VERACODE
The Most Powerful Application Security Platform on the Planet

WHITE PAPER

The Internet of Things: Security Research Study

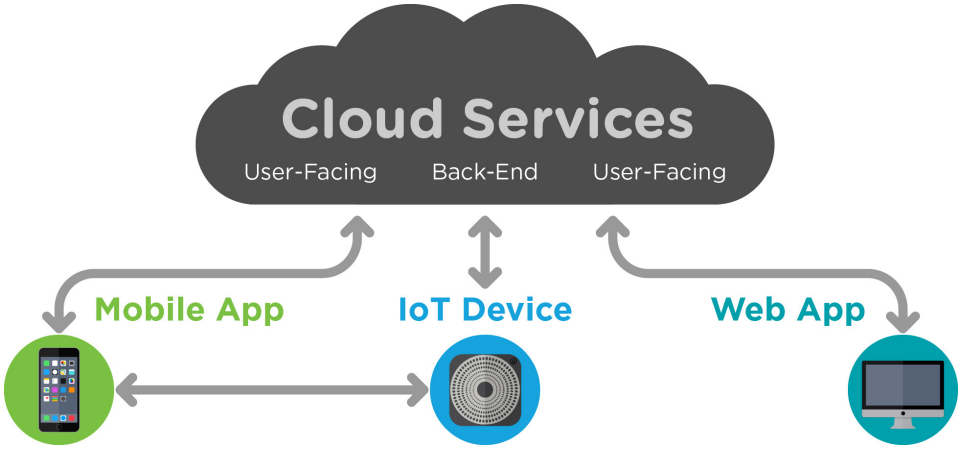
Introduction

As the Internet of Things (IoT) continues to gain traction and more connected devices come to market, security becomes a major concern. Businesses are increasingly being breached by attackers via vulnerable web-facing assets[1]; what is there to keep the same from happening to consumers? The short answer is nothing. Already, broad-reaching hacks of connected devices have been recorded[2] and will continue to happen if manufacturers do not bolster their security efforts now. In this light, Veracode's research team examined six Internet-connected consumer devices and found unsettling results.

We investigated a selection of always-on consumer IoT devices to understand the security posture of each product. The result: product manufacturers weren't focused enough on security and privacy, as a design priority, putting consumers at risk for an attack or physical intrusion.

Our team performed a set of uniform tests across all devices and organized the findings into four different domains: user-facing cloud services, back-end cloud services, mobile application interface, and device debugging interfaces. The results showed that all but one device exhibited vulnerabilities across most categories. It's clear there is a need to perform security reviews of device architecture and accompanying applications to minimize the risk to users.

Further, the study presents results of a threat modeling exercise, discussing the potential impact to users under a number of hypothetical breach scenarios. For example, since the Ubi fails to secure its communications, if attackers were to gain access to eavesdrop on the traffic of Ubi's cloud service – for instance, through a network breach – they would be able to see the full contents of every Ubi user's voice commands and responses, giving the attackers a clear view into the usage patterns of people interacting with devices in their homes and offices.



The security of the Internet of Things (IoT) involves web and mobile applications — and supporting cloud services — as well as the devices themselves.

Device Overview

Selection Criteria

Many categories of devices and services lie under the IoT umbrella. Instead of casting a wide net, we chose to focus on devices that had the following characteristics:

- **Customer oriented:** The device is marketed and sold to end users who don't require special technical expertise to use it.
- **Always on:** The device is designed to remain on and connected to the Internet permanently.
- **Potential for real-world impact:** The device contains the capability to significantly interact with the physical environment around it, either built-in (e.g., hardware sensors) or through communication with other devices.

The Devices

Chamberlain MyQ Garage (Chamberlain Group Inc.)

The MyQ Garage enables Internet-based remote control of a garage door. It cannot physically move garage doors; instead, it pairs wirelessly with existing door openers from many manufacturers. It acts as a hub that remains connected to a Wi-Fi network and sends RF commands to open or close a garage door, just as the door's wireless remotes would.

The system contains two devices – the hub itself (model MYQ-G0201) and a door sensor that can detect motion and orientation of a garage door (model 041D7924).

The product is primarily marketed towards smartphone users, though it is accessible from any device through a web interface.

Chamberlain MyQ Internet Gateway (Chamberlain Group Inc.)

The MyQ Internet Gateway (model CIGBU) enables Internet-based remote control of garage doors, interior switches, and electrical outlets. Compared to the MyQ Garage, MyQ Internet Gateway can pair with a relatively limited set of door openers (those that speak the MyQ protocol).

