.com, for a complete list of models featuring this technology.

Figure 1. Security components associated with Intel® Identity Protection Technology (Intel® IPT).

---

4. No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd generation or higher gen Intel® Core™ processor enabled chipset, firmware, and software. Available only on participating websites. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit [http://ipt.intel.com](http://ipt.intel.com). Copyright © 2014 Intel Corporation. All rights reserved. Core Inside, Intel, the Intel logo, Intel Core, Intel vPro, and Ultrabook are trademarks of Intel Corporation in the U.S. and other countries.

* Other names and brands may be claimed as the property of others.