WAVESTONE

THE INTERNET OF THINGS

THE 4 SECURITY DIMENSIONS OF SMART DEVICES

Like all major technological revolutions, digital transformation is spreading over many areas: home automation, physical security, mobility, healthcare, etc.

The Internet of Things (IoT) plays an important role in this trend, through the emergence of numerous connected devices. The figures are indeed tremendous: many analysts consider there will be between 20 and 200 billion connected devices in the world by 2020.

AUTHOR

CHADI HANTOUCHE
chadi.hantouche@wavestone.hk

AT THE HEART OF DIGITAL TRANSFORMATION

No industry can ignore this trend today, and enterprises are seizing the opportunity. While new companies designing smart devices appear every day, partnerships are emerging between vendors and traditional industries – like insurance, automotive, utilities or banking – in order to offer additional services to customers through various connected items.

A BROADER ATTACK SURFACE FOR CYBERCRIMINALS

Concurrently with the growing number of devices, security has regrettably not always been taken into account.

One of the most striking studies is the one led by HP Fortify[1]: while testing the top 10 IoT devices being used today, they found an average of 25 vulnerabilities per device. Most of them are related to common security issues: **data protection**, **insufficient authorisation**, **no encryption**, **insecure web interface**, **overall inadequate protection**, etc.

That lack of hardening increases vulnerabilities disclosures affecting all kinds of devices: fridges, cars, light bulbs, baby monitors, and even toys. Risks, which were limited to the cyberspace, are becoming more and more physical.

FROM SCIENCE-FICTION TO REALITY

En 2013, a remote attack on a politician’s pacemaker was depicted in the hit series “Homeland”. The same year, former U.S. vice president Dick Cheney declared that the wireless capabilities of his own heartbeat regulation device were disabled by doctors, in order to prevent any tempering attempt.

In July 2015, two hackers demonstrated a complete remote control of a Jeep Cherokee SUV, including the ability to kill the engine, engage or disable the brakes, or track the car’s GPS position. This case led Fiat-Chrysler to recall more than a million vehicles, several regulators to start in-depth investigations, and American senators to plan the introduction of an automotive security bill.

CARA: IN WHICH RISK SETTING ARE YOU?

As far as companies are concerned, the risks depend on the setting. These settings can be gathered under the acronym “**CARA**”, as shown in the table below. Companies can either **Create**, **Acquire**, **Recommend** or **Accommodate** connected devices, and the associated risks are specific to each case. Once the setting is identified, the risks and mitigation measures can be specified.

AN EFFECTIVE ASSESSMENT TOOL: THE HEAT MAP

In order to assess the risk, the Wavestone methodology consists of using a heat map that classifies risks depending on their seriousness, but also on the setting.

The next page shows a heat map example in a banking setting that covers a diverse range of services. In this context, triggering money transactions is obviously more risky than just checking an account balance. But customising the security features on a device employees or customers come up with can be much more difficult than hardening a product you chose, acquired from a provider, or even designed from scratch.

This heat map will eventually allow a pinpointing of the risks that require greater attention.

The Wavestone CARA method provides guidances for each setting

	Scope	Generic risks	Major Security Guidance
CREATE	Companies that manufacture connected devices must take security into account from the design phase, since they have a responsibility towards their customers	Discovering security flaws in connected devices could endanger users or their data, and therefore the reputation and liability of the manufacturer	Integrate security in the early design phases, ensure in particular security update capabilities throughout the (possibly long) device lifecycle
ACQUIRE	Companies that buy connected devices and deploy them internally share responsibilities on technologies choices and integration phases	Integration of these new technologies within the business process without proper security, which could increase the IT systems’ attack surface	Ensure that device identities are properly managed Request custom hardening from the manufacturers
RECOMMEND	Companies that recommend connected devices to their customers have a diffused responsibility that extends over time regarding the customers	Leakage of (possibly personal) data or physical damages that could lead to a company liability, or reputation damage	Clearly define liabilities (and data ownership) Ensure regulatory compliance Ensure the recommended devices have a proper security level
ACCOMMODATE	Companies that allow the use of employees’ connected devices (as a BYOD service), have to protect professional data	Loss or theft of corporate data to which connected devices have access, or intrusion facilitation	Make users aware of their responsibilities Enforce a user charter Build on previous BYOD projects

USUAL SECURITY FEATURES, NEW WAYS OF IMPLEMENTATION

Once the setting and the use cases are clear, security questions have to be addressed. In this regard, one relevant reference is the "IoT Project" launched by the non-profit organization OWASP (Open Web Application Security Project). It includes an interesting and comprehensive – although precise – list of security recommendations[2].

The first thing to notice is that this guide is divided into 3 categories for specific audiences: manufacturers, developers, and consumers. This structure makes sense, to the extent **that security is shared between the ones who design the devices** (hardware or software), **and the ones who use them**.

One other important fact about the security features is that they have to be holistic – **hardening the IoT is not only about the devices, but about the whole attack surface**: physical, hardware, software, database, local or remote, etc. In this regard, the recommendations are mainly built upon the security industry's best practices.

The real change with the Internet of Things is the way you actually have to implement these features.

Several aspects of these connected devices must be taken into account:

/ **User-friendliness:** the size and form-factor of the devices will influence the security features that are acceptable for users – typing a password on a 1.5" screen is not.

