Cryptography: Is Staying with the Herd Really Best?

Terry Ritter, Ritter Software Engineering

A recent Internet Watch column argues that new cryptography is bad cryptography. Drawing an analogy to the medical profession, it says, "A good doctor won't treat a bacterial infection with a medicine he just invented when proven antibiotics are available." That certainly sounds reasonable. But, in a very real and practical sense, there *is* no proven cryptography. And this is not just an issue of mathematical proof: The cryptographic profession simply can't tell whether or not a cipher really is protecting data. It is as though medical doctors were telling us about their cures when in reality they couldn't even tell if their patients were alive or dead.

It is not that we want to avoid cryptanalysis; indeed, we want all the analysis we can get. And it is true that a brand new cipher has had scant time for analysis. But the result of even deep analysis is not a proven design; it is just something that we don't positively know to be weak. This slight shift of meaning is the basis for understanding what cryptography can and can't do. For one thing, it means that any cipher—no matter how deeply analyzed—could be weak in practice. And that means that anyone concerned with real security probably should consider using something other than the same cipher as everyone else. One possibility is using new cryptography in new ways, which is the exact opposite of what that previous column suggests.

Editor: Ron Vetter, University of North Carolina at Wilmington, Department of Computer Science, 601 South College Rd., Wilmington, NC 28403; voice (910) 962-3667, fax (910) 962-7107; vetterr@uncwil.edu.

There is neither proof nor a test of overall strength for either new or old cryptosystems.

Surely, we all would like to have a fully reviewed library or cipher in the same way that we would like to have a fully debugged program. But not even lengthy review or analysis guarantees either cryptographic strength (the ability to resist attack) or a lack of program bugs. For example, most crypto experts probably would agree that just because 20 years of analysis of the US Data Encryption Standard has not found an easy break doesn't mean that no easy break exists. And if a break does exist, it may have been actively exploited for years without our knowing. We certainly couldn't call that a strong cipher. In practice, even extensive review is not a rational or scientific indication of strength.

This is not an issue of perfection versus reality, and it isn't like software where we tolerate various bugs and still get real work done. In software, the bugs are generally peripheral to our goals, and we usually know if we are getting what we want. But in cryptography, we have no idea whether or not someone can break our cipher, even if there are no bugs at all in the program.

CONFIDENCE IN CIPHERS

Perhaps the central problem in cryptography is how we can have confidence in a cryptographic design. Ways often mentioned to gain confidence in ciphers include mathematical proof, practical tests, open cryptanalysis, and long use.

Mathematical proof and practical tests

Despite more than 50 years of mathematical cryptography, there is no complete mathematical proof of strength for any practical cipher, at least not in the open literature. (A one-time pad is often assumed to be secure, but is impractical in most cases.)

Likewise, there is no set of tests that measures all possible weaknesses in a cipher. The very feature we need—strength against unknown attack—is something we can't measure. This is like a publisher who can measure the quality of paper, printing, and binding yet still not know the quality of a book or articles. The essence of a cipher is not the measurable ciphering process itself, but rather the effect that process has on confounding each opponent. Cipher quality is necessarily contextual, and we can't know the context.

Cryptanalysis

Cryptanalysis is the art of trying to find an easy way around a security design's cryptographic protections. While many specific attacks are known in an expanding literature, the number of possibilities is essentially unbounded. There is no exhaustive theory of cryptanalysis. Without such a theory, cryptanalysis that does not find a problem does not testify that no problems exist. Cryptanalysis gives us an upper bound for strength, but not the lower bound that describes the minimum effort needed to break a cipher.

Nor does cryptanalysis provide evidence that our cipher is strong. Surely we use only ciphers we can't break. But predicting what an opponent can do on the basis of what we can do is at the very essence of weak cryptography. The classic examples occurred in Germany and Japan in World War II, but every broken system is a failed assumption of strength. We can either learn from history or repeat it on the losing side.

Long use

Our opponents operate in secrecy and do not reveal their successes. If they break our cipher and take some care to protect the results, we will continue to use that broken cipher, all the while assuming our data is protected. Confidence from long use is a self-delusion that springs from not specifically being told that our cipher has failed. We hope that our lack of knowledge means that our cipher has not been broken. But if hope were enough, we wouldn't need cryptography.

THE CRISIS OF CIPHER CONFIDENCE

There is no known proof, measurement, or analysis that provides confidence in cipher strength. Cryptosystems both new and old are in exactly the same boat: Against unknown attack, even an extensively reviewed system may not be as strong as one not reviewed at all. An implied problem with a new cryptosystem is that we can't know that it is strong. But the real problem is that we can't know that the old system is strong—and that is the system we are actually using.

If academics refuse to address patented cipher designs on a rational, technical basis, they won't develop the background to understand or compare the new cryptographic technologies. It is even possible that there may be a practical security advantage to a patented cipher: Since no one can prove that any cipher is secure, absolute confidence is simply not available. Any cipher can fail at any time. But if a patented cipher fails, we may be able to prove that someone used an unlicensed deciphering program and take legal steps to recover our losses.

There is no known proof, measurement, or analysis that provides confidence in cipher strength.

WHAT CHOICES DO WE HAVE?

Even if we consider every cipher as possibly insecure, we do have alternatives. Instead of reacting to rumor or waiting for academic breakthroughs, we can proactively use new approaches and new technology. We can, as a matter of course, multicipher our data: We can use one cipher on the plaintext, a different cipher on the resulting ciphertext, and yet another cipher on that result. In general, if even one of the three ciphers is strong, our data is protected. And even if each cipher has a weakness, it may be impossible to exploit those weaknesses in the multiciphering context. For example, multiciphering protects individual ciphers from known plaintext attacks.

Another alternative is to use a wide variety of structurally different ciphers and to randomly select ciphers by automatic negotiation. In addition to terminating any existing break, this spreads our information among many different ciphers, thus reducing the reward for breaking any particular one. Another step is to continually add to the set of ciphers used. This increases costs for our opponents, who must somehow acquire, analyze, and construct software (or even hardware) to break each new cipher. But new ciphers would be only a modest cost for us.

Absent a mathematical theory to assure a high cost of cipher-breaking, experimentation is the main way to test a cipher's strength, but real designs are far too large to know in any depth. So another alternative is to construct scalable designs that produce both tiny toy ciphers (which can be broken and deeply examined experimentally) and large serious ciphers from the same specification.

Despite the frequent cryptography articles in IEEE journals, cryptography is an art, not an engineering discipline: The property we seek to produce—strength against unknown attack—is not measurable, and so it is literally out of control. But if we avoid new technology, we help our opponents, who certainly don't want to deal with a wide array of new ciphers.

Not applying new technology is wrong—wrong for an innovator who seeks compensation, wrong for the user who wants the best systems, and wrong for those who want the field to mature. It is necessary, therefore, to take recommendations against using new cryptography along with a healthy dose of reality. ❖

Terry Ritter is the owner of Ritter Software Engineering. He received a BS in engineering science from the University of Texas at Austin. He is a member of the IEEE Computer Society and the ACM. Contact him at ritter@io.com.

For More About Cryptography

Additional information about related topics can be found on Ritter's Web site (http://www.io.com/~ritter/), including a basic introduction to cryptography (http://www.io.com/~ritter/LEARNING. HTM), an extensive crypto glossary (http://www.io.com/~ritter/ GLOSSARY.HTM), literature surveys, Usenet conversations, crypto links, and his own work.