

World's toughest encryption scheme found 'vulnerable'

August 23 2011, by Jennifer Seberry, Professor of Computer Security at University of Wollongong

It was [announced](#) last week that cryptography researchers have found a “vulnerability” in the encryption scheme used in the vast majority of secure online transactions – a scheme known as [AES-256](#).

Every important electronic transaction you make online is encrypted – your banking, your census form, your credit card payments.

AES-256 – the Advanced Encryption Standard – was approved by the US National Institute of Standards in 2002 to be used in all unclassified communications.

As well as its almost almost-ubiquitous use in e-commerce, AES-256 is used to secure household WiFi connections, mobile phone connections and a range of other applications.

So how does AES-256 work?

Simply, it takes the data you are trying to encrypt – your online banking username and password, for example – and scrambles it with with a secret “key” 256 bits in length.

If you know the encryption key (as the bank does) then you can decrypt the scrambled information and use it accordingly – logging you in, in the case of online banking.

Firstly, it's worth noting that the recent attack was part of a program undertaken by renowned cryptanalysts at Microsoft and the Katholieke Universiteit of Leuven in Belgium – a university famous for its design and analysis of cryptographic algorithms.

This is an attack by the “good guys” to determine how hard it would be for someone with less-than-noble intentions to access encrypted information.

Media reports suggest the researchers found a way of decrypting AES that is three to five times faster than any previous method.

Fine. Good. But let's put that into context.

Until this new development, any attempts to decrypt information encrypted with AES-256 would have taken many times the length of the universe to carry out. This is due simply to the number of possible encryption keys that need to be guessed.

Three or four times faster than the age of the universe is still billions of years and as a result, circumventing AES-256 encryption is still incredibly impractical, to put it mildly.

Even if the largest botnet ever discovered – the 30-million-computer-strong [Bredolab](#) botnet – was given the task of attacking an AES-256 implementation, the sheer number of possible combinations would make the task virtually impossible.

So, should you be worried about your electronic transactions being insecure? At the moment, no.

The newly-discovered vulnerability is certainly interesting but plenty of further study is needed before we are even close to thinking AES

implementations are insecure.

This story has been republished from [The Conversation](#) (theconversation.edu.au). [licensed under Creative Commons — Attribution/No derivatives]

More information: Research paper research.microsoft.com/en-us/p..._yptanalysis/aes.aspx

Source: The Conversation

Citation: World's toughest encryption scheme found 'vulnerable' (2011, August 23) retrieved 19 July 2024 from <https://phys.org/news/2011-08-world-toughest-encryption-scheme-vulnerable.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--