The back door to your PCs, smartphones that can’t close

John Naughton
London
THE OBSERVER

A remarkable conference held at the Aspen Institute in 2011, Gen. Michael Hayden, a former head of both the National Security Agency and the Central Intelligence Agency, said something very interesting. In a discussion of how to secure the “critical infrastructure” of the United States, he described the phenomenon of compromised computer hardware — namely, chips that have hidden “back doors” inserted into them at the design or manufacturing stage — as “the problem from hell.” And, he went on, “frankly, it’s not a problem that can be solved.”

Hayden is an engaging, voluble, likable fellow; he’s popular with the hacking crowd because he doesn’t talk like a government suit. But sometimes one wonders if his agreeable persona is actually a front for something a bit more disingenuous. Earlier in the Aspen discussion, for example, he talked about the Stuxnet worm — which was used to destroy centrifuges in the Iranian nuclear program — as something that was obviously created by a nation state. But he affected not to know that the United States was one of the nation states involved.

Given Hayden’s background and level of security clearance, it seems inconceivable that he didn’t know who built Stuxnet. So already one had begun to take his contributions with a modicum of salt. Nevertheless, his observation about the intractability of the problem of compromised hardware seemed incontrovertible. This is because covertly modified hardware is hard to detect — much more so than dodgy software. The hardware in a computer can do things like access data in ways that are completely invisible even to the machine’s security software. At the Black Hat security conference in August 2012 in Las Vegas, for example, a researcher named Jonathan Brossard demonstrated software that can be burned into the hardware of a PC, creating a back door that would allow secret remote access over the Internet. And — here’s the really scary bit — the secret entrance couldn’t even be closed by switching off the computer’s hard disk or reinstalling its operating system.

The reason why this is so scary is because virtually every bit of kit that runs your computer is susceptible to this kind of attack. Each piece of hardware is designed by another company, which in turn employs third parties to design and manufacture it. And each of those companies will employ yet another vendor to create the software that will run on it. The result is a tangled web of possible back doors, with no clear way to check that each chip hasn’t been modified in some way.

The problem is made worse by the fact that the chips themselves are often produced in China, where the authorities have access to a vast database of computer hardware specifications. This database is used by companies like TSMC, the world’s largest chip producer, to ensure that the chips it makes conform to international standards. And, worryingly, the same database is used by the Chinese government to ensure that its chips are not compromised.

So what can be done to address this problem? One solution is to make sure that all hardware is designed and manufactured by companies that have a proven track record of producing secure products. This would require a major overhaul of the global supply chain, and it would be expensive. But it could be done.

Another solution is to ensure that all hardware is tested for security before it is sold. This would require a major investment in testing infrastructure, but it could be done. And it’s not just hardware that needs to be tested; software needs to be tested as well.

In the end, however, the best solution is to make sure that all hardware is designed and manufactured by companies that have a proven track record of producing secure products. This will not be easy, but it is essential if we are to protect our critical infrastructure from the threat of compromised hardware.
software. At the Black Hat security conference in August 2012 in Las Vegas, for example, a researcher named Jonathan Rosea demonstrated software that can be burned into the hardware of a PC, creating a back door that would allow secret remote access over the Internet. And — here's the really scary bit — the secret entrance couldn't even be closed by switching off the computer's hard disk or reinstallation of its operating system.

The reason it's not happened yet is because virtually every bit of kit that runs the Internet — the machine on which you compose your emails, the tablet or smartphone with which you browse the Net, the routers that pass on the data packets that comprise your email or your Web search, everything — is a computer. So the thought that all this stuff might someday be under the control of the NSA in ways that are impossible to detect is terrifying. It's this fear that underpins American (and British) reservations about network products made by the Chinese company Huawei — the suspicions (vexingly denied by Huawei, of course) that the kit has secret back doors installed in it to facilitate a Chinese cyber-army's penetration of Western networks. As the Washington Post reports: "It is a problem from hell. If the hardware that runs the Internet has been polluted or infiltrated then we're all screwed, because there's no bit of cyberspace you can trust. And I know, I know: it sounds like paranoia — until you discover that Darpa, the research arm of the U.S. Department of Defence (DoD), has launched a massive research project into compromised hardware.

The department's growing dependence on the global supply chain, it says, "makes device, software and firmware security an imperative. Back doors, malicious software and other vulnerabilities unknown to the user could enable an adversary to use a device to accomplish a variety of harmful objectives, including the exfiltration (extraction) of sensitive and the sabotage of critical operations. Determining the security of every device DoD uses in a timely fashion is beyond current capabilities."

At this point we enter a Kafka-esque world of smoke and mirrors. Because one of the most obvious inferences from the Edward Snowden revelations published by The Guardian and The New York Times and ProPublica recently is that the NSA has indeed been up to the business of inserting covert back doors in networking and other computing kit. The reports say that, in addition to undermining all of the mainstream cryptographic software used to protect online commerce, the NSA has been "collaborating" with technology companies in the United States and abroad to build entry points into their products.

These reports have, needless to say, been strenuously denied by the companies, such as Cisco, that make this networking kit. Perhaps the NSA omitted to tell Darpa what it was up to? In the meantime, I hear that some governments have decided that blacklisting these companies is the only way to ensure these electronic communications at all, and are returning to employing couriers who travel the world handcuffed to locked dispatch cases. We're back to the future, again.