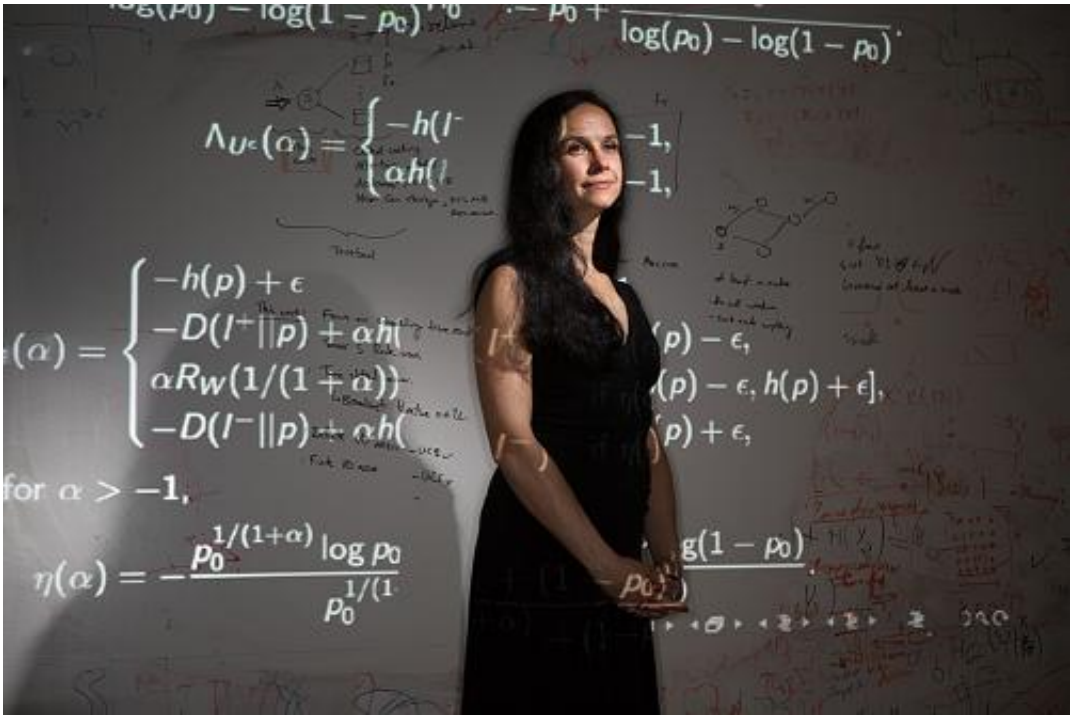
Encryption is less secure than we thought

August 14 2013, by Larry Hardesty



Muriel Médard is a professor in the MIT Department of Electrical Engineering. Credit: BRYCE VICKMARK

Information theory—the discipline that gave us digital communication and data compression—also put cryptography on a secure mathematical foundation. Since 1948, when the paper that created information theory first appeared, most information-theoretic analyses of secure schemes have depended on a common assumption.

Unfortunately, as a group of researchers at MIT and the National

University of Ireland (NUI) at Maynooth, demonstrated in a paper presented at the recent International Symposium on Information Theory (view PDF), that assumption is false. In a follow-up paper being presented this fall at the Asilomar Conference on Signals and Systems, the same team shows that, as a consequence, the wireless card readers used in many keyless-entry systems may not be as secure as previously thought.

In information theory, the concept of information is intimately entwined with that of entropy. Two digital files might contain the same amount of information, but if one is shorter, it has more entropy. If a compression algorithm—such as WinZip or gzip—worked perfectly, the compressed file would have the maximum possible entropy. That means that it would have the same number of 0s and 1s, and the way in which they were distributed would be totally unpredictable. In information-theoretic parlance, it would be perfectly uniform.

Traditionally, information-theoretic analyses of secure schemes have assumed that the source files are perfectly uniform. In practice, they rarely are, but they're close enough that it appeared that the standard mathematical analyses still held.

