CHAPTER 8

Looking to the Future

Emerging Security Capabilities

> *Learn from yesterday, live for today, hope for tomorrow. The important thing is not to stop questioning.*
>
> —Albert Einstein

The Web has existed for two decades, yet it's only in the last few years that we've gained a clearer picture of what the Internet may become, and how the emerging capabilities may shape the future.

As early as 1993, companies like AOL started offering access to online newsgroups, soon followed by dial-up Internet access using early web browsers. As laptops became more affordable, many people started accessing the Internet while on the move. The rise of smartphones introduced built-in sensors, such as cameras, global positioning system receivers, and touch-sensitive screens, into consumers' everyday computing experiences. Businesses began using the information gathered from users' devices to offer personalized experiences, ranging from location-based driving directions to selected advertisements. The variety of Internet-connected devices rapidly expanded to include tablets, home DVRs, appliances, and cars. Devices also became smarter, with improved voice and gesture recognition.

We're now entering a world in which these elements will be combined to create much richer context-aware experiences for users and new opportunities for businesses. Our devices will know us, and they will know other devices. In fact, devices may almost become part of us: many companies are working on wearable computers, including technology embedded in clothing to diagnose sleeping problems and self-adjusting prosthetics to enable amputees to walk more naturally. To improve our fitness, smart garments may monitor our bodies' performance and send the information to a handheld device, on which a virtual trainer app will create "tailored workouts that know you better than you know yourself" (Etherington 2012).

Each day, billions of computing devices will perform functions on our behalf, often communicating among themselves to get the job done. Much more information will be collected from sensors such as cameras, microphones, and GPS receivers embedded into the user devices. This data will be combined with other information to create context-aware experiences that are far more personalized and compelling. Already, cameras and image recognition technology, combined with behind-the-scenes analytical software, can be used to identify a user's age bracket and gender, and tailor their experience accordingly. Early applications based on this technology are being piloted and in some cases deployed by large companies, including retailers (see sidebar).

Context-aware technologies are expected to create huge business opportunities affecting an estimated USD 96 billion of annual consumer spending worldwide by 2015, according to Gartner, Inc. (2011a). By that time, more than 15 percent of all payment card transactions will be validated using contextual information, the research firm estimates.

RICHER EXPERIENCES IN THE RETAIL ENVIRONMENT

As they seek to entice customers into stores, retailers are experimenting with technology that provides a glimpse into how future shopping experiences could be richer and more context-aware. Several of these solutions, developed in collaboration with Intel, are entering the pilot stage or already deployed (Intel 2012).

LEGO brand retail stores give shoppers the opportunity to star in a game as a LEGO Minifigure, in which an animated character mimics the player's movements. Featured at a branded store in Chicago, the interactive window display uses animation and gesture recognition software.

Adidas created a virtual footwear wall that addresses a common problem—when shoppers visit a store, they often can't find the exact shoe model or size they need. The virtual footwear wall demonstrates how retailers can give in-store shoppers access to much more detailed information about their expanded online inventory via a digital display. The display detects the shopper's age bracket and gender, and displays an appropriate selection of shoes. Using touch screens, shoppers can select products from a virtual shelf, view them from any angle, zoom in for more detail and technical information, see what others are saying on social networks, and ultimately purchase products directly from the wall.

Several other retailers are using technology that detects a user's approximate age and then uses the information to offer personalized services. Among them is Kraft Foods, which created a product sampling platform that dishes up complimentary samples of Temptations desserts—offered to adults only, of course.

These new technologies also introduce new risks, as I described in the discussion of emerging threats and vulnerabilities in Chapter 6. The sensors and other new capabilities embedded into millions of intelligent new devices can be exploited for malicious purposes. Malicious individuals might be able to remotely access home security surveillance systems to determine when you're not at home. Attackers might try to remotely control the brakes and other functions of an Internet-enabled car.

As security professionals, we may tend to focus obsessively on this darker side of the picture. Looking for threats and vulnerabilities is part of our role. We've seen that attackers find ways to exploit new technologies almost as soon as they appear. Analysis of emerging threats conducted by Intel's information risk and security group indicates that this trend will continue. As attackers adapt, we must adapt, too. In fact, our role will be more important than ever. As more aspects of people's daily lives are based on technology, it will become increasingly important to secure the technology. The Protect to Enable mission will expand accordingly.

The positive news is that new technologies can also be used to enhance security. As information risk becomes an even more high-profile concern, suppliers are building more security into their products and services. Devices will include a greater level of baseline security hardening to reduce the likelihood of compromise and minimize the impact.

