Interested in learning more about security?

SANS Institute InfoSec Reading Room

The Day DES Died

Everyone knows how important it is to encrypt private or sensitive data as it transfers over the public Internet. There are several different types of encryption including symmetric, asymmetric, and hash algorithms. Key lengths of 1,024 bits and cipher strength of 128 bits are to be used at minimum. We know this because DES, previously known as a U.S. Department of Commerce standard, has been broken during the course of public challenges sponsored by RSA Security. How was DES broken? How do you know what cryptosystems ...

The Day DES Died

Version 1.0

Prepared by

Paul Van De Zande

For

GSEC Practical

July 22, 2001

Introduction

Everyone knows how important it is to encrypt private or sensitive data as it transfers over the public Internet. There are several different types of encryption including symmetric, asymmetric, and hash algorithms. Key lengths of 1,024 bits and cipher strength of 128 bits are to be used at minimum. We know this because DES, previously known as a U.S. Department of Commerce standard, has been broken during the course of public challenges sponsored by RSA Security.

How was DES broken? How do you know what cryptosystems work? Which ones are best? This paper won't answer all those questions, but it will take a closer look at DES. The characteristics of the RSA challenges will be discussed. Finally, we'll compare DES to other cryptosystems to discover which ones are secure and why. Understanding more about this long-term standard encryption algorithm may help to secure implementations of cryptography in your environment. I hope that you'll find this paper interesting and a little fun too!

History of DES

The organization known today as NIST (National Institute of Standards and Technology) requested proposals for cryptographic algorithms that would be considered for national standard in 1972. The algorithm had to be inexpensive, widely available to the public, easily integrated with business applications, and secure. Two years later, IBM submitted the Lucifer algorithm for analysis. Assisted by the NSA (National Security Agency), NIST evaluated Lucifer based on criteria specified in the proposal.

After two years of analysis, NIST reduced the 128-bit key length to 56-bits, changed the name to Data Encryption Standard, and declared DES a national standard on November 23, 1976. The evaluation of Lucifer was "troubled" by mistrust and widespread public skepticism that manifested in accusations claiming NIST had reduced the key length and installed a "back door" to permit government eavesdropping and espionage. These accusations have never been proven. Fueled by government backing, acceptance of DES was promoted into various industries, especially finance and retail.

Since its introduction, DES's adequacy has been re-evaluated every five years.[1] Attacks to brute force guess DES encryption keys have been drawing attention since the specification was published in January of 1977. Until the computing power of the 1990's was realized, claims that DES encryption keys could be brute-force guessed were refuted. However, poorly implemented DES encryption solutions were found to be susceptible to attack.

[1] Loshin, Pete. "Cryptographic Turning Points." *Computerworld* 28 August 2000. 25 June 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO49003,00.html

Between 1997 and 1999, RSA sponsored a series of challenges designed to crack the DES algorithm. Each challenge was increasingly more difficult, requiring the contestants to find the DES encryption key in less time than was done in the previous challenge. All three challenges were met with success. More recently, in early 1999, Distributed.Net used the DES Cracker and a worldwide network of nearly 100,000 PCs to win the RSA DES Challenge III in a record breaking 22 hours and 15 minutes. The DES Cracker and PCs combined were testing 245 billion keys per second when the correct key was found.[2]

56-bit key lengths are no longer considered to have the capacity to withstand an attack. Unauthorized access to sensitive data and business applications requiring a higher-level of security are at risk. Consequently in 1997, NIST recommended that DES be retired and replaced with a stronger cryptographic algorithm. The new national standard would be called (Advanced Encryption Standard). Only recently has NIST adopted Rijndael as our national encryption standard, a block cipher having a key size between 128 and 256 bits, and absolutely no back doors.

The DES Algorithm

DES is a symmetric encryption algorithm that uses a single, 64-bit key to encrypt a 64-bit block of plaintext into a 64-bit block of ciphertext. With one parity bit for each byte of the key, the key strength is only 56-bits. DES operates in any of four modes: electronic code book, cipher block chaining, cipher feedback or output feedback.

