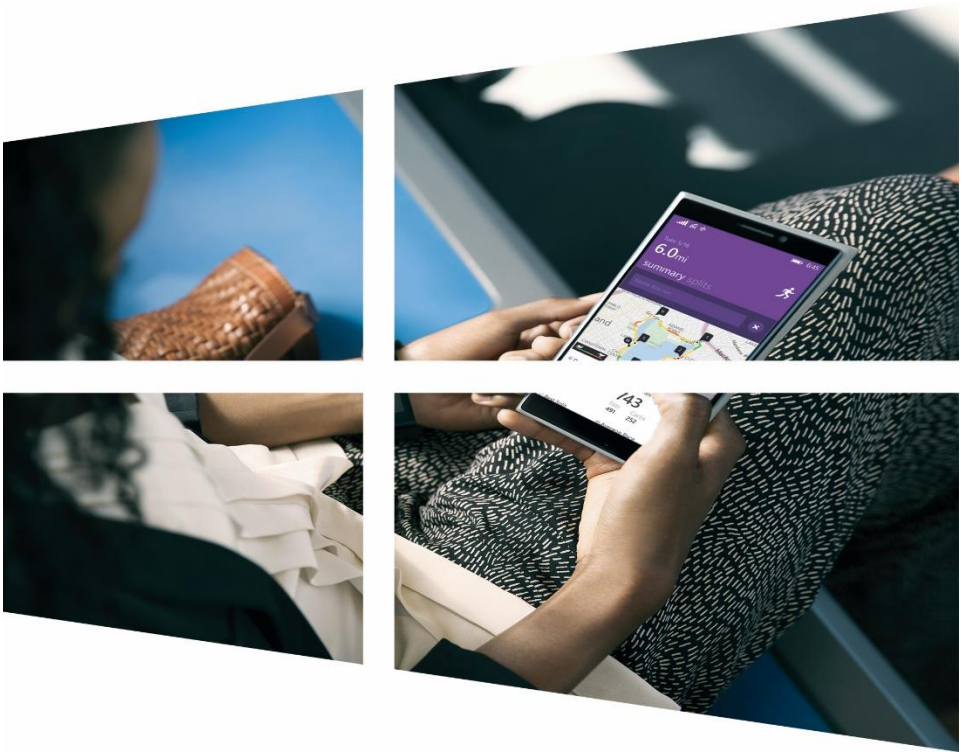
Windows 10



Windows 10 IoT Security

Published July 15, 2016
Version 2.0

Executive Summary

This whitepaper will discuss how the Windows 10 IoT product family – Windows 10 IoT Enterprise, Windows 10 IoT Mobile, and Windows 10 IoT Core – offers one platform designed for the security requirements of a range of device types. As the Internet of Things (IoT) continues to evolve, it becomes increasingly important to build devices on an IoT platform that correctly balances security needs, the user experience, and the resource constraints of diverse devices. Windows 10 IoT is that platform. Windows 10 IoT provides robust security capabilities through strong identities (both device identities and user identities), secured data, and secured connections. This paper will discuss key aspects of IoT security and how Windows 10 IoT empowers original equipment manufacturers (OEMs) to create secured devices that will delight customers.

Security in the modern era of IoT

Today we are witnessing a rapid digital transformation and the emergence of the Internet of Things (IoT). This digital transformation is bringing about a world of effectively infinite connections between actively communicating smart IoT devices. We are already seeing new possibilities emerge as our devices communicate with one another; in the next few years, we will continue to see a revolutionary integration of devices, from the smallest sensors to the largest industry platforms. And just as the early days of the internet brought network vulnerabilities (often appearing faster than security measures could be created to combat them), we will see a growing awareness of the security concerns surrounding the Internet of Things. Presently, the exponential proliferation of IoT devices and the optimism surrounding their integration can make it all too easy to overlook many real security hazards that this vast array of devices and device-types will present. However, focus on security will grow as IoT continues to mature.

IoT devices are at the edge of the network generating, consuming, and aggregating valuable data. These devices need robust security features to prevent their identities and data from becoming compromised. Today there exists no specific IoT security standards for device security. Without a framework in place to ensure devices are built from the ground-up for security, each new device added to an enterprise's technology ecosystem is effectively a new vulnerability. Securing and maximizing the Internet of Things is crucial and Windows 10 IoT is designed to be a cutting edge platform to securely fulfill the promise of IoT.

Securing and maximizing the Internet of Things is crucial and Windows 10 IoT is designed to be a cutting edge platform to securely fulfill the promise of IoT.