Context-aware computing also introduces new privacy concerns. By definition, context-awareness involves taking advantage of information about the user to create personalized experiences. This makes it even more important to appropriately protect users' information and privacy. A clear organizational commitment to privacy will be important to ensure this protection. Intel, like a growing number of other organizations, has formally committed to compliance with a single set of privacy rules worldwide.

An organization's privacy commitment must also extend to applications and systems. Suppliers are becoming increasingly aware of this, and some are already taking additional steps to ensure user data is collected anonymously. The new baseline security capabilities built into products, such as hardware-enforced protection and accelerated encryption, may also help enhance privacy by protecting user data. In addition, the information provided by sensors can be used to create context-aware security. Today, some cars can automatically adjust seat, mirror, and pedal positions to suit different drivers. They adjust these settings when they detect the presence of the driver's personal car key. In the future, as cars become more intelligent and include more sensors, they might identify the driver using a camera and microphone. If they don't recognize the driver, they might disable the car and alert the owner via their built-in wireless Internet connection. Cars might include a maintenance mode that lets mechanics drive it while when it's being serviced, but only within a radius of a few miles. Similarly, as I'll discuss later in this chapter, the sensors in an enterprise-class device, such as a business laptop PC, could be used to prevent theft and help protect the information it contains.

From the perspective of the enterprise information security team, these emerging capabilities will allow increased trust in users and their devices. When we have a higher level of trust, we can provide the user with greater access to sensitive enterprise information and other resources.

The idea of dynamically evaluating trust is a key aspect of the new security architecture that we're implementing at Intel IT, as I discussed in Chapter 7. Employees may want to access our systems from a variety of devices and locations—including personal smartphones and tablets as well as business PCs. When a user requests access to enterprise systems, our architecture will dynamically calculate trust based on contextual information such as the user's identity, the security features of the device they're using, their physical location, and the resources they're trying to access. The architecture then will decide whether to grant access, and the level of access that should be allowed. As manufacturers increase the security capabilities in their devices, our model will be able to take this into account. We'll have increased trust in a device, and we'll be able to provide a correspondingly greater level of access.

In this chapter, I'll take a closer look at some of the emerging security capabilities that we can expect in products and services. First, though, I'd like to set the stage by examining some of the key underlying trends that make these security capabilities both necessary and possible.

Internet of Things

Many everyday objects are becoming more intelligent. They're acquiring processors, sensors, software, and the ability to communicate. This trend is made possible by Moore's law: processors and other hardware components continually become faster and less expensive, and, therefore, ubiquitous as a result. This accelerating trend is creating the Internet of Things—a massive expansion of the Internet as it swells to include billions of devices and household objects. Intelligent devices in cars, home electronics, and other "things" may far outnumber those in more conventional computing platforms and even those in mobile devices such as smartphones. Intel estimates that by 2015, more than 15 billion connected devices will be in use (Intel 2011).

Gartner, Inc. (2011b) identifies several key technologies and capabilities contributing to this trend, including sensors, image recognition, and wireless payments using *near field communications* (NFC) technology. Sensors that detect and communicate changes in their environment are being embedded not just in mobile devices, but in an increasing number of places and objects. Emerging applications will take advantage of this information. For example, camera-based image recognition technologies are expanding from mainly industrial applications to broad consumer and enterprise uses. These systems gather information about users and then analyze this information to personalize the user experience. Intel is working with a number of retail companies to build experiences that include image recognition (see sidebar). Wireless NFC, based on an emerging communications standard analogous to the Radio Frequency Identification (RFID) technology already established in some industries, lets users make payments by waving a mobile phone in front of a compatible reader.

With technologies such as NFC, the concept of the Internet may broaden to include an even wider variety of "dumb" objects, like drink cans or fertilizer bags (Gartner 2011b). This trend will provide opportunities for innovations that were not previously possible. Today, items in stores may include 2D bar codes that can be read by smartphones. In the future, store items may include NFC on the packaging or shelf label allowing them to wirelessly identify themselves to nearby devices, such as a shopper's smartphone. The shopper will then be able to learn not only about the product, but also alternatives, and could even view cross-selling and up-selling suggestions.

