Ensuring payment terminals, transactions and apps are secure

——The first in a two-part security blog

Andrea Zucchiatti, Chief Product & Services Officer, PAX EMEA
Aileen Liu, Director of Payment Technology, PAX China
LeAnn Hostetler, Chief Security Compliance Officer, PAX US

Part Two

In Part One of this security blog, we explained the high importance PAX Technology gives to security and how this applies right across the organisation to our products, processes and people. We looked at how our devices are made secure from both a hardware and software aspect, the numerous certifications we have achieved and how our Value Added Services (VAS) such as Remote Key Injection (RKI) are secured.

In this Part Two we consider App and Marketplace security, Vulnerability management and Privacy protection.

App and marketplace security

Our Android powered SmartPOS devices run multiple apps simultaneously. These are managed by MAXSTORE which is our secure App Store marketplace and Device Management platform. (To understand MAXSTORE's value and the new world of Android SmartPOS apps for merchants, read the second blog in our series).

No sensitive payment data is ever shared out of a PAX terminal payment application to a non-payment app. This is simply not possible as data is only sent using defined message protocols. The architecture and security controls implemented within MAXSTORE ensure that unauthorised access is prevented. 'Triple digital signing' of apps by the app developer, marketplace owner and PAX is required before any software can be deployed to devices. This approach means that the terminal deployer has an intrinsic role to play in the security responsibilities chain. Secure key injection at time of manufacturing further ensures access is restricted to legitimate users.

Every software app is subject to comprehensive security reviews to ensure that no malware or viruses end up on PAX devices. All software developed by PAX Technology is reviewed by two separate teams and then verified using our AppScan service to check for security weaknesses.

MAXSTORE has been deployed on the Amazon Web Services (AWS) cloud infrastructure, bringing multiple levels of security protection, including access and infrastructure control. This does mean that different IP addresses will be used as the AWS cloud front-end uses dynamic (rather than static) - and a range of varied - IP addresses. Secure independent instances of MAXSTORE can be created and licensed users have full control over which apps can be deployed.

A key (optional) security feature offered by PAX is that of geo-location. This tracks the physical location of each device to a very accurate position and provides real-time notification and automatic blocking if the device appears outside of its agreed security boundary fence. Geo-location services offered by PAX are managed by two highly respected service providers, one located in North America and the other in China - customers may choose which they prefer.

The support for multiple apps (payment & non-payment) on a single device and new features available from the Android operating system does mean that security understanding must be increased to identify legitimate use. Differences in how SmartPOS products operate does not mean there should be a security concern. For example, Android captures far more data elements than legacy terminal operating systems ever did, and shares these with MAXSTORE. Therefore data packet sizes will vary dependent on multiple criteria including model type, application version, processor protocol, terminal activity, wireless network performance and for purposes of legitimate terminal management and preventative maintenance.

A detailed independent security review conducted at the end of 2021 by the respected Unit 42 of Palo Alto Networks Inc. confirmed that no malicious traffic and events have ever been identified in the network traffic activity they reviewed in PAX solutions.

Vulnerability management

PAX Technology operates a comprehensive vulnerability management procedure that follows ISO/IEC 30111 and ISO/IEC 29147 international standards. Processes and workflows have been set up across the four phases of: vulnerability identification, verification, repair, and disclosure.

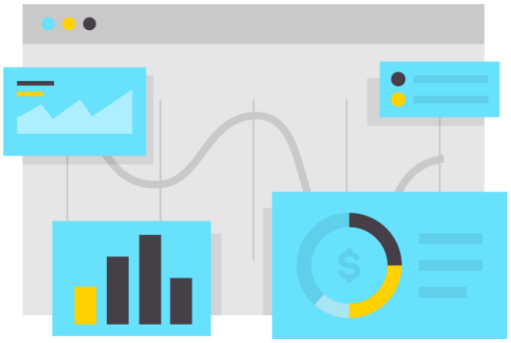
This includes monitoring news and security websites, public known vulnerability databases, and engaging with data security professional communities. We also actively monitor information and concerns relating to open source and third-party libraries that we use.

Vulnerability verification includes investigating reports received from partners and customers, raised via the PAX Vulnerability Disclosure program, or found during the product development stage. Vulnerability impact assessments and repair is promptly completed for all non-End of Life (EOL) products. Disclosures are published in bulletins and on the customer support portal to provide information on recommended action and appropriate software updates.

Additionally, internal and external specialist resources are continually tasked with conducting penetration testing on products and services, with the aim of identifying and eliminating vulnerabilities before they become a security concern. State of the art testing methodologies and technologies are used as we understand that cyber criminals are always on the lookout for vulnerabilities. PAX Technology constantly learns from penetration and vulnerability testing results, updating our processes and designs accordingly to ensure PAX products deliver the highest possible levels of security protection.

Privacy protection

At PAX, we attach high importance to privacy protection, following a privacy management framework that encompasses matters such as privacy by design, 3rd party protection, data subject requests, impact assessments and incident response procedures. We always ensure our products are compliant with regulatory requirements including the European Union's GDPR, Brazil's LGPD and Singapore's PDPA.



Our privacy protection work covers software products, terminal devices, MAXSTORE and VAS service that delivers business intelligence to clients following data analysis.

The PAX perspective

PAX Technology attaches high importance to all aspects of security and applies this to all hardware and software products, value added services, internal processes and people management. We recognise our responsibilities and accordingly design security into our products from the outset and consider the topic of security holistically. We conduct annual security audits as part of our processes and seek to constantly improve security protection levels.

Our global network of customers also have security obligations and ultimate responsibility for PCI DSS. They must check and digitally sign apps, making sure they have the necessary security expertise required for the deployment of next generation Android SmartPOS solutions.

We offer a secure App marketplace and through digital signing ensure only verified apps can be installed to devices. Our recent PCI DSS certification further confirms the security of our worldwide MAXSTORE deployments.

Vulnerability management, penetration testing and privacy management are further items covered as part of our overall security procedures. We continue to invest more money & resources into these areas.

The PAX brand is synonymous with high quality & high security. To date, no payment transaction security issues have ever been identified by customers worldwide who use PAX products; likewise, no payments data has ever been compromised, none of PAX Technology's certifications have ever been withdrawn, nor has malicious traffic or events ever been identified in network traffic activity.

Our regional Chief Product Security Officers will be pleased to answer any further questions you may have.

PAX

www.paxtechnology.com