Intel Corporation
2200 Mission College Blvd.
P.O. Box 58119
Santa Clara, CA 95052-8119

Backgrounder

Intel Innovates Security Technology Across Computing Spectrum

Cyber attacks are increasingly prevalent today, posing a significant threat to people, businesses and government. Statistics compiled by security software leader, McAfee, tell a sobering story. In 2011, more than 55,000 new unique pieces of malicious software — called malware — were created every day, and more than 200,000 computers became zombie machines after falling victim to command-and-control networks. Also in 2011, an average of 2 million new malicious websites cropped up every month.

Intel Corporation recognizes the increasing challenge as mobility grows and the "Internet of Things" touches everything from devices to the cloud. Combining hardware and software expertise, visionary thinking, unrivaled product development, cutting-edge research facilities and a compelling industry engagement model, Intel is uniquely positioned to advance security technology and deliver solutions at the forefront of prevention, protection and recovery.

Security is an imperative today — and growing more so due to a handful of key trends:

- **Internet traffic is growing exponentially.** By 2015, 3 billion people are expected to connect to the Internet; up from 1 billion in 2011[1]. The "Internet of Things" is headed to 50 billion this decade[2], enabling smart computing experiences in communications, energy, industrial, medical, retail and transportation industries. From smartphones and TVs to cars and embedded retail systems, computing devices today are increasingly mobile, Web-enabled and connected. This trend has tremendous benefits, but carries risk as digital information travels faster and farther, reaching more people, devices and locations than ever before.

- **Rapid growth of cloud computing**. According to forecasts, consumers will store more than a third of their digital content in the cloud by 2016, compared to 2011 when that figure was estimated at 7 percent[3]. Delivering services, software and information via private and public networks, including the Internet, offers efficiency, agility and competitive advantages, but makes more personal and business information vulnerable to malicious electronic attacks, fraud, theft and other intrusions.

1 http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=324003
2 www.cisco.com/web/about/ac79/iot/index.html
3 Gartner, "Cloud adoption driving unexpected surge in IT, telecom spending," June 2012

- **More malware and cybercrime.** In 2011, there were 75 million unique pieces of malware reported[4] and they are becoming more sophisticated, trending toward stealthy forms with anti-detection and forensic capabilities. These security threats enter computers and electronic systems worldwide, including airport security systems, phones and cars.

- **Growth of social media.** As millions rush to use Facebook*, Twitter* and other social applications — and bring their smartphones and iPads* into the workplace to do so — social computing has become another potential access point for hackers.

Intel has stepped up its efforts to resolve security issues for consumers, IT organizations and government agencies. Intel focuses on innovation and leadership in five key areas:

Strengthening Security through Software and Hardware
As part of its holistic approach to security, Intel acquired security software company, McAfee, in 2011. Melding McAfee's deep knowledge of malware methodology with Intel's understanding of system architecture helps enable the companies to jointly innovate in the realm of secure computing. The first fruit of Intel and McAfee together is the McAfee DeepSAFE technology platform. Sitting below the operating system, it provides a direct view into system memory and processor activity. Intel® Cloud Single Sign-On, helps enterprise users manage access to popular Software-as-a-Service (SaaS) applications with improved security authentication.

Intel is committed to working closely with a full roster of companies in the global software security ecosystem, including Check Point*, Cisco*, Huawei*, Kaspersky*, Symantec* and Trend Micro*. Intel also has a long history of working with Microsoft to enhance the security of Intel-based platforms running Windows*. Most recently, this work has focused on improvements designed to secure the boot operation with the pending launch of Microsoft Windows* 8.

Building Security into Silicon
Intel has infused security into its silicon for decades, in efforts to combine software-based efforts with hardware-based technologies to help protect people and businesses against security breaches. The security technologies built into Intel architecture include:

- **Identity.** Intel® Identity Protection Technology (Intel® IPT) is two-factor authentication technology that makes it harder for attackers to steal a person's identity through online transactions.
- **Malware.** Intel® Trusted Execution Technology (Intel® TXT) protects IT infrastructures against software-based attacks.
- **Data and asset protection.** Intel® Anti-Theft Technology is now enabled on all 3rd generation Intel® Core™ processor-powered Ultrabook devices and Intel® VPro™- powered computers. Intel Anti-Theft Technology helps deter data and asset theft, keeping personal information personal. If a user's device is stolen, it can be disabled over the Internet automatically or the user can notify the service provider to disable the system.
- **Recovery.** Intel is developing hardware with verification procedures designed to get users back to work quickly after a system hack.