Devices such as the Nest Learning Thermostat may provide a glimpse of the future. This home heating controller is designed to be intuitive and simple to operate, replacing complex menus and instructions with a single big button and a dial (Nest Labs 2012). Users can remotely monitor and set the temperature from their smartphones, so they know the house will be warm by the time they get home. But perhaps the most interesting capability is that, as its name suggests, it can learn. The Nest monitors use of the heating system and attempts to learn the user's preferences—when the heating is switched on and off, and the desired temperature. After studying the use patterns for a while, the Nest begins to predict and autonomously set the temperature and timing itself.

I believe that devices like this are early examples of a much larger trend. As the Internet of Things grows, more interactions will occur directly between devices, rather than between people and device. Devices and objects will interpret and act on information provided by other objects. This will enable much more intuitive and streamlined experiences in many different fields. Consider the following scenario, described by Plantronics CTO Joe Burton (2012). A doctor visits a patient in a hospital room. A smart device the doctor is wearing turns on the doctor's workstation in the room, then authenticates the doctor to the patient management system, detects which patient is near the doctor, and pulls up the patient's record. When the doctor leaves the room, the information accumulated during the visit is saved and the workstation powers down.

Compute Continuum

Users now demand the same quality of experience in the workplace that they've become accustomed to in their personal lives. This includes the ability to access information across a continuum of devices, including PCs, smartphones, and tablets. They expect to be able to move from one device to another. They also expect intuitive applications on all of these devices, with the application's features tailored to the device's size and capabilities.

IT therefore needs to provide users with a consistent experience across devices and the ability to seamlessly transition between them. As enterprise information security professionals, we need to focus on the user experience and on enabling this broader range of devices while managing the risks.

Cloud Computing

The cloud is as much a new business model as it is a technology shift. The ability to obtain flexible IT services on demand lets businesses operate more dynamically—quickly taking advantage of business opportunities and growing or shrinking infrastructure capacity to meet demand. Cloud services can also potentially reduce cost.

However, cloud computing can also add new security complexities and data-protection concerns. Organizations may use multiple cloud providers, while also operating a private cloud for the most sensitive applications. Users need to be able to easily access services delivered from any of these multiple environments. From the enterprise perspective, we need to enable a seamless user experience while minimizing risk. This implies a federated model in which the user needs to log in only once; the user's credentials can then be used to access multiple applications. However, this also means that an attacker may only need to gain access once in order to compromise several environments.

Business Intelligence and Big Data

Businesses have quickly realized the value of analytical tools for real-time analysis of massive amounts of unstructured data. In the future, these analytic capabilities will increasingly be used to interpret data from sensors as well as from databases, social media, and other sources. The analysis of this information will then be used to create new personalized experiences, like the retail examples discussed in the sidebar "Richer Experiences in the Retail Environment."

This analysis can also be integrated with existing enterprise systems to create sophisticated customer-focused services. Here's a scenario described by Accenture (2012): a rental car company automatically detects when an accident with one of its cars has happened, initiates emergency services if needed, and issues a replacement rental car to meet the renter at the scene, greatly improving the chances of creating a loyal customer for life.

Business Benefits and Risks

By now, it should be apparent that the richer experiences enabled by these capabilities are as important to businesses as they are to users. New, context-aware experiences may attract customers and create new revenue. Furthermore, focusing on the user experience may be essential for business survival. If we don't provide rich and appealing user experiences, customers may gravitate toward competitors that do.

Our challenge is to manage the risks associated with these new experiences. The good news is that new security capabilities are emerging to help us do so.

New Security Capabilities

The IT ecosystem is increasingly focusing on building security into hardware, software, and services. We'll all be able to take advantage of this security to protect users and the enterprise. I think of these capabilities as the equivalent of termite-resistant building materials used in construction. They may not prevent termite attacks altogether, but they can stop some of them and minimize the impact of others.

Suppliers will need to frequently enhance these defenses to ensure they remain effective. As I noted in Irrefutable Law #6 in Chapter 1, security controls operate in a dynamic environment in which attackers are constantly learning and adapting their approach. Unless the defenses also adapt, they will lose their effectiveness over time.

I expect the ecosystem will increasingly view these security features as a way to differentiate products to meet the needs of distinct categories of customers. As a parallel, think about how the auto and other consumer industries developed. Initially, manufacturers focused on getting the public to buy cars en masse. Accordingly, the focus was on mass-producing just a few models at the lowest cost. As Henry Ford famously said, "Any customer can have a car painted any color that he wants so long as it is black" (Ford and Crowther 1922). Ford's mass-production strategy was enormously successful in popularizing cars among the American public. By 1918, half of all cars in the United States were Model Ts (The Henry Ford Museum 2003). But once consumers became more familiar with cars, they started demanding models that met specific needs. As manufacturers responded, the industry began to develop the huge variety of models that we see today.