"We thought we'd establish that the basic premise that everyone was using was fair and reasonable," says Ken Duffy, one of the researchers at NUI. "And it turns out that it's not." On both papers, Duffy is joined by his student Mark Christiansen; Muriel Médard, a professor of electrical engineering at MIT; and her student Flávio du Pin Calmon.

The problem, Médard explains, is that information-theoretic analyses of secure systems have generally used the wrong notion of entropy. They relied on so-called Shannon entropy, named after the founder of information theory, Claude Shannon, who taught at MIT from 1956 to 1978.

Shannon entropy is based on the average probability that a given string of bits will occur in a particular type of digital file. In a general-purpose communications system, that's the right type of entropy to use, because the characteristics of the data traffic will quickly converge to the statistical averages. Although Shannon's seminal 1948 paper dealt with cryptography, it was primarily concerned with communication, and it used the same measure of entropy in both discussions.

But in cryptography, the real concern isn't with the average case but with the worst case. A codebreaker needs only one reliable correlation between the encrypted and unencrypted versions of a file in order to begin to deduce further correlations. In the years since Shannon's paper, information theorists have developed other notions of entropy, so¬me of which give greater weight to improbable outcomes. Those, it turns out, offer a more accurate picture of the problem of codebreaking.

When Médard, Duffy and their students used these alternate measures of entropy, they found that slight deviations from perfect uniformity in source files, which seemed trivial in the light of Shannon entropy, suddenly loomed much larger. The upshot is that a computer turned loose to simply guess correlations between the encrypted and unencrypted versions of a file would make headway much faster than previously expected.

"It's still exponentially hard, but it's exponentially easier than we thought," Duffy says. One implication is that an attacker who simply relied on the frequencies with which letters occur in English words could probably guess a user-selected password much more quickly than was previously thought. "Attackers often use graphics processors to distribute the problem," Duffy says. "You'd be surprised at how quickly you can guess stuff."

In their Asilomar paper, the researchers apply the same type of

mathematical analysis in a slightly different way. They consider the case in which an attacker is, from a distance, able to make a "noisy" measurement of the password stored on a credit card with an embedded chip or a key card used in a keyless-entry system.

"Noise" is the engineer's term for anything that degrades an electromagnetic signal—such as physical obstructions, out-of-phase reflections or other electromagnetic interference. Noise comes in lots of different varieties: The familiar white noise of sleep aids is one, but so is pink noise, black noise and more exotic-sounding types of noise, such as power-law noise or Poisson noise.

In this case, rather than prior knowledge about the statistical frequency of the symbols used in a password, the attacker has prior knowledge about the probable noise characteristics of the environment: Phase noise with one set of parameters is more probable than phase noise with another set of parameters, which in turn is more probable than Brownian noise, and so on. Armed with these statistics, an attacker could infer the password stored on the card much more rapidly than was previously thought.

"Some of the approximations that we're used to making, they make perfect sense in the context of traditional communication," says Matthieu Bloch, an assistant professor of electrical and computer engineering at the Georgia Institute of Technology. "You design your system in a framework, and then you test it. But for crypto, you're actually trying to prove that it's robust to things you cannot test. So you have to be sure that your assumptions make sense from the beginning. And I think that going back to the assumptions is something people don't do often enough."

Bloch doubts that the failure of the uniformity assumption means that cryptographic systems in wide use today are fundamentally insecure.

"My guess is that it will show that some of them are slightly less secure than we had hoped, but usually in the process, we'll also figure out a way of patching them," he says. The MIT and NUI researchers' work, he says, "is very constructive, because it's essentially saying, 'Hey, we have to be careful.' But it also provides a methodology to go back and reanalyze all these things."

The paper is titled "Brute force searching, the typical set, and guesswork."

More information: arxiv.org/pdf/1301.6356.pdf

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology