Secure device identity using PUFs

802.1AR [1] Secure Device Identity is an IEEE standard. It specifies a unique device identification (DevID) which is cryptographically bound to the device. This DevID can be used to create trust between the devices. The standard also specifies the ways to authenticate the devices using the secure identity. The DevID can also help in authenticated key exchange in other protocols e.g 802.1AF, 802.1X [2].

The 802.1AR standard is not widely used in current networks. The problem with this standard is that it does not specify how to generate the cryptographically bound DevID. One way to generate this DevID is to attach a hardware based security module such as TPM chip to the device. This solution can work for high-end devices like servers, but it is inefficient to add these hardware security chips to low power IoT devices, which constitute most of the Internet today.

Our Idea is to generate the 802.1AR DevID by using PUFs. Uninitialized memory on the IoT devices can be used as PUF. We can use fuzzy extraction algorithm [3] to generate the DevID for the device. The Advantage of this PUF implementation is that it is fully software based and there is no need for additional hardware security chips like TPM to generate DevID. A white list of valid DevIDs can be installed in the devices before deployment to enable trust between the devices. PKI based solution can also be used to establish the trust when a new device joins a network.

References

[1] Ieee standard for local and metropolitan area networks - secure device identity. *IEEE Std 802.1AR-2009*, pages 1–77, Dec 2009.

[2] Ieee standard for local and metropolitan area networks–port-based network access control. *IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004)*, pages 1–205, Feb 2010.

[3] Reyzin Leonid Smith Adam Dodis, Yevgeniy. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Advances in Cryptology - EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings*, 2004.