1-1-2011

Cracking bin Laden's computer code: unlikely

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Cracking bin Laden's computer code: unlikely

Abstract

It has been reported that Osama bin Laden's hard drives have been seized, hard drives that could conceivably contain information regarding the membership, funding and future plans of al-Qaeda. Information of this type would help anti-terrorism agencies enormously. The hard drives were recovered from bin Laden's compound in the Pakistani city of Abbottabad and are said to be encrypted with a encryption method known as AES-256. AES-256 is the current world standard for data encryption and is used by the likes of Wikileaks and the US Government to encrypt sensitive information.

Keywords

bin, cracking, laden, computer, code, unlikely

Disciplines

Engineering | Science and Technology Studies

Publication Details

Seberry, J. (2011). Cracking bin Laden's computer code: unlikely. The Conversation, (06 May),

6 May 2011, 10.50am AEST

Cracking bin Laden's computer code: unlikely

Author

1. 

   Jennifer Seberry

   Professor of Computer Security at University of Wollongong

Disclosure Statement

Jennifer Seberry receives funding from the ARC.

UNIVERSITY OF WOLLONGONG Provides funding as a Member of The Conversation.

uow.edu.au

Recovering information from Osama's hard drives may be impossible. wokka/Flickr

It has been reported that Osama bin Laden's hard drives have been seized, hard drives that could conceivably contain information regarding the membership, funding and future plans of al-Qaeda.

Information of this type would help anti-terrorism agencies enormously.

The hard drives were recovered from bin Laden's compound in the Pakistani city of Abbottabad and are said to be encrypted with a encryption method known as AES-256.

AES-256 is the current world standard for data encryption and is used by the likes of Wikileaks and the US Government to encrypt sensitive information.

How it works

To understand how encryption works, you first need to understand binary.

The smallest possible piece of digital information is known as a bit. This piece of information can have one of two states: off or on, 0 or 1.

Computer encryption works by taking data in this binary form – a stream of 0s and 1s – breaking it into blocks 256 bits long and then entering this block into a special encryption algorithm.

This algorithm is designed to cause as much confusion as possible by using a "secret key" which also comprises 256 bits of binary data.

If you know the encryption key you can "decrypt" the data and return it to its original form. For this reason, encryption keys are kept secret.

(This short animation created by Enrique Zabala from Paraguay demonstrates just how complicated the AES encryption process actually is.)

Data encryption using the AES is ubiquitous. It is used by banks, business, governments, and in computer programs such as Skype.

Where did AES come from?

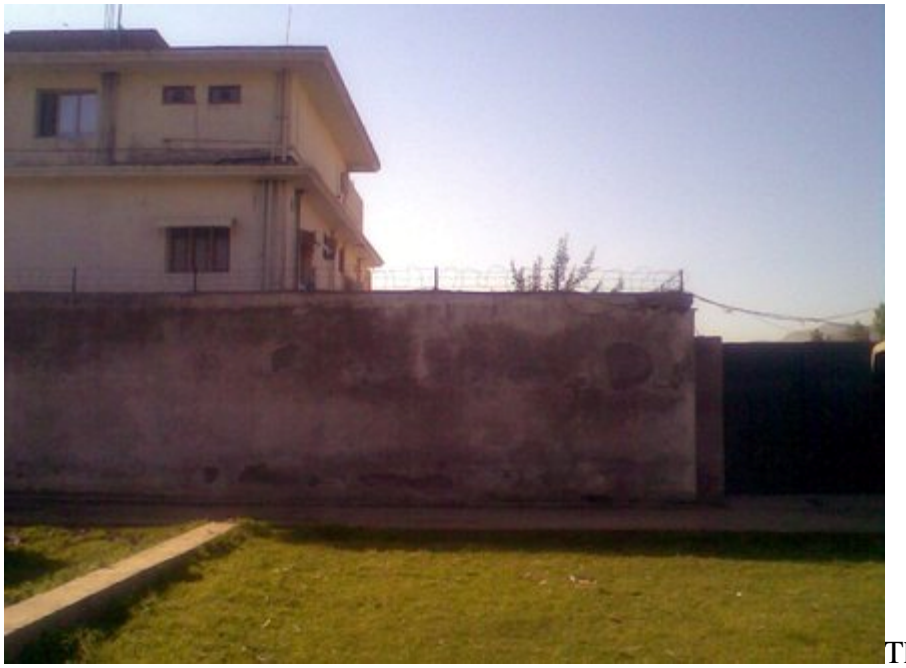
In 1997, representatives of the US Department of Commerce called for cryptologists around the world to submit an encryption algorithm that would replace the previous standard: Data Encryption Standard (DES).

As director of the Centre for Computer Security Research at the University of Wollongong, I was part of a research group that submitted an entry, called LOKI, a symmetric encryption algorithm.

Our algorithm was quickly removed from contention in the global competition as other researchers found ways to get around our encryption method.

The winning algorithm – developed by two Belgian cryptologists, Joan Daemon and Vincent Rijmen, and known as Rijndael – was selected by the cryptographic world community and announced by the US Government as its Federal standard on May 26 2002.

The name Rijndael was chosen as a combination of the authors' names and as a gentle poke at the fact few people can pronounce Flemish names without getting their tongues-tied.


The compound in Abbottabad, Pakistan, where bin Laden was killed on May 2. EPA

Getting bin Laden's data

Because the US Government was involved in the creation of this encryption scheme, there have been rumours in recent days that they may have covertly engineered a so-called "backdoor" into AES-256, allowing top US officials to decrypt any data encrypted using this method.

I personally don't believe this "backdoor" exists, for the following reasons:

1) The open process by which candidate algorithms were submitted and analysed by the world cryptographic community would seem to render this impossible.

2) The fact the technology has been widely accepted by many, non-American governments (and apparently bin Laden) would suggest its robustness.

3) The process used in the encryption is both "state-of-the-art" and, in computing terms, "best practice", which would make vulnerabilities of the type allowing a "backdoor" unlikely.

Assuming bin Laden's files are indeed encrypted using AES-256, the only way I can see to break the encryption would be to use a painstaking "brute force" technique.

This would involve trying all of the 2^{256} possible encryption keys. This works out at 1.16×10^{77} different codes to try (the number one with 77 zeroes after it).

This process would require hundreds of thousands of specially-built machines, the likes of which do not currently exist. Even if they did, we would need many, many times the length of the universe's lifespan to carry out the search.

In other words, it's not going to happen.

Assuming bin Laden's data is encrypted using the AES-256 method, the US will be lucky to learn anything from his hard drives about al-Qaeda's plans.