Global Information Assurance Certification Paper

Weaknesses in Modern Cryptography
SANS Practical Assignment for GSEC, version 1.2b
By Tim White

Modern cryptography has become the savior of the Internet, promising to secure our most important information and communications by guarantying it may be not be deciphered by any other than the intended recipient. This ideology has two flaws: Advances in mathematics and computation may render current algorithms obsolete; Key management and authentication in a large and complex environment are so difficult that they undermine the mathematical strength of the best cryptographic algorithms.

Futures, Anyone?

In its purest form cryptography is a mathematical panacea of wonder and excitement. Modular arithmetic, discrete mathematics, complex prime number calculations and elliptic curve algorithms form the basis of our current cryptographic algorithms. Such mathematics relies upon one thing… Complexity. In order for an algorithm to provide security to data, it must be computationally infeasible to deduce the original message from knowledge of the algorithm and encrypted message. Such algorithms are relatively simple to compute in one direction, yet intangible in reverse without knowledge of another piece of information, typically a number or set of numbers known as the key[1].

For as long as the calculations to reverse the cryptographic algorithm take longer than the valuable lifetime of the data it protects, it may be considered secure. There is an inherent problem with this statement, given that none of us can predict what breakthroughs will occur in either the field of computation or mathematics.

When not obeying Murphy's Law, Moore's law seems to be held in place. Traditional computing devices keep getting faster and faster, at rates even the wealthiest of us cannot keep up with. The following excerpt from the Intel web site shows this trend in detail:

> *Moore's observation, now known as Moore's Law, described a trend that has continued and is still remarkably accurate. It is the basis for many planners' performance forecasts. In 26 years the number of transistors on a chip has increased more than 3,200 times, from 2,300 on the 4004 in 1971 to 7.5 million on the Pentium¨ II processor.*

And it won't stop here. Scientists continue to make amazing breakthroughs in miniaturization. Recent developments in nanotechnology have lead to molecular transistors, micron scale mechanical devices and micron scale tubes (remember the Tube radio?). Such breakthroughs are condensing the volume in which electronics are placed, increasing speed and storage capacities at rates that would make Gordon Moore proud[2]. Ivars Peterson reported on a recent paper by Seth Lloyd of MIT, published in the Aug. 31 edition of Nature magazine[3]. Lloyd contends that the speed limit for Turing (modern computational theory) based computers is 10^{51} computations per second. He deduced this limitation from studies of physical limitations on matter, quantum mechanics, thermodynamics, and other such disciplines of physics. According to the article, modern

technology has achieved rates of 10^{13} operations per second. To put that in perspective, breaking the DES encryption algorithm at this rate would take approximately 2 hours[4]. At the maximum theoretical rate, it would take approximately $7 * 10^{-35}$ seconds. An encryption algorithm with a key strength of 128 bits would take a lengthy $3 * 10^{-13}$ seconds to decrypt by trying each key individually.

Of course, this technology won't be available at the local electronics store tomorrow, but it illustrates that such breakthroughs are possible within the confines of classical physics. The Rijndael Algorithm, selected as the new AES standard, when computed at its maximum strength of 256 bits could take many times the age of the universe to attack by brute force, according to Science News author Ivars Peterson, at current computing speeds. Even if we could achieve 10^{30} operations per second within ten years, such a large key-space would require approximately $4 * 10^{39}$ years to exhaust, unless mathematical breakthroughs render brute force attacks useless.

On the other hand, the same was thought of the nug30 quadratic problem, a problem that deals with the assignment of facilities to fixed locations to minimize shipping costs of materials between those facilities. This problem was thought to take 100 times the age of the universe at 10^{9} operations per second when initially analyzed in the late 60's, but early last year several research centers created a computational grid consisting of over 1000 computers, and solved the problem in about a week[5].

With mathematical complexity at the heart of the algorithms, what happens when a new breakthrough in mathematics occurs? History has shown that major advances in mathematical thought do not necessarily occur linearly. In the scheme of things, calculus, complex number theory, and many other mathematical breakthroughs occurred overnight. Browsing through recent math and popular science publications one will most certainly find many articles discussing recent breakthroughs in modular mathematics and prime number theory. These sorts of mathematics are at the heart of the most popular algorithm, used to implement SSL, RSA. If a mathematician wakes up tomorrow and uncovers how to calculate prime factors of large numbers, like those used to generate PKI Certificates, our entire encryption infrastructure would have to be redeployed.

There is considerable effort on behalf of the mathematical community to uncover the complexities behind these sorts of mathematics. According to Ivars Peterson, A British publisher is funding a $1M reward for breakthroughs in proving the Goldbach conjecture stating that every even number is the sum of two primes[6]. This work is founded on breakthroughs made by Srinivasa Ramanujan's work with partitions and congruence[7]. There are many more examples appearing throughout the math world. With such backing and many brilliant minds working out these problems, we may see major advances in linear solutions of these exponentially complex problems.

