Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org
Twitter @PCISSC

Payment Card Industry
Security Standards Council, LLC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI SECURITY STANDARDS COUNCIL RELEASES BEST PRACTICES FOR MOBILE SOFTWARE DEVELOPERS

— Mobile attack demo at PCI Community Meeting highlights need for more secure development practices; PCI Mobile Payment Acceptance Security Guidelines to provide more secure solutions for merchants —

WAKEFIELD, Mass., September 13, 2012 —At its North America Community Meeting today, the PCI Security Standards Council (PCI SSC), a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS), released best practices for mobile payment acceptance security. The *PCI Mobile Payment Acceptance Security Guidelines* offer software developers and mobile device manufacturers guidance on designing appropriate security controls to provide solutions for merchants to accept mobile payments securely.

The guidance supports the need for more secure development practices for mobile payment acceptance solutions. According to security experts Trustwave SpiderLabs, that specialize in data breach investigations and malware analysis, mobile computing, commerce, and malware are still in their infancy. Existing platforms limit users' ability to ensure the security of transactions conducted on mobile technology.

At a presentation today at the PCI Community Meeting in Orlando, Nicholas J. Percoco, senior vice president, Trustwave SpiderLabs, demonstrated some of the top attacks that threaten the security of payments over mobile acceptance devices, including malware and rootkits, jailbreaking vulnerabilities and SSL-man-in-the-middle attacks.

"It is important that a best practice guide be developed, by the industry, to educate mobile app developers on methods of securing commerce transactions and risks of not doing so." said Percoco.

The Council formed an industry taskforce in 2010 as part of a dedicated effort to address mobile payment acceptance security. Since then, the Council has released guidance on how merchants can apply its current standards to mobile payment acceptance by addressing mobile applications with the Payment Application Data Security Standard (PA-DSS), and leveraging the PIN Transaction Security (PTS) and Point-to-Point Encryption (P2PE) standards to accept payments on mobile devices more securely.

The guidance for developers is the next piece of the Council's work in this area. The document organizes the mobile payment-acceptance security guidance into two categories: best practices to secure the payment transaction itself, which addresses cardholder data as it is entered, stored and processed using mobile devices; and guidelines for securing the supporting environment, which addresses security measures essential to the integrity of the broader mobile application platform environment. Key recommendations include:

- Isolate sensitive functions and data in trusted environments
- Implement secure coding best practices
- Eliminate unnecessary third-party access and privilege escalation
- Create the ability to remotely disable payment applications
- Create server-side controls and report unauthorized access

"Applications are going to market so quickly – anyone can design their own app today that can be used to accept payments tomorrow," said PCI SSC Chief Technology Officer Troy Leach in his presentation to PCI CM attendees. "It's our hope that in educating this new group of developers, as well as device vendors on what they can do to build security into their design process, that we'll start to see the market drive more secure options for merchants to protect their customers' data."

In 2013, the Council plans to release further guidance for merchants to help them leverage mobile payment acceptance securely, while continuing to collaborate with industry subject matter experts to explore how card data security can be addressed in an evolving mobile acceptance environment, and whether additional guidance or requirements must be developed.

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linkedin.com/company/pci-security-standards-council
Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###