Hypercom White Paper

www.hypercom.com

PCI PED Considerations

for New Purchase Decisions

- **Early Security Standards**
- **Maintaining Security**
- **What this means for Retailers**
- **Real World Solutions**
- **Summary**

Early Security Standards

Prior to 2004, each of the card brands policed their own PIN Entry Device (PED) requirements for security. In 2004, Visa® and MasterCard® collaborated to align their specifications and PCI PED was born. Subsequently additional card brands collaborated. The PCI SSC (Payment Cards Industry Security Standards Council) was formed in 2006 with the PCI-DSS (Data Security Standard) standard in its scope. PCI PED was brought under the PCI SSC umbrella in September 2007.

The initial release of PCI PED, we'll call it version 1.0, harmonized the requirements of Visa and MasterCard and provided a security baseline that the card brands felt represented a minimum level of security required in any PIN accepting device. The standard attempted to balance the cost of compliance with the expense a criminal would need to invest in an attack on a PED.

Maintaining Security

As the security threats have evolved in both number and sophistication, PCI PED has been enhanced to maintain that balance of compliance and expense. PCI participants have agreed that, in general, PED security and associated test requirements will be updated every three years. Minor updates are made on an ad hoc basis as new security threats are identified. As these changes to requirements are made, the PCI SSC (Payment Card Industry Security Standards Council) publishes the transition dates between versions. They usually publish a date whereby the previous version product can no longer be certified as being compliant with the current version of the standard and a second date at which time that version product can no longer be purchased.

Today, July 2009, we are in a transition between PCI PED version 1.3 and PCI PED version 2.0. PCI PED version 1.3 devices are no longer being certified but can be sold until 2014. PCI PED version 2.0, which was published in July 2007 and in effect since 2008, is now the requirement for all new devices being certified by PCI endorsed laboratories. Under the current rules each major PCI PED certification level (ie: 1., 2.x) carries a 9 year approval cycles from their affectivity date. As such

PCI PED 2.0 devices can be sold until 2017. For a visual representation, see Figure 1: PCI PED Terminal Timetable on page 4.

What this means for Retailers

So why should a retailer making a product purchasing decision today (2009) care about the difference between PCI PED versions 1.3 and 2.0. The most fundamental answer is to reduce the risk of compromise and to extend the potential serviceable life of the product selected today.

Real World Solutions

All changes to the PCI PED standards are driven as a result of actual product attacks that are detected in the field, by an analysis of criminals increasing skill and sophistication and by the ever decreasing cost of technology. All security requirement decisions are a risk assessment that associates the cost of mounting an attack with the value that is delivered by compromising the device. As technology capability continues to increase and technology cost continues to decrease, the risk – reward ratio continually changes.

When you purchase the latest version PCI PED certified product you are ensuring that the device can withstand the latest generation of attacks and will remain sufficiently secure for the longest period of time. It should be noted that in this rapidly changing world it is quite possible that an attack will be mounted that forces PCI to alter the current dates for installation and usage of a particular version of device.

