Dr. Jon's Wireless Security

Cellular Networking Perspectives

Author: Dr. Jon Hamilton Editor: David Crowe Vol. 1, No. 4 June, 1999

The Crypto Answer Man

If you have a question about wireless security or cryptography that may be of general interest, submit it to our anonymous on-line cryptographer, known only as the "Crypto Answer Man". We will post any questions that we decide are of general interest, along with his answers, on our website:

www.cnp-wireless.com/cryptoqa.html

Occasionally we may print especially interesting questions in *Dr. Jon's Wireless Security* as well.

Glossary of Acronyms

All of the acronyms, and some of the terms, used in *Dr. Jon's Wireless Security* are defined at:

www.cnp-wireless.com/glossary.html

Security Issues for Wireless Networks

One of the most important aspects of a modern security system is the strength of its cryptographic algorithms. In this issue we discuss security for cryptographic algorithms for wireless networks, focusing on the issue of how strong ESA and ESP cryptographic algorithms should be. What is meant by a strong cryptographic algorithm? What does it mean to *break* a cryptographic algorithm?

The level of cryptographic security required by an application depends on the worth of the data and the length of time for which it is relevant. Table 1 illustrates this. Secrets vital to the security of a nation require the highest level of protection as one must assume that other countries are continually trying to break the codes of other nations— as recent news reports of the "Twinkle" attack make clear. Financial data such as interbank transfers and credit card infor-

Table 1: Security Requirements Vary with Type of Data

Data Type	Worth	Lif etime	Required Cryptographic Strength
National Security	Highest	20 - 50 years	Highest
Financial Data	High	2 - 10 years	High
Authentication Center's Data Base of User Cryptographic Keys	High	2 - 5 years	High
Mobile Station Cryptographic Key (A-Key)	Low to Medium	2 - 5 years	Medium
Mobile Station SSD or Session Key	Low	1 - 25 weeks	Low

About *Dr. Jon's Wireless Security*

Price

The stand-alone subscription price for *Dr. Jon's Wireless Security* is 75% of the cost of the corresponding *Cellular Networking Perspectives* subscription (e.g. $225 for a basic subscription).

Current subscribers to *Cellular Networking Perspectives* can extend their subscription to include *Dr. Jon's Wireless Security* for only a 50% premium over their current *Cellular Networking Perspectives* subscription price. For example, subscribers to our standard 10-copy license paying $300 per year for *Cellular Networking Perspectives* would pay only an additional $150 per year for *Dr. Jon's Wireless Security*.

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Month's Major Topic

Wireless Network Security Issues. Updates on ESA and ESP.

Next Issue Due...

July 13th, 1999.

Future Topics

Interim CAVE • Global Authentication • UIM • Export Control Laws • ESA/ESP Implementation Guidelines

Dr. Jon's Wireless Security is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary AB, T2N 3W1, Canada.
Contact Information: Phone: 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** http:/www.cnp-wireless.com/djws.html.
Subscriptions: $150 for current *Cellular Networking Perspectives* subscribers for delivery in the USA or Canada, US$200 elsewhere. Non-subscribers pay $225/yr. for delivery in the USA or Canada, US$300/yr. elsewhere. Payment is accepted by cheque, bank transfer, American Express, MasterCard or Visa. **Delivery:** Email or 1st class mail.
Back Issues: Available individually for $20 in the US and Canada and US$25 elsewhere, or in bulk at reduced rates. **Discounts:** Educational and small business discount: 25% off any order. **Copies:** Each subscriber is licensed to make up to 10 copies of each issue or back issue. Please call for rates to allow more copies.

mation also require a high level of strength in the cryptographic algorithm and keys as discovery by an opponent could lead to significant financial loss. For wireless networks, the most important data is the primary cryptographic key or A-key. As up to a million such keys will reside in each AC (Authentication Center), its database should be safeguarded by a level of cryptographic security similar to that required for financial data. Thus the A-keys within each AC should be encrypted by a strong cryptographic algorithm which can assure their security for several years. A single Mobile Station A-key (or cryptographic key) or indeed SSD (session key) is not as highly valued a target for an opponent and therefore does not require the same level of cryptographic security as the A-key database containing many keys in one convenient location. However, if the mobile phone is going to be used for more sensitive operations than merely making calls, such as financial transactions, then an enhanced level of security is required.

Two Types of Attack

There are two types of attacks on a cryptographic process: brute force and cryptanalytic.

Attack Type 1: Brute Force

Brute force means that the opponent has the cryptographic algorithm and both cipher and plain text. The opponent tries all possible combinations of the cryptographic key in the cryptographic algorithm to determine which cryptographic key is being used. A measure of merit for a brute force attack is the length of time (and processing power) required to exhaustively analyze all possible cryptographic key combinations in the cryptographic key space.

The Cryptographic Key Space

The *Cryptographic Key Space* is the total number of possible cryptographic keys. For example, for a 64 bit cryptographic key there are 2^{64} possible keys and the cryptographic key space is 2^{64}. A brute force attack would, on average, have to search half of them (2^{63}) to break a single key.

Attack Type 2: Cryptanalytic

Cryptanalytic attackers seek to discover hidden weaknesses in the cryptographic algorithm which allow them to reduce the effective cryptographic key space. The strength or success of a cryptanalytic attack is determined by how much the key space is reduced.