If the threat of mathematical breakthroughs and faster Turing computers were not enough, there is also the new field of Quantum Computation. The basis of quantum computation is founded in a phenomenon called Wave-Particle duality. Energy levels of a particular particle are assigned a state of one or zero. In addition to this standard state,

due to Heisenburg's uncertainty principle, a particle may occupy both states by superposition. This assignment of energy levels to computational values is called a quantum bit, or qubit. When the state is measured, it is possible to set up a problem such that when measured, invalid answers will end up in the superposition thus canceling out any invalid answers and revealing the solution to the problem via quantum interference. Several applications of this new theory of computation have been simulated, such as games theory, search algorithms, cryptography, and mathematics[8]. Recently there have been new breakthroughs in molecular physics allowing the construction of an actual quantum computer. Recently, an IBM researcher announced the first implementation of a molecular quantum computer[9]. Although the initial problem solved by this computer was relatively simple, the system was significantly more efficient at solving the problem than a conventional Turing based computer. This initial system was a 5-qubit machine, but more complex algorithms are being developed to expand on this initial success. This is the science of the future, today. Such a system may be able to make child's play out of our currently complex mathematical algorithms, thus rendering our modern cryptography obsolete.

Although our cryptographic implementations are based on hopes that future developments in mathematics and computation theory do not advance, they are relatively secure for non-classified and commercial use, at least for the short term. Breaking the cryptography is the least concern when facing the new digital economy. Calculating the lifetime of the data and insuring lengthy life spans are not an issue is the most important thing to defeating the uncertainty of the future with regards to cryptography.

What's the Key?

To the end user, cryptography is almost as magical as a light switch. With the click of a button, all information is mysteriously secured from the prying eyes of the digital underworld. Complex protocols and irreversible mathematical algorithms are completely obfuscated from all users and most programmers. Herein lies the immediate problem with modern cryptography.

Computer users are overwhelmed by complexity each day, and our programmers have taken steps to remove this complexity from their minds. Behind the scenes, automated applications handle key management and trust verification before utilizing our cryptographic keys to sign and encrypt information. This is the real world equivalent of leaving your house keys under your doormat.

These keys are generally protected via a password, but in a world where one more pass phrase to remember is a daunting task, they are generally encrypted with a simple or no pass phrase. After obtaining a certificate for personal use and installing it into a browser, little to no protection is made to verify that the person utilizing the certificate is the one who received it. Anyone who can execute code on that computer may be able to recover the client side SSL certificates. Users typically do not realize that weak key management is the most likely way their data can be compromised.

Forensic experts rarely have to break the cryptography to recover a message. Simply recovering the key off of a floppy or hard disk often gets them in[10].

Recent compromises have been revealed with Additional Decryption Keys, or ADK's, implemented within the PGP email encryption application. The ADK functionality was designed to overcome the problem corporations have with encryption – the ability to recover encrypted information if an employee is terminated or unable to provide decryption keys. ADK's overcome the inherent complexities of key escrow for recovering encrypted information. As reported to the general public by Bruce Schneier, this introduced a vulnerability to the key management protocol that allows an attacker to regenerate a public key pair such that the attacker receives a copy of any text encrypted to that public key[11].

Even with educated users and good key management, the only way that I can think of to absolutely secure a key is to memorize it and never enter it into a computer. This may sound extreme, but think about the vulnerabilities inherent in allowing an electronic device to perform calculations given the key. Many forensic methods are available for calculating or intercepting the key, without ever having to break the encryption algorithm. Van-Eck monitoring may be used to intercept good pass phrases from your system, memory written to disk may be analyzed to recover traces of your public key from overwritten virtual memory, differential power dissipation analysis can utilize temperature or electricity usage statistics to narrow down key space to allow faster calculation of keys. And even if you keep your key in your memory and manually perform all encryption operations mentally it may be possible in the future (distant) to recover such information from your mind. This introduces value into the encryption equation. Not only must encryption provide timely protection to your information, it must do so in correlation to recovery costs. Vulcan mind melts to recover encryption keys may be quite costly to perform, so only data valuable enough to require such protection needs to be considered for the mathematical genius encryption system.

Smart cards can provide tamper-resistant methods for encrypting and managing keys, and there are methods available to prevent leakage of information from the crypto-system from compromising its security. These technologies are expensive and not always necessary.

Another problem related to encryption and key management is the communication itself. Both the information related to the message and its communication path can reveal information to an observer. Algorithms exist to reduce the amount of information the attacker can infer about a given communication, commonly referred to as perfect forward secrecy algorithms. These algorithms utilize message randomization, padding or SALT, consistent message blocks, obfuscation of encrypted message headers, and other techniques to guarantee that an attacker cannot utilize transmission information to reveal a key.

One issue that is difficult to overcome is the pure fact that the communication between two entities occurred in the first place. The FBI commonly monitors communications

between parties, and even if encrypted the fact that criminal A is constantly calling criminal B provides an investigating tool that reveals behavior. Algorithms such as anonymous re-mailers exist to overcome such issues, so that the true recipient is obscured from the eyes of any would-be eavesdropper[12].

