Military Grade Security for Video over IP

Jed Deame, CEO, Nextera Video
Agenda

• Why Secure Video over IP?
• Security Primer
• NMOS Security
• Customer Case Study
Why Secure Video over IP?

• High value content may require protection
• Keep unauthorized/unintended streams off air
• Hackers everywhere
• Threats INSIDE the facility
3 Classes of Protection

1. Essence Encryption (Military, Mission Critical, etc.)
2. Control Encryption (NMOS)
3. Physical/Environmental Protection
Security Primer

1. Cryptographic Security Standards
   - FIPS 140-2
   - NSA Suite B

2. Cryptographic Algorithms
   - Encryption Algorithms
   - Key Establishment
   - Digital Signatures
   - Secure Hash Algorithms (SHA)
1. Cryptographic Security
FIPS 140-2 Ports & Interfaces

- **Input Port**
  - Data Input Interface (Essence & Keys)
  - Control Input Interface (Commands)

- **Cryptographic Module**
  (e.g.: IP Gateway)

- **Output Port**
  - Data Output Interface (Essence & Keys)
  - Status Output Interface
Security Level 1 – Lowest
(Physically protected environments)

- Approved Cryptographic Algorithm & Key Management
- Standard Compute Platform, unvalidated OS
- No Physical Security
Security Level 2

• Approved Cryptographic Algorithm & Key Management
• Standard Compute Platform
• Trusted OS (Tested)
  – meets Common Criteria (CC) Evaluation Assurance Level 2 (EAL2)
  – Referenced Protection Profiles (PP’s)
• Tamper Evidence
• Identity or Role-based Authentication
Security Level 3

• Approved Cryptographic Algorithm & Encrypted Keys
• Standard Compute Platform
• Trusted OS (Tested) – meets CC EAL3, Referenced PP’s
• Tamper Response (zeroizes data)
• Identity-only based Authentication
• Plaintext Keys/passwords must be entered on separate ports
  – Physical or Logical Separation with a trusted path
Security Level 4 – Highest
(Suitable for Physically Unprotected Environments)

- Approved Cryptographic Algorithm & Encrypted Keys
- Standard Compute Platform
- Trusted OS (Tested) – meets CC EAL4, Referenced PP’s
- Tamper Response (zeroizes data and plaintext keys)
- Identity-only based Authentication
- Plaintext Keys/passwords must be entered on separate ports
- Protected for voltage and temperature extremes
## Crypto/Physical Security (FIPS 140-2)

<table>
<thead>
<tr>
<th>Security Level 1</th>
<th>Security Level 2</th>
<th>Security Level 3</th>
<th>Security Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cryptographic Module Specification</strong></td>
<td>Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cryptographic Module Ports and Interfaces</strong></td>
<td>Required and optional interfaces. Specification of all interfaces and of all input and output data paths.</td>
<td>Data ports for unprotected critical security parameters logically or physically separated from other data ports.</td>
<td></td>
</tr>
<tr>
<td><strong>Roles, Services, and Authentication</strong></td>
<td>Role-based or identity-based operator authentication.</td>
<td>Identity-based operator authentication.</td>
<td></td>
</tr>
<tr>
<td><strong>Physical Security</strong></td>
<td>Production grade equipment.</td>
<td>Locks or tamper evidence.</td>
<td>Tamper detection and response for covers and doors.</td>
</tr>
<tr>
<td><strong>Operational Environment</strong></td>
<td>Single operator. Executable code. Approved integrity technique.</td>
<td>Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.</td>
<td>Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Referenced PPs plus trusted path evaluated at EAL4.</td>
</tr>
<tr>
<td></td>
<td>Security Level 1</td>
<td>Security Level 2</td>
<td>Security Level 3</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cryptographic Key Management</td>
<td>Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.</td>
<td>Secret and private keys established using manual methods may be entered or output in plaintext form.</td>
<td>Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.</td>
</tr>
<tr>
<td>Self-Tests</td>
<td>Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mitigation of Other Attacks</td>
<td>Specification of mitigation of attacks for which no testable requirements are currently available.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# NSA Suite B Cryptography