The Internet Gateway also allows for remote control of electrical lights and appliances when used with the external modules PILCEV/PILCEVC (Remote Lamp Control), which switches an individual electrical mains outlet; or the WSLCEV/WSLCEVC (Remote Light Switch), which is designed as an interior wall switch.

Like the MyQ Garage, the MyQ Internet Gateway is designed to be used primarily from smartphones, providing applications for both Android and iOS; however, it is accessible from any device with a web browser.

SmartThings Hub (SmartThings, Inc.)

The SmartThings Hub is a central control device for a variety of home automation sensors (and other tools, such as switches and door locks). It remains in constant contact with the SmartThings cloud services and has the capability to communicate with sensors using Z-Wave, ZigBee, and IP-based standards.

The SmartThings hub has no UI of its own; it can be controlled using a mobile application or through the web portal.

Ubi (Unified Computer Intelligence Corporation)

The Ubi is an always-on, voice-controlled device that acts as a tool for answering questions, performing tasks, and controlling home automation devices. It can send emails and SMS messages; play music from a third-party service provider; and access data from home automation APIs (such as those provided by SmartThings and Nest).

Voice commands to the Ubi start with the wake-up phrase "OK Ubi", followed by a request or question. In addition to a microphone, the Ubi also has onboard sensors to determine the ambient air pressure, temperature, light level, and humidity. This data, along with the current ambient sound level, is sent to the Ubi service periodically.

Though the Ubi is primarily a voice-operated device, it can also be configured and used through a mobile application and a web portal.

Wink Hub (Wink Inc.)

The Wink Hub (model PWHUB-WH01) is a central control device for a variety of home automation products. Like the SmartThings Hub, it remains connected with supporting cloud services and can communicate with sensor products using numerous other protocols.

The Wink Hub has no UI of its own; its control interface is the Wink mobile application.

Wink Relay (Wink, Inc.)

The Wink Relay (model PRLAY-WH01) is a combination hub and control device for home automation sensors and products. It combines much of the hub functionality of the Wink Hub with a built-in touchscreen device (running the Wink mobile application) and programmable switches.

The Wink Relay may be used in combination with the Wink Hub; the latter supports a greater range of protocols for communicating with products.

Methodology

In all cases, we installed and configured the devices as directed by the documentation. We used testing environments that were configured to allow us to monitor and capture all communications between the devices and their surroundings, as well as perform tests for the vulnerability to interception (man-in-the-middle) and other techniques against the devices. Each device was tested separately.

We also used reverse-engineering techniques to investigate the security of the communication between the mobile applications and the devices, where applicable.

Though we captured all traffic sent from the devices where possible, our objective was not to gain unauthorized access to the cloud services themselves, and we did not run any active tests against user-facing web applications or back-end cloud services associated with the devices and their mobile applications. Rather, we monitored traffic to and from these services to assess the security of the devices themselves.

The devices were purchased new in late December, 2014. All test findings were against versions of the firmware that were up-to-date in mid-to-late January, 2015.

Findings

We performed a set of uniform tests across all devices, looking at vulnerabilities across four domains that would enable access to the devices and their client mobile applications.

Authentication and Communication with User-Facing Cloud Services

This domain covers authentication and communication with cloud services that are directly accessible by users, whether they be through a web browser, custom embedded device, or mobile application.

1. Cryptography Allowed
Test: Does the service allow users to protect communication in transit with strong cryptography (e.g., TLS/SSL)?

Impact: Allowing encrypted communication protects data in transit, including authentication credentials. The lack of such a scheme allows attackers with network access to passively capture such data.

2. Cryptography Required
Test: Does the service require users to use cryptography to protect communication in transit?

Impact: Mandating that all access to a service be conducted using strong cryptography reduces the chance of a data leak through user error or architectural weaknesses (such as those that enable HTTPS-stripping attacks).

3. Strong Passwords Enforced
Test: If the service allows users to create passwords, does it require that users follow password-strength guidelines?

Impact: Enforcing the use of strong (i.e. complex) passwords increases the cost to attackers employing brute-force and dictionary attacks against live services. Additionally, in the event of a service breach leading to theft of a hashed-password database, it can increase the effort required to successfully crack passwords.

4. TLS Certificate Validation
Test: If official mobile applications are designed to work with the service, do those applications follow best practices and properly validate the server's TLS certificate?