As tomorrow's devices are designed and marketed for mass adoption with the flattest learning curve, we will see progressively deeper device integration into sensitive facets of our business and personal lives. As a result, a tidal shift in security thinking is already underway. As data-

security and personal privacy concerns unfold in the public arena, well-designed security is increasingly being seen and marketed as a business imperative. We have already seen this process take root for enterprise systems; demands for tight controls are driving design of large-scale systems built with security in mind. As awareness of the role of various device types within IoT frameworks grows, we will see a similar shaping of the market around IoT devices offering the most robust security capabilities.

Traditionally, the implementation of security measures has created roadblocks in the user experience. Security has been seen less as a parallel track of design and more as an inconvenient requirement. Basic security measures must be accompanied by good security design that handles risks and threats without negatively impacting the user experience or device functionality. A leading IoT platform should go one step further by providing security without sacrificing a quality user experience.

Increased focus on the security of IoT devices will drive design and innovation, but it will be of equal importance that all the devices within a given business environment are enabled for the same security platform and are interoperable. We are still in the infancy of IoT, and universal security standards for IoT devices have yet to emerge. Devices built for disparate security platforms will tend to cause vulnerabilities, and devices lacking interoperability will suffer as standardization emerges. Device manufacturers who build around a platform offering both robust integrated security controls and support for an interconnected technology ecosystem will realize a competitive advantage.

A proper IoT platform must accommodate the business scenarios and resource constraints particular to various device types. Conscientious device manufacturers and businesses seeking to securely integrate smart devices will face resource constraints on many IoT components. Small, low-end devices (such as environmental sensors) must be lightweight and therefore lack the traditional power, memory, storage, and cryptographic capabilities available to traditional systems (PCs, phones, et al.). In light of the risks and the complexity of after-market security adaptations for small devices, end-users are certain to rely heavily on manufacturers who find a way to offer a full complement of out-of-the-box security capabilities (strong device identity, tamper resistance, remote attestation, encryption, etc.) in spite of these resource constraints.

An enterprise-grade platform must correctly balance various device resource constraints, security needs, and the user experience. Functionally, this means that an enterprise-grade secure platform will be one that provides and verifies secured identities, secured data, and secured connections. The Windows 10 security platform is engineered to address all three.

Windows 10 is designed to provide robust secured device identities, secured user identities, and secured connections.

Secured Identities

Proper IoT security requires strong, secured user identities and also strong security measures intrinsic to the devices themselves. Windows 10 offers innovative capabilities to secure both user identities and device identities.

Secured device identities

In most of the IoT world, connected devices communicate with each other constantly. Generally, user interaction is not required for ongoing communications. A device that has been granted ongoing access to communicate must remain secured after the initial credentialing handshake. Using security protocols and encrypted communication does not guarantee trust since these mechanisms have historically worked under the assumption that attackers do not have physical access to the device. Microsoft's perspective is that security implementations that are only external to IoT devices will not suffice; robust security must be intrinsic to these devices. Windows 10 only views a system as enterprise-grade secure provided that each device is inherently secured and resilient – protecting customer data, maintaining privacy, and limiting access to other systems even if breached. Further, advanced security controls within Windows 10 allow the user to differentiate device-identity protocols based on device-type – a low-level device (e.g., temperature sensors) can be identified with appropriate security protocols to accommodate its resource constraints and business scenarios, while more robust demands are applied to more sensitive, mission-critical devices. These comprehensive security capabilities ensure that all device identities are secured and verified, regardless of resource constraints.

Microsoft's perspective is that security implementations that are only external to IoT devices will not suffice; robust security must be intrinsic to these devices.

Secured User Identities

Windows 10 IoT's ability to monitor and verify the security of devices has opened new avenues for ensuring secured user identities. In the past, authentication efforts relied on users to provide identity information (passwords, pins, etc.) before secured data could be accessed. But these authentication models also implicitly rely upon the user to keep this identity information secret and use strong passwords, which they often do not, to help ensure communication channels are not compromised. Even when multiple pieces of information are required, this method is only as secure as its weakest point. Windows 10 IoT's device identity security methods allow the use of the device itself as one factor in a multi-factor authentication model (additional authentication factors can be added for credentialing devices for even firmer authentication, including physical proximity to, and interaction with, correlated secured devices). Coupled with a pin or biometric support (facial, iris, and fingerprint) a secured device (such as a phone or smart watch) provides the strongest authentication method yet, which will eventually surpass single-factor as the predominant user authentication method.

Secured Data

Data must be secured both at rest and in transit. The Windows 10 IoT security philosophy is built upon a layered approach; users must have confidence that their data is not vulnerable, even if the written volumes themselves are compromised through loss or theft. Windows 10 IoT protects users' data with Microsoft's industry-leading full disk encryption technology that encrypts the entire system volume and any partitioned data volumes on Windows 10 IoT devices.