---

4 http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2011.pdf

Creating a Safe Online Commerce Experience for Merchants and Consumers
Working with global payment leaders such as MasterCard and Visa, Intel aims to enhance the security and consumer payment experience for consumers shopping online with Intel-powered Ultrabook devices and with their Intel-based smart phones. At Mobile World Congress 2012, Intel, along with Visa, focused on mobile payments and extending the company's ecosystem alliances to mobile commerce across tablets and smartphones. Intel also announced a mobile commerce-ready Intel Smartphone Reference Device that can support open, flexible delivery of NFC services.

In November 2011 Intel and MasterCard jointly announced a multi-year strategic collaboration to further enhance the security and consumer payment experience for online shopping. Intel showcased the results of its efforts at the Intel Developer Forum 2011.

Fostering Security in Research and Development
Intel Labs places heavy emphasis on security. Intel's Security Research Lab engages in proactive research in the fields of identity, malware, data protection and security in the cloud.

- **Identity.** Research focuses on creating a highly secure means of authentication that is "unspoofable." Current authentication options — from biometrics, such as fingerprinting, to hardware tokens that generate one-time passwords — are somewhat successful, but Intel Lab's vision is to provide multiple, seamless levels of protection that deliver true ease-of-use and ironclad security.

- **Malware.** Intel Labs is researching better methods of detection and prevention to help thwart a rapidly growing fraud ecosystem. Today, malware detection methods typically recognize known occurrences of "bad" software. The newest research focuses on detecting never-before-seen attacks, known as zero-day attacks. This malware exploits vulnerabilities that software vendors are not yet aware of.

- **Data protection.** Security attacks target popular platforms and devices which are attractive for data stored on them — a person's social security number, credit card information or the intellectual property of an employer. In an environment where one is free to browse, click and download at will, Intel Labs research not only focuses on malware protection, but data protection even in the presence of malware.

- **Security in the cloud.** Consumers are increasingly dependent on cloud security policies to protect their media (photos and videos) while being able to share it with friends and family. Intel Labs is looking at novel techniques to protect the user data once it's left their platform by providing advanced data use controls that enables consumers to preserve privacy while granting access to authorized parties.

Promoting Security through Policy
Intel recognizes every country wants to be secure, and strong collaboration is key to achieving it. To create an environment that fosters technology innovation and empowers individuals to protect their personal data, Intel works to inform policy stakeholders in the legislative, regulatory, academic and standards arenas. Intel pursues the following security policy strategies and efforts:

- **Identity.** Intel supports worldwide efforts to create identity systems, with the understanding that security and privacy must be considered intrinsically linked. One key goal is to make it easier for regulatory authorities to identify and punish malicious actors who access networks

or systems. Intel champions technology-neutral regulations allowing for innovative identity technology solutions.

- **Malware.** Concerns about the potential impact of malware on a country's critical infrastructure — such as power, transportation and telecommunications — often lead governments to regulate the equipment purchases and IT operations of organizations that deliver such services. Intel shares these concerns and works to inform governments of appropriate restrictions that will help ensure current, effective security technologies. Intel also supports efforts to create public-private partnerships that encourage industry and government to share information about malware and other threat data.
- **Data protection.** Intel supports legislative efforts aimed at security breach notification that informs individuals if their personal data is compromised. Intel is helping to define effective notification and inform policy decisions based on industry best practices and conventions for data protection and network security.
- **Recovery.** Intel works within the policy community to discuss recovery, acknowledging that security is not a problem the industry can solve 100 percent of the time. Thus, preparedness is imperative to a quick recovery. Regulations related to critical infrastructure should require organizations to build a recovery component into their technology plans and deployments.

In addition to collaborating with legislators, regulators and academic experts, Intel works to frame security policy through standards. Today's global digital infrastructure makes a strong case for policies, regulations and standards that apply globally and inspires Intel to work closely with international industry standards bodies, including the Trusted Computing Group (TCG), the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO).

-- 30 --