A Survey of Secure Boot Schemes for Embedded Devices

Rui Wang*, Yonghang Yan**

*School of Computer Science and Technology, Xidian University, Xi'an, China

** School of Computer Science and Information Engineering, Henan University, Kaifeng, China,
**corresponding author

ruigelwang@163.com, yanyonghang@henu.edu.cn

***Abstract*—With the rapid development of Internet of things and wireless communication technology, embedded devices are widely used in every aspect of our daily lives. Due to the lack of built-in security mechanism, the embedded devices are facing more and more threats from the malicious code attack, DDoS attack and so on. Secure boot technology can assure that the device boots up with an untampered and authorized software provided by a legitimate vendor and becomes a critical step in the device firmware and software security at the booting time. Aiming at designing and implementing the secure booting schemes, researchers have presented many effective approaches. This paper summarizes existing secure boot schemes for embedded devices and compares and analyses the advantage and disadvantages of these existing schemes.**

***Keyword*—secure boot; embedded devices; TPM; TrustZone; TEE**

Rui Wang (M'2021, Luoyang, 1995) received B.S. degree in computer science and technology from Henan University at 2018. And now she is a postgradute in computer science and technology from Xidian University, Xi'an, China. Her research interest contains trusted computing.

Yonghang Yan (Zhoukou, 1981) received B.S. degree in computer science and technology from Zhengzhou University at 2004, M.S. degree in computer science and technology from Beijing Institute of Technology at 2007 and Ph.D degree in computer science and technology from Beijing Institute of Technology at 2014. His research interests include computer network, Mobile Ad hoc and Sensor Network, UAV network, mobile computing network and QoS.
Now he is an associate professor in the School of Computer and Information Engineering at Henan University, Kaifeng, China. He is the head of advanced network technology laboratory.