In the same way, suppliers will offer a range of products or services with differing levels of security, including higher-security versions for the most sensitive enterprise uses and less-secure versions for consumers. This trend has already been evident for some time in products such as servers and PCs, and we're beginning to see it in cloud services.

In a closely connected trend, we'll see increasing use of contextual information to improve security. Some of this context will be provided by the sensors built into devices, such as cameras and GPS receivers. In addition, analytical and monitoring tools will be able to gather valuable contextual information from the environment. For example, they may examine databases containing information about users' access history and other relevant data.

Baseline Security

A greater level of baseline, hardware-enforced security features will be important in all categories of device, from smartphones to full-featured PCs. These capabilities will protect the information on the device itself, and the information that is accessed from the device. They'll enable greater trust in the device, and because of this trust we'll be able to provide users of the device with access to more resources, as I described in Chapter 7. The potential business benefits include increased user satisfaction and productivity.

I believe that these features will become particularly valuable as the Internet of Things takes shape. Many new, connected devices and objects won't be powerful enough to run traditional software security controls. Do I expect the computers that control my car or my home to run full intrusion prevention systems or antivirus suites? No. But I do believe that they should include protection that limits their functions to the desired purpose, reducing the risk that they could be successfully attacked and manipulated via wireless networks.

For enterprise security, these baseline hardware security capabilities will provide help in key focus areas, including threat management, ID and access management, data protection, and remote monitoring. Some expected baseline capabilities include protected environments, encryption, hardware acceleration, enhanced recovery, and integration with security software, as described next.

Protected Environments

Increasingly, hardware will provide protection for essential functions and data in the form of trusted layers and execution environments. I think of this approach as analogous, at the hardware level, to the way we're implementing network security zones within Intel's enterprise environment (as described in Chapter 7). The most valuable and critical functions receive the greatest protection, as well as increased monitoring and recovery capabilities.

Attackers have become increasingly adept at compromises using tools, such as rootkits, that operate at or below the operating system level—making them harder to detect and prevent by security applications. Implementing protection at the hardware level can help prevent compromise of firmware, operating systems, hypervisors, and other fundamental system components. Hardware-level protection can also help alert security professionals to attempted attacks and aid in system recovery.

Encryption

Many organizations already use disk encryption to protect data against loss or theft. But in a world where devices are always on and always connected, traditional software-based hard disk encryption is not sufficient. New capabilities will make encryption an even more pervasive technology used to protect information throughout its life—both when it is stored and when it is transmitted. Devices will include self-encrypting drives that maximize protection while minimizing the performance impact; encrypted input-output will help protect data during communications. Capabilities that currently exist in larger systems, such as total memory encryption, will become common in PCs and other end-user devices.

Hardware Acceleration

There's often a trade-off between security and performance. Controls, such as software-based encryption and malware scans, certainly help increase protection, but the performance impact can also increase frustration for users, to such an extent that some may avoid using the security features altogether. Accelerating functions in hardware can shift the balance in favor of security by decreasing the impact, both on users and on enterprise systems. For example, complex calculations required by standard encryption algorithms can be accelerated using hardware instructions rather than executed entirely in software.

Enhanced Recovery

As I've discussed in previous chapters, we must assume that compromise is inevitable, despite our best efforts to prevent it. As attacks become increasingly sophisticated, the ability to recover from compromises will become even more important. Future capabilities will help organizations recover from low-level attacks that target fundamental system components such as firmware or the BIOS. The system will be able to detect changes in these components, whether due to malicious attacks or accidental corruption. It will then be able to take steps to restore the components to a known good state, alerting users and the security team when necessary. Other anticipated recovery features include enhanced capabilities to revoke cryptographic keys to reduce the spread and impact of compromise.

Integration with Security Software and Other Applications

Existing security suites and other applications will continue to play valuable roles in detecting, preventing, and recovering from attacks. They will be able to provide an even greater level of protection when they are integrated with hardware-based security. This integration will enable software to more closely monitor the underlying hardware for attacks that might otherwise go undetected. For example, security software may use hardware features to detect symptoms, such as memory state changes, caused by specific types of attack. The software will then be able to take action to remove the threat.

Context-Aware Security

The theme of context awareness underlies many of the rich user experiences described in this chapter. Context awareness can also enhance security: the same sensors and analytical tools that help organizations create personalized experiences can also be used to mitigate risk.

