Strong Cryptography and Public Policy

a talk delivered to the Connecticut Bar Association,
May, 2002

by

Charles W. Neville, Ph.D.
cwneville@cwnresearch.com

PHILOSOPHY is worth supporting.
Even PURE MATHEMATICS is worth supporting.

1. How Computation Came To Be.

David Hilbert: 1900 International Congress of Mathematicians.
Russell and Whitehead: Reduction of arithmetic to symbolic logic.
Kurt Goedel: Goedel's undecideability theorem.
Alan Turing: Turing machines.
The Church – Turing thesis.
Burks, Goldstein and Von Neumann: The stored program computer.

The Dramatis Personae

Russell and Whitehead were PHILOSOPHERS.

Hilbert, Goedel, Turing, Church, and Von Neumann were PURE MATHEMATICIANS.

2. The Relation To Cryptography And Other Things.

Bertrand Russell wrote much of his and Whitehead's great work while in JAIL in 1918 on war resistance charges.

Alan Turing, lead the successful effort to break the German Enigma Codes during World War II.

Cmdr. Rochefort and Col. Friedman broke the Japanese Naval Codes and the Japanese Diplomatic Codes.

Official (until very recently) U.S. Government encryption standard is the Digital Encryption Standard or DES. Every cryptographer who worked on it was acutely aware of the fatal weaknesses of the supposedly unbreakable Enigma.

More consequences of the work surrounding Hilbert's 2nd problem.

1. Higher level computer languages such as FORTRAN, C and Java.

2. Virtual machines. (Can you see how this follows from the Church – Turing thesis? Answer in appendix C.)

3. Artificial Intelligence. (Can you see how this also follows from the Church – Turing thesis? Answer in appendix C.)

And even more consequences

4. The identification by Cook of certain maximally hard problems solvable by guesswork, such as the travelling salesman problem.

5. Public key cryptography. You use public key cryptography every time you buy something on the Internet.

3. Public Key Cryptography.

Cryptography, the art and science of putting messages into code. Also the art and science of breaking codes.

The KEY DISTRIBUTION problem.

Public key cryptography SOLVES THE KEY DISTRIBUTION problem.

How public key cryptography works.

There are TWO keys:

A PUBLIC KEY which you make public, and which is used to encrypt messages (put messages into code).

A PRIVATE KEY which you do not make public, and which you use to decrypt messages (decode messages).

The public key gives away lots of information.

Public key cryptography requires VERY STRONG cryptographic methods.

These methods are based on the existence of very difficult problems called "one way functions." (The existence of these was conjectured by Church and (almost) proved by Cook.)

An example of a one way function.

This underlies several VERY STRONG public key methods, including the RSA method:

Given two factors of a number, it is easy to multiply them together to get the the product. For example,

$$3 \times 7 = 21.$$

But given the product number, it is much harder to find the factors. For example,

$$21 = 3 \times 7.$$

Here's a harder one,

$$7406887751585867569251795143059236193447477077486728197406579496917297622889002203758802524412805681036642783314685956495693901714336056843776952571316739000549531257469006228006245716108881002895059 57$$

can be factored into

$$1509402497293445260998365996277047451139493435867383880425876691549588470411353603813444238679891122 1$$

$\times$

$$4907165427954027778108059597498789269411765580199490474427239837091547927832034451262331586358355121 7$$

In the RSA method,

The PUBLIC KEY used for putting messages into code is the very large 200 digit integer.

The PRIVATE KEY, used for decoding messages, is the pair of 100 digit factors.

4. How Secure Is The RSA Method?

Breaking the RSA method involves FACTORING THE PUBLIC KEY into its two prime factors.

The empirical and theoretical evidence is that the RSA method is unbreakable if you use a BIG ENOUGH PUBLIC KEY.

But the safe key size keeps growing as our knowledge and computer power increase.

The empirical evidence:

The Bank of England used to use an 80 decimal digit public key.