Comprehensive encryption of data at-rest will protect written volumes from penetration. But total data security measures do not stop here. Windows 10 IoT's security platform is designed to ensure data security not just while at-rest, but also in-transit, as discussed below.

Secured Connections

Ensuring that communications between IoT devices are secured when sensitive information is exchanged is the third pillar in the Windows 10 IoT security platform. Windows 10 IoT is designed to natively support multiple encryption methodologies for communications between industry and mobile devices, and supports communications protocols for resource-constrained devices as well, helping to prevent vulnerabilities, regardless of the device types involved.

To better understand how Windows 10 IoT capabilities secure device identities, let's look at a few device scenarios at Contoso.

Contoso Scenario Stories

Using the power of the Windows 10 IoT, Contoso is now winning over its customers with a more enjoyable, safer way to conduct ATM transactions. Contoso has enhanced its mobile banking app by integrating it with customers' ATM experiences. The mobile banking app allows customers to conduct the majority of their ATM transactions from their own mobile phones before even approaching the ATM. Customers have full control over their mobile devices, allowing them to interact with their Contoso mobile banking app anytime - conveniently and privately.

Protecting Contoso's Customer Identities

Contoso understands that verifying customer identities via vulnerable usernames and passwords is generally not enough in today's security landscape. With this in mind, Contoso implements a multi-layered approach to help prevent unauthorized access to customers' accounts and identities. This approach includes employing **Multi-Factor Authentication**. Customers complete initial enrollment in the mobile banking app only after supplying a secondary form of identity verification, such as a one-time password sent to the customer via email or text. If the device has **Windows Hello** compatible hardware, then it can use biometric authentication – face, iris, or fingerprint – to verify identity in a way that traditional passwords cannot.

Once the customer submits a transaction, the app generates a two-dimensional barcode, which the customer scans at the ATM. No more glancing nervously while entering a PIN and

navigating menus or worrying that the ATM has been modified by identity thieves to steal pin and bank card information. Cash is dispensed and the whole transaction is completed quickly. Contoso's customers are delighted by the ease and enhanced security of the new ATMs. Customer loyalty increases because customers appreciate that Contoso has implemented advanced technologies designed to protect their identities and financial data from vulnerabilities.

Protecting the Communications between the ATM Kiosk Application and Contoso's Cloud Software

Contoso is equally delighted in knowing that Windows 10 IoT's layered approach to security and robust features has empowered the company to design its Internet of Things with strong security in mind. The application on the ATM device communicates with Contoso's backend cloud applications via state-of-the-art encryption and transmission security protocols, ensuring that fewer applications and less data resides locally on the device. Hosting software in the cloud is cost effective for Contoso because it eliminates many of the costs associated with managing and maintaining software on thousands of devices. The communication between the ATM's application and Contoso's cloud applications is protected by **Secure Remote Access**, a VPN function that works on an application-specific basis to establish a secured connection between the cloud and the ATM's installed application. Contoso further protects communications with **Network Access Protection**, which evaluates the system health state of any device connecting to or through its network and quarantines non-compliant devices. Contoso uses **Windows Firewall** to help actively block unwanted network communication.

With Windows 10 IoT, Contoso is always up-to-date with the latest **transport layer security (TLS) cryptographic protocol** to help ensure its data is encrypted and transported securely across a public network. For enterprise devices, Windows 10 offers the latest in **VPN technology**.

Protecting Contoso's ATM Kiosk Application

With Windows 10 IoT, Contoso has improved the security of its ATM kiosk application while also creating a consistent and predictable user experience. By their nature, the ATMs are still unattended devices. They are thus still susceptible to inadvertent or purposeful power-cycling. Comprehensive security for IoT devices means planning for all conceivable scenarios and minimizing downtime; Windows 10 IoT is designed from the ground-up to prevent unexpected reboots from compromising device and data security.

To deliver the proper user experience, Contoso must ensure that its ATM kiosk application launches directly into the desired application. To do so, Contoso uses **Shell Launcher**, which prevents intrusions by suppressing the start screen and launching straight into Contoso's proprietary ATM kiosk application. The same functionality exists for launching into Universal Windows Platform (UWP) apps by using **App Launcher** to suppress the start screen and launch straight into the app, and **Assigned Access** to implement policies that restrict the user from closing or switching out of the app using hotkeys, touch gestures, or other methods.

