US, British spy agencies crack Web encryption

WASHINGTON, USA: US and British intelligence agencies have cracked the encryption that secures a wide range of online communications including emails, banking transactions and phone conversations, according to newly leaked documents.

The documents provided by former US intelligence contractor Edward Snowden to The New York Times, ProPublica and The Guardian suggest that the spy agencies are able to decipher data even with the supposedly secure encryption to make it private.

The US National Security Agency, working with its British counterpart, GCHQ, accomplished the feat by using supercomputers, court orders, and some co-operation from technology companies, the documents indicate.

If the reports are accurate, the highly secretive programme would defeat much of the protection that is used to keep data secure and private on the Internet, from emails to chats or communications using smartphones.

The Guardian report said the two spy agencies had "covert partnerships" with technology companies and Internet providers which allows the insertion of "secret vulnerabilities - known as back doors or trap doors - into commercial encryption software."

"It's pretty shocking," said Joseph Hall of the Center for Democracy and Technology, a digital rights organisation. Hall told AFP that if the reports are true, it means that the elements that keep information secure in transit are fundamentally undermined.

Explosive revelations

Bruce Schneier, a cryptographic specialist who follows national security issues, called the revelations "explosive."

"Basically, the NSA is able to decrypt most of the Internet. They're doing it primarily by cheating, not by mathematics,"

Schneier wrote on his blog.

Schneier, who has been working with The Guardian's Glenn Greenwald, also wrote in a commentary on the British newspaper's website: "This is not the Internet the world needs, or the Internet its creators envisaged. We need to take it back."

The reports noted that US intelligence officials asked the Times and ProPublica not to publish articles on the subject, fearing it would prompt foreign targets to switch to new forms of encryption or communications that would be harder to collect or read.

ProPublica, an independent, non-profit organisation devoted to investigative journalism, which has partnered with The Guardian and The New York Times to review documents from Snowden, said it decided to go ahead with the article because of its importance to the public.

"The story, we believe, is an important one. It shows that the expectations of millions of Internet users regarding the privacy of their electronic communications are mistaken," ProPublica's editors said in a note.

"These expectations guide the practices of private individuals and businesses, most of them innocent of any wrongdoing. The potential for abuse of such extraordinary capabilities for surveillance, including for political purposes, is considerable," ProPublica's editors said.

The reports said the NSA has been working on breaking Internet encryption for more than a decade after the agency lost a battle to force technology companies to provide encryption "keys."

The New York Times report noted that while the ability to break encryption can be used to thwart terror plots, it can have unintended effects by weakening the security of communications.

"The risk is that when you build a back door into systems, you're not the only one to exploit it," cryptography researcher Matthew Green told the daily. "Those back doors could work against US communications, too."

Contacted by AFP, US intelligence officials had no comment on the reports.

Source: AFP via I-Net Bridge