Entropy as a Service

Unlocking the full potential of cryptography

The Challenge

In today's ever-more-connected world, everything from traditional devices to devices on the Internet of Things (IoT) must communicate securely on the Internet, otherwise critical information could be at stake, whether that is a username/password, mobile banking information, or important medical records.

Cryptography is critical for securing data at rest or in transit on the IoT. But cryptography fails when a device uses weak keys, low-entropy randomness, or inaccurate time sources.

Why Should You Care?

Standard deterministic computers have trouble producing good randomness, especially IoT-class devices that have little opportunity to build entropy locally before they begin network communications. The best sources of true randomness are based on unpredictable physical phenomena, such as quantum effects but they can be impractical to include in IoT devices.

Finding ways to unlock the full potential of cryptography to secure data on the IoT can offer hope for better future.

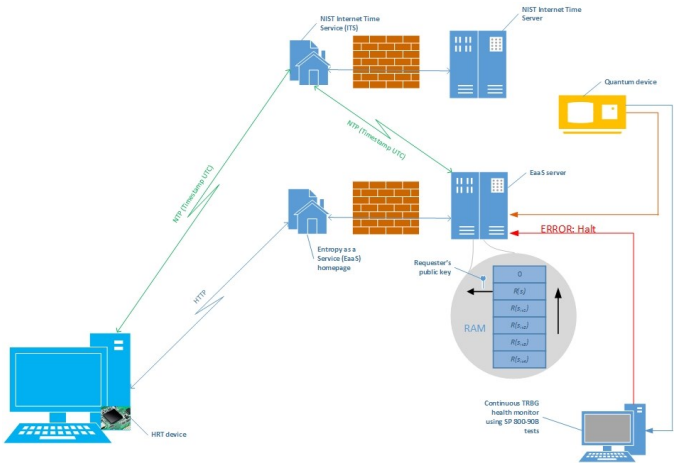

Figure 1: Basic Architecture of EaaS

Our Solution

Entropy as a Service (EaaS) is a novel Internet service architecture providing secure time and quantum entropy sources to IoT devices. The main components of the base EaaS architecture are shown in Figure 1. The critical components are the quantum entropy device, the EaaS server and a hardware root of trust device (TPM, Intel® IPT, ARM® TrustZone®) in the client system.

EaaS does not generate keys; it only enables client systems to generate strong cryptographic keys without any possibility for the EaaS server to gain any insight into the client keys.

Many today do not trust any centralized authority for a service of such fundamental importance. EaaS is designed to distribute and aggregate trust across a scalable collective of participants, yielding a collective authority. By combining known cryptographic techniques in novel ways, EaaS provides fresh timestamps and entropy to IoT devices on boot. The architecture distributes trust across thousands of servers scattered around the world: scalable enough that every country's government and every major technology company in the world could participate directly in the decentralized root of trust, each actively and independently ensuring that all others "stay honest." The architecture is open and reviewable by experts.

More Information Available: http://csrc.nist.gov/projects/eaas/	**Contacts:** Apostol Vassilev, Apostol.Vassilev@nist.gov Harold Booth, Harold.Booth@nist.gov Robert Staples, Robert.Staples@nist.gov