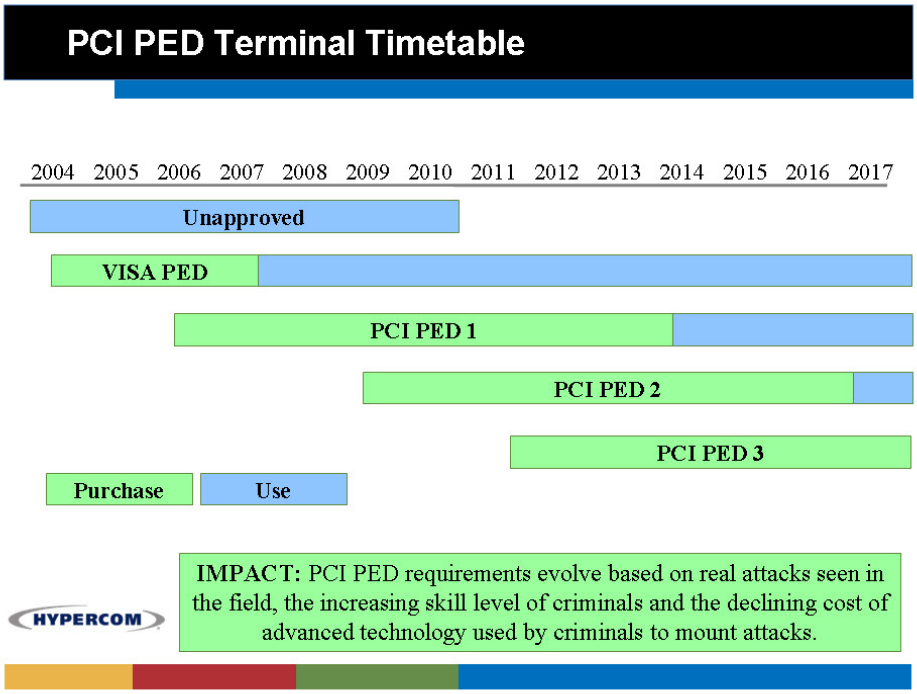

Figure 1: PCI PED Terminal Timetable

There are some significant differences between PCI PED version 1.3 and PCI PED version 2.0 that all retailers should be aware of:

- PCI PED version 2.0 strengthens and protects against the undetected insertion of a PIN disclosing bug by altering the security requirements surrounding the replacement of a devices top housing (plastic enclosure). This may appear to be an innocuous or minor change but it reflects actually experience from the field where PIN disclosing bugs have been found in operational PED's.

- PCI PED version 2.0 explicitly calls out the requirement to protect the magnetic swipe reader assembly form from modification or substitution. This perhaps obvious requirement has not been explicitly identified in previous PCI PED versions and has therefore not been tested during the certification process. It is therefore quite possible that the MSR reader assembly of an operational device can be tampered with or compromised without detection.

- PCI PED version 2.0 requires the device to support more sophisticated cryptographic key management schemes. These schemes require equivalent changes to be made on the transaction acquiring host. The acquiring side change is not as yet mandated but given recent breaches and the exposure these breaches have attracted within both press and government, it is highly likely that these key management changes will be implemented by some acquirers within the lifetime of a product purchased today.

- Some elements of PCI 1.x were removed in V2.x. For example the tamper evidence compliance path and DUKPT waiver. These elements originated in the former VISA PED requirements which date back to 2000. They were left in PCI 1.x to facilitate the transition from VISA PED to PCI PED. These lower security compliance paths (PCI 1.3 requirement A2 and A3) were originally defined to be valid for evaluation only during the first year of PCI 1.x implementation, but were extended until PCI 1.3 expiration.

- PCI PED version 2.0 strengthens protections around the chip card reader. This is related to the first bullet and is particularly applicable to countries implementing EMV (Canada etc).

- Remote Key Distribution capability is not a PCI PED requirement today but is a feature that should be carefully considered when purchasing new equipment. Automated remote key loading significantly increases the level of security by removing the human element from the key loading process. It also has the added value of reducing the cost of deployment at time of initial installation or following a repair or maintenance cycle.

Summary

In closing, it is Hypercom's strong recommendation that any retailer making a device purchase decision in 2009 or later seriously considers the risks associated with purchasing a non-PCI version 2.0 device. Technically PCI PED version 1.3 devices can be installed through 2014 although there is a possibility those dates may change if a new threat appears. There may also be a temptation to bypass PCI PED version 2.0 in anticipation of PCI PED version 3.0 which may be published at some time in 2010 but it should be remembered that the initial requirements of PCI PED version 1 where written in 2004 and the sophistication of technology and skill of criminals has progressed significantly since then.

Hypercom Corporation
8888 E. Raintree Drive, Suite 300
Scottsdale, Arizona 85260 USA
TEL: +1.480.642.5000
FAX: +1.480.642.4655
www.hypercom.com