In the event that Contoso's ATM powers-off and restarts, **Unified Write Filer (UWF)** helps Contoso's ATM kiosk applications return to the same known state on a restart for a predictable and reliable user experience. UWF intercepts all writes to a protected volume and instead writes them to an overlay so they will not persist on a restart. To allow desired changes to persist, UWF provides an exception capability that allows IT administrators to specify files, folders, or registry keys to persist through the write filter. System Center Configuration Manager, which is part of the Microsoft System Center 2012 platform, is "write filter aware," meaning it has the ability to turn off the write filter on a device before any updates are downloaded, apply the updates, and then turn the write filter back on again. Windows 10 helps streamline the security features and management of these read-only devices and allows Contoso to achieve its desired user experience.

Contoso must protect its ATMs against untrusted applications or files. Windows 10 IoT is enabled with **AppLocker**, which allows Contoso granular administrative control over which apps and files can run (including executable files, scripts, Windows Installer files, dynamic-link libraries [DLLs], packaged apps, and packaged app installers). Additionally, **Device Guard** adds yet another layer of protection by creating a configuration state in which, even if the ATM were compromised, it would be incapable of running untrusted executable software (including zero-day exploits). Contoso is in control of what sources Device Guard considers trustworthy for its ATM kiosk and it comes with tools that make it easy to sign UWP or even Win32 apps that may not have been originally signed by the software vendor. Importantly, while AppLocker exists within Windows security administrative controls, Device Guard is enabled outside the operating system, creating overlapping defense against malware exploits.

Protecting the Physical ATM Device

Contoso must also protect its ATM from physical intrusions. This includes securing the unattended ATM by reducing vulnerability and risk of data loss posed by unapproved peripherals. Windows 10 IoT is enabled with **USB policy**, which helps secure devices from unapproved USB peripherals. Contoso's IT staff has the ability to authorize its desired USB devices, meaning the kiosk is protected against unapproved peripheral uses without inhibiting approved business uses.

In the event that the ATM were physically compromised, Contoso protects the device with **BitLocker**, Microsoft's full disk encryption technology that protects data by preventing unauthorized users from breaking Windows file and system protection on lost, stolen, or inappropriately decommissioned computers. Contoso can further protect the data on the ATM device by using **Mobile Device Management (MDM)** to set policies for different users - like a service technician or a branch manager with an in-branch ATM - that determine the users' abilities to change or update the device. MDM also allows Contoso to view logs to determine if changes have been made to the device, whether it is an appropriate change made by a technician or a change made by an intruder. If the device were stolen, Contoso's MDM policy

would initiate a system shut down and even total data wipe based on Contoso's pre-determined trigger criteria.

Contoso's IoT ecosystem does not stop there - Contoso saw an opportunity to capitalize on the versatility and power of Windows 10 IoT, adding an array of small environmental sensors to monitor conditions in and around each ATM. These devices gather data on factors like temperature and lighting, and report specifics of machine health back to the bank. Scanners and proximity sensors analyze the number of passersby and their responsiveness to a range of advertising options. All of these small devices communicate their data to a gateway device, which is then responsible for relaying to the bank's cloud market analysis application.

To ignite this sensor ecosystem, advanced security controls within Windows 10 allow Contoso to differentiate device-identity protocols based on device-type – a low-level device (e.g., temperature sensors) can be identified with appropriate security protocols to accommodate its resource constraints and business scenarios, while more robust demands are applied to more sensitive, mission-critical devices. Even the smallest of devices running Windows 10 IoT can provide support for industry standard **Trusted Platform Module (TPM)**.[1] Discrete or firmware based TPM implementations provide the foundation for strong, hardware-bound cryptographic identities for authentication, secured key storage and policy based key usage, as well as platform integrity and health attestation through use of tamperproof platform measurements. These security capabilities help ensure that all device identities are secured and verified, regardless of resource constraints.

Contoso's system is secured because each device is inherently secured and resilient – protecting customer data, maintaining privacy, and limiting access to other systems. Customers are pleased. Contoso is equally delighted in knowing that Windows 10 IoT's layered approach to security and robust features has empowered the company to design its Internet of Things with strong security.

Conclusion

As IoT continues to evolve, it becomes increasingly important to build devices on an IoT platform that correctly balances security needs, the user experience, and the resource constraints of diverse devices. With this in mind, Windows 10 IoT offers one platform designed for the security requirements of diverse device types – from small, low-cost devices to sophisticated industry machines. Windows 10 IoT brings enterprise-grade security to protect your user and device identities, data, and connections. Windows 10 IoT empowers you to build your internet of things today with advanced security technologies, and build on a platform that is always innovating to meet tomorrow's demands.

[1] Windows 10 requires TPM 2.0 or higher.