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 One

Criminals recognise the opportunity of compromising payment systems in order to commit fraud. Globally, payment fraud losses (of all types) have more than tripled since 2012 to $34 billion and are expected to rise to over $40 billion by 2027. These losses impact financial institutions, merchants, consumers, and society at large, with criminal gangs often using the funds for drugs trafficking purposes, money laundering, terrorist financing and to exploit vulnerable individuals. That is why security must be the number one priority for everyone within the payments industry.

PAX Technology understands this and places security at the centre of everything we do. We design highly secure products to protect our clients and their end users, ensuring customer sensitive data is unassailable. We have attained ISO/IEC 27001 certification which is the most authoritative and widely adopted of all international security management approvals (note that the United States of America is not in scope of this certification). We operate a multi-level security management structure across our organisation, overseen by an Information Security Management Committee that reports directly to the board. Day-to-day responsibility has been assigned to an Information Security Group with representation from all departments and they have been given a charter to look after security matters at all stages of the product lifecycle, internal processes, and people aspects. Each of PAX Technology's global regions has someone nominated to perform the role of Chief Product Security Officer, Chief Security Compliance Officer or similar.

Security relies on technology, processes and people

Payment technology security encompasses much more than just hardware design; software increasingly has greater importance than hardware features. Delivering highly secure technology relies on effective processes and qualified people. It is helpful to think of an analogy of a three-legged stool where stability is removed if any of the three legs are compromised. Criminals always look to exploit the weakest link and continually adapt their attack profile to commit fraud. We are committed to investing more to ensure our products and services offer the highest levels of security.

PAX Technology’s five security pillars

At PAX, we think of security within five discrete pillars and will discuss each of these in this two-part blog series. Our security responsibilities have increased as the product range has expanded into new solution categories.

i. **Device security (hardware & software) - Payment, Merchant and IoT devices**
ii. **Value Added Services security**
iii. **Device Management System and Marketplace security**
iv. **Vulnerability management**
v. **Privacy protection**

In Part 2 of this security blog, we will look at App and Marketplace security, vulnerability management and privacy protection.

Device security

Payment terminals are required to comply with multiple rigorous industry standards which are set by the international payment networks, either working together through the auspices of the Payments Card Industry (PCI) Security Standards Council (PCI SSC), EMVCo (owned by 6 international card brands), or individually, as well as meeting regional and acquirer requirements and/or standards. These security assessments encompass the entire payment ecosystem (products & services), as all aspects are intrinsically linked.

The PCI PIN Transaction Security (PCI PTS) Point of Interaction (POI) security requirements are the most important global requirements for us. This comprehensive list of security requirements ensure security for the protection of consumer PINs and the secure handling at all stages of transaction processing. It covers hardware design, encryption, key management, and software development. To date we have achieved 86 certifications for our device models, with 17 of these being the latest version, PCI PTS 6.x. This positions PAX as a security leader and demonstrates our commitment to being an early adopter of the most up-to-date PCI PTS standards in order to provide our customers with the confidence to maximise security protection. Our products include tamper resistant security modules and use dedicated security processors. PCI approved 3rd party Qualified Security Assessors (QSAs) conduct detailed assessments to confirm compliance to PCI specifications. All new payment devices launched by PAX will, of course, be certified for PCI PTS.

In addition, PAX has certified 14 products against an additional international security standard created by the Common Security Evaluation and Certification Consortium (Common.SECC) that is required in the UK, Germany and a growing number of countries, the most popular of which is the best-selling A920Pro (the rising popularity of Android payment terminals was discussed in our first blog series). The thorough IT security evaluation is performed by government accredited security laboratories using the ISO standardized Common Criteria (CC) methodology that delivers security assurance irrespective of the application being run on the device.

Our payment terminals are also certified according to EMVCo Level 1 and 2 standards for the secure acceptance of contact & contactless chip cards. These certifications are expected by all PAX customers, and we have a good track record of passing them quickly to avoid delay in new product launch and customer availability. The global implementation of Chip & PIN technology and EMV standards has dramatically reduced the level of fraud committed in a face-to-face environment, causing criminals to look for easier targets and shift their attention to eCommerce.