/ **Processing power:** as of today, small embedded systems still have limited calculation capabilities. Some operations cannot all be processed on them within a reasonable delay. For instance, Apple advises the developers not to code features that perform long-running tasks on the Apple Watch.

/ **Connectivity:** the Internet of Things devices typically use Bluetooth or NFC protocols, with limited bitrates and ranges, and don't always offer proper embedded security.

/ **Battery life:** complex algorithms (like real-time asymmetric encryption/decryption) can be hard on battery consumption, even if they offer a better protection level. This has to be taken into account in the design phase.

/ **Update capability:** security update has to be deployed without interfering with the object usage. This is particularly striking in the case of cars that you cannot drive while they are being updated, and this could take more than 45 minutes.

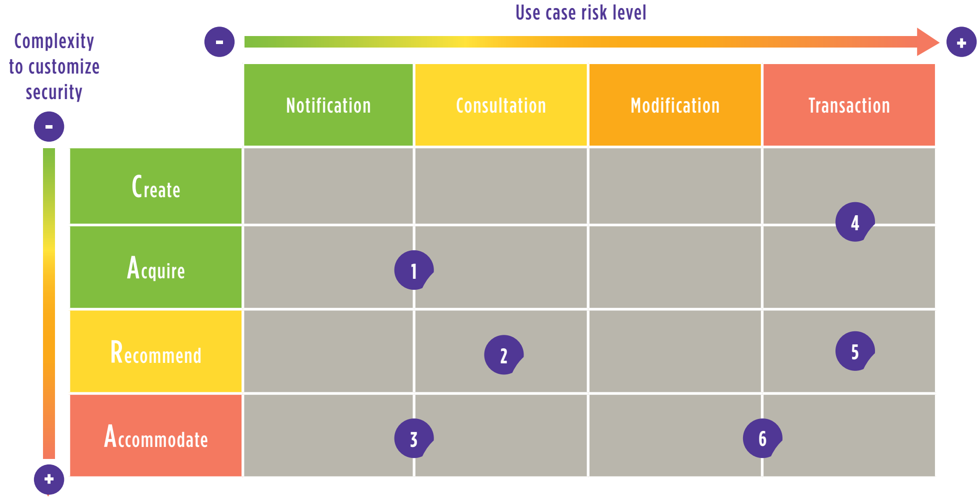
In addition to security, privacy is also a must have for the customers and a requirement from the authority. Implementation could be tricky but several initiatives for IoT privacy have emerged in the last years.

One of the most interesting is the European PRESERVE project[3], which offers the automotive industry a new way of using PKI and digital certificates for smart connected cars and roads. They use the principle of using a frequently changing "pseudonym" to ensure that the car drivers stay anonymous while ensuring that communication between the vehicles and the road infrastructure is authenticated and secured.

We have entered a time where security and data privacy have become criteria in the customers' choices. This fact cannot be denied by providers: **they have to integrate it, whether they design, build, recommend or sell smart devices**.

Source1: http://go.saas.hp.com/fod/internet-of-things
Source2: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
Source3: https://www.preserve-project.eu/

Heat map instance in a B2C banking context



1 Client identification with Google Glasses

2 Stock portofolio 3D visualization with Occulus Rift

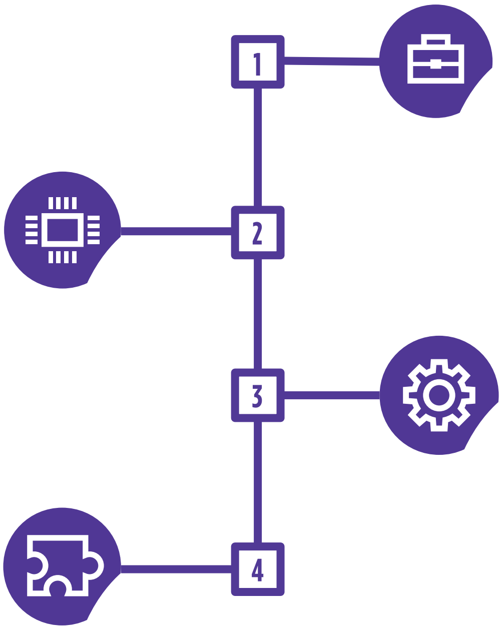
3 Account notification and checking with a smartwatch

4 Digital signature with a smartwatch

5 Contactless payment with connected wristband

6 Account data change or transaction with a smartphone

HOW TO SECURE THE INTERNET OF THINGS



Talk with the business stakeholders

It is important to understand the business stakes during the whole device lifecycle, in order to clarify and anticipate possible risks.

Clarify the use case

The risks of connected devices may differ depending on the usages and the setting (CARA). Furthermore, depending on your industry, the devices will not be used the same way.

Analyze the market and the platforms

Two relatively similar devices may not be equally secured. It becomes necessary to identify the specifics of the platforms and the associated limits.

Think outside the box to implement security

Take into account the context in which connected devices evolve, as well as their characteristics: autonomy, range, user experience...

WAVESTONE

www.wavestone.com

Wavestone is a consulting firm, created from the merger of Solucom and Kurt Salmon's European Business (excluding retails and consumer goods outside of France).

Wavestone's mission is to enlighten and guide their clients in their most critical decisions, drawing on functional, sectoral and technological expertise.