Brute Force Attacks

In the following discussion, we focus on a brute force attack against cryptographic algorithms. This assumes that the opponents have *not* found a cryptanalytic attack that reduces the size of the key space, and that the cryptographic algorithms are available to the public. The efficacy of a brute force attack depends on:

- the length of cryptographic key, and
- the amount of time required to execute the cryptographic algorithm.

The length of the key is fixed but the execution time for the cryptographic algorithm is dependent on:

- the execution speed of the processor,
- the processor time required (i.e. the efficiency of the software and hardware), and
- the number of processors used (i.e. parallel processing).

Table 2 summarizes the capabilities of a brute force attack against various cryptographic key lengths when the opponent uses a single state-of-the-art PC. Note that keys of 32 bits or less are extremely vulnerable to even a single PC in the hands of a fairly competent opponent. However, for key lengths in excess of 64 bits, they are quite safe.

By their nature, brute force attacks do not include an analysis of the algorithm being attacked, but there are still significant differences in the speed at which brute force algorithms can search the key space. These differences are due to the efficiency of the software, and possibly the hardware, designed for the attack. Extremely optimized software can be many orders of magnitude faster than the most straight-forward software that might be written by a junior cracker.

DES: A Case Study

DES, when used with a 56 bit key, falls within the 'quite safe' category. About a year ago, it was announced that DES was 'broken". How did this come about? Look at Table 3 and the entry for DES for an opponent using 10,000 processors (PC). Actually the crackers that broke DES were somewhat lucky in that it took them only a few months. It is highly improbable that breaking a single cryptographic key for a mobile station would be worthy of this mammoth effort.

Table 2: Brute force Attack with a Single Processor

Key Length	Junior Cracker	Average Cracker	Senior Cracker	World's Best
32	6 months	2 days	4 hours	20 minutes
56 (DES)	7 million years	10,000 years	7,000 years	700 years
64	10^9 years	10^7 years	10^6 years	10^5 years
90	10^{17} years	10^{15} years	10^{14} years	10^{13} years
96	10^{18} years	10^{16} years	10^{15} years	10^{14} years
128	10^{28} years	10^{26} years	10^{25} years	10^{24} years

Table 3: Brute Force Attacks Using Parallel Processing

Key Length	1000 Processors	10,000 Processors	Million Special Pur pose Processors	Best Possible Using Current Technology
32	2 minutes	2 seconds	Real time	Real time
56 (DES)	70 years	8 months	6 hours	2 minutes
64	10,000 years	100 years	3 months	15 minutes
90	10^{12} years	10^{10} years	10^{7} years	10^{3} years
96	8 x 10^{13} years	8 x10^{11} years	8 x10^{8} years	8 x 10^{4} years
128	3 x 10^{23} years	3 x 10^{21} years	3 x 10^{18} years	3 x 10^{4} years

Parallel Processing

Table 3 provides estimates of the time required for cracking various key lengths when the attacker exploits parallelism using multiple PCs networked together or more loosely coupled through the internet. The last two entries in the table assume that the opponent has gone to the trouble of developing special purpose hardware to compute the cryptographic algorithm and then used massive parallelism for the computation process. Such capabilities are currently probably only feasible by government agencies with virtually unlimited budgets. Notice the significant change in vulnerabilities when the opponents are sophisticated and use parallel processing. An opponent with enormous resources at their disposal can certainly break cryptographic algorithms with keys of length 64 bits and higher. However, for a key length of 90 bits, even a very sophisticated opponent requires 1,000 (10^3) years to break the code using brute force techniques.

Cryptanalytic Approaches

In the above discussion we assumed that the opponent had to use brute force and that no cryptanalytic attacks were available to reduce the size of the key space. This is a critical assumption, but not necessarily a good one. A cryptographic algorithm is developed with the intention that no cryptanalytic attack is possible. All this means is that the developers could not find a successful attack. It does not mean that other clever cryptanalysts cannot find one. History is replete with cryptographic algorithms that were initially judged unbreakable, but that were quickly found to be eminently breakable. It is this unknown ability to reduce the size of the key space through cryptanalytic attacks that leads to our recommendation of a key length of 128 bits for both ESA and ESP, when 90 bits would certainly suffice against a brute force attack.

DES has been around for over 20 years and NO public cryptanalytic attack has been successful in determining the key (excluding the ECB – Enhanced Code Book – version of DES, which does not use feedback to prevent a *plain text* attack). However the demonstration of a successful brute force attack against DES means that it and its 56 bit key should not be used to safeguard financial data or A-keys in an AC.

The CAVE algorithm currently used in TIA/EIA-41 authentication is 64 bits in length. Several cryptanalytic attacks have been made against CAVE with the result that the key space for CAVE is now down to around 2^{35}. A quick glance at Table 2 shows that CAVE is vulnerable to a very good cracker using the latest PC. Associates have told me that they have a successful cryptanalytic attack against CAVE that would reduce the size of the key space considerably further. If this is publicly announced then CAVE would be extremely vulnerable to even a junior grade cracker.

Dr. Jon's Recommendation

If key lengths in excess of 90 bits are selected for both ESA and ESP, these algorithms would remain invulnerable to brute force attack for the next 10 to 20 years. However *our recommendation is for a 128 bit key length for both ESA and ESP* to provide some additional safety against a successful cryptanalytic attack reducing the effective size of the key space. Based on similar reasoning, a cryptographic algorithm and key length of 128 bits is also recommended for the encryption of cryptographic keys (A-keys) within the authentication center.