When new certifications are introduced by international brands, such as Mastercard's Enhanced Contactless (Ecos) certification, PAX ensures that the latest generation of its payment devices are certified, such as the multilane A35 Android Smart PINpad. We recognise the necessity for security certifications and are proud of the deep security expertise we have built up within the PAX group and the wider PAX community of global channel partners and payment system integrators, as well as the secure design of our products and efficiency in completing evaluations.

For many years we have also ensured our devices are validated against the Mastercard Terminal Quality Management (TQM) standard that looks at the overall security and performance of payment terminal hardware.

PAX products also complete exhaustive accreditations & certifications with acquirers and/or processors worldwide, to help ensure that payment transactions are always processed securely. Major Financial Institutions (FIs) have completed detailed risk assessments on our products and services, and these in-depth reviews confirm the high levels of security provided by PAX solutions.

Ultimately, our customers are responsible for their PCI Data Security Standard (PCI DSS) compliance, but we assist them by delivering hardware and software products that incorporate high security features and which can be operated in a secure manner. One example is our PCI certified Point to Point Encryption (P2PE) Secure Reading and Exchange of Data (SRED) component that ensures that cardholder account data (non PIN) is accepted securely at the point of acceptance and protected through the use of high level encryption. A growing number of our customers are adopting P2PE to ensure cardholder data is encrypted, and for them PAX Technology's SRED module acts as a foundation layer for creating a secure P2PE infrastructure.

The latest PAX PINpad models have been designed to support a Kensington security slot and the ability to mount the PEDs in secure mounting brackets. This helps deliver additional physical access security options for our customers.

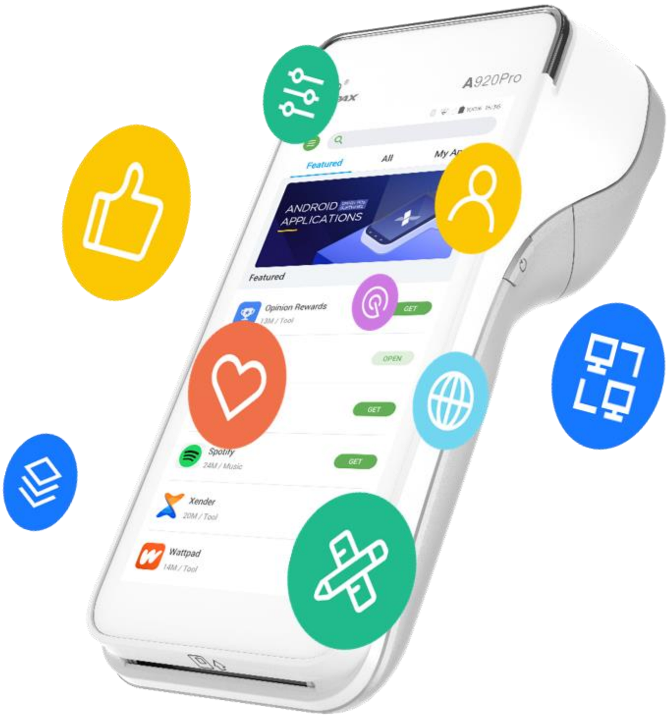
Merchant and IoT devices

With the expansion of the PAX product line into smart (EPOS) merchant devices that integrate store operations and payments in an all-in-one solution, we now have new security obligations that focus on merchant data security. We need to secure sales processing, ordering, inventory management, loyalty program data, printing, and secure communications. This is handled separately from payment transaction processing, but we treat it equally seriously. We also ensure high levels of security protection is included with our new generation Unattended, PayPhone and PayTablet products.

Our entry into the Internet of Things (IoT) and world of connected commerce will equally demand strong security, so we are designing appropriate high level security features into these products from the outset, including secure cloud and IoT management frameworks. This will, amongst other aspects, include device authentication, secure integration, and communication between devices.

