

Interview with Bruce Schneier

Bruce Schneier, Counterpane, schneier@counterpane.com
 Marc Ruef, scip AG, maru@scip.ch

Bruce Schneier is an expert for cryptography and computer security, developer of popular crypto algorithms, author of many books and co-founder of Counterpane Internet Security.



scip AG: Hello Bruce. Thank you very much for your time. How is it going? Your assistant told me you were on a trip? Working off your speaking schedule (<http://www.schneier.com/schedule.html>)?

Bruce Schneier: Most of my travel involves some speaking these days. I've just come back from participating in a seminar called "The Politics of Fear" at Tufts University. Next week I am speaking to staffers in Congress about data mining, and giving a lecture at "The Politics of Fear". Later in the month, I head to Europe for a series of conferences. Quite a bit of my working life is like that these days.

When was the first time you seriously started with cryptography? Was math always a hobby of yours?

Cryptography was always a hobby, and I can remember the various children's cryptography books I used to own. I did some work in cryptography for the U.S. government, but I didn't become seriously immersed in the field until the early 1990s, when I was writing Applied Cryptography.

Usually artists and programmers have their "Baby": a creation they love very much. Regarding your developments in cryptography algorithms, which one are you most proud of? Why?

Like many engineers, I'm proud of the algorithms I developed that are being used. For that reason I would point to Twofish and Blowfish. But cryptography has an interesting twist on that: the true measure of a cryptographer is his breaks. When I look back at my work, it is my cryptanalysis papers-the papers that broke other people's algorithms in new and interesting ways-that I am most proud of.

Is there something you are working on at the moment that would be interesting for our readers?

Most of what I am doing these days is about how security works in context. It's not enough to have a good technical security solution, because so much of security has nothing to do with security. It's important to understand the economics of security, the psychology of security decision making, and the legal framework in which security works.

As you replied some years ago to my private email, you would not do a 3rd edition of your book, Applied Cryptography, because so many things have changed and new techniques introduced. Are you still denying a prospectively issue? This way, readers of Applied Cryptography would get some new intellectual food...

I've written a conceptual sequel; it's called Practical Cryptography (John Wiley & Sons, 2003). It's not the same book, though. Applied Cryptography was broad; it tried to survey the whole field of cryptography. Practical Cryptography is much more focused. It takes the basic problem of cryptography-setting up a secure channel between two people-and examines every aspect of it. I think it's a better book for someone who wants to understand cryptography, and a much better book for an engineer who is trying to learn how to code a cryptographic system.

„Cryptography has an interesting twist: the true measure of a cryptographer is his breaks.“

Do you think without code breaking World War II would have had a different ending? Some people say that WW I was won by chemists, WW II was won by physicists, and WW III will be decided by cryptologists. Do you think this is true? Is global terrorism the running World War?

Certainly cryptanalysis was a huge factor in World War II. Modern historians think that it shortened the war by two years or so. The reason is unique in history: the encryption machines were adding machine-era electromechanical devices, and the code-breaking machines were the world's first digital computers. That isn't true any more. While computer and network security techniques, both offensive and defensive, will play an important role in any hypothetical future "world war," I think cryptanalysis will play a minor role.

As to the "war on terror," that's a rhetorical war and not a real war. It makes no sense to declare war on an abstract noun. It makes no sense to declare war on a tactic. Further, it makes no sense to declare war on a tactic that has been with us for thousands of years, and will be with us for as long as we are a human civilization. Wars are declared by countries against countries, and end when one country is defeated or the two countries mutually declare peace. We already know what to call a tactic that has been with us since the beginning of civilization and will be with us until the end of civilization: crime. Terrorism is a particularly heinous and awful crime, but it is still a crime. Calling it a war only clouds our ability to deal with terrorism.

Restriction of the (public) use of cryptography allows the government to control and limit the behaviour and information exchange of the people. In most dictatorships this kind of censorship keeps the system "healthy." Do you think a democratic system should not allow the limitation of private information exchange? Or does the democratic community exchange their "freedom of secure speech" for security/safety (e.g. terrorism may be able to co-ordinate assessments)?

All technologies have good and bad uses. In this way, cryptography is no different from anything else. We all use cars to drive around, and the bad guys use them to flee from robberies. We all use telephones to communicate, and the bad guys use them to plan crimes. This is okay because society is overwhelmingly made up of good and honest people, and the positive uses of these technologies far outweigh the negative uses. Restricting cryptography is, as you said, a tool of a dictatorship. It's a tool of a police state. Any rhetoric about it being a way to fight terrorism is a lie; it's a way to control the rest of the population.

