THE INTERNET: ANONYMOUS FOREVER

Universal identification is portrayed by some as the holy grail of Internet security. Anonymity is bad, the argument goes; and if we abolish it, we can ensure only the proper people have access to their own information. We will know who is sending us spam and who is trying to hack into corporate networks.

And when there are massive denial-of-service attacks, such as those against Estonia or Georgia or South Korea, we will know who was responsible and take action accordingly.
The problem is that it will not work. Any design of the Internet must allow for anonymity. Universal identification is impossible. Even attribution - knowing who is responsible for particular Internet packets - is impossible. Attempting to build such a system is futile, and will only give criminals and hackers new ways to hide.

Imagine a magic world in which every Internet packet could be traced to its origin. Even in this world, our Internet security problems would not be solved. There is a huge gap between proving that a packet came from a particular computer and that a packet was directed by a particular person. This is the exact problem we have with botnets, or pedophiles storing child porn on innocents' computers. In these cases, we know the origins of the DDoS packets and the spam; they are from legitimate machines that have been hacked. Attribution is not as valuable as you might think.

Implementing an Internet without anonymity is very difficult, and causes its own problems. In order to have perfect attribution, we would need agencies - real-world organizations - to provide Internet identity credentials based on other identification systems: passports, national identity cards, driver's licenses,

whatever. Sloppier identification systems, based on things such as credit cards, are simply too easy to subvert. We have nothing that comes close to this global identification infrastructure. Moreover, centralizing information like this actually hurts security because it makes identity theft that much more profitable a crime.

And realistically, any theoretical ideal Internet would need to allow people access even without their magic credentials. People would still use the Internet at public kiosks and at friends' houses. People would lose their magic Internet tokens just like they lose their driver's licenses and passports today. The legitimate bypass mechanisms would allow even more ways for criminals and hackers to subvert the system.
On top of all this, the magic attribution technology does not exist. Bits are bits; they do not come with identity information attached to them. Every software system we have ever invented has been successfully hacked, repeatedly. We simply do not have anywhere near the expertise to build an airtight attribution system.

Not that it really matters. Even if everyone could trace all packets perfectly, to the person or origin and not just the computer, anonymity would still be possible. It would just take one person to set up an anonymity server. If I wanted to send a packet anonymously to someone else, I would just route it through that server. For even greater anonymity, I could route it through multiple servers. This is called onion routing and, with appropriate cryptography and enough users, it adds anonymity back to any communications system that prohibits it.
Attempts to banish anonymity from the Internet will not affect those savvy enough to bypass it, would cost billions, and would have only a negligible effect on security. What such attempts would do is affect the average user's access to free speech, including those who use the Internet's anonymity to survive: such as dissidents in countries violating human rights.

Mandating universal identity and attribution is the wrong goal. Accept that there will always be anonymous speech on the Internet. Accept that you will never truly know where a packet came from. Work on the problems you can solve: software that's secure in the face of whatever packet it receives, identification systems that are secure enough in the face of the risks. We can do far better at these things than we are doing, and they will do more to improve security than trying to fix insoluble problems.
The whole attribution problem is very similar to the copy-protection/digital-rights-management problem. Just as it is impossible to make specific bits not copyable, it is impossible to know where specific bits came from. Bits are bits. They do not naturally come with restrictions on their use attached to them, and they do not naturally come with author information attached to them. Any attempts to circumvent this limitation will fail, and will increasingly need to be backed up by the sort of real-world police-state measures that the entertainment industry is demanding in order to make copy-protection work.

Just as the music industry needs to learn that the world of bits requires a different business model, law enforcement and others need to understand that the old ideas of identification do not work on the Internet. For good or for bad, whether you like it or not, there is always going to be anonymity on the Internet.

http://www.schneier.com/essay-308.html
This essay previously appeared in Information Security and in Forbes as the first half of a point-counterpoint with Marcus Ranum (counterpoint which can be found at http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1380347,00.html)
This article was republished with the author's permission.

* Bruce Schneier is an internationally renowned security technologist and author. Described by The Economist as a "security guru", he is the author of Applied Cryptography, Secrets and Lies, Beyond Fear and Schneier on Security. Regularly quoted in the media - and subject of an Internet meme - he has testified on security before the United States Congress on several occasions and has written articles and op eds for many major publications, including The New York Times, The Guardian, Forbes, Wired, Nature, The Bulletin of the Atomic Scientists, The Sydney Morning Herald, The Boston Globe, The San Francisco Chronicle, and The Washington Post. Schneier also publishes a free monthly newsletter, Crypto-Gram, with over 150,000 readers. In its ten years of regular publication, Crypto-Gram has become one of the most widely read forums for free-wheeling discussions, pointed critiques, and serious debate about security. Schneier is the Chief Security Technology Officer of BT.

More from the author can be found at www.schneier.com