Software security is key

Security considerations are addressed in each of the seven steps of our secure software development lifecycle process (S-SDLC) and international best practices are always followed during initial design, requirements analysis, software development, testing, release, and maintenance phases. These are reviewed by external Qualified Security Assessors (QSA) as part of the PCI certification process. Software release procedures require separate security code reviews by both Quality Assurance (QA) and Development teams. Both teams must digitally sign applications before any software can be released and deployed. Access to sensitive design and security documentation is tightly controlled to appropriately selected individuals, software development teams physically sit separately and new hires are vetted.



Our new generation SmartPOS terminals run a special locked down version of the Android operating system that we call PayDroid. This restricts access to features like card readers, keyboards, cameras, and microphones that could create security vulnerabilities. It also prevents sensitive payment & cardholder data being shared with non-payment apps being run on the same device. New versions of the PayDroid OS are regularly released throughout the year and security patches are applied at least on a quarterly basis, but immediately if necessary.

Strong encryption and key management

PAX supports a range of symmetric and asymmetric cryptographies within our products to protect sensitive information. These include, but are not limited to, Data Encryption Standard (DES), RSA, Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC). Also, we operate a range of key management processes including Triple DES (TDES)/AES Master key/Session key and TDES/AES Derived Unique Key Per Transaction (DUKPT). (Note that TDES has been deprecated).

Security throughout the full lifecycle

PAX is certified to the internationally recognized ISO9001 Quality Management System which includes many security requirements. Our approach to security applies right through a PAX product's lifecycle - from initial design, software development, manufacturing processes, shipping, software deployment, merchant usage, to handling at authorized repair centres.

Securing value added services

We offer a developing range of VAS to our customers with one of the most important being a secure Key Injection service. This loads a unique security key into each device at the time of manufacturing, ensuring subsequent full control over who can load software and which applications can be run. We operate the paxRhino secure key injection service at three Remote Key Loading (RKI) centres located respectively in Italy (for Europe, Middle East, and Africa), the USA (for North & South America) and China (for Asia). Each of these ultra-secure facilities have been inspected and certified to PCI standards. Key security capabilities include: building design security features, the restriction of access to people through electronic badges, CCTV systems equipped with monition detection, use of high security hardware modules, restricting the possibility of observation and preventing the passing or sending of restricted information. Our RKI centres also operate intrusion prevention systems, firewalls, and have been securely segregated from corporate networks. RKI offers a highly secure but more cost-effective alternative to Local Key Injection (LKI) but these can also be supported if preferred by a customer. The RKI service additionally provides options for enterprise merchants to control device usage within their estate. Additionally, we are a PCI certified Certificate Authority (CA) service provider and have been serving customers securely with this capability for several years.

Importantly, PAX achieved PCI DSS certification in February 2022 for the PAXSTORE platform and the supporting VAS that we supply. This confirms we have the necessary information security controls in place to ensure that sensitive information and data are handled correctly during acceptance, processing, transmission and storage and that data leakage is prevented. We have been certified against PCI DSS's 6 objectives and 12 requirements, with over 300 items under review. Our PCI DSS compliance shows that we have in place the necessary controls to manage cardholder data, information security management processes, network security design, data protection, security monitoring and vulnerability management.

The PAX perspective

Part One of this security blog highlights the importance PAX attaches to security and how this applies to our products, processes, and people. We design security into our products from the outset and consider it holistically. Our payment devices comply with relevant security standards and have been certified by multiple bodies. Our approach is to be proactive, fast adopters of the latest version of specifications and to promptly address any security concerns raised.

Our secure implementation of the Android operating system restricts access to sensitive data and separates payments processing from non-payment apps. Security is addressed throughout the entire software development process and the SRED module provides a certified P2PE component for customers implementing end-to-end encryption. Our VAS like RKI have also been certified to PCI specifications. Key security principles we follow include: maintaining segregated environments, adopting the latest security specifications, applying frequent operation system and security updates, digitally signing all software before it can be deployed and securing data and communications through the use of strong cryptography and key management.

In Part Two of this security blog we will explain how PAX addresses App and Marketplace security, Vulnerability management and Privacy protection.

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