We also trust third party verification services to authenticate our keys for us, establishing hierarchical trust trees with which we decide which keys are valid. Recently the inevitable occurred - Verisign issued certificates to two persons masquerading as Microsoft employees[13]. These certificates may now be used to sign digital code, which may trick end users into trusting applications that may in fact be malicious. Such a breakdown is naturally a breakdown of human processes. There is no way to circumvent this without better methods for authenticating users whom we do not know. The protocols provide methods for handling such breaches in security, but the complexity and diverseness of the Internet impedes the quick distribution of information about revoked or compromised keys. Personal verification of all trust is a must to insure security of information transmitted to an individual. This is a problem computers alone cannot solve.

Where do we go?

As Bruce Schneier pointed out in his book, Secrets & Lies, the math and the protocols are fairly reliable, but the people are fallible. Any security requires common sense, and sometimes it's just better not to share certain information with others electronically. Unfortunately, this impedes the speed and openness we have come to rely upon in our high paced digital world. We must simply keep up to date and educate users. We must reveal the magic behind the curtain so that users of cryptographic systems understand the limitations. Communication must remain intact, and as learned by the media industry with the DVD encryption algorithm[14], don't rely on your own algorithms if they haven't been reviewed openly.

We need to plan ahead as well. We must not only consider the security of the transport of information, but of its storage, age, and value. Above all, our encryption research needs to be one step ahead of mathematical and technological advances. We hopefully will have the next new technology before the old one is broken. Work in quantum cryptography and development of the Advanced Encryption Standard will hopefully take us in the right direction.

Maintaining the security of information will continue to be a challenge, regardless of the technology. Protecting our resources and using reasonable methods to secure and encrypt information while insuring growth in education and better authentication methods is the only way to protect ourselves from the digital underworld

Bibliography & Additional Reading

[1] Intel Corporation. "What is Moore's Law?" Processor Hall of Fame. (2001) 1 Apr. 2001 <http://www.intel.com/intel/museum/25anniv/hof/moore.htm>

[2] Reed, Mark A. and James M. Tour. "Computing with Molecules." Scientific American June 2000: 87-93

[3] Peterson, Ivars. "Going to digital extremes." Science News 158-12 (2000) 189

[4] Peterson, Ivars. "Global contest nets encryption standard." Science News 158-15 (2000) 231

[5] Peterson, Ivars. "Computer grid cracks problem" Science News 158-8 (2000) 125

[6] Peterson, Ivars. "Prime conjecture verified to new heights." Science News 158-7 (2000) 103

[7] Peterson, Ivars. "The Power of Partitions – Writing a whole number as the sum of smaller numbers springs a mathematical surprise." Science News 157-25 (2000) 396:7

[8] Peterson, Ivars. "Quantum Games – Taking advantage of quantum effects to attain a winning edge." Science News 156-26 (1999) 334:5

[9] Peterson, Ivars. "Computation Takes a Quantum Leap." Science News 158-9 (2000) 132

[10] Scneier, Bruce. Secrets & Lies: Digital Security in a Networked World. New York: John Wiley & Sons, Inc., 2000

[11] Scneier, Bruce. "PGP Vulnerability Discovered." In a message posted to: Slashdot Computer Forum (2001). 1 Apr. 2001 <http://slashdot.org/articles/00/08/24/155214.shtml>

[12] Scneier, Bruce. Secrets & Lies: Digital Security in a Networked World. New York: John Wiley & Sons, Inc., 2000

[13] Symantec Corporation. "Security Alert – Fraudulent Digital Certificate issued by Verisign." Symantec Incident Response Center (2001). 1 Apr. 2001 <http://www.symantec.com/avcenter/sirc/fraudulent.digital.certificate.html>

[14] Grossman, Wendy. "DVDs: Cease and DeCSS?" Scientific American May 2000: 44-45

Other General Reading

Scneier, Bruce. Applied Cryptography. 2nd Ed. New York: John Wiley & Sons, Inc., 2000

Coveney, Peter and Roger Highfield. Frontiers of Complexity: The Search for Order in a Chaotic World. New York: Ballantine Books, Inc., 1996

Nickels, Hamilton. Secrets of Making and Breaking Codes. New York: Barnes & Noble Books, Inc., 1990

Denning, Dorothy. Cryptography and Data Security. Addison-Wesley Publishing Co., Inc., 1982

Deutsch, David. The Fabric of Reality: The Science of Parellel Universes – and Its Implications. Penguin USA, 1998

National Institute of Standards and Technology. "Cryptographic Toolkit." NIST - Computer Security Resource Center (2001) 1 Apr. 2001 <http://csrc.nist.gov/encryption/>

Van-Oorschot, Paul C., Scott A. Vanstone and Alfred Menezes. Handbook of Applied Cryptography. CRC Press, 1996

Peters, Ivars. The Mathematical Tourist: New and Updated Snapshots of Modern Mathematics. New York: Barnes & Noble Books, Inc., 2001

Simmons, Gustavus J. Contemporary Cryptography: The Science of Information Integrity, IEEE, 1992