In-Flight Encryption

Jim Theodoras
Feb 2014
OSI Model

**Top of Stack**
- Application
- Presentation
- Session

**Transport Layer**
- TCP, UDP

**Network Layer**
- IP/MPLS

**Data Link Layer**
- MAC

**Physical Layer**
- PHY

**Bits**

**Packets**

**Segments**

**Frames**

**Data Unit**

**Data**
Getting from Point A to Point B
Home Security Analogy

Single layer of security
- a locked front door
  - Key left under front door mat
  - Neighbor given the key
  - Lock not re-keyed
  - Yard not gated

Multiple layers of security
  - Lockbox for key for maid
  - Re-keyed before move in
  - Yard gated
  - Alarm - Intrusion detection
Secure End-to-End Data Transport

- Proper key management
- Multiple layers of security
- Intrusion detection
Layers of Security

• Layered security is not just a Hollywood plot device.
• Layered and tiered security works.
Sideways Attacks
Mathematical Sleight-of-Hand

- 64,000 possible combinations
- A “sideways attack” reduces that to 100 possible combinations.
- A “backdoor” renders the lock useless.
Examples of Sideways Attacks

- Copying Encryption Keys
  - If stored in DRAM
  - Freeze spray slows down decay
  - Unplug adjacent linecard
  - Put on probe
  - Freeze DRAM
  - Unplug/Replug linecard
  - Read encryption keys
Examples of Sideways Attacks

- *(not so)* Random Number Generation
  - Hardware Random Number generation is great, but slow
  - Random number only used for seed
  - Seed then used for pseudorandom number generation
  - Knowing details of process reduces possible solution set
  - “lack of entropy” in pseudorandom number
Sidewaysing a Brute Force Attack

• “Brute Forcing” is using a HPC to go through every combination.
• You do not have to go through every permutation, just every reasonable guess.
• “Relational data” greatly reduces number of potential guesses.

Example: AES-256

• A supercomputer that could check $10^{18}$ keys/sec would require $10^{51}$ years to exhaust 256 bit key space.
• A typical mining rig can brute force 30 billion passwords/sec, cracking all eight-character passwords in just a few hours.
• Relational data reduces this to mere minutes.
Cryptographic Goals
Cryptographic Goals

• **Confidentiality**
  • Nobody can read content of message ("Encryption")

• **Integrity**
  • Modification of message will be detected ("Checksum")

• **Authenticity**
  • Verify that I am really connected to whom I expected.
Alice wants to send Bob a message.

Eve is either listening or is directly intercepting the line and can manipulate all messages to Bob.
Confidentiality (privacy) - "Encryption"

- Eve cannot understand message from Alice
- Eve could manipulate message to Bob. - Encryption does not protect against manipulation.

Example: Alice sends message "transfer 10€ to Bob's bank account". When Eve knows the position in the message, where the value is located, she can change the value without knowing anything else.
**Integrity - "Cryptographic Checksum"**

- Eve cannot manipulate message from Alice, because this will be detected by Bob.
- Cryptographic Checksums add latency, because message must be stored and verified on receiving side.
Encryption Basics
Cryptographic Goals

Authenticity - "Authentication"

• Alice and Bob can detect, whether they are connected.
Encryption Basics
Encryption Basics
Symmetric Encryption

Symmetric Encryption:
• Alice and Bob use the same algorithm
• Alice and Bob use the same secret key

Disadvantage
› Alice and Bob must exchange the secret key and must keep it secret
Encryption Basics
Symmetric Encryption with AES

AES

input 128 Bit

key 128, 192 or 256 Bit

output 128 Bit

128 Bit = 16 Byte data

round key

14 rounds for AES 256

Mix
Mix
Mix
Mix
Encryption Basics
Asymmetric Encryption

Asymmetric Encryption:

- Alice and Bob generate a key-pair with public and private key.
- The private key must be kept secret, but the public key can be distributed everywhere.

Alice can encrypt message with Bob's public key.

Only Bob can decrypt the message, because only he has his private key.

Disadvantage: Asymmetric Encryption is very slow.
Encryption Basics
Asymmetric Encryption within Diffie Hellman algorithm

Assumption: multiplying is much simpler as calculating logarithm

g is a common number, known to Alice, Bob and Eve

random number $r_A$

$g^{r_A}$

$g^{r_B}$

$(g^{r_B})^{r_A} = g^{(r_A r_B)}$

$(g^{r_A})^{r_B} = g^{(r_A r_B)}$

Eve must 1x calculate logarithm to get the same result
## Encryption Basics
### Symmetric vs. Asymmetric Encryption

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Asymmetric Encryption</th>
<th>Symmetric Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires secure channel for key-exchange</td>
<td>😊 No</td>
<td>😞 Yes</td>
</tr>
<tr>
<td>Is very slow</td>
<td>😞 Yes</td>
<td>😊 No</td>
</tr>
<tr>
<td>Can be implemented in hardware (FPGA)</td>
<td>😞 No (only partially)</td>
<td>😊 Yes</td>
</tr>
<tr>
<td>Encrypt large amount of data</td>
<td>😞 No</td>
<td>😊 Yes</td>
</tr>
</tbody>
</table>

