IoT Payments: addressing the protection problem

An SPA Paper

February 2019

The proliferation of interconnected IoT devices offers exciting new opportunities to develop payment applications – in the home, on the move and in a wide range retail, automotive and industrial environments. But a lack of standardization, slow adoption in the financial sector, and a complex technology ecosystem presents considerable challenges that threatens to stifle innovation and market evolution. SPA investigates.

1. Introduction

While market projections differ – from Gartner's much cited 50 billion connected devices by 2020, to IHS Markit's rather more conservative 30.73 estimate – there's little doubt that the Internet of Things (IoT) is a massive and growing opportunity for payment services.

At the same time, the financial services sector has been slow to embrace IoT payments. To date, the sector has been more focused on mobile applications and wallets. This is slowly beginning to change. New use cases and commercial IoT applications capable of initiating remote payment are certainly emerging, including smart (voice-enabled) assistants and in-car dashboard systems. But the pace could be accelerated.

There are significant security risks that must be addressed if this is to happen. According to security firm, Symantec, the number of malicious attacks on IoT-enabled devices grew some 600% between 2016/17. IoT is certainly a large and growing target, and with personal data 'gold' on offer for successful hackers, there's every reason to assume attacks will continue to grow in volume, ferocity and sophistication.

This shouldn't come as a surprise. As IoT becomes a ubiquitous part of everyday lives, we're exposing every greater amounts of sensitive, personal and financial data to a host of semi (or completely) autonomous, connected devices. As consumers, it's almost impossible to know whether our connected cars, smart homes and healthcare systems are adequately protected – particularly as a new crop of immature application developers and device manufacturers appears. Added to which, in many use cases, the payer is not physically present. The authority to initiate the payment is therefore delegated to the device – which poses its own set of issues.

However, while broadening the list of connected 'things' certainly broadens the risk, this is by no means a good reason to put the brakes on change. Indeed, where payment is concerned the opportunities are many. SPA believes we should push ahead, but do so with caution and a better understanding of how to protect these internet-connected devices to minimize the risk of attack and fraud.

2. The potential of IoT payment

One of the big 'customer experience' wins of the widescale drive to IoT is payment. In the automotive space, our connected vehicles become the payment instrument for a range of services including buying fuel, paying for tolls and parking, and multiple drive-thru retail scenarios. At home, IoT is opening up a host of pay-per-use payment models linked to the consumption of water and energy utilities, for example. We're already familiar with payment-enabled in-home smart assistants like Amazon's Alexa or Google's Assistant to buy music. There's a lot more to come.

In the retail environment, for example, payment options – from app-enabled purchasing to contactless payment on wearables – is eliminating friction and improving buying experiences. While in financial services, embedded payment options are not only facilitating person-to-person payments and payments in unattended environments, they are driving the development of more accurate financial risk management systems (by capturing information from IoT devices and networks).

These examples barely scratch the surface of what is possible in an increasingly connected world. But, irrespective of application or operational context, they all have one thing in common: data. Whether user-directed or fully autonomous, IoT devices (and particularly payment-enabled ones) generate, store and process huge volumes of sensitive data.

Today, it's at risk. And not just from cybercriminals intent on monetizing stolen data or creating havoc by initiating fraudulent payments. Corporations are also facing more regulatory pressure than ever before to effectively and securely manage (and ethically leverage) sensitive IoT-derived data.

Governments and payment regulators certainly have an important role to play promoting the design and deployment of secure IoT solutions. So too, banks and fintechs have a role in developing and demonstrating the viability (and security) of payment IoT applications.

3. The importance of the network

This is not just an applications issue. Connectivity is crucial too. Last year, wireless IoT received a major boost with the commercial launch of Narrowband-IoT (NB-IoT) networks – part of the Low Power Wide Area (LPWA) category of communications. NB-IoT makes it considerably more commercially and operationally viable to connect low bandwidth devices, via a SIM card, to a network – particularly those in hard to reach, rural or remote locations.

Giving impressive power efficiency, NB-IoT devices can run on batteries for up to ten years in the field, while the devices themselves can be built cheaply – for under $10. With this kind of price and

performance, we'd expect to see significant deployments at scale in 2019. Added to which, the arrival of 5G through 2019 will be important - particularly for higher bandwidth applications.

4. Exploring the protection imperative

At the most fundamental level, IoT payment security poses a volume challenge – both in terms of the number of devices and the diversity of use cases. The more connected devices on the network – particularly if they are poorly protected – the higher the chance that one or more could be compromised by the latest mutating malware. Not only are devices designed to be easy to access remotely, they often lack the processing power and memory to support conventional security approaches – particularly in terms of managing the regular software updates required by today's signature-based AV approaches.

As above, the diversity of devices and platforms is also an issue. We're still in the Wild West of IoT deployments when it comes to many payments use cases. Securely embedding payment into IoT devices, and then doing the same with platforms as diverse as connected cars, smart meters and virtual assistants, creates a slew of design, integration and lifecycle challenges – from remote software provision to regular firmware updates to secure those IoT devices with long lifetimes. Moreover, devices need to be able to monitor and report on unauthorized access attempts – so future attacks can be blocked, or compromised devices isolated.

