ETSI Quantum Safe Cryptography Workshop

William Copeland
Verizon
Emerging Technologies
November 7, 2019
Entropy looks like this

22 ad 9e 59 b5 b1 9c 05 ff b4 88 67 fe 94 b5 80 2f 64 4b ba 4c 06 57 3c 5a 68 f0 b4 74 d1 dd ae aa eb dd 77 ec d7 03 90 09 88 84 75 0b dc 70 3a c9 c5 35 4b 26 b1 fd 7d 08 4a 21 99 07 d9 2e 8c ca a5 52 d3 89 da 03 1d ca 80 cb f7 b2 c3 8b 74 d2 27 0d 33 74 ad ad 5b 21 e0 55 f5 bb bb 30 5e f3 1a 22 86 fe 9a e3 6d fa 0e 1f 62 e4 ca 0f 9b 51 fa 1b 22 c6 2d b2 14 d2 24 2c f7 8b 48 0e f7 79 d4 8d c5 61 d2 7f 49 69 93 74 e0 13 7b 05 d6 f3 ba b6 55 f3 c4 46 4a 60 56 39 75 56 73 c0 61 15 c9 45 f8 d9 17 ed b6 37 5e 1d 51 44 f3 8e 04 f0 e4 9a 3c 72 ae 93 01 04 b0 54 02 0a 9c 44 35 e7 a2 d6 f4 81 1d cf d9 05 b2 42 bf e8 c2 69 4d 6c 8c d8 12 20 e8 e5 07 51 33 2f 47 b0 db b8 15 26 26 73 50 48 60 b2 0f 5c d9 41 a9 75 bf bf ab 30 4b b7 4c 0d b9 66 94 64 5c d8 a8 4f d6 16 d3 fa bf ca e2 3a eb c0 95 93 97 19 fc 1e 15 c0 cd c1 2c 34 c3 e4 36 c0 b4 f9 91 81 03 03 22 87 7d ed 80 5c 24 47 b9 6b fc 26 1b b2 cc 84 a9 98 77 a5 08 fa 21 4c 98 70 ad ad 44 b6 03 79 b4 57 c4 82 0d 03 b2 a8 33 6f bf 97 d3 c4 99 7f 56 2f 49 dc 7b 9f a5 c2 d9 b3 77 b3 c5 7c c9 05 58 48 bc 0f 65 a9 18 73 bf fa 0f 9c 8d cd e6 9c b7 fd 9e b7 d6 c4 28 ef 30 93 c3 7f ea 0f 16 7f 48 f7 06 4a fa bf 1f d5 4c bf b1 89 5b 8d 71 24 ab ca 66 70 e2 41 81 37 6b 57 26 38 7a 26 7d 53 37 42 6a 3c 48 9c cc 6a f8 c7 d0 1e 12 b1 27 7a ec 13 97 ef 22 84 4b d9 cb 2b 61 2b d4 a3 cd 54 2f f3 d8 2c 59 9f e7 67 d7 4c dd a3 d9 d3 25 41 bf 6b e9 99 92 a9 34 48 8b 33 43 b4 58 21 58 fd 3e e4 d1 02 4f da 39 6e ab bc 89 3c 2d 77 a3 ce 3c ec 10 50 d7 9c fc

https://www.random.org/cgi-bin/randbyte?nbytes=500&format=h
Earlier tests: Pass/Fail + Statistic (p value)

- Frequency (Monobits) Test
- Frequency Test within a Block
- Runs Test
- Test for the Longest Run of Ones in a Binary Matrix Rank Test
- Discrete Fourier Transform (Spectral) Test
- Non-Overlapping Template Matching Test
- Overlapping Template Matching Test
- Maurer’s “Universal Statistical” Test

- Linear Complexity Test
- Serial Test
- Approximate Entropy Test
- Cumulative Sums (Cusum) Test
- Random Excursions Test
- Random Excursions Variant Test

A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010

NIST Tests of Entropy Quality

Later tests: Non-IID and IID Tracks

Handy software yields a "best of 8" score (assuming non-IID)

NIST Special Publication 800-90B
A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, January 2018
Quantum Based Entropy-as-a-Service

Entropy is the source of randomness used for encryption. Most entropy comes from local hardware/software.

Recent events have caused a loss of trust in the security of equipment manufactured abroad.

Using the randomness of quantum physics creates a stronger entropy source for keys and certificates.

Diversification through a multi-layer approach with primary and secondary entropy sources.
What is the Software Defined Perimeter (SDP) ?

SDP sits between users and servers
- Developed by Cloud Security Alliance (CSA)
- Separate control and data planes
- A dedicated CA with pinned certificates to a trusted root (very short chain of trust)
- Modified TLS handshake that avoids RSA/DH exposure
- Cipher suite: TLS_ECDHE_RSA_WITH_AES_GCM_SHA384

SDP is the Zero-Trust Approach to Networking
What is the Software Defined Perimeter (SDP)?

SDP sits between users and servers

- Client to Controller: requires attestation prior to connection with prior onboarding, Single-Packet Authorization (SPA), and finally mTLS
  - Learn IP addresses of resources
- Client to Server: client and server mutually authenticate via Single-Packet Authorization (SPA) and mTLS encryption
Details

To connect to controller, client presents:

Single Packet Authorization, unique device certificate(s), fingerprint signature(s), and software hash information that the Controller uses to determine the authenticity of the device and software for potential connectivity to the protected application and resources.

If the client is authenticated, proceed with remainder of TLS handshake

Opportunities to inject quantum entropy:

- PKI certificates (public and private keys)
- SPA
- TLS session key generation

SPA = UID, CTR, OTP

Where:

- UID = Universal ID of SDP Client
- CTR = Counter incremented prior to use to mitigate playback attacks
- OTP = One-Time Password
  - OTP = HMAC \[Ks, UID || ++ CTR\]
- Ks = shared key for HMAC OTP generation
Software Defined Perimeter using Quantum-Based Entropy

Proof of Concept demonstrates adding entropy to PKI certificate and session key production

Prototype
- Produces quantum entropy
- Streams to PKI crypto server
- Injects entropy into Linux pools
- Provides the strongest public and session keys possible with PKI

Proof-of-Concept Prototype
PKI Integration

Entropy Integration
• Standards-drive

Verizon provides Certificate Authorities (CAs):
PKI Service / HSMs for corporate, governmental, and internal use