**Combine both methods?** 😊

Hybrid approach uses asymmetric method for generation of encryption key ("Diffie-Hellman") and symmetric method for encryption ("AES")
Encryption Methods
Optical transmission security
Principles of encryption

**IPsec / MACsec Encryption**

Site A
- Router
- FC switch
- WDM-transport

WAN

Site B
- Router
- FC switch
- WDM-transport

**Appliance based Encryption**

Site A
- Router
- FC switch
- TDM

WAN

Site B
- Router
- FC switch
- TDM

**xWDM based Encryption**

Site A
- Router
- FC switch
- WDM-transport

WAN

Site B
- Router
- FC switch
- WDM-transport

Speed, throughput and simplicity
Encryption Method vs Layer

- Overlay Transport Virtualization (OTV)
  - Traditionally used for VPN services
  - 82 Bytes overhead
  - Only select Bytes in header encrypted and authenticated.

- MACsec/TrustSec
  - Point-to-Point Ethernet encryption
  - 32/40 Bytes overhead, respectively
  - Only select Bytes in header encrypted and authenticated.

- Traditional Transport
  - Point-to-point and multipoint
  - Zero bytes overhead, so no loss of throughput with shorter packets.
  - Only select Bytes in header encrypted and authenticated.

- Bulk Transport Encryption
  - Point-to-point
  - Zero bytes overhead, so no loss of throughput with shorter packets.
  - Protocol/ I/F agnostic (Ethernet, FC, IB, Sonet/SDH)
  - All Bytes in header and checksum are encrypted with payload.
Maximum Throughput Comparison

Throughput

Max. MTU-Size?

Max. Throughput?

Framesize / Bytes

Transport Encryption
- MACsec
- TrustSec
- IPsec
- OTV
Encryption from 10Gb/s to 100Gb/s

- Applying an AES256 w/ dynamic key exchange to a 10Gb/s line signal of a WDM card generates a multi-protocol encryption solution.
- With DC services moving to 16GFC and 40GE/100GE Encryption on 100G WDM technology becomes key.
- Complete DC service coverage through combination of 10Gb/s and 100Gb/s WDM solutions.

White Noise for key generation
100G Encryption – Live Demo

- **Sender**: Video → XG210 (GbE to 10GbE Converter) → 100GbE
- **Intruder**: 100GbE → XG210 (GbE to 10GbE Converter) → Video
- **Receiver**: Video → XG210 (GbE to 10GbE Converter) → 100GbE → 10GbE

Type of transmission:
- **Encrypted**: Video to 100GbE, 100GbE to receiver
- **Non-encrypted**: Intruder, sender to 100GbE, 10GbE to receiver
Quantum Key Distribution?

So why the continuing interest in QKD?

• Transmission of key is non-breakable, as the key is not actually transmitted!
• Intrusion detection: Reading the key changes it.
• Often overlooked: Key is truly random, preventing sidewaysing.
• ADVA will be announcing QKD real-world field results at OFC.
Recent Vulnerabilities Exposed
Balancing Act

- Encryption too hard to break
- Threats have total anonymity

- Encryption too easy to break
- Threats have access to all data
The Reality of Cloud Connectivity

- While in our heads, we envision connecting to the cloud in one way, the reality is much different.
IPsec Compromised from Day 1

• From Gilmore threads:
  • Same initialization vector used throughout a session.
  • “null” encryption
  • 56-bit DES
  • 768-bit Diffie-Hellman
  • FreeS/WAN Linux implementation not secure

• Given processing power \textit{at the time}, there was legitimate concern that undesirables would have total anonymity.

• Problem: Given today’s processing power, the club of entities that can decipher at will has grown too large.
OSI Model – Where Vulnerabilities Exist

Top of Stack

7. Application
   Presentation
   Session

6. Transport Layer
   TCP, UDP

5. Network Layer
   IP/MPLS

4. Data Link
   MAC

3. Physical
   PHY

Bits

Frames

Segments

Packets

Data

Fed mandated backdoors
Cookies
Malware

Non-random numbers
Key intercept

Fed mandated access

Vulnerabilities inserted into IPsec

Co-location
Inline spoofing
Replication

Fiber Optic Cable Taps
Undersea Taps
Coastal Gateways
Secure End-to-End Data Transport

1. Physical PHY
2. Data Link MAC
3. Network Layer IP/MPLS
4. Transport Layer TCP, UDP
5. Application Presentation Session
6. IPsec
7. MACsec

In-Flight
Intrusion Detection
In-Flight
Recommendations

• Layer your security
  • Encrypt at every layer, when possible
  • Encrypt all transport (not client) links, inside and outside of private network.
  • If someone else is carrying your traffic, have them encrypt and you keep the keys.

• Encrypt, encrypt, encrypt, but don’t only rely on IPsec.
  • Confidentiality
  • Integrity
  • Authenticity

• Intrusion Detection
  • Secure facilities (RF shielding)
  • Secure hardware and supply chain
  • Physical layer monitoring

• Focus on prevention of sideways attacks
Thank you

info@advaoptical.com