Global Information Assurance Certification Paper

Advancement in Advance Encryption Standard (AES)

On October 2, 2000**,** the National Institute of Standards and Technology (NIST), an agency of the Commerce Department's Technology Administration, announced its selection of the "Rijndael" cryptographic algorithm for the proposed Advanced Encryption Standard.[1] This announcement marks a major milestone in the security industry. As previously discussed within SANS, "Rijndael" was one of the five finalists in the 1997 NIST contest to replace DES and to potentially become the de facto world wide standard.[2]

The purpose of this document is to highlight and expand upon a number of significant insights that Harish Bhatt and Stepehen Northcutt have made in the SANS Encryption II course. Perhaps the most important lesson taught relative to AES was that the secret to ultimately ensuring secrecy is developing an algorithm in an open manner. The strength of the algorithm improves under the intense public scrutiny of the global cryptographic community.[3] Other important concepts that will be explored include identifying why Rijndael was chosen over the other finalists and summarizing the impact that AES will have on security throughout the world.

Rijndael was devised by a collaborative effort between two Belgium cryptographers. Dr Vinvent Rijmen is a researcher at the Computer Security and Industrial Cryptography (COSIC) research laboratory at the Electrotechnical Engineering Department of the Catholic University of Leuven.. Dr Joan Daemen is a member of Proton World International. [4] The name of the algorithm reflects the collaborative effort of the authors. (Note that the Rijndael Webpage states that the pronunciation is similar to "Rain Doll or Rhine Dhal"[5] Almost any pronunciation except "Region Deal" is ok with the author).

The importance of the international involvement and scrutiny was noted by Dr. Cheryl Shavers, the Under Secretary of Commerce for Technology, at the AES press briefing on October 2nd, 2000.[6] In fact, the NIST Advanced Encryption Standard Fact Sheet clearly indicated that "the involvement of the international crypto community has been necessary for the development of a high-quality standard." [7] The conclusion is that the strength of the algorithm is its worldwide exposure to scrutiny. Strength is not in the obscurity of the algorithm.

---

[1] P Bulman, *Commerce Department Announces Winner of Global Information Security Competition*, October 2, 2000 available at http://www.nist.gov/public_affairs/releases/g00-176.htm.
[2] *Rijndael Algorithm, Jointly Devised by Proton World Expert, Adopted as New World Standard*, October 3, 2000 available at http://www.protonworld.com/press/releasses/press69.htm
[3] Harish Bhatt, *SNAP - Introduction to Encryption II,* March 18, 2000 available at http://www.sans.org/momaudio/s=1.2.6/a=a0YlZCvcybv/encryption2
[4] *Rijndael Algorithm, Jointly Devised by Proton World Expert, Adopted as New World Standard*, October 3, 2000 available at http://www.protonworld.com/press/releasses/press69.htm
[5] Vincent Rijmen, *Rijndael FAQ*, October 3, 2000 available at http://www.esat.kuleuven.ac.be/~rijmen/rijndael
[6] Dr. Cheryl Shavers, *Advanced Encryption Standard (AES) Press Briefing*, October 2,2000 available at http://real.nist.gov/aes_briefing.htm
[7] *Advanced encryption Standard (AES) Fact Sheet*, October 3, 2000 available at http://csrc.nist.gov/encryption/aes/round2/aesfact.html

Now that this critical theme has been reiterated, let us consider some other factors that lead to its higher degree of protection than previously released algorithms such as DES. Note that the manner of development is actually critical to the creation of a strong algorithm.

The time that is estimated to crack AES is considerably higher than the estimate for cracking DES. DES keys are 56 bits long. AES will specify key sizes at 128, 192, and 256 bits. Even at the 128-bit specification, there are 10^{21} times more keys than DES has to offer. We are aware of "DES Crackers" that could recover a DES key after a few hours. Even if a method exists to recover a key in a second, it would still take 149 trillion years to crack the 128-bit AES key.[8] Note that even with these figures, the official press release from Proton World International states that "it is anticipated that AES will be used for the next 25-30 years".[9]

The October 2, 2000 NIST Report on the Development of the Advanced Encryption Standard (AES) clearly states that all five algorithms appear to have adequate security for AES.[10] Why then was Rijndael chosen? Insights are given by reviewing excerpts from the Summary Assessments of the Finalists.[11] Rijndael demonstrates above average encryption and decryption speed for 128-bit keys. It consistently has the fastest key setup of all finalists. Rijndael has very low RAM and ROM requirements and is very well suited to restricted space environments when either encryption or decryption is implemented. It had one of the best hardware throughputs of the finalists. It uses operations that are among the easiest to defend against power and timing attacks. The Report on the Development of the Advanced Encryption Standard concludes that "Rijndael's combination of security, performance, efficiency, implementability, and flexibility make it an appropriate selection for the AES for use in the technology of today and in the future"

We have established that Rijndael was chosen as the proposed AES algorithm, why the algorithm is stronger than predecessors such as DES, and what characteristics that distinguish it from its competitors. What does this all mean? Is Rijndael the replacement for DES? How will it be used?

It should be noted that the October 2, 2000 milestone indicates that NIST has met its objective in announcing its AES selection by the early fall of 2000.This does not mean that AES is now the official U.S. government standard. According to the AES Fact Sheet, a draft Federal Information Processing Standard (FIPS) will be published for public comments in November 2000 The comment period is scheduled to close in February 2001. It is anticipated that the standard will be adopted as an official

---

[8] *Advanced encryption Standard (AES) Fact Sheet*, October 3, 2000 available at http://csrc.nist.gov/encryption/aes/round2/aesfact.html

[9] *Rijndael Algorithm, Jointly Devised by Proton World Expert, Adopted as New World Standard*, October 3, 2000 available at http://www.protonworld.com/press/releasses/press69.htm

[10] *Report on the Development of the Advanced Encryption Standard (AES),* October 2, 2000 available at http://csrc.nist.gov/encryption/aes/round2/r2report.pdf

[11] *Report on the Development of the Advanced Encryption Standard (AES),* October 2, 2000 available at http://csrc.nist.gov/encryption/aes/round2/r2report.pdf

Government standard in the April-June 2001 timeframe. The standard will then be formally re-evaluated no less than every five years.[12]

After AES is published, it will be identified as an approved encryption algorithm that can be used by U.S Government organizations to protect sensitive information. Non-U.S. Government and commercial organizations are not required to use the algorithm, but are encouraged to do so. As the official Commerce Department press release notes, AES will replace the aging Data Encryption Standard (DES) which NIST adopted in 1977. Many government agencies are expected, but will not be required, to use the algorithm. It is anticipated that many financial institutions will use the algorithm. Since hundreds of encryption products currently employ DES technology, potentially millions of consumers and businesses will be affected by the selection of the Rijndael algorithm.[13]

In conclusion, the selection of the "Rijndael" cryptographic algorithm on October 2, 2000 will have a major impact on security strategies that will be used in the beginning of the twenty-first century. The strength of the algorithm is largely due to the manner in which it was developed and reviewed. Although all finalists in the NIST contest appear to have a secure solution, the "Rijndeal" algorithm offered the best overall algorithm for the Advanced Encryption Standard.

[12] *Advanced encryption Standard (AES) Fact Sheet*, October 3, 2000 available at http://csrc.nist.gov/encryption/aes/round2/aesfact.html

[13] P Bulman, *Commerce Department Announces Winner of Global Information Security Competition*, October 2, 2000 available at http://www.nist.gov/public_affairs/releases/g00-176.htm.

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor