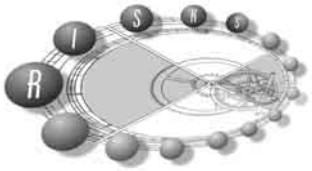

Why Security Standards Sometimes Fail

Security experts have long been saying that secure systems, and especially security standards, need to be designed through an open process, allowing review by anyone. Unfortunately, even openly designed standards sometimes result in flawed cryptographic systems. A recent example is the IEEE 802.11 wireless LAN standard, in which several serious cryptographic failures were found (see [1–3]) after millions of flawed hardware devices were sold.

Finding a cryptographic design flaw in an approved standard is bad news—especially after systems using it are in widespread use. Such a flaw is typically costly to fix. And, ironically, once a flawed system is widely deployed, future *fixed* versions of the system will almost certainly have a backward-compatibility mode, making them vulnerable as well. Cryptanalyzing the standard *before* it is ratified is clearly better for society and better for vendors. But is it better for the cryptanalyst? Unfortunately, we shall see that the answer is sometimes "no."

Cryptanalysts are usually scientists who make their own choices about which problems to work on. Furthermore, scientific success is measured by publications. Publishing high-visibility scientific articles in respected journals or conference proceedings can help establish academic fame, fortune, and tenure. So, consider a cryptanalyst, Carol, who is looking for a project to work on. Would she want to get involved in a standardization effort?

Working on a standard has its own set of challenges. A standards body involves many parties with conflicting agendas, many of them powerful corporations. Furthermore, a standard is not measured by excellence or novelty. It should be a working design that is an acceptable compromise between the interests of all the parties involved. In short, a standards body is not an environment that encourages scientific discourse. Finally, even supposedly open standards bodies sometimes have onerous requirements that may discourage scientists from participating.

Suppose that despite the challenges, Carol does get involved, and finds a cryptographic flaw in the standard's draft. Would this advance her scientific career? Unfortunately, not by much. First, it may be difficult for her to get the standards body to take action, because doing so might conflict with the interests of other parties. Secondly, Carol can expect very little credit for her contribution. A standard typically has no authors, and only the standard's editors are personally recognized. If Carol tries to publish an article describing her discovery, it will surely be rejected by any respectable scientific venue: every standard goes through drafts, many of them faulty; so, why should a specific flaw in an early draft be interesting? Finally, if the standard ends up not being used, then Carol's work (indeed, the work of the whole standards body) would go to waste.

Now consider what would happen if Carol finds the same flaw *after* the standard has been ratified, and after technology based on it is in widespread use. As an individual, she has much more to gain. Her work has obvious technical impact, because, by choice, the standard is already in use. She can certainly author an article about her findings; publishing it in a top-notch scientific venue would be relatively easy because of the public interest. Furthermore, security vulnerabilities are considered newsworthy outside of scientific circles: reporting services for such discoveries (such as BugTraq and CERT) have wide readership, and stories are occasionally reported by the general media. Such publicity is an effective way to cause Fortune 500 corporations to fix their products. All this excitement can make Carol a star in her field.

We see that for an individual scientist, cryptanalyzing an established standard is, potentially, much more rewarding than working to ensure the standard is secure in the first place. Luckily for society, there are reasons why many security standards do better than IEEE 802.11. Standardization is altruistic volunteer work for many participants, and this includes cryptanalysts. Also, cryptanalysts working in corporate research labs may be well motivated to contribute to a standard. But the basic conflict between the public good and the individual scientist's interests is a cause for concern. C

PAUL WATSON

References

1. Arbaugh, W.A. Shankar, N., and Wan, Y.C.J. Your 802.11 wireless network has no clothes. *IEEE Conference on Wireless LANs and Home Networks*, 2001.
2. Borisov, N., Goldberg, I., and Wagner, D. Intercepting mobile communications: The insecurity of 802.11. In Proceedings of the *7th ACM Conference on Mobile Computing and Networking*, 2001.
3. Fluhrer, S. Mantin, I., and Shamir, A. Weaknesses in the key scheduling algorithm of RC4. In *Proceedings of the 8th Workshop on Selected Areas in Cryptography*, 2001 .

Avishai Wool (yash@eng.tau.ac.il) is a senior lecturer in the Department of Electrical Engineering Systems, Tel Aviv University, Israel.