Computer Crime Investigative Unit
U.S. Army Criminal Investigation Command

Cyber Crime Alert Notice

2CAN 0039-07-CID221-9H 19 July 2007

Virtual Pickpocketing

Overview:

Radio Frequency Identification (RFID) technology is utilized by major retailers and the US Government to track shipments and inventory. RFID technology allows scanners to use the radio signals at varying distances to read information stored on a computer chip. But RFID technology can also have adverse privacy and security consequences: A new type of credit card that uses RFID technology can transmit your personal information to anyone who gets close enough with a scanner.

CID elements are encouraged to brief supported installations and units on the contents of this 2CAN.

The Threat:

According to a 2006 study, many of these cards will transmit your name, the credit card's number, and its expiration date (but not the three-digit credit card verification code) unencrypted to anyone nearby with an RFID scanner. RFID chips have also found their way into new American passports, a move that has angered some privacy and civil liberties advocates. These concerns are unfounded, because the U.S. State Department has implemented several layers of safeguards to protect the privacy of passport bearers.

RFID credit cards in circulation today could be vulnerable to sniffing or skimming attacks that collect names and other credit card details. A sniffing or skimming attack uses a normal reader, or perhaps one that has been enhanced to read cards from a greater distance, to retrieve the unencrypted data from the card. Credit cards use an encrypted security code to verify a transaction, which can protect the cardholder from certain types of fraud. However, it does not protect the cardholder from someone who obtains your name and credit card number from a card and then uses this information to make certain online purchases.

"Without even removing their cards from wallets or pockets, consumers can potentially see their privacy and security compromised," Ari Juels, an author of the paper, stated in a blog post. "A scanner in a crowded subway station might surreptitiously harvest credit-card data from passersby."

An important point to keep in mind about RFID: Since fraud schemes using RFID technology require physical proximity to victims, online ID theft (phishing, keyloggers, and social engineering) will likely remain more popular with criminals. Additional information about phishing and keyloggers can be found in previous 2CANs.

Examples of RFID scanners

Contact Information:
Cyber Criminal Intelligence Program
9805 Lowen Road, Building 193
Fort Belvoir, Virginia 22060-5598

Phone: 703.805.3499 (DSN 655)
Fax: 703.805.2351 (DSN 655)
E-mail:
cybercrimintel.cciu@us.army.mil

CCIU Web Page:
www.cid.army.mil/cciu.htm

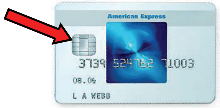
CID Cyber Lookout
On Point for the Army

Distribution:
This document is authorized for wide release with no restrictions.

"Do What Has To Be Done"

The Counter Threat:

How can you tell if your credit card has an RFID chip? On American Express Blue cards, you can see the actual chip:



The Visa Contactless card has this unique symbol:)))

If you want to know for sure, contact your financial institution and inquire. The wide variety of credit cards available means that, at least for now, there are many non-RFID choices.

For the especially paranoid (or cautious), you can block RFID signals with a device called a Faraday cage, which uses a metal mesh or casing. A Faraday cage can be a large apparatus in a laboratory or even integrated into a wallet.

Additional RFID Resources:

University of Massachusetts:
http://prisms.cs.umass.edu/~kevinfu/papers/RFID-CC-manuscript.pdf

Security Focus:
http://www.securityfocus.com/brief/336

ZD Net:
http://news.zdnet.com/2100-9588_22-5589512.html

SANS.Org:
http://www.sans.org/newsletters/newsbites/newsbites.php?vol=8&issue=85#sID200

Federal Trade Commission:
http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf

ICE

CCIU is now using the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.

Disclaimer: The appearance of hyperlinks in this 2CAN, along with the views and opinions of authors, products or services contained therein does not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations. Such links are provided consistent with the stated purpose of this 2CAN.

CCIU's "Toucan Lan" keeps an eye on cyber crime issues of interest to the Army community.