Electronic code book mode uses a single 56-bit key to encrypt 64-bit blocks of plaintext until the message is encoded. Cipher block chaining mode improves on that approach by XORing the next block of plaintext with the last generated block of ciphertext. The XOR result is then encrypted with a 56-bit DES key. Cipher Feedback mode is used to encrypt blocks of plaintext less than 64-bits in size, and output feedback mode converts DES into a stream cipher.

DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the ciphertext. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially.[3]

Thousands of United States financial institutions offer privacy, confidentiality, and data integrity for approximately $2.3 trillion in daily fund transfers alone. This protection is offered through custom developed implementations of DES.

Cryptographers say steady increases in computer power and a trend to network computers have eroded the effectiveness of the DES algorithm. The risk doesn't come from casual

[2] Tropical Software. "DES Encryption." 25 June 2001. www.tropsoft.com/strongenc/des.html
[3] Tropical Software. "DES Encryption." 25 June 2001. www.tropsoft.com/strongenc/des.html

hackers, but from well-funded corporations and foreign intelligence agencies that are bent on economic espionage.[4]

Should U.S. financial institutions be afraid? Will foreign attackers who are economically challenged attempt to gain unauthorized access to this honeypot of U.S. fund transfers? What do you think? Many believe that all banks should immediately convert their application to integrate with triple-DES, which uses two or three different keys in three iterations of the DES algorithm. Triple-DES also offers a 128-bit key length.

On the other hand, Stephen T. Kent, chief scientist for security technology at Bolt Beranak and Newman, Inc. said the banking industry's interest in triple-DES is misplaced because triple-DES is aimed primarily at strengthening confidentiality, while the industry has traditionally been more worried about message integrity and user authentication. [5] So what's wrong with DES anyway, and how was it cracked? Let's take a closer look at how DES works and the RSA challenges that led to its ill repute.

The RSA Challenge

RSA first announced a public challenge to crack the DES encryption algorithm in late January 1997. Any individual or team that could decipher the encrypted message stood to gain a $10,000 prize. Four months later, the DES encryption key was found using the collective resources and computing power of literally thousands of computers. The RSA challenge was met and the message was decrypted. Protected by the DES algorithm, the encryption key that had deciphered the challenge message was only one of 72 quadrillion possibilities.

A programmer in Salt Lake City using a 90-MHz Pentium-based PC found the correct key after fewer than 25% of the potential combinations were attempted.[6] The story generated a flurry of claims that the RSA Challenge I was not representative of DES encryption techniques integrated in financial business applications. Others publicly discounted the results of the challenge stating that attackers have limited computing resources available to them, not a fleet of thousands of processors and unlimited memory capacity.

The voice of RSA Challenge supporters was heard equally as loud, and the message was clear: DES could not provide adequate protection to ensure security and privacy. In fact, many boasted that the time it took to discover a 56-bit DES encryption key could also be improved upon. RSA soon organized another challenge to find out.

---

[4] Anthes, Gary H. "Standard Encryption Vulnerable to Attack." *Computerworld* 12 February 1996. 25 June 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO13904,00.html

[5] Anthes, Gary H. "Security Upgrade Rattles Banking Industry." *Computerworld* 12 December 1994. 25 June 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO12049-,00.html

[6] Machlis, Sharon. "Effort To Crack DES Encryption A Success." *Computerworld* 20 June 1997. 25 June 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO21037-,00.html

The 2nd and 3rd Challenges

In response to doubts about the legitimacy of the first challenge, RSA used its popular data security conference as a format to launch DES Challenge II. The second challenge was issued during the opening ceremonies of an RSA Data Security Conference almost twelve months after the initial challenge was made public. That was January 13, 1998.

The second challenge would consist of an encrypted message being posted on the RSA web site. The randomly generated key would be immediately destroyed to prevent any possibility of unauthorized disclosure or misuse. The fist message was available from www.rsa.com later that same day, and the second message was expected to be posted on the web exactly six months later on July 13, 1998.