Impact: The improper validation of certificates allows attackers with the capability to perform a man-in-the-middle attack, which could give them access to all data sent between the application and the service.

Test	Wink Hub	Wink Relay	Ubi	SmartThings Hub	MyQ Garage	MyQ Gateway
Cryptography Allowed	YES	YES	YES	YES	YES	YES
Cryptography Required	YES	YES	NO	YES	YES	YES
Strong Passwords	NO	NO	NO	YES	NO	NO
App SSL Validation	YES	YES	YES	YES	YES	YES

Authentication and Communication with Back-End Cloud Services

This domain covers authentication and communication with cloud services that are accessed directly by the devices themselves.

1. Device-to-Service Authentication
Test: Does the device use a strong authentication mechanism to identify itself to the service?

Impact: If the device fails to uniquely authenticate itself (e.g., through the use of credentials or a unique identifier) during each communication session, it could be vulnerable to impersonation from an attacker pretending to be the device to the service.

2. Encryption Employed
Test: Does the device use encryption in all of its communication with control service(s)?

Impact: If the device fails to encrypt communications with its control services, an attacker with the ability to passively monitor the traffic would gain access to all sensitive data sent by the device as well as any authentication credentials or session tokens.

3. Protection Against Man-In-The-Middle Attacks
Test: Is there sufficient protection against man-in-the-middle attacks from an attacker who has not gained physical access to the device itself?

Impact: Without adequate protection against man-in-the-middle attacks, an attacker with the ability to intercept and forward traffic between the device and its service could receive and modify traffic sent in both directions.

Such protection can be achieved through the use of authenticated encryption (e.g., TLS with proper certificate validation).

4. Sensitive Data Protected
Test: Is all sensitive data sent to or from the device encrypted?

Impact: Without adequate protection against passive observers, sensitive data can be

monitored by attackers with the capability to observe network traffic.

This attack can be avoided with the use of encryption or the absence of messages that include sensitive data.

5. Protection Against Replay Attacks
Test: Does the device have adequate protection against replay attacks from a passive observer?

Impact: If the design of the protocol does not contain sufficient protection against this attack, an attacker with the ability to capture traffic is able to reuse a previously-captured message to perform an unauthorized action against the device or service.

Test	Wink Hub	Wink Relay	Ubi	SmartThings Hub	MyQ Garage	MyQ Gateway
Device-to-Service Authentication	YES	YES	YES	YES	YES	YES
Encryption Employed	YES	YES	NO	YES	NO	YES
Protection Against MITM	NO	NO [1]	NO [1]	YES	NO	NO
Sensitive Data Protected	YES	YES	NO	YES	N/A	YES
Replay Attack Protection	YES	YES	NO	YES	NO	NO

[1] Proper TLS certificate validation was used in the device's update mechanism, but not used in other normal device communication.

Mobile Application Interface

This domain covers direct communication between mobile applications and a device (e.g., over Wi-Fi or Bluetooth). This does not cover indirect communications, such as those through a back-end service.

1. Sensitive Data Secured
Test: Is all sensitive data sent between the device and mobile applications encrypted?

Impact: Without adequate protection, sensitive data can be monitored by attackers with the capability to observe local network traffic.

This attack can be avoided with the use of encryption or the absence of messages that include sensitive data.

2. TLS Certificate Validation
Test: If mobile applications employ TLS/SSL, do those applications follow best practices and properly validate the device's TLS certificate (e.g., through certificate pinning)?

Impact: The improper validation of certificates allows attackers with the capability to perform a man-in-the-middle attack, which could give them access to all data sent between the application and the service.

Test	Wink Hub	Wink Relay	Ubi	SmartThings Hub	MyQ Garage	MyQ Gateway
Sensitive Data Secured	NO [1]	N/A	NO [1]	YES	NO [1]	N/A
TLS Validation	N/A	N/A	N/A	N/A	N/A	N/A

[1] The information in question (Wi-Fi network passwords) was sent using short-range Bluetooth communication or unencrypted Wi-Fi directly to the device, and only during initial setup.

N/A: There is no direct communication between a mobile application and the device (this does not cover indirect communication via a back-end cloud service).

Device Debugging Interfaces

This domain covers services or interfaces that are running on the device, but not intended to be used by end-users. This is a broad category – it can cover anything from on-chip debugging ports (e.g., JTAG testing and ISP ports) to extra service code running on the device itself and accessible to network users.

