Cyber attack on Europe exposes big flaws in Internet security

September 12 2011, By Ken Dilanian

A major cyber attack in Europe that apparently was launched from Iran has revealed significant vulnerabilities in the Internet security systems used to authenticate websites for banking, email and e-commerce around the world.

The attack over the summer wrought havoc in the Netherlands, where the Justice Minister warned the public last Sunday that the only secure way to communicate with the Dutch government was with pen, paper and fax machine.

The digital assault compromised a Dutch company called DigiNotar, which issues digital certificates, small pieces of computer code that assure browsers that a website is what it appears to be. The certificates also encrypt communications between the user and the site so that they can't be intercepted.

The Dutch government has seized control of DigiNotar, which was recently purchased by Vasco Data Security, a Chicago-based company that specializes in Web authentication. Vasco said in a statement that it had not integrated DigiNotar's products with its own.

The attackers produced 531 fake DigiNotar certificates for heavily used websites, including Google, Microsoft, Twitter and Facebook - as well as the public websites for the CIA, and the spy services for Britain and Israel, according to an interim audit by Fox-IT, a Dutch security company.

The audit showed that nearly all the 300,000 IP addresses using the bogus certificates to visit Google in a single day originated in Iran. On Thursday, Google instructed Iranians to change their Gmail passwords.

Iran's uranium enrichment program was targeted in 2009 by Stuxnet, a highly sophisticated cyber weapon that sent nuclear centrifuges spinning out of control. Outside experts who have studied the case believe U.S. and Israeli engineers designed the worm to derail Iran's nuclear program, but neither government has acknowledged responsibility.

In the latest case, a hacker who said he was a 21-year-old Iranian acting alone, posted comments claiming responsibility for the attack. His identity is unknown, but many U.S. experts are convinced that Iran's government directed the massive operation in an effort to spy on its citizens and ferret out political dissidents.

In April this year, the same hacker claimed credit for an attack on Comodo, an Internet security company based in Jersey City, N.J. In that case, nine certificates were forged, the company said.

The company said the perpetrator had "executed its attacks with clinical accuracy," and that "circumstantial evidence" suggests the attack originated in Iran and was likely "a state-driven attack."

Communications, rather than financial domains, were targeted in both the April attack and the latest cyber invasion, said Roel Schouwenberg, a security specialist with Kaspersky Lab, a Russian-based computer security firm with regional offices in Woburn, Mass.

"It's not about finance," he said. "It's all very clearly aimed towards intelligence, and this has all the hallmarks of a government operation."

Whatever the motivation, the Dutch government, which uses DigiNotar

certificates, announced last week that it could no longer trust the security of its own websites, a move that threw communications in the Netherlands into chaos. Dutch lawyers were told to file court documents on paper, for example.

"What somebody has figured out - and if it's the Iranians, that means the Chinese and the Russians, have figured it out too - is that if you can compromise this infrastructure, you immediately get access to all sorts of cool things and people don't necessarily know about it," said Jim Lewis, a cyber expert at the Washington-based Center for Strategic and International Studies.

"This is big deal," said Joel Brenner, former general counsel of the National Security Agency, the Pentagon agency responsible for protecting government communications. "The certificate authorities vouch for who's who. If you can penetrate a certificate authority and falsify certificates, then nobody knows who they are dealing with. You've got to suspect a security service is behind this."

The Fox-IT audit accused DigiNotar of lax security procedures, and the company's certificates were not widely used in the U.S. But experts worry that some of the 500 other providers of certificates also may be compromised.

A Belgium-based company, GlobalSign, suspended production of new certificates last Monday after the hacker claimed to have penetrated it as well. The company said it plans to restore service next Monday, saying it had been the victim of "an industrywide attack."

"What this means is that anybody who uses those certificates cannot be assured of the person who is on the other end," said Jeff Hudson, chief operating officer of Venafi, an encryption company based in Sandy, Utah, that produces software that manages digital certificates. "The

whole trust model gets a little shaky. Nobody thought this was going to happen and people aren't ready for it."

VeriSign, which is the largest certificate provider in the United States and is owned by security software giant Symantec Corp., based in Mountain View, Calif., says it is confident it can withstand a cyber attack.

"Not all certificate authorities are created equal," said Michael Lin, senior director of product management at Symantec. "We've invested heavily in what we feel is a very secure, very robust infrastructure that protects us from these types of attacks."

But hackers have broken into some of the most trusted names in computer security.

In March, RSA was the victim of an attack that stole information related to the company's SecurID two-factor authentication products. SecurID adds an extra layer of protection to a login process by requiring users to enter a secret code number displayed on a key fob.

Attacks against three major U.S. defense contractors that used the compromised technology - Lockheed Martin, L-3 Communications and Northrop Grumman - were later discovered, and traced to servers in China.