Security flaws in online banking sites found to be widespread

July 22 2008

(PhysOrg.com) -- More than 75 percent of the bank Web sites surveyed in a University of Michigan study had at least one design flaw that could make customers vulnerable to cyber thieves after their money or even their identity.

Atul Prakash, a professor in the Department of Electrical Engineering and Computer Science and doctoral students Laura Falk and Kevin Borders examined the Web sites of 214 financial institutions in 2006. They will present the findings for the first time at the Symposium on Usable Privacy and Security meeting at Carnegie Mellon University July 25.

These design flaws aren't bugs that can be fixed with a patch. They stem from the flow and the layout of these Web sites, according to the study.

The flaws include placing log-in boxes and contact information on insecure web pages as well as failing to keep users on the site they initially visited. Prakash said some banks may have taken steps to resolve these problems since this data was gathered, but overall he still sees much need for improvement.

"To our surprise, design flaws that could compromise security were widespread and included some of the largest banks in the country," Prakash said. "Our focus was on users who try to be careful, but unfortunately some bank sites make it hard for customers to make the right security decisions when doing online banking."

The flaws leave cracks in security that hackers could exploit to gain access to private information and accounts. The FDIC says computer intrusion, while relatively rare compared with financial crimes like mortgage fraud and check fraud, is a growing problem for banks and their customers.

A recent FDIC Technology Incident Report, compiled from suspicious activity reports banks file quarterly, lists 536 cases of computer intrusion, with an average loss per incident of $30,000. That adds up to a nearly $16-million loss in the second quarter of 2007. Computer intrusions increased by 150 percent between the first quarter of 2007 and the second. In 80 percent of the cases, the source of the intrusion is unknown but it occurred during online banking, the report states.

The design flaws Prakash and his team looked for are:

• Placing secure login boxes on insecure pages: A full 47 percent of banks were guilty of this. A hacker could reroute data entered in the boxes or create a spoof copy of the page to harvest information. In a wireless situation, it's possible to conduct this man-in-the-middle attack without changing the bank URL for the user, so even a vigilant customer

could fall victim. To solve this problem, banks should use the standard "secure socket layer" (SSL) protocol on pages that ask for sensitive information, Prakash says. (SSL-protected pages begin with https rather than http.) Most banks use SSL technology for some of their pages, but only a minority secure all their pages this way.

• Putting contact information and security advice on insecure pages: At 55 percent, this was the flaw with the most offenders. An attacker could change an address or phone number and set up his own call center to gather private data from customers who need help. Banks tend to be less cautious with information that's easy to find elsewhere, Prakash says. But customers trust that the information on the bank's site is correct. This problem could be solved by securing these pages with the standard SSL protocol.

• Having a breach in the chain of trust: When the bank redirects customers to a site outside the bank's domain for certain transactions without warning, it has failed to maintain a context for good security decisions, Prakash says. He found this problem in 30 percent of the banks surveyed. Often the look of the site changes, as well as URL and it's hard for the user to know whether to trust this new site. The solution, Prakash says, is to warn users they'll be moving off the bank's site to a trusted new site. Or the bank could house all of its pages on the same server. This problem often arises when banks outsource some security functions.

• Allowing inadequate user IDs and passwords: Researchers looked for sites that use social security numbers or e-mail addresses as user ids. While this information is easy for customers to remember, it's also easy to guess or find out. Researchers also looked for sites that didn't state a policy on passwords or that allowed weak passwords. Twenty-eight percent of sites surveyed had one of these flaws.

• E-mailing security-sensitive information insecurely: The e-mail data path is generally not secure, Prakash says, yet 31 percent of bank Web sites had this flaw. These banks offered to e-mail passwords or statements. In the case of statements, users often weren't told whether they would receive a link, the actual statement, or a notification that the statement was available. A notification isn't a problem, but e-mailing a password, a link or a statement, isn't a good idea, Prakash says.

Prakash initiated this study after noticing flaws on his own financial institutions' Web sites. The paper is "Analyzing Web sites for user-visible security design flaws." Falk and Borders are students in the Department of Electrical Engineering and Computer Science.

Provieded by University of Michigan