By Joseph Menn
Sun Sep 8, 2013 9:25am IST

reuters.com

Internet experts want security revamp after NSA revelations

A general view of the large former monitoring base of the U.S. intelligence organization National Security Agency (NSA) in Bad Aibling south of Munich, June 18, 2013. Credit: Reuters/Michaela Rehle

(Reuters) - Internet security experts are calling for a campaign to rewrite Web security in the wake of disclosures that the U.S. National Security Agency has developed the capability to break encryption protecting millions of sites.

But they acknowledged the task won't be easy, in part because internet security has relied heavily on brilliant government scientists who now appear suspect to many.

Leading technologists said they felt betrayed that the NSA, which has contributed to some important security standards, was trying to ensure they stayed weak enough that the agency could break them. Some said they were stunned that the government would value its monitoring ability so much that it was willing to reduce everyone's security.

"We had the assumption that they could use their capacity to make weak standards, but that would make everyone in the U.S. insecure," said Johns Hopkins cryptography professor Matthew Green. "We thought they would never be crazy enough to shoot out the ground they were standing on, and now we're not so sure."

The head of the volunteer group in charge of the Internet's fundamental technology rules told Reuters on Saturday that the panel will intensify its work to add encryption to basic Web traffic and to strengthen the so-called secure sockets layer, which guards banking, email and other pages beginning with Https.

"This is one instance of the dangers that we face in the networked age," said Jari Arkko, an Ericsson scientist who chairs the Internet Engineering Task Force. "We have to respond to the new threats."

Other experts likewise responded sharply to media reports based on documents from former NSA contractor Edward Snowden showing the NSA has manipulated standards.

Documents provided to The Guardian, the New York Times and others by Snowden and published on Thursday show that the agency worked to insert vulnerabilities in commercial encryption gear, covertly influence other designs to allow for future entry, and weaken industry-wide standards to the agency's benefit.

In combination with other techniques, those efforts led the NSA to claim internally that it had the ability to access many forms of internet traffic that had been widely believed to be secure, including at least some virtual private networks, which set up secure tunnels on the Internet, and the broad security level of the secure sockets layer Web, used for online banking and the like.

The office of the Director of National Intelligence said Friday that the NSA "would not be doing its job" if it did not try to counter the use of encryption by such adversaries as "terrorists, cybercriminals, human traffickers and others."

Green and others said a great number of security protocols needed to be written "from scratch" without government help.

Vint Cerf, author of the some of the core internet protocols, said that he didn't know whether the NSA had truly wreaked much damage, underscoring the uncertainty in the new reports about what use the NSA has made of its abilities.

"There has long been a tension between the mission to conduct surveillance and the mission to protect communication, and that tension resolved some time ago in favor of protection at least for American communications," Cerf said.

Yet Cerf's employer Google Inc confirmed it is racing to encrypt data flowing between its data centers, a process that was ramped up after Snowden's documents began coming to light in June.

Author Bruce Schneier, one of the most admired figures in modern cryptography, wrote in a Guardian column that the NSA "has undermined a fundamental social contract" and that engineers elsewhere had a "moral duty" to take back the Internet.

RELYING ON NSA FOR HELP

But all those interviewed warned that rewriting Web security would be extremely difficult.

Mike Belshe, a former Google engineer who has spearheaded the IETF drive to encrypt regular Web traffic, said that his plan had been "watered down" in the committee process during the past few years as some companies looked after their own interests more than users.

Another problem is the relatively small number of mathematical experts working outside the NSA.

"A lot of our foundational technologies for securing the Net have come through the government," said researcher Dan Kaminsky, famed for finding a critical flaw in the way users are steered to the website they seek. "They have the best minds in the country, but their advice is now suspect."

Finally, governments around the world, including democracies, are asserting more authority over the Internet, in some cases forbidding the use of virtual private networks.

"As much as I want to say this is a technology problem we can address, if the nation states decide security isn't something we're allowed to have, then we're in trouble," Kaminsky said. "If

security is outlawed, only outlaws will have security."