An RSA challenge message with a public key of 129 decimal digits was published 1977.

Rivest's estimate: 40 QUADRILLION YEARS of computer time to factor the public key and break the code.

In 1993, 600 volunteers and 1600 machines from all over the Internet and broke the code in only 8 MONTHS.

The Bank of England now uses a MUCH LARGER PUBLIC KEY.

The decoded challenge message was, "THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE." This is really deep stuff, isn't it!

The current factorization record: a 155 decimal digit public key in roughly 8.4 years of total computer time (divided among hundreds or thousands of computers).

A 310 decimal digit public key would take approximately 1.6 billion times as long, so for the time being, public keys of 300 or more decimal digits are safe.

But even 100 decimal digit public keys are beyond the capacity of Harry Hacker or Script Kiddie to crack.

The theoretical evidence:

All efforts to find really efficient factorization algorithms, or to break the RSA method without actually factoring the public key, have failed.

So have all efforts to find really efficient algorithms for solving NP complete problems (maximally hard problems such as the travelling salesman problem, solvable quickly by inspired guessing, if only one could guess the right answer).

The theoretical justification for the assertion that public key methods like the RSA method are inherently unbreakable rests on the following widely believed but UNPROVED ASSUMPTIONS:

Breaking the RSA method is equivalent to factoring the public key.

Factorization is not as hard as an NP complete problem like the travelling salesman problem, but is still so hard that it takes EXPONENTIAL TIME to solve.

NP complete problems take exponential time to solve. (This is the famous NP vs P problem, first posed by Cook, which is now one of the Clay Mathematics Institute's 7 Millennium Prize Problems.)

The theoretical foundation for all internet cryptographic security rests on the assumed but UNPROVED truth of these three assumptions. It's a bit shaky, isn't it?

5. How Available Are The RSA And Other Strong Cryptographic Methods?

Strong encryption technology is available to almost anyone.

The RSA cryptosystem is sold commercially by RSA Security, Inc.

Anyone can download and use FREE open source versions of the RSA cryptosystem.

Phil Zimmerman's PGP (Pretty Good Privacy) program has been available for years. As RSA Security's patent expired in 2001, anyone can now legally use PGP without a license from RSA Security.

The FBI and CIA are not happy about this.

6. What Are The National Security Implications?

In a word, DIRE.

For years, the U.S. Government tried to prevent the export and distribution of strong cryptographic methods. They failed because:

The cat was already out of the bag. The basic algorithms had been openly published, and strong cryptographic systems were freely sold abroad.

Many did not trust the Government to hold keys in escrow, fearing that the Government would simply spy on all of us.

Do terrorists and criminals use strong cryptographic methods to hide their schemes? YES.

Terrorists tend not use PGP or similar systems to encrypt email only because sending encrypted email attracts unwanted attention.

The terrorists in the Manila plot to blow up 11 US owned commercial airliners used strong encryption to encrypt files on their laptop computers.

The first mob case involving strong cryptography is now being prosecuted.

Alleged New Jersey mobster Nicodemo S. Scarfo used PGP to encrypt files which the Government asserts contain records of his loansharking operations.

The files were cleverly named "Factors."

The FBI used a "keystroke sniffer" to record Scarfo's computer keystrokes and snare his private key.

The key was based on his father's federal prison number.

7. Can We Simply Legislate Against Using Strong Cryptography?

In a word, NO.

Confidential Internet transactions, such as credit card transactions, HAVE TO BE ENCRYPTED because:

By the very nature of the Internet, it is not only easy, but also legal and NECESSARY for others to listen in to Internet transactions.

Unlike telephone calls, there is no direct dedicated connection for Internet messages.

Instead, messages are divided into PACKETS, and each packet is DYNAMICALLY ROUTED from source to destination.

One packet may go VIA LONDON, another THROUGH BOSTON, all part of the same message from HERE TO LA.

