A Novel Trusted Boot Model for Embedded Smart Device without TPM

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*—Embedded smart devices are widely used in people's life, and the security problems of embedded smart devices are becoming more and more prominent. Meanwhile lots of methods based on software have been presented to boot the system safely and ensure the security of the system execution environment. However, it is easy to attack and destroy the methods based on software, which will cause that the security of the system cannot be guaranteed. Trusted Computing Group proposed the method of using Trusted Platform Module (TPM) to authenticate the credibility of the platform, which can solve the disadvantages of using methods based on software to protect the system. However, due to the limited resource and volume of embedded smart devices, it is impossible to deploy TPM on embedded smart devices to ensure the security of the system operating environment. Therefore, a novel trusted boot model for embedded smart devices without TPM is proposed in this paper, in which a device with TPM provides trusted service to realize the trusted boot of embedded smart devices without TPM through the network and ensure the credibility of the system execution environment.**

***Keyword*—Trusted Boot; Embedded Smart Devices; Trusted Services; TPM**

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.