In the home, TVs might be able to recognize when a child is watching, and show only appropriate channels. In supermarkets, cameras that are already used for physical security could help increase the efficiency of automated checkout stations. As I described, image recognition technology can determine a shopper's approximate age. By using this information, perhaps in conjunction with data from a scanned driver's license, the system could help avoid the need for cashiers to manually approve alcohol sales—leading to faster checkouts for consumers and reduced costs for stores.

The sensors in portable devices, such as mobile PCs and smartphones, may also be used to help protect against theft and unauthorized use. A simple case might utilize the device's camera, microphone, and GPS receiver to help authenticate you as the device's owner. If the user looks and sounds like you, and the PC is at your house, we have more confidence that the person using it is really the owner.

Additional technologies in portable devices, such as NFC, will allow more sophisticated examples of context-aware security. Devices will know when they're no longer in proximity of their owner, and may enter a protected state to prevent data loss. If your phone is near your laptop, we have greater confidence that you are the user trying to access the information on the laptop. When your phone moves away, the laptop deduces that you have moved away, too, and begins to armor itself by locking the screen. As you move progressively farther away, the laptop first goes into standby to save power, and then begins encrypting its contents for protection.

The GPS receiver in a portable device can also be used to geofence the device and the data it contains. If the receiver detects that a PC has moved outside a specific area, the device could alert the owner and the enterprise support team. The same capabilities could help protect data whose movement is restricted by specific geography-related requirements such as export controls. The device could detect when it's in a country subject to these controls, and encrypt the data it contains to protect it.

Cloud Security and Context Awareness

Cloud service providers recognize that many businesses have been reluctant to move critical data to external clouds due to security, regulatory, and privacy concerns. Suppliers have been working to add security capabilities designed to address these concerns. As they do so, we can expect more cloud services that are differentiated based on the level of trust they offer.

Suppliers might offer a "plain vanilla" cloud service for noncritical applications, along with a more expensive high-trust cloud service. Besides offering additional technical controls, secure clouds might include guarantees that the supplier will meet specific privacy and other data-protection regulatory requirements. This tiered strategy resembles the zoned approach to network security that we are implementing within Intel's private cloud as part of our new security architecture. Zones that host critical applications are protected by a variety of controls, ranging from network segmentation and hardened virtualization host servers to additional monitoring.

Within our private cloud, we are also moving toward using context awareness to improve security. I expect external clouds to adopt this approach as well, including the use of client-aware clouds in combination with cloud-aware clients.

A basic level of client awareness already exists in web-based services. Client browsers may warn you if you're being directed to a suspicious-looking site; web services recognize that you're using a smartphone.

In the future, client-aware cloud services will be able to tailor the access they provide based on the security capabilities of the client in order to mitigate risk. In our private cloud, a fully managed device that includes hardware-based enterprise security features and a full software security suite may get more access than an unsecured personal device. At the same time, a cloud-aware client will be able to validate that the cloud service it is accessing is genuine, and that it offers the required level of security.

As businesses use a growing number of cloud services, security requirements become more complex. A single enterprise may use multiple external cloud services while also operating a private cloud and a traditional computing environment. It will be important to streamline access for users. We can expect more emphasis on technology that eliminates the need for users to authenticate to each individual service.

Business Intelligence and Data Protection

Security context can be provided not only by sensors, but also by analyzing information about the enterprise environment and the threat landscape. As attackers become stealthier, this analysis will become an increasingly important part of an organization's defenses. Within Intel, we are moving toward the use of business intelligence tools to analyze patterns of network traffic and system use. I expect to see increasingly sophisticated external services that analyze a broad range of information in order to detect and prevent attacks.

As information is used on more devices outside the enterprise network perimeter, it will also be increasingly important to focus on controls that are integrated with the data itself. Many organizations, including Intel, are already protecting information with technologies such as enterprise rights management. In the future, these capabilities are likely to become more sophisticated and automated, allowing businesses to define policies that automatically store sensitive data in highly secured locations.

Conclusion: The Implications for CISOs

New technologies bring challenges, but they also bring opportunities for the CISO and for the organization overall.

The rich context-aware experiences that I've described in this chapter are entirely dependent on IT. To deliver these experiences, organizations will need to understand and manage the risks. As the experts in information risk, CISOs and other security professionals should have opportunities to become closely involved in the development and implementation of key business initiatives. This will result in a higher profile for the information risk and security team across the entire organization.

To fully take advantage of these opportunities, CISOs will need broad business and people skills as well as a thorough knowledge of security controls. I'll discuss these skills further in the next chapter.