# World's toughest encryption scheme found 'vulnerable'

23 August 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.

If you don't know the encryption key and want to get access to it, you effectively need to try all of the possible combinations - a so-called "brute force" attack.

Being a 256-bit key, there are a lot of possible combinations: $2^{256}$ to be precise or, written in it's full form: 116,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000.

That's more than the number of atoms in the entire universe.

AES emerged from a competition in which cryptographers were asked to submit their attempt at a secure encryption scheme. Fifteen submissions from all around the world were considered, including one called LOKI which was developed by myself and my colleagues.

After a lengthy analysis process by academics and government agencies the winning algorithm - known as Rijndael - became the new international encryption standard.

Academics and government analysts continue to study algorithms - such as AES-256 - long after they have been deployed by industry as there is always new research and new improvements in computer technology that might make an algorithm insecure.

Academics say an algorithm is "broken" if it has a "certification weakness". Simply, an encryption implementation is said to have a certification weakness if the content of the encrypted message can be read in less time than it would take to try every possible key.

So what does the vulnerability discovered in AES-256 mean for those of us using online transactions?

Firstly, it's worth noting that the recent attack was part of a program undertaken by renowned cryptanalysists 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 you 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.



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

Source: The Conservation