New Scoring System Protects Credit Card Transactions

November 8 2007

Credit: Unsplash/CC0 Public Domain

As this year's holiday season approaches, your credit card transactions may be a little more secure thanks to standards adopted by the payment card industry.

The latest incarnation of these standards include the Common Vulnerability Scoring System (CVSS) Version 2 that was coauthored this year by researchers at the National Institute of Standards and Technology and Carnegie Mellon University in collaboration with 23 other organizations.

When you make an electronic transaction—either swiping a card at a checkout counter or through a commercial Web site—you enter personal payment information into a computer. That information is sent to a payment-card "server," a computer system often run by the bank or merchant that sponsors the particular card. The server processes the payment data, communicates the transaction to the vendor, and authorizes the purchase.

According to NIST's Peter Mell, lead author of CVSS Version 2, a payment-card server is like a house with many doors. Each door represents a potential vulnerability in the operating system or programs. Attackers check to see if any of the "doors" are open, and if they find one, they can often take control of all or part of the server and potentially steal financial information, such as credit card numbers.

For every potential vulnerability, CVSS Version 2 calculates its risks on a scale from zero to 10, assesses how the vulnerability could compromise confidentiality (exposing private information such as credit card numbers), availability (could it be used to shut down the credit card system?) and integrity (can it change credit card data?). The CVSS scores used by the credit card industry are those for the 28,000 vulnerabilities provided by the NIST National Vulnerability Database (NVD), sponsored by the Department of Homeland Security.

To assess the security of their servers, payment card vendors use software that scans their systems for vulnerabilities. To promote uniform standards in this important software, the PCI (Payment Card Industry)

Security Standards Council, an industry organization, maintains the Approved Scanning Vendor (ASV) compliance program, which currently covers 135 vendors, including assessors who do onsite audits of PCI information security.

By June 2008, all ASV scanners must use the current version of CVSS in order to identify security vulnerabilities and score them. Requiring ASV software to use CVSS, according to Bob Russo, General Manager of the PCI Security Standards Council, promotes consistency between vendors and ultimately provides good information for protecting electronic transactions. The council also plans to use NIST's upcoming enhancements to CVSS, which will go beyond scoring vulnerabilities to identify secure configurations on operation systems and applications.

To learn more, see:

CVSS Web site: www.first.org/cvss
National Vulnerability Database: nvd.nist.gov

Source: NIST