U.S. Secret Service

8 September 2015

Joint Advisory Bulletin: Mobile Payment System Vulnerability

This advisory was prepared by the United States Secret Service (USSS) in collaboration with the Payment Card Industry (PCI) Security Standards Council.

Growing Criminal Exploitation of Provisioning in Mobile Payments

The Secret Service has observed a steady increase in criminals exploiting vulnerabilities in the account provisioning and verification process for near field communication (NFC) payments to commit fraud. Specifically, criminals are using stolen identity information (e.g., credit reports, tax records, healthcare and employee records that contain personally identifiable information) to establish fake accounts on NFC devices and make illicit transactions both online and at "brick and mortar" retailers. Over the last several months, perpetrators have conducted numerous fraudulent transactions using this particular method of exploitation affecting many high-end retailers and banking institutions across the Northeastern portions of the United States.

The payment provisioning aspect of the NFC payment system process has proven particularly vulnerable as it contains a variety of weak security controls. For example, if fraud concerns arise during the transaction process, a determination to proceed with the transaction is often based on the user calling from a recognized number in their profile and/or answering a series of standard security questions (e.g., mother's maiden name, last four digits of the social security number, or other attempts to verify financial account information). These common security controls are often circumvented by criminals to compromise payment card data.

Further, compromised Card Verification Value (CVV) codes, when coupled with hacked account information derived from certain popular music and media download sites put consumers at risk for fraud. Hacked customer data from these popular music sites can

be purchased for as little as $8 USD per account in criminal underground forums and used to facilitate a variety of illicit transactions in the mobile payment space.

Mitigation & Best Practice Recommendations

In the mobile payments space as described above, the vulnerabilities fall into two general categories:

- Theft of payment credentials
- Falsification of payment credentials

The first category applies to pre-existing credentials where a perpetrator compromises one or more elements of the system to obtain credentials (e.g., primary account number (PAN) or Track 1 data) or where a perpetrator gains control over the use of the credential (which might remain otherwise unknown to the perpetrator). Preventing the compromise of credentials requires the application of physical and logical security controls by those that handle, store, or process credentials.

National and international industry standards that directly apply to this include *PCI Data Security Standards*, ISO 9564 series *Financial Services — Personal Identification Number (PIN) management and security*, ISO/TR 13569: *Financial services – Information security guidelines*, and ANSI X9.112 *Wireless Management and Security*.

As discussed in the previous section, the ease of identity theft has led to an increase in falsification of payment credentials. While measures to prevent identity theft are important to mitigating falsification of payment credentials, issuers (e.g., banks and credit unions) must assume that stolen identities will continue to exist. To prevent falsification of payment credentials, issuers need to control the registration process and the issuance of payment credentials by strengthening the verification process.

Ongoing security awareness training for customer service personnel is critical. Additional technologies and methods that enhance the vetting process should be considered. These include:

- Geolocation (i.e., GPS, cellular triangulation, IP)
- Device fingerprinting (i.e., obtaining a collection of data from a device that may identify the device and detect imposter devices)
- Biometrics (i.e., obtaining a valid exemplar biometric for use in authentication)
- Usage patterns (i.e., heuristics that are indicators of atypical behavior)
- Sharing of registration data across financial institutions to identify duplicate registration attempts (e.g., same device for multiple identities, same identity with multiple devices or different physical locations)

Ultimately, the falsification of credentials is a threat that stakeholders will have to manage. Building awareness, applying vigilance in maintaining security controls as well as educating employees on processes and protocols is critical to managing and mitigating these types of threats.

Payment card fraud, to include through the use of NFC, is a violation of multiple federal, state and local statutes. When organizations detect suspicious payment activity, they are encouraged to report this suspected criminal activity to relevant law enforcement agencies.

Contact Information:

- Suspected criminal activity related to payment cards or computer intrusions should be reported to local Secret Service field offices. Contact information for local field offices is available at: http://www.secretservice.gov/field_offices.shtml

- Any questions regarding this advisory can be directed to the USSS Criminal Investigative Division, Cyber Investigations at 202-406-9330.

- The PCI Security Standards Council (PCI SSC) encourages affected merchants to report any observed fraudulent activity to their respective acquiring financial institution and to contact the card brands whose cards they accept. Information on how to contact the brands may be found on the PCI SSC website under Frequently Asked Question - Article Number: 1142. Individual cardholders should contact the card brand via the telephone number given on their card or on the document associated with the account provisioning on the mobile device.

- For general inquires or to report a cybersecurity incident, contact NCCIC/US-CERT at (888) – 282-0870 | soc@us-cert.gov | nccic@us-cert.gov