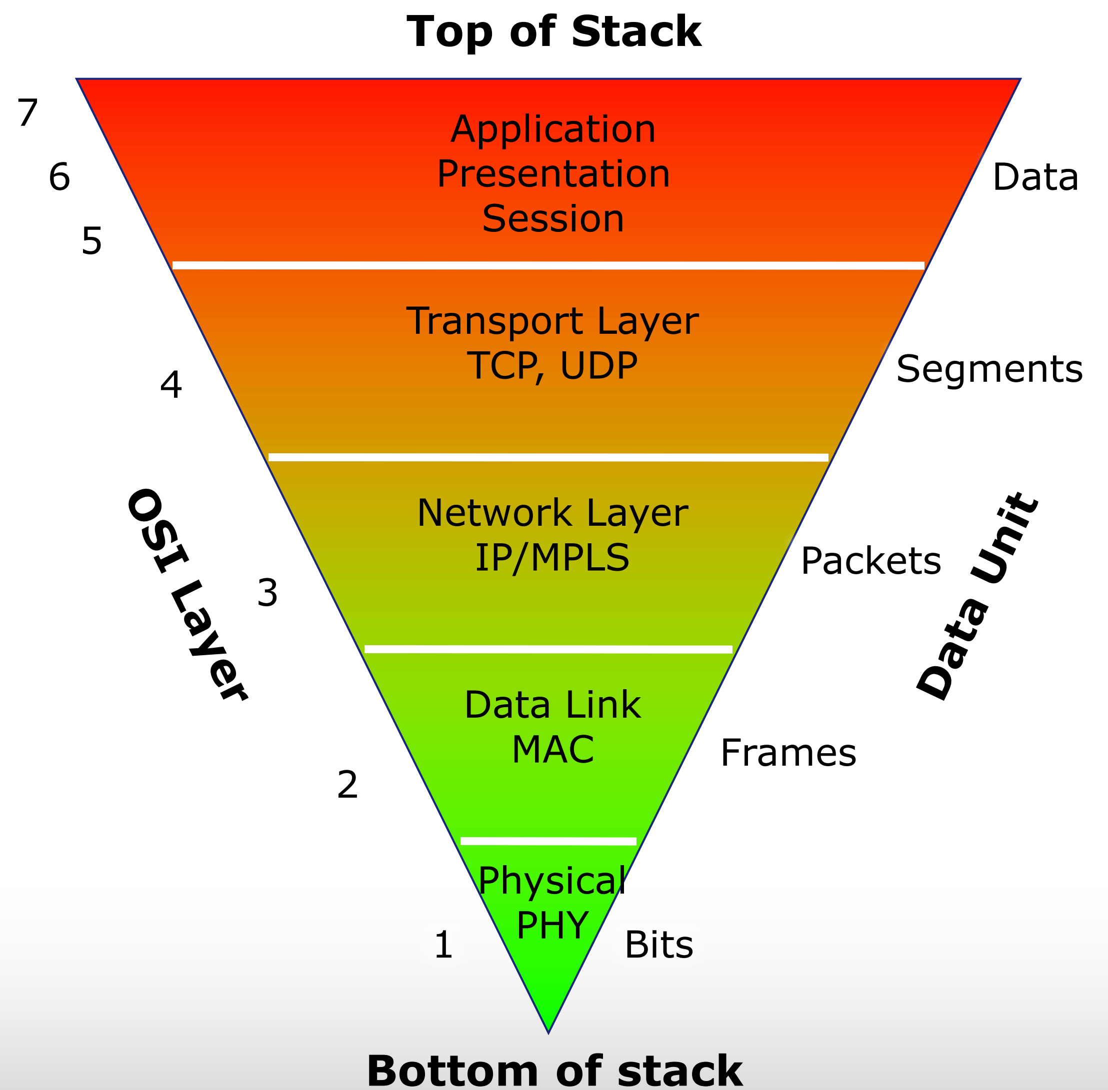
ADVA™ Optical Networking

In-Flight Encryption