The goal of each contest is not only to recover the secret key used to DES-encrypt a plain-text message, but to do so faster than previous winners in the series. As before, a cash prize will be awarded for the first correct entry received. Unlike previous contests, the amount of the prize will be based on how quickly the key is recovered.[7]

With the benchmark from RSA Challenge I set at ninety days, the contestants needed to beat that time by 25% to get any cash reward. If the time improved only 25%, $1,000 was awarded. Further motivation and potential capital for additional computer resources was warranted in larger cash prizes. $5,000 if the DES key was found in half the time (or 45 days) and $10,000 if found in only a quarter of the previous time or less. Only the first correct entry would receive a prize.

The first of two secret challenge messages was cracked again by Distributed.Net in 41 days. The attack team that won the second challenge was equally well prepared. The EFF (Electronic Frontier Foundation) developed a computer specifically designed to crack DES. Their efforts and investment were proven worthwhile when their "cracker" delivered the secret encryption key for the second secret challenge message in only 56 hours.

For the third challenge, Distributed.Net and the EFF combined their forces and collective resources to enter the contest. Using another custom designed network of computers, fondly named "Deep Crack", 245 billion DES keys were tested each second to win RSA DES challenge III in less than half of the previously recorded time.

On that 19th day of January, 1999, the secret message "See you in Rome" was unveiled as the answer to the third DES challenge. Rome hosted the 2nd AES conference where five potential DES replacements were discussed and analyzed by cryptographic experts. John Gilmore, EFF co-founder and project leader, said "the government's current encryption policies favoring DES risk the security of the national and world infrastructure." [8] All

[7] RSA Security. "RSA to Launch 'DES Challenge II' at Data Security Conference."
17 December 1997. 25 June 2001. www.rsasecurity.com/news/pr/971217.html
[8] RSA Security. "RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF)." 19 January 1999. 25 June 2001. www.rassecurity.com/news/pr/990119-1.html

who attended the RSA Data Security Conference that day in San Jose heard the message loud and clear.

In all three RSA challenges, DES was cracked by launching an exhaustive, brute-force search for the secret key. This attack technique examines all 72 quadrillion possible key values until the correct key is found to decrypt the ciphertext. A brute-force key search is possible against any encryption algorithm, and is likely to become more commonplace.

How Strong Is Encryption?

The strength of an encryption algorithm is measured by two factors: the effective length of the key and its ability to withstand attack. That ability is ultimately dependent upon its implementation. A critical component of any cryptographic implementation is the key management techniques used. A key management strategy answers the questions: what key is used how often? Where is it stored and who has access to it? How is it to be kept secret?

Encryption keys must often be shared or distributed for an effective implementation. In these cases, public/private key pairs can be generated to secure key distribution. As a DES encryption key is generated, it can be encrypted by the recipient's public key before it is sent. The private keys used for distribution and decryption should have restricted access and be changed as often as needed to ensure adequate privacy and security.

A DES symmetric key can also be used to encrypt data to be stored on file systems or in databases. Again the secret key should have limited access and change periodically. One approach is to define a usage pattern for multiple keys, and encrypt all keys with a master key having stronger encryption. Master keys can be changed more often with less effort. The basic concept here is that a moving target is harder to shoot.

DES Compared

Several variants of DES have been developed since the encryption algorithm was first announced back in the late 70's. DESX is a variant that depends on the generation of two 64-bit encryption keys: K1 and K2. The plaintext is first XORed with K1, encrypted by DES, and the resulting ciphertext is XORed with K2. DESX provides an effective key size of about 120 bits for exhaustive search – with essentially no impact on encryption and decryption time.[9]

G-DES is another variant that applies the same 16 rounds of the main DES algorithm using encryption keys with a larger block size. It has been demonstrated that G-DES is unable to withstand attack using its recommended parameter sizes for encryption keys.

Another approach uses a DES key to generate sixteen 48-bit subkeys for use in each of the 16 rounds of the main DES algorithm. Although this approach makes a brute-force key search more difficult, it is still subject to differential and linear attacks as is DES.

