CHARLES ARTHUR

Academics should not remain silent on hacking

The revelation that US and British spy agencies have undermined a commonly used encryption code should alarm researchers, says **Charles Arthur**.

Secrecy doesn't come naturally to journalists, but sometimes it is thrust upon us. Earlier this year, there was a room in *The Guardian*'s offices in London that nobody could enter alone. On a table outside by a security guard was a tidy collection of phones and other devices; nothing electronic was allowed. Inside were a coffee maker, a shredder, some paper and a few computers. All were brand new; none had ever been connected to the Internet. None ran Microsoft Windows. All were encrypted; each required two passwords, held by different people.

This is where the biggest news stories of this year lived — away from the Internet. This was where *The Guardian* analysed the 'Snowden files' (classified documents released to the press by former US National Security Agency (NSA) contractor Edward Snowden). These revealed, among other things, that the NSA and the United Kingdom's GCHQ were running enormous efforts to crack encrypted communications online, and that they had worked to undermine the strength of encryption standards such as that used — and recommended — by the US National Institute of Standards and Technology (NIST). (The computers sadly are no more — smashed in *The Guardian* basement on the orders of the British government.)

NIST's standard for random numbers used for cryptography, published in 2006, had been weakened by the NSA. Companies such as banks and financial institutions that rely on encryption to guarantee customer privacy depend on this standard. The nature of the subversions sounds abstruse: the random-number generator, the 'Dual EC DRBG' standard, had been hacked by the NSA so that its output would not be as random as it should have been. That might not sound like much, but if you are trying to break an encrypted message, the knowledge that it is hundreds or thousands of times weaker than advertised is a great encouragement.

ACADEMICS IN CRYPTOGRAPHY AND SECURITY SHOULD MAKE THEMSELVES A PROMISE: 'WE WON'T GET FOOLED AGAIN.'

It was, to be frank, a big deal. In the world's universities, computer scientists and mathematicians spend their careers trying to develop secure systems, and yet here was evidence of a systematic — and successful — attempt to undermine that work. Executives at companies such as Google, Yahoo, Facebook and Microsoft, which discovered that their internal networks were being tapped and their systems infiltrated, were furious. But a few isolated shouts of protest aside, the academic community has largely been silent.

That's disappointing. Academia is where we expect to hear the free flow of ideas and opinions. Yet it has been the commercial companies that have made the most noise — because the revelations threaten trust in their businesses. Don't academics also see the threat to open expression, and to the flow of dissident ideas from countries where people might fear that their communications are being tapped and, even if encrypted, cracked?

➲ NATURE.COM
Discuss this article online at:
go.nature.com/rklbwy

Some get it. Ross Anderson, a security researcher at the University of Cambridge, UK, has been highly critical and outspoken. When I spoke to him in September, soon after the NIST revelation, he called it "a wake-up call for a lot of people" and added: "This has been a 9/11 moment for the community, and it's great that some people are beginning to wake up."

Kenneth White, principal scientist at health-information company Social & Scientific Systems in Silver Spring, Maryland, says: "Just a year ago, such a story would have been derogated by most of my colleagues as unwarranted suspicion at best and outright paranoia at worst. But here we are."

Anderson has an explanation for the muted response: he says that a number of British university departments have been quietly coerced by the GCHQ. The intelligence-gathering agency has a substantial budget, and ropes in academics by offering access to funds that ensures their silence on sensitive matters, Anderson says. (If that sounds like paranoia, then see above.)

I have not been able to confirm his claims, but what are the alternatives? One is that the academics are simply too busy going back over their own work looking to see if they agree with the claimed weaknesses. The other is that they simply don't care enough.

For those who do care, White and Matthew Green, who teaches cryptography at Johns Hopkins University in Baltimore, Maryland, have embarked on an ambitious effort to clean up the mess — one that needs help.

They have created a non-profit organization called OpenCryptoAudit.org, which aims to recruit experts to provide technical assistance for security projects in the public interest, especially open-source security software. A similar effort initiated by White and Green is checking the open-source software called TrueCrypt, which is widely used to lock down hard drives during foreign travel (see go.nature.com/nsvdjh).

Concerns over the security of the NIST Dual EC DRBG standard were raised in 2007, but too few academics spoke out then. The events of 2013 must make them rethink. Cryptography rarely reaches the headlines, but now it has done so for all the wrong reasons. For 2014, academics working in cryptography and security should make themselves a promise: 'We won't get fooled again.' And most of all, 'We won't go down quietly.' ■

Charles Arthur *is technology editor of* The Guardian *in London.*
e-mail: charles.arthur@gmail.com