AXIADO

PRESS RELEASE

For Immediate Release on September 27th, 2018

Axiado announces a truly secure boot that doesn't "brick" the system

SAN JOSE, California, September 27, 2018—In response to the market need for a truly secure system as evidenced by recent DDoS attacks, such as VPNFilter, Axiado has developed a boot subsystem that achieves true security without the risk of "bricking" the system. Axiado's secure boot includes tamper proof authentication of both the code and the user, and full encryption of the code.

"The boot process is the most fundamental part of every system start-up. If the boot code is compromised, nothing else matters, because either the system is dead or hacked," says Axel Kloth, founder and CTO of Axiado.

The boot sequence has recently become a popular attack point for hackers, because it is the initial start-up process of every digital system, hence providing access to changing the behavior of the system to gain complete access. Until now, developers have claimed a boot process that provides some level of security. Nevertheless, today's processors fail to provide a truly secure start up since they do not authenticate the user executing the BIOS update nor the integrity of the boot code, and they do not guarantee that the code is free of malware or that it has not been tampered with. In these processors, an interrupted or compromised boot code "bricks" the device, which prevents subsequent booting and makes the device inoperable permanently. The currently accepted but unsecure practice of attempting to recover from bricking is to disable the Trusted Platform Module (TPM) coprocessor. This procedure, however, makes it possible to install malicious software into the BIOS, resulting in either an non-secure or a possibly permanently inoperable system.

Axiado's boot subsystem does three things that other developers have not been able to demonstrate: (1) it authenticates the person or organization executing the BIOS update, (2) authenticates (signs) the code, and (3) encrypts the code. Due to these capabilities and Axiado's unique architecture, attacks against Axiado's secure boot will not be able to penetrate the system and alter the BIOS, and hence, not result in bricking. Furthermore, systems that require continuous availability will benefit from in-service upgrades of the firmware. To our knowledge, no one else has been able to do this yet.

“What we have achieved is the foundation for a secure internet,” said Ashok Babbar, CEO and Chairman of Axiado. “Axiado’s fully secure boot can be deployed, for example, in financial services, manufacturing, businesses, and data centers. It is the first one of a comprehensive set of proactive defenses that are built in Axiado’s security platform.”

Rik Turner, an analyst at Ovum says that “if Axiado can demonstrate that its boot is truly secure, they can claim having the primary pillar for an impenetrable digital system.”

View a demonstration of Axiado’s secure boot at https://axiado.com/secureboot/

About Axiado

Axiado is a fabless cybersecurity processor company securing the digital infrastructure at the 1st point of intrusion™. The company has rearchitected both the computational and networking stacks, and developed a breakthrough cybersecurity platform from the ground up to remove the security holes that processors and operating systems exhibit today. Axiado's security platform comprises of a microprocessor, firmware, OS kernel and APIs.

Press kit available at https://axiado.com/press/

Discover more at https://axiado.com and follow us on Twitter at security@axiado.corp.

Axiado™ and Axiado logo are trademarks of Axiado Corporation.

MEDIA CONTACT:
Minna Holopainen, VP Communication

Axiado Corporation
minna.holopainen@axiado.com