[9] Kaliski,Burt. "Life After DES." 11 July 2001. www.rsasecurity.com/rsalabs/des3/des3_bk.html

Triple-DES can also be considered a DES variant since it is intended to execute the main DES algorithm three times, using a different key each time. Triple-DES gives up 16 bits for parity leaving an effective key size of 112 bits. The turnaround time for encryption and decryption is not improved, therefore performance should be carefully considered. Triple-DES can even be implemented to be backward compatible with DES, and still be considered strong. Triple-DES has not been successfully cracked.

Conclusion

The primary conclusion to be drawn from this paper is that encryption algorithms with fixed-length key sizes will always be subject to brute-force key search attacks. Experts such as Bruce Schneier, founder and CTO of Counterpane, believe that a minimum key length of 90-bits is able to withstand attack for only another decade, perhaps a bit more.

Despite what everyone else tries to tell you, cryptographic key length has almost nothing to do with security. A short key means bad security, but a long key does not mean good security. Randomly generated keys aren't necessarily better, because now the random number generator must produce keys with maximum entropy. Entropy is a measure of uncertainty. The more uncertain something is, the more entropy there is in that thing.[10] In addition to being dependent upon the implementation of cryptography within a given business application, the chosen algorithm must make effective use of the key space.

Key management strategies should be defined at a high-level, incorporating appropriate flexibility to work with any business application, yet still provide security and privacy. The concept of a master key can be used to control access to application level encryption keys.

The ability for a cryptography implementation to withstand attack should be tested on a regular basis in conjunction with a review of the key management strategy. Proprietary encryption algorithms can not substantiate their true strength unless they are subjected to the public scrutiny of the cryptographic community.

The bottom line is that DES is dead and algorithms that sport a 56-bit fixed key length can not be counted on to protect security and privacy of sensitive or confidential data. I hope that you learned something new about cryptography, and enjoyed reading the paper as much as I did writing it. Perhaps AES will be the subject of my next paper?

[10] Schneier,Bruce. "Key Length And Security." 5 October 2000. 11 July 2001. http://www.counterpane.com/crypto-gram-9910.html#KeyLengthandSecurity

List of References

1. Loshin, Pete. "Cryptographic Turning Points." *Computerworld* 28 August 2000. 25 June 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO49003,00.html

2. Tropical Software. "DES Encryption." 25 June 2001. www.tropsoft.com/strongenc/des.html

3. Tropical Software. "DES Encryption." 25 June 2001. www.tropsoft.com/strongenc/des.html

4. Anthes, Gary H. "Standard Encryption Vulnerable to Attack." *Computerworld* 12 February 1996. 25 June 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO13904,00.html

5. Anthes, Gary H. "Security Upgrade Rattles Banking Industry." *Computerworld* 12 December 1994. 25 June 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO12049-,00.html

6. Machlis, Sharon. "Effort To Crack DES Encryption A Success." *Computerworld* 20 June 1997. 25 June 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO21037-,00.html

7. RSA Security. "RSA to Launch 'DES Challenge II' at Data Security Conference." 17 December 1997. 25 June 2001. www.rsasecurity.com/news/pr/971217.html

8. RSA Security. "RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF)." 19 January 1999. 25 June 2001. www.rassecurity.com/news/pr/990119-1.html

9. Kaliski,Burt. "Life After DES." 11 July 2001. www.rsasecurity.com/rsalabs/des3/des3_bk.html

10. Schneier, Bruce."Key Length And Security." *Crypto-Gram* 5 October 2000. 11 July 2001. http://www.counterpane.com/crypto-gram-9910.html#KeyLengthandSecurity

11. Hayes, Frank. "Broken Code." *Computerworld* 27 July 1998. 25 June 2001. http://www.computerworld.com/cwi/story/0,1199,NAV47_STO31963-,00.html

12. RSA Security. "DES Challenge III Questions and Answers." 11 July 2001. http://www.rsasecurity.com/rsalabs/des3/des3_qa.html

13. RSA Security. "DES." 11 July 2001. http://www.rsasecurity.com/rsalabs/faq/3-2.html

14. Federal Information Processing Standards. "Dederal Information Processing Standards Publication 46-2 Data Encryption Standard (DES)." 11 July 2001. http://www.itl.nist.gov/fipspubs/fip46-2.htm

Last Updated: June 25th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Paris 2017	OnlineFR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced