The Problems of Weak Entropy are well known

Entropy as a Service (EaaS)

Proposal:
- Essential for CMVP automation.
- High entropy random data available as service over the network.
- Provably robust entropy source
- Secure delivery
- Serves large number of needy devices

Entropy Server
- Quantum entropy source provides continuous random data to FIFO buffer in memory
- Responds to client requests by removing random values, encrypting, sending to client

Client Devices
- Request and consume entropy (key establishment, nonces, authentication)
- Dedicated software protected by trusted hardware (e.g., TPM, Arm TrustZone)


EaaS Architecture

EaaS: Request/Response Protocol

NIST:
• HTTP GET request
• XML response with encrypted, signed payload
• NTP timestamps prevents replay attacks

Our suggestion:
• HTTP over TLS (HTTPS) GET request
• Eliminate NTP
• JSON response from server

EaaS Req/Rsp: HTTP over TLS (HTTPS)

**TLS 1.3** (or 1.2 for now)
- Authentication
- Encryption
- Replay protection

• Leverage standard implementation
• Connection-level encryption handles need to encrypt entropy
• TLS 1.3 reused for secure data exchange and EaaS.

**Bootstrapping? Solutions:**
- Pre-configured symmetric key (AES)
- Pre-configured entropy bits
- Generate quality entropy bits through longer boot time
- Weak entropy source, but used only for brief initial time window
- Secure Enclave

---

EaaS: Entropy Source

NIST:
• True RBG = True Random Bit Generator (e.g., quantum device)
• SP 800-90B compliant
• Continuous monitoring solution

Client Entropy Usage:
• IoT device: May not trust underlying entropy source
• VMs/Containers in cloud: Cloning replicates DRBG state, requires reseeding
• Mixing function can be used to combine weak entropy with high-quality EaaS entropy, or to mix entropy sources
EaaS Scaling: JSON command set Prototype

Setup Notes:

- EaaS Server: running VMware ESXi
- Clients: VMware Photon OS running on ESXi
EaaS Scaling: Two Servers, Network Connection

Shows:
- Number of IoT devices that can be comfortably supported over a network

Setup notes:
- Includes 100 Gbps network between EaaS server and emulated IoT devices
- But, no appreciable transmission time, queuing delay, congestion effects
Call to Action

• Critical steps for EaaS adoption:
  • Updating 800-90B in recognizing EaaS as an entropy source
  • Formal procedure to validate EaaS service
    • Or existing entropy test & justification procedure is good enough?
  • Experience in running EaaS service
    • This experiment falls under this bucket
    • Select a security system which allows proactive policy to be set according to your organization’s needs
    • Drive an implementation project to protect all critical databases

• Can you help with EaaS JSON command set definitions?
• What are your device case studies?
  • Especially in 5G and cloud environments
Wanna help EaaS JSON protocol Development?

1. **Get in touch**
   
   Ravi Jagannathan
   jravi@vmware.com

2. **Interested in prototyping?**
   
   Need people in Cloud environment with Containers

3. **IoT / 5G devices?**
   
   Interested? Contact Ravi Jagannathan, jravi@vmware.com

4. **Any other thoughts?**
   
   Please get in touch.
Acknowledgment

Apostol Vassilev
Research Team Lead
Security Test, Validation and Measurement Group
NIST

Robert Staples
Security Test, Validation and Measurement Group
NIST

Thank You!
Thank You!

vmware®
Thank You!