Sometimes customers would like to see "black-box" testing of their environment (e.g. network site or software development). As you have written in relation to cryptography, such "security by obscurity" is never real security at all. But do you think such "closed-source" testing may be useful in some cases or steps of a long-term project?

Of course. Security testing of closed-source systems can be very effective in improving products. It's time-consuming and expensive, but it's very effective. And it's exactly the same with

open-source testing. The difference is the economic model. In the closed-source model, the company developing the software pays experts to test and evaluate the security. In the open-source model, the developers throw the software out there and hope experts evaluate it out of the goodness of their hearts. Both models can result in well-tested software, and both models can result in lousy software. It's not whether the code is open or closed; it's who has evaluated it.

Phil Zimmermann's PGP (Pretty Good Privacy) is a nice solution and available to everyone who is interested in secure data exchange. But, surprisingly, not many companies or individuals are using it. What do you think are the reasons for this flop of PGP? Perhaps because the implementation is not well designed from user view? Or, perhaps because the concept of public key solutions is too complex for the average user? Do you use PGP on a regular basis?

PGP is not a flop. PGP Corporation is a viable company, and PGP is selling better than ever. It's taken this long for PGP to be successful for a number of reasons, primarily the fact that it was too hard to use. PGP Corporation has spent a lot of effort making its user interface better, and in many cases invisible.

„Any rhetoric about limiting cryptography being a way to fight terrorism is a lie.“

It's also true that e-mail encryption doesn't solve the most pressing security problems. Your data isn't likely to be eavesdropped on when it is in transit. It's much more likely to be eavesdropped on when it is sitting on your computer, by some bad guy who hacks into your network. PGP doesn't solve this problem.

PGP has another product, PGP Disk, that encrypts files and directories and drives - but that's something different entirely.

Do you think IPv6 and the security advantages of next generation IP protocol will solve most of today's privacy and network security issues? What do you think is the medium-term prediction for security businesses? Will companies be selling "magic security boxes" in the future, or will the consulting part of the business become more important than ever?

What will information security look like in 10 years?

Security is a process, not a product. The industry shows no sign of disappearing, but the solutions are looking more like services and less like products. This makes sense; the solutions need to react quickly as the threats evolve, and service-based solutions are better suited for that. I see this trend continuing. Another, parallel, trend is outsourcing. Organizations simply don't have the expertise or resources to deal with security issues directly, and it makes far more sense to outsource it. These trends have combined in Managed Security Services, which will take over more and more of security.

Do you know the TV series "Numb3rs" (2005)? What do you think of the idea of solving every problem with math and algorithms? Is this naïve, or is the real world truly assembled by numbers?

Every tool has its purpose, and no tool is useful in every situation. There are problems that lend themselves to math, and there are problems that don't. Security is one of those problems that doesn't, by the way. We can use the mathematics of cryptography to solve a very specific class of security problems, but the really hard ones are people problems.

And my last question, which is not a serious one at all. John Forbes Nash (American mathematician, shared the 1994 Nobel Prize in Economic Sciences) once said he is a very bad chess player. How is your chess game? Or do you prefer Scrabble?

I'm not a good chess player, either, although I couldn't tell you if it is from lack of ability or lack of practice. And I've never been good at memorization, which is what separates the serious Scrabble players from the hobbyis.

Thank you very much for the interesting interview. I wish you good luck for your journeys and chess games.

Publisher



scip AG
Technoparkstrasse 1
CH-8005 Zürich
+41 44 445 1818
<mailto:info@scip.ch>
<http://www.scip.ch>



Responsible person:
Marc Ruef
Security Consultant
+41 44 445 1812
<mailto:maru@scip.ch>

scip AG is an independent joint-stock company from Zürich, Switzerland. Since the founding in September 2002 the scip AG is focussed on consulting tasks in the field of IT security. Our main goal is given in the auditing and assessment of implemented security solutions so we can guarantee a maximum value of safety and security in the tested environments. To reach this goal and to provide a long-term benefit we do our penetration testing and security auditing with standardized and comprehensible procedures. Also further investigation if an exploitable weakness or a proofed incident has been detected is possible (log management or forensic analysis). Before the assembly of our team of specialists in 2002 all of the employees were already working together in the field of implementation of security architectures. So we possess some of the most important certifications in our field (e.g. Solaris, Linux, Checkpoint, ISS, Okena, Finjan, TrendMicro, Symantec), which are the foundation-stone of all of our projects. Just a bunch of information in penetration testing can be gathered in classes – Just years of real-world experience are able to be a guarantee for detecting all possible flaws and to make all attack attempts comprehensible at any time.