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Function</th>
<th>Specification</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Encryption Standard (AES)</td>
<td>Symmetric block cipher used for information protection</td>
<td>FIPS Pub 197</td>
<td>Use 256 bit keys to protect up to TOP SECRET</td>
</tr>
<tr>
<td>Elliptic Curve Diffie-Hellman (ECDH) Key Exchange</td>
<td>Asymmetric algorithm used for key establishment</td>
<td>NIST SP 800-56A</td>
<td>Use Curve P-384 to protect up to TOP SECRET.</td>
</tr>
<tr>
<td>Elliptic Curve Digital Signature Algorithm (ECDSA)</td>
<td>Asymmetric algorithm used for digital signatures</td>
<td>FIPS Pub 186-4</td>
<td>Use Curve P-384 to protect up to TOP SECRET.</td>
</tr>
<tr>
<td>Secure Hash Algorithm (SHA)</td>
<td>Algorithm used for computing a condensed representation of information</td>
<td>FIPS Pub 180-4</td>
<td>Use SHA-384 to protect up to TOP SECRET.</td>
</tr>
<tr>
<td>Diffie-Hellman (DH) Key Exchange</td>
<td>Asymmetric algorithm used for key establishment</td>
<td>IETF RFC 3526</td>
<td>Minimum 3072-bit modulus to protect up to TOP SECRET</td>
</tr>
</tbody>
</table>
# Commercial National Security Algorithm Suite (CNSA)

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA 3072-bit or larger</td>
<td>Key Establishment, Digital Signature</td>
</tr>
<tr>
<td>Diffie-Hellman (DH) 3072-bit or larger</td>
<td>Key Establishment</td>
</tr>
<tr>
<td>ECDH with NIST P-384</td>
<td>Key Establishment</td>
</tr>
<tr>
<td>ECDSA with NIST P-384</td>
<td>Digital Signature</td>
</tr>
<tr>
<td>SHA-384</td>
<td>Integrity</td>
</tr>
<tr>
<td>AES-256</td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>
Security Primer

1. Cryptographic Security Standards
   - FIPS 140-2
   - NSA Suite B

2. Cryptographic Algorithms
   - Encryption Algorithms (AES)
   - Secure Hash Algorithms (SHA)
   - Key Establishment (ECDH)
   - Digital Signatures (DSA)
Encryption Algorithms

• AES – Advanced Encryption Standard
  – Symmetric Key Algorithm
  – 128 bit block size, Key Sizes of 128, 192 and 256 bits
    • Plaintext -> Ciphertext
    • Key size specifies # transformation rounds (AES256 = 14 rounds)
  – CTR (Counter) Mode for low bandwidth traffic
  – GCM (Galois/Counter Mode) for high bandwidth traffic
  – Adopted by US Gov’t and used worldwide
  – NIST FIPS PUB 197 (2001)
Brute Force Attacks

• AES-128 (HDCP)
  – Requires $2^{128} - 1$ bit flips. The energy required is $\sim 10^{18}$ joules, which is equivalent to consuming 30 gigawatts of power for one year, which is 262.7 TWh (more than 1% of the world energy production)

• AES-256
  – Fifty supercomputers that could check a billion billion ($10^{18}$) AES keys per second (if such a device could ever be made) would, in theory, require about $3 \times 10^{51}$ years to exhaust the 256-bit key space
Secure Hash Algorithms

Mapping of arbitrary sized data to fixed size. Must be:

1. Deterministic
2. Quick to compute
3. Infeasible to generate a message from its hash value
4. A small change in message yields a large change in the digest
5. No two messages with the same hash value

- Multiple rounds (up to 80) of AND, XOR, NOT, ROT
- Published by NIST/FIPS PUB 180/202 (SHA 0/1/2/3 224-512)
SHA Example

**Input**
- Fox
- The red fox jumps over the blue dog

**Digest**
- SHA-1: DFCD 3454 3B8E 788A 751A 696C 24D9 7009 CA99 2D17
- SHA-224: 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
- SHA-256: 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
- SHA-384: FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
- SHA-512: 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C
Key Establishment

1. Public Key Encryption
2. Digital Signatures
3. Public Key Infrastructure (PKI)
Public Key Encryption

- Simple & Effective
- Subject to man-in-the-middle attacks
Digital Signatures

• A mathematical scheme for verifying the authenticity of digital messages
Digital Signature Algorithm (DSA)

- Gov’t Standard for Digital Signatures (*NIST FIPS 186-4*)
  1. Specify Hash Function (SHA)
  2. Specify Key Length L&N (3072, 256)
  3. Choose prime numbers p, q, & g that may be shared
  4. Randomly choose a secret private key
  5. Compute a Public Key
  6. Sign the Key by hashing a random number (PS3)

- Elliptic Curve Digital Signature Algorithm (ECDSA)
  - OpenSSL
How to transfer Encryption Keys?

