Schneier on Security

Quantum Cryptography: As Awesome As It Is Pointless

Bruce Schneier
Wired
October 16, 2008

Quantum cryptography is back in the news, and the basic idea is still unbelievably cool, in theory, and nearly useless in real life.

The idea behind quantum crypto is that two people communicating using a quantum channel can be absolutely sure no one is eavesdropping. Heisenberg's uncertainty principle requires anyone measuring a quantum system to disturb it, and that disturbance alerts legitimate users as to the eavesdropper's presence. No disturbance, no eavesdropper — period.

This month we've seen reports on a new working quantum-key distribution network in Vienna, and a new quantum-key distribution technique out of Britain. Great stuff, but headlines like the BBC's "'Unbreakable' encryption unveiled" are a bit much.

The basic science behind quantum crypto was developed, and prototypes built, in the early 1980s by Charles Bennett and Giles Brassard, and there have been steady advances in engineering since then. I describe basically how it all works in *Applied Cryptography, 2nd Edition* (pages 554-557). At least one company already sells quantum-key distribution products.

Note that this is totally separate from quantum computing, which also has implications for cryptography. Several groups are working on designing and building a quantum computer, which is fundamentally different from a classical computer. If one were built — and we're talking science fiction here — then it could factor numbers and solve discrete-logarithm problems very quickly. In other words, it could break all of our commonly used public-key algorithms. For symmetric cryptography it's not that dire: A quantum computer would effectively halve the key length, so that a 256-bit key would be only as secure as a 128-bit key today. Pretty serious stuff, but years away from being practical. I think the best quantum computer today can factor the number 15.

While I like the science of quantum cryptography — my undergraduate degree was in physics — I don't see any commercial value in it. I don't believe it solves any security problem that needs solving. I don't believe that it's worth paying for, and I can't imagine anyone but a few technophiles buying and deploying it. Systems that use it don't magically become unbreakable, because the quantum part doesn't address the weak points of the system.

Security is a chain; it's as strong as the weakest link. Mathematical cryptography, as bad as it sometimes is, is the strongest link in most security chains. Our symmetric and public-key algorithms are pretty good, even though they're not based on much rigorous mathematical theory. The real problems are elsewhere: computer security, network security, user interface and so on.

Cryptography is the one area of security that we can get right. We already have good encryption algorithms, good authentication algorithms and good key-agreement protocols. Maybe quantum cryptography can make that link stronger, but why would anyone bother? There are far more serious security problems to worry about, and it makes much more sense to spend effort securing those.

As I've often said, it's like defending yourself against an approaching attacker by putting a huge stake in the ground. It's useless to argue about whether the stake should be 50 feet tall or 100 feet tall, because either way, the attacker is going to go around it. Even quantum cryptography doesn't "solve" all of cryptography: The keys are exchanged with photons, but a conventional mathematical algorithm takes over for the actual encryption.

I'm always in favor of security research, and I have enjoyed following the developments in quantum cryptography. But as a product, it has no future. It's not that quantum cryptography might be insecure; it's that cryptography is already sufficiently secure.

Categories: Computer and Information Security

Tags: Wired

← Why Society Should Pay the True Costs of Security

Time to Show Bottle and Tackle the Real Issues →