The core principles of IoT security are simple: protecting the physical smart devices and the network that sends and receives data online to and from authorized components. The operational reality is rather more complex. The IoT technology stack includes network infrastructure, IoT devices, cloud platforms and databases, decision-making (and self-learning) processes, communication networks and so on. Added to which, back-compatibility with existing payment systems, delegation to the IoT device, payment credential management and strong customer authentication implementations are all required (and challenging) in the payment context.

This complex environment is difficult to monitor and control with a robust certification process. Plus, the multiplicity of attack points that cause data leakage, and the lack of understanding of how to apply security controls in a payments environment, are major issues.

It's not only about the technology. The protections (and regulations) required for healthcare-based IoT systems are clearly different from those in the payments arena. Getting security right in every operational context not only requires a lot of hard technical thinking, it also need a deep awareness of the regulatory landscape in each case. The constraints posed by the General Data Protection Regulation (GDPR) and upcoming e-Privacy regulations in the European Union and beyond are a case in point.

5. Attack scenarios in the payment context

5.1. IoT administration system compromise

The compromise of an IoT administration system grants the attacker access to all the assets (devices, networks, gateways) under the control of that administration system.

The attacker is now capable of performing a range of nefarious actions including extracting confidential information, creating malfunctions or directly affecting the behaviour of the IoT environment. Since a compromised administration system leads to several assets being compromised over a long period of time and without being detected, the impact of this attack can be critical.

Current Payment Systems Security Architecture is designed with multiple control points that are well adapted to the characteristics of a limited number of certified acceptance points (i.e., terminals) using certified products (i.e., payment cards). Therefore, the integration of IoT systems may be difficult due to the scalability challenges for the security infrastructure.

5.2. Value manipulation in IoT devices

The manipulation of calibration parameters established for the sensors allows undesired values to be accepted when they should not – an issue that poses severe threats to critical systems.

In this attack, the sensor processing and knowledge model levels of the control system of an industrial robot in a factory is targeted. In payment systems, the attack targets Real-Time Risk Management Systems in payment networks authorization computing facilities.

5.3. Botnet command injections

A botnet is a network of automatic devices that interact to accomplish some distributed task.
The attack entails the exploitation of some vulnerability inside a device to inject commands and obtain administrator privileges, with the purpose of creating a botnet made up of those vulnerable IoT devices.

Due to the characteristic interconnection of IoT devices and their poor configuration, carrying out such an attack is (at least in theory) relatively simple. Unsecure IoT constitutes vulnerable entry points to payment systems. Command Injection may include fake payment authorization requests/responses.

5.4. Designing countermeasures

What then is the solution? The first step is to fully understand the limitations of the IoT device – its lower computation power, the constrained communications channels, and the integration challenges of the diversity of environments and platforms. It is also necessary to take into account the certification vs unitary cost for payments in this IoT context.

Added to this, applications developers, payment providers, device manufacturers and integrators must also be aware of the security constraints. These include the need for authentication at scale, the multiplicity of attack points as well as the need to provide security beyond the perimeter of the system. Encrypting data at rest and in transit on the network is important too. There are also some lightweight cryptography standards that fall under ISO/IEC 29192 that can be used to reduce impacts on device performance in the NB-IoT environment.

Biometrics are playing an increasingly important role in securing IoT. We've seen fingerprint biometry become ubiquitous for Apple Pay and Google Pay solutions, and now the schemes and banks are adding match-on card biometrics to the next generation of smart payment cards.

Indeed, Visa sees a future where consumers will be able to swipe their hands over IoT-connected terminals without the need for a payment card, watch or any other device. Already its Visa Ready program provides a path to secure payment functionality in cars, wearables, household appliances, retail environments, and more. In this growing ecosystem, device manufacturers can look to approved Token Service Providers (TSPs) to enable tokenized payment functionality in IoT devices.

Similarly, the Mastercard Engage program offers solutions to help manufacturers of IoT devices more easily and quickly enable their devices with secure payments.

Looking beyond the Schemes, we have seen significant national public administration initiatives to harden IoT against cyberattack. A recent example is the proposal by the European Commission to strengthen and expand the European Network and Information Security Agency's (ENISA) mandate by addressing certification and standardization of ICT products, as well as wider plans to increase cooperation relating to preparing and addressing cross border cybersecurity challenges in Europe. Similar work is happening in the UK, with the Government here promoting secure-by-design principles and the development of best practices in the design of IoT systems.

At present however, there remains no specific financial industry standardization initiative for IoT-enabled payments or security architectures. Both of which are critical to drive development and adoption of a broad range of IoT payments applications and services.

More work needs to be done across the IoT ecosystem to enhance and extend security –whether that be new device and user authentication approaches, securing payment account information, or the wider adoption a rapidly evolving tokenization infrastructure.

SPA is exploring these and other approaches to securing IoT-enabled payment in its Workgroup program.

If you are interested in joining the SPA Retail Advisory Council, click here: https://www.smartpaymentassociation.com/index.php/about-us-smart-payment-association/join-us-smart-payment-association