We chose to only report on interfaces that are accessible over the network – either the local network (which may be potentially exposed due to misconfiguration) or the Internet at large. We believe this more accurately reflects most users' security concerns and expectations than focusing on attacks that require physical access to the device.

1. Debugging Interfaces Restricted
Test: Are all debugging or informational interfaces running on the device restricted to users with physical access to the device?

Impact: While "hidden" services running on the device may be invaluable during the development, testing, and manufacturing processes, they are often vectors for information leakage and authentication bypass. These should be properly restricted to avoid abuse by attackers. Debugging services can leak sensitive information, provide privileged access to attackers or allow for remote code execution.

2. Debugging Interfaces Secured
Test: Are all open interfaces protected against unauthorized access (e.g., with a password or physical process to enable the service), or is it possible for an attacker to bypass the device's normal authentication process?

Impact: While some services may be relatively innocuous – storing relatively public information, such as the name of the currently-connected Wi-Fi network or the time since device boot – others may allow users an alternate interface to device functionality.

3. Arbitrary Code Restricted
Test: Are all open interfaces designed to prevent an attacker who gains access from running arbitrary code on the device?

Impact: If a debugging service allows its users to execute arbitrary code, either through a vulnerability or by design, an attacker with access to the service may be able to install a remote access tool or access hardware peripherals (e.g., a microphone or speaker) without the legitimate users' knowledge, and more.

Test	Wink Hub	Wink Relay	Ubi	SmartThings Hub	MyQ Garage	MyQ Gateway
Debugging Interfaces Restricted	NO (http)	NO [1] (ADB)	NO (ADB, VNC)	NO (telnet)	NO (http)	YES
Debugging Interfaces Secured	YES	NO	NO	YES	YES	YES
Arbitrary Code Restricted	YES	PARTIAL [2]	NO	YES	YES	YES

[1] ADB has been disabled on the Wink Relay's most recent firmware update. Firmware does not auto-update, though the user is prompted to initiate a software update. Some users will do this and others will not.

[2] ADB was not running with root privileges on the Wink Relay, and we did not execute arbitrary code. However, we were still able to execute the available tools already on the device to record and exfiltrate audio recordings. We believe that given sufficient time it might be possible to leverage other Android weaknesses to achieve arbitrary code execution.

Here are the details on the network services found. All of these are accessible from the network local to the device in question.

- The Wink Hub runs an unauthenticated HTTP service on port 80; this is used during setup to configure wireless network settings.
- The Wink Relay runs an ADB (Android Debug Bridge) service.
- The Ubi runs an ADB service and a VNC service (providing access to the Android UI) with no password. Accessing shell via adb provides root access to the device.
- The SmartThings Hub runs a telnet server, but it is password-protected.
- The MyQ Garage runs an HTTP server with basic connectivity information.

Discussion: Hypothetical Cloud Service Data Risk

While the tables in the above findings provide a clear way to assess some fundamental aspects of a device's security at a glance, it became clear to us that the systems around which these devices were built depended heavily on their accompanying cloud services. For many of the devices above, basic functionality can be disabled entirely by disrupting connectivity to the device's back-end cloud service. Similarly, virtually all commands from mobile applications we surveyed are relayed through cloud services instead of being sent directly to the devices.

Reliance on these cloud services is worth discussing, because it means that users of these devices can be exposed to risks in the event that a breach of these services occurs. We chose to take a closer look at the potential impact on users if the following distinct **hypothetical** scenarios were to occur:

1. Account Compromise
In this scenario, a user's account on a user-facing cloud service (mobile application, web portal, etc.) is compromised without his or her knowledge, through a number of means such as malware on a user's device.

2. Network Breach
In this scenario, the network perimeter of a service (or one of its upstream providers) is breached, allowing an attacker to passively monitor all traffic to or from the services.

3. Full Service Breach
In this scenario, all user-facing and back-end services are breached, allowing attackers with access to send commands and view all historical data that has been sent to the service.

MyQ Garage

1. Account Compromise
Access to a user's account would provide an attacker with the ability to view the current state of the garage door: open, closed, or in motion. It would also allow the attacker to open or close the door and add rules to notify an email address or mobile application (via a push message) when the door is open or closed.

If the user has set up previous notification rules, past alerts would be visible as well, allowing an attacker to get historical data on garage-door usage. This could aid in building a profile of users' habits.

