;login:

THE MAGAZINE OF USENIX & SAGE

February 2001 • volume 26 • number 1

inside:

EDGAR DANIELYAN:
AES: ADVANCED ENCRYPTION
STANDARD IS COMING

USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

AES: advanced encryption standard is coming

by Edgar Danielyan

Edgar Danielyan CCDP, CCNP(Security) is a UNIX and internetworking consultant. His interests include Internet security, privacy, and their social and legal aspects.

<edd@danielyan.com>

Much has changed since introduction of the Data Encryption Standard (DES) in 1977. Hardware is faster and cheaper, memory is plentiful and cheap, and use of computer networks in all areas of human activity is increasing. This is the good news; the bad news is that it all comes at a cost – in many cases the cost is security.

Widely used DES has been proven, on several occasions, to be inadequate for many applications – especially those involving transmission of sensitive information over public networks such as the Internet, where the entire transmission may be intercepted and cryptoanalyzed. Specialized hardware has been built which can determine a 56-bit DES key in a few hours. All these considerations signaled that a new standard algorithm and longer keys were necessary.

Fortunately, in January 1997, the National Institute of Standards and Technology (NIST) realized that it was time for a new encryption standard – Advanced Encryption Standard – and issued a call for candidate algorithm nominations in September 1997. The deadline for submissions was June 1998, and a total of 15 algorithms were submitted for consideration. What follows is the timeline of events and a brief non-mathematical description of the Rijndael algorithm, which was chosen as the proposed Advanced Encryption Standard (AES) in October 2000.

Below is a timeline of the process, followed by a summary of the final technique chosen for encryption in the 21st century.

Timeline

April 1997
NIST organizes a workshop to consider criteria and submission guidelines of candidate algorithms.

September 1997
An official call for nominations is published in the Federal Register.

June 1998
By June 1998, 15 algorithms have been submitted to the NIST for consideration:

- CAST-256 (Entrust Technologies)
- CRYPTON (Future Systems)
- DEAL (Richard Outerbridge, Lars Knudsen)
- DFC (National Centre for Scientific Research, France)
- E2 (NTT)
- FROG (TecApro Internacional)
- HPC (Rich Schroeppel)
- LOKI97 (Lawrie Brown, Josef Pieprzyk, Jennifer Seberry)
- MAGENTA (Deutsche Telekom)
- Mars (IBM)
- RC6 (RSA)
- Rijndael (Joan Daemen, Vincent Rijmen)
- Safer+ (Cylink)
- Serpent (Ross Anderson, Eli Biham, Lars Knudsen)

- Twofish (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson)

August 1998
First AES candidate conference is held in California.

September 1998
NIST asks for public comment on the 15 submitted algorithms and sets the date for the second AES candidate conference.

March 1999
Second AES conference is held in Rome, Italy, to consider comments and analyses of the 15 candidate algorithms. Additionally, the candidate algorithms are tested from both cryptographical and performance viewpoints. One of the original NIST requirements for the algorithm was that it had to be efficient both in software and hardware implementations. Java and C reference implementations are used for performance analysis of the algorithms.

August 1999
NIST press release announces the selection of five out of 15 algorithms which survived rigorous testing and cryptoanalysis. The selected algorithms are Mars, RC6, Rijndael, Serpent, and Twofish. These algorithms are accepted as cryptographically strong and flexible, as well as able to be efficiently implemented in software and hardware.

September 1999
Call for public comments on the finalist candidates is published in the Federal Register.

April 2000
Third AES conference held in NYC.

August 2000
National Security Agency develops and publishes VHDL model for algorithm's performance testing when implemented in hardware.

October 2000
NIST press release announces the selection of Rijndael as the proposed Advanced Encryption Standard.

Rijndael

Rijndael (pronounced, according to the authors, as either "Reign Dahl," "Rain Doll," or "Rhine Dahl") was designed by Joan Daemen, Ph.D. (Proton World International, Belgium) and Dr. Vincent Rijmen (Catholic University of Leuven, Belgium). Both authors are internationally known cryptographers. Rijndael is an efficient, symmetric block cipher. It supports key and block sizes of 128, 192, and 256 bits. Main design goals for the algorithm were simplicity, performance, and strength (i.e., resistance against cryptoanalysis). When used in CBC MAC mode, Rijndael can be used as a MAC algorithm; it also may be used as a hash function and as a pseudo random number generator. In their specification of the algorithm, the authors specifically state the strength of Rijndael against differential, truncated differential, linear, interpolation, and Square attacks. While Rijndael is not based on Square, some ideas from Square design are used in Rijndael. Of course, the length of the key used is also very important, especially since the most efficient known attack against Rijndael is exhaustive key searching. It would take 2^{255} runs of Rijndael to find a key 256 bits long. To the credit of the authors, Rijndael does not use "parts" or tables from other algorithms, which makes it easy to implement alone (especially in hardware, such as smart cards). Rijndael also fully satisfies the requirement for an algorithm which may be efficiently and easily implemented in both hardware and software.

Summary

It is expected that AES will be officially published as a Federal Information Processing Standard (FIPS) in April–June 2001, and implementations of AES in various security systems probably will pop up shortly thereafter. In the meantime authoritative information on AES developments may be found on NIST's Web site at <*http://csrc.nist.gov/encryption/aes/*>. The full mathematical specification of the algorithm and reference implementations in C and Java are also available from the same Web site.