- Paper key list via Trusted Courier
- What if we could jointly establish a secret key over an insecure channel?
Key Agreement

• Two or more parties agree on a key whereby both influence the outcome (perfect forward secrecy)

• Diffie-Hellman protocol first
Diffie Hellman Key Exchange (Ephemeral)

1. Private = 5
   \[(6^5) \mod 13\]
   \[(7776) \mod 13\]
   Public = 2

2. \[(9^5) \mod 13\]
   \[(59049) \mod 13\]
   Shared Secret = 3

3. Agree upon two numbers:
   P Prime Number
   G Generator of P
   P = 13
   G = 6

4. Randomly generate a Private Key
   Private = 4

5. Calculate Public Key:
   \[(G^\text{Private}) \mod P\]
   \[(6^4) \mod 13\]
   Public = 9

6. Exchange Public Keys

7. Calculate the Shared Secret
   \[(\text{Shared Public} \cdot \text{Private}) \mod P\]
   \[(2^4) \mod 13\]
   Shared Secret = 3
Public Key Infrastructure (PKI)

• A set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption.
NMOS BCP-003-01 Example

Authentication Server

Broadcast Controller

IP Source

IP Destination

Auth Request (OAuth)

Token (JWT)

Activation (JWT)

Essence Flow (2110)

Activation (JWT)

Public Key
Core Technologies

• PKI (Public Key Infrastructure)
• HTTPS (HTTP over TLS)
  – Connection Security (Encrypted Control Signals)
• REST (HTTPS PUT & GET)
• JSON (Key-Value Parameter sets)
• OAuth 2.0
  – Clients Authenticate with Authentication Server
• JWT (JSON Web Token)
  – Client Authorization (issue access tokens) – RSA with SHA-256
NMOS Security Goals

- **Confidentiality** - Data passing between client and the APIs is unreadable to third parties.
- **Identification** - The client can check whether the API it is interacting with is owned by a trusted party.
- **Integrity** - It must be clear if data travelling to or from the API been tampered with.
- **Authentication** - The client can check if packets actually came from the API it is interacting with, and vice versa.
NMOS Cipher Suite

- TLS ECDHE ECDSA WITH AES 128 GCM SHA256
- TLS ECDHE ECDSA WITH AES 256 GCM SHA384
- TLS ECDHE ECDSA WITH AES 128 CBC SHA256
- TLS ECDHE ECDSA WITH AES 256 CBC SHA384
- TLS ECDHE RSA WITH AES 128 GCM SHA256
- TLS ECDHE RSA WITH AES 256 GCM SHA384
- TLS DHE RSA WITH AES 128 GCM SHA256
- TLS DHE RSA WITH AES 256 GCM SHA384
- TLS ECDHE RSA WITH AES 128 CBC SHA256
- TLS ECDHE RSA WITH AES 256 CBC SHA384
- TLS DHE RSA WITH AES 128 CBC SHA256
- TLS DHE RSA WITH AES 256 CBC SHA256
- TLS ECDHE ECDSA WITH AES 128 CCM 8

Johnny Quest Decoder Ring:

TLS = Transport Layer Security
ECDHE = Elliptic Curve Diffie-Hellman Ephemeral KE
ECDSA = Elliptic Curve Digital Signature Algorithm
AES = Advanced Encryption Standard (#bits)
GCM = Galois/Counter Mode
CBC = Cipher Block Chaining (XOR)
SHA = Secure Hash Algorithm (#bits)
CCM = Counter with CBC-MAC (Cyber Block Chaining Message Authentication Code)

←——— Minimum Requirement
Customer Case Study – Secure KVM

1 Gb/s Switch Fabric

RX GW RX GW RX GW RX GW RX GW
TX GW TX GW TX GW TX GW
Remote Monitor

SDI Sources

SERVERS/Workstations

User Authentication

Optionally Encrypted Video/Audio/USB

Secure Control

SYSTEM MANAGER

RX GW RX GW RX GW RX GW RX GW

TX GW TX GW TX GW TX GW

Customer Case Study – Secure KVM

Optionally Encrypted Video/Audio/USB

User Authentication
Summary

- Security is crucial in the internet age
  - Especially if you have high value content
- The US Government has been working on this for years
  - Leverage work from NIST, NSA, DoD
- NMOS Control Security is a great first step
  - https, Authentication Servers, etc.
- For Highest Security, Essence encryption is readily available
  - Compatible with any transport (2110, 2022, RTP, etc)