Flaw found in securing online transactions

February 16 2012

Researchers on Wednesday revealed a flaw in the way data is scrambled to protect the privacy of online banking, shopping and other kinds of sensitive exchanges.

Researchers on Wednesday revealed a flaw in the way data is scrambled to protect the privacy of online banking, shopping and other kinds of sensitive exchanges.

A program used to generate random number sequences for encrypting digital information worked properly 99.8 percent of the time, meaning that two out of every thousand "keys" wouldn't thwart crooks or spies, the report warned.

"We found that the vast majority of public keys work as intended," said a report based on work by a team of US and European researchers led by Arjen Lenstra of Ecole Polytechnique Federale de Lausanne (EPFL).

"A more disconcerting finding is that two out of every one thousand RSA moduli that we collected offer no security."

Online rights champion Electronic Frontier Foundation (EFF) supplied key data for the research, and said that Lenstra's team found tens of thousands of keys that essentially failed to guard data in supposedly encrypted online sessions.

"The consequences of these vulnerabilities are extremely serious," the EFF's Dan Auerbach and Peter Eckersley said in a blog post.

"In all cases, a weak key would allow an eavesdropper on the network to learn confidential information, such as passwords or the content of messages, exchanged with a vulnerable server."

Hackers could also pose as trusted websites, such as an online bank, in what are referred to as man-in-the-middle attacks, according to the EFF.

The non-profit EFF said it is working "around the clock" with EPFL to warn operators of computer servers using encryption keys offering no protection.