2. Network Breach
The MyQ Garage uses unencrypted UDP for communication. An attacker with access to the service's network traffic can gain information about the state of the doors belonging to all MyQ Garage users as well as corresponding IP addresses.

Since the packet format is predictable and unencrypted, an attacker could also use the ID from captured packets to spoof traffic from the server to MyQ Garage devices, causing doors to open or close.

3. Full Service Breach
A breach of the MyQ Garage's services would allow for all of the above, plus the ability to modify and view history for every user of the MyQ Garage.

MyQ Internet Gateway

1. Account Compromise
Access to a user's account would provide an attacker with the ability to view the current state of the paired companion products (e.g., whether a MyQ-enabled garage door is open or closed; or whether a MyQ light switch is turned off or on). It would also allow the attacker to modify the state of the user's products and add rules to notify an email address or mobile application (via a push message) when the state of a product has changed.

2. Network Breach
An attacker with access to the service's network traffic can gain information about the activity of the users. Though the content of the messages is encrypted, the MyQ Internet Gateway is vulnerable to replay attacks in certain circumstances. An attacker could replay captured packets from the back-end service to the device. For example, an attacker could replay the server command that instructs the Internet Gateway to turn on a light switch.

3. Full Service Breach
A breach of the MyQ Internet Gateway's services would allow the attacker to have full access to the states of the paired products for all users of the Internet Gateway, as well as the ability to modify them (e.g., open a door or turn off a switch).

SmartThings Hub

1. Account Compromise
Access to a user's account would provide an attacker with the ability to view and manipulate all of the products and services paired with the Hub. This may include light/power switches, door sensors, and more.

2. Network Breach
Since the SmartThings Hub uses strongly-encrypted communications for its traffic, a passive observer would gain no detailed information about the state of any paired devices.

3. Full Service Breach
A breach of the SmartThings Hub's services would provide an attacker with the ability to view and manipulate the state of all products and services paired with every SmartThings Hub user.

Ubi

1. Account Compromise
A compromise of an Ubi user's portal account would allow the attacker access to the history of voice commands and their responses, as these are logged and visible in the Ubi portal. Additionally, the user's contact database (email/SMS info) would be accessible. Commands may be sent to the user's Ubi, as this functionality is available in the mobile application.

The Ubi portal provides historical data from its sensors: temperature, humidity, air pressure, ambient light and sound levels. These would also be accessible to an attacker.

2. Network Breach
The traffic between the Ubi and its back-end services is entirely unencrypted HTTP. An attacker with the ability to observe all traffic to this service would see the flow of sensor data coming from every Ubi device as well as the text of virtually all voice commands and responses.

3. Full Service Breach
A full breach of the Ubi services would result in all of the above, applicable to all Ubi users. Additionally, an attacker would be able to modify state and history for Ubi users.

Wink Hub

1. Account Compromise
Compromise of a Wink Hub user's account would provide an attacker with the ability to view and manipulate all of the products and services paired with the Hub. This may include light/power switches, door sensors, and more.

2. Network Breach
Traffic to both the user-facing and back-end services is encrypted. Though connections between the Hub and its back-end services are vulnerable to a man-in-the-middle attack due to lack of TLS certificate validation, a purely passive observer would get no detailed information about any Hub or its paired devices.

3. Full Service Breach
A breach of the Wink services would provide an attacker with the ability to view and manipulate the state of all products and services paired with every Wink Hub or Relay user.

Wink Relay

1. Account Compromise
Compromise of a Wink Relay user's account would provide an attacker with the ability to view and manipulate all of the products and services paired with the Relay or any Hubs. This may include light/power switches, door sensors, and more.

2. Network Breach
Traffic to both the user-facing and back-end services is encrypted. Though connections between the Hub and its back-end services are vulnerable to a man-in-the-middle attack due to lack of TLS certificate validation, a purely passive observer would get no detailed information about any Relay or its paired devices.

3. Full Service Breach
A breach of the Wink services would provide an attacker with the ability to view and manipulate the state of all products and services paired with every Wink Relay or Hub user.

Acknowledgements

Jared Carlson, Senior Security Researcher
Brandon Creighton, Security Research Architect (Lead Researcher)
Darren Meyer, Senior Security Researcher
Jason Montgomery, Senior Security Researcher
Andrew Reiter, Senior Security Researcher

End Notes

1. Verizon Data Breach Incident Report, 2014, p. 14.
2. "Russian webcam hackers spy on bedrooms and offices", http://www.cnbc.com/id/102202954