'Back Door' Discovered in Chip Used in Boeing 787 and Military Systems

by Charles Arthur via styx - Guardian UK *Wednesday, May 30 2012, 2:05pm*
international / mass media / other press

> This is not a new discovery. It has been known for some time that major chip manufacturers create 'back doors' in their products. The usefulness of these undocumented features will soon be weighed against the extreme dangers they pose.

Two Cambridge experts have discovered a "back door" in a computer chip used in military systems and aircraft such as the Boeing 787 that could allow the chip to be taken over via the internet.

The discovery will heighten concerns about the risks of cyber-attacks on sensitive installations, coming on the heels of the discovery this week of the 'Flamer' virus which has been attacking computer systems in Iran, Syria and Saudi Arabia.

In a paper that has been published in draft form online and seen by the Guardian, researchers Sergei Skorobogatov of Cambridge University and Chris Woods of Quo Vadis Labs say that they have discovered a method that a hacker can use to connect to the internals of a chip made by Actel, a US manufacturer.

"An attacker can disable all the security on the chip, reprogram cryptographic and access keys ... or permanently damage the device," they noted.

Woods told the Guardian that they have offered all the necessary information about how the hack can be done to government agencies – but that their response is classified.

"The real issue is the level of security that can be compromised through any back door, and how easy they are to find and exploit," Woods said.

The back door may have been inserted by Actel itself, whose ProASIC3 chip is used in medical, automotive, communications and consumer products, as well as military use.

Woods said that "a back door is an additional undocumented featured deliberately inserted into a device for extra functionality" – in effect, a secret way to get into the chip and control it.

Crucially, in this case it exists as part of the design of the silicon chip – meaning that it cannot be removed because it is inherent in how the chip reacts to certain inputs. He suggested that it may have been put there by design by Actel, because there are some traces of the existence of such a back door in the system files of Actel development software.

But, he said, that creates serious risks: "The great danger comes from the fact that such a back door undermines the high level of security in the chip making it exposed to various attacks. Although Actel makes a big claim that their devices are extremely secure because there is no physical path for the configuration data to be read to the outside world, a back door was added with a special key to circumnavigate all the security set by themselves or one of their users."

Connecting to the chips would be comparatively easy over the internet if the chip is wired to an internet-enabled controller, he said. Normally a special cryptographic key would be needed, but the back door does not need an encrypted channel.

Among applications where the ProASIC3 are used are remote surveillance systems, drones, and for flight-critical applications on the new Boeing 787 Dreamliner.

Actel did not respond to requests for comment by the time of publication.

Rik Ferguson, director of security research at the online security company Trend Micro, said: "This kind of flaw that gives somebody access right into the device has inherent flaws. The fact that it's in the hardware will certainly make it harder – if not impossible – to eradicate. We're already seeing a steady flow of devices such as digital picture frames coming out of factories with malware already on them – but that's software which can be fixed. If you have this sort of flaw, then you need to replace the hardware, which means the chips."

But suggestions that it is part of a cyber-attack by China, where the chip is made, have been discounted.

"It was very likely done at the design stage," said Woods. "However, the traces left in the Actel development software suggest that this feature was well thought through from the very beginning." He doubts it is part of a Chinese state-sponsored sabotage attempt.

Skorobogatov and Woods will present a paper on their findings at a conference in Belgium in September.

© 2012 Guardian News and Media Limited

http://www.guardian.co.uk/technology/2012/may/29/cyber-attack-concerns-boeing-chip?intcmp=239