EVERY COMPUTER at EVERY INTERMEDIATE POINT has to READ EVERY PACKET to see where the packet is addressed, and to forward the packet if necessary.

Possible solutions:

Legislate against reading the data contained in the BODY of packets addressed to others, allowing only the reading of the ADDRESS header of the packet.

This would be similar to the way we deal with ordinary surface mail – you can read the address on the envelope, but you can't open the envelope unless it is addressed to you.

But this would be MUCH HARDER TO ENFORCE than current laws outlawing reading other peoples mail or intercepting other peoples telephone messages.

I call this the"transparent envelope problem."

Legal note:

It is ILLEGAL for a PERSON to read the content of packets addressed to someone else. But it is LEGAL for that person's computer to read the packets, and even to temporarily store them for necessary processing (decision making and forwarding). This is what makes enforcement so difficult.

Another approach, tried in Germany,

Outlaw storing ENCRYPTED FILES and sending encrypted email, unless the owner is prepared to provide the decryption key on court order.

In the U.S., this might run afoul of the 5th Amendment.

Conclusion:

As a society, we seem to have made a FAUSTIAN bargain.

We have traded the economic benefits of Internet commerce, which requires strong cryptography, for added vulnerability to terrorist attack.

It is probably too late to turn back the clock.

8. The Real Threat – Digital Steganography

Steganography, the art and science of hiding messages. Also the art and science of detecting hidden messages.

Steganography is real "spy vs spy" stuff.

It used to involve things like microdots – messages stored on pieces of microfilm the size of a period and inserted into apparently innocuous documents.

Digital steganography works by subtly altering image or music files to hide messages. One scheme:

Start with a 128 color GIF image.

The GIF image format allows 256 colors, so you can subtly alter the colors to hide a message.

These alterations are not noticeable to the human eye.

The good news:

This particular scheme is easy to spot using computerized statistical analysis of the image's color distribution.

The bad news:

Schemes involving JPEG images, the most common images on the Internet, are said to be

UNDETECTABLE USING CURRENT TECHNOLOGY.

How prevalent is digital steganography?

In a word, VERY.

There are over 100 free downloadable steganography programs on the Internet.

There have been over a million downloads of the technology, from all over the world.

To quote from the New York Times of October 30, 2001,

"Mr. Hosmer's company began looking at millions of digital pictures that were posted on the Internet. They scanned auction sites and pornographic sites, where people can post and download digital images anonymously.

" 'We started getting hits,' Mr. Hosmer said, adding that about 0.6 percent of millions of pictures on auction and pornography sites had hidden messages. The messages they found on eBay were encrypted and unreadable, he said."

Do terrorists use digital steganography to hide their schemes? YES

To quote from the same New York Times article again,

"Intelligence officials have not revealed many details about whether, or how often, terrorists are using steganography. But a former French defense ministry official said that it was used by recently apprehended terrorists who were planning to blow up the United States embassy in Paris.

“The terrorists were instructed that all their communications were to be made through pictures posted on the Internet, the defense official said.

“The leader of that terrorist plot, Jamal Beghal, told French intelligence officials that he trained in Afganistan and that before leaving the country for France, he met with an associate of Osama Bin Laden. The plan was for a suicide bomber to drive a minivan full of explosives through the embassy gates.”

Can we legislate against steganographic technology?

In a word, NO.

The very same techniques used in steganography are used to "watermark" images and music to provide protection against Internet piracy.

A possible solution:

We could exempt watermarking from a legislative ban on steganography, distinguishing watermarks from other hidden messages by their intended use.

But this would not solve the problem of people posting steganographic images from abroad, unless a broad international consensus against steganography could be formed.

Conclusion:

We seem to have made another FAUSTIAN bargain.

We have traded the economic and cultural benefits of posting images and music on the Internet for added vulnerability to terrorist attack.

Again, it is probably too late to turn back the clock.

9. Credits.

No Microsoft software was used in the making of this talk.
No monsters were hurt in the making of this talk.