UABDIVULGA
BARCELONA RECERCA I INNOVACIÓ

05/2008

Bruce Schneier, expert on computer security

"The problem is not the cryptography in a communication process, the problem is everything around it"

Bruce Schneier, often described as a computer security guru, is an internationally renowned security technologist and author. Schneier is the founder and chief technology officer of BT Counterpane, a company that sells managed computer network security services. Regularly quoted in the media, Schneier has written numerous pieces for several major newspapers, and has testified on security before the United States Congress on many occasions. Bruce Schneier visited the UAB on the occasion of the celebration of the Year of Computing.

Bruce Schneier, often described as a computer security guru, is an internationally renowned security technologist and author. Schneier is the founder and chief technology officer of BT Counterpane, a company that sells managed computer network security services. Regularly quoted in the media, Schneier has written numerous pieces for several major newspapers, and has testified on security before the United States Congress on many occasions. Bruce Schneier visited the UAB on the occasion of the celebration of the Year of Computing.

At a personal level, wich is the best way to maintain our data and our computers secure? Any practical advice?

For most users the best thing they can do is make back-ups. Because for most people, security equals reliability, and when something bad happens to their computers they loose their data. After that, having an antivirus program. That's important. Turn on the Windows firewalls… those are little things you can do. But make good back-ups and keep making good back-ups. That is the most important thing.

Is free software more or less secure than privative software?

Secure software is software that has been analysed, and there are two ways for analize software. One is a company can hire people to analyse software, and the other is free software whose open source can be analysed by the comunity. In both cases there is a lot of free software that nobody looks at, there is lot of commercial software that is not analysed, so both can be secure and both can be insecure. So it is not a matter of free software being more secure or less secure. There is a different method for software analysis. Software that is analised by experts is more secure.

Is any hardware platform (mac or pc) more secure than the other one?

You allways want to now wich hardware is more secure. There are two different questions to ask. One is, wich one is theoretically more secure out of box. If you take Windows, Makintosh and Unix and analyse them, wich one will be more secure. The other one is wich one is operationally more secure. And we don't the answer to the first, but we know the answer to the second: Windows is the least secure because is the biggest target. If you are a hacker, you are going to write software that will affect the most possible machines. So you're more secure with Mac or Unix not necessarily because they are more secure operating systems, but because they are less popular.

Do you consider cyber-crime as serious problem?

I don't think that cyber-crime is serious yet. But it is getting more serious every year. Criminals have discovered cyberspace as a source of money, as a source of fraud. And they are increasingly using it. And cyber-crime is becoming more popular, so it is becoming more professional. We are seeing more organized crime, more cybercrime with the bussiness model. I think it is becoming increasingly a big problem until we solve it.

Being quite pessimistic, a general attack and collapse of the communication and data storage system of a whole country would be very devastating. Do you think it could really happen?

I think a wide internet collapse is much less likely than the press likes to talk about. Internet is surprisangly survivable. Certainly its survivable against hardware attacks, and even software attacks. We see them again and again and the internet doesn't collapse, eventhough it is very fragile. So it is more resilient than people give it the credit for.

Is quantum criptography absolutely reliable for the interchange of information?

There are lots of encription methods that are absolutely secure. Nobody needs quantum cryptography because the none quantum sfuff is so good. The problem is not the cryptography, the problem is everything around the cryptography: the computer, the network, the user. Those are the problems. Regardless of the algorithm we use, whether it is quantum or not, it doesn't matter, those problems don't change. We already have us much cryptography as we need. And it is as secure as it can possibly be. And no one will break it. But everything else is so bad that no one has to break the cryptography.

One of the main quotidiane problems of general users is the spam. Is there any effective solution for that?

Really, spam is one of computer security success stories. There are lots of companies out there that would clean spam out of your Inbox, and they all work really well. Whether it is Red Condor, or Postini, or any of the others. I don't get any spam anymore. Spam is a huge problem in the backbone. But they are really good at getting rid of it after receiving it. If you get a lot of spam is because you are not using a spam filter. So go to an ISP that uses spam filter, and you will not get spam anymore.

Why don't we have spam on the mobile phone?

There is spam on the mobile phone, just not a lot of it. And we are going to see more of it. I do get ocassionally SMS spam. And I do see spam on my mobile e-mail address. Not a lot, but a little bit. But as it becomes more popular, you are going to see more as a vehicle of spam.

Entrevista: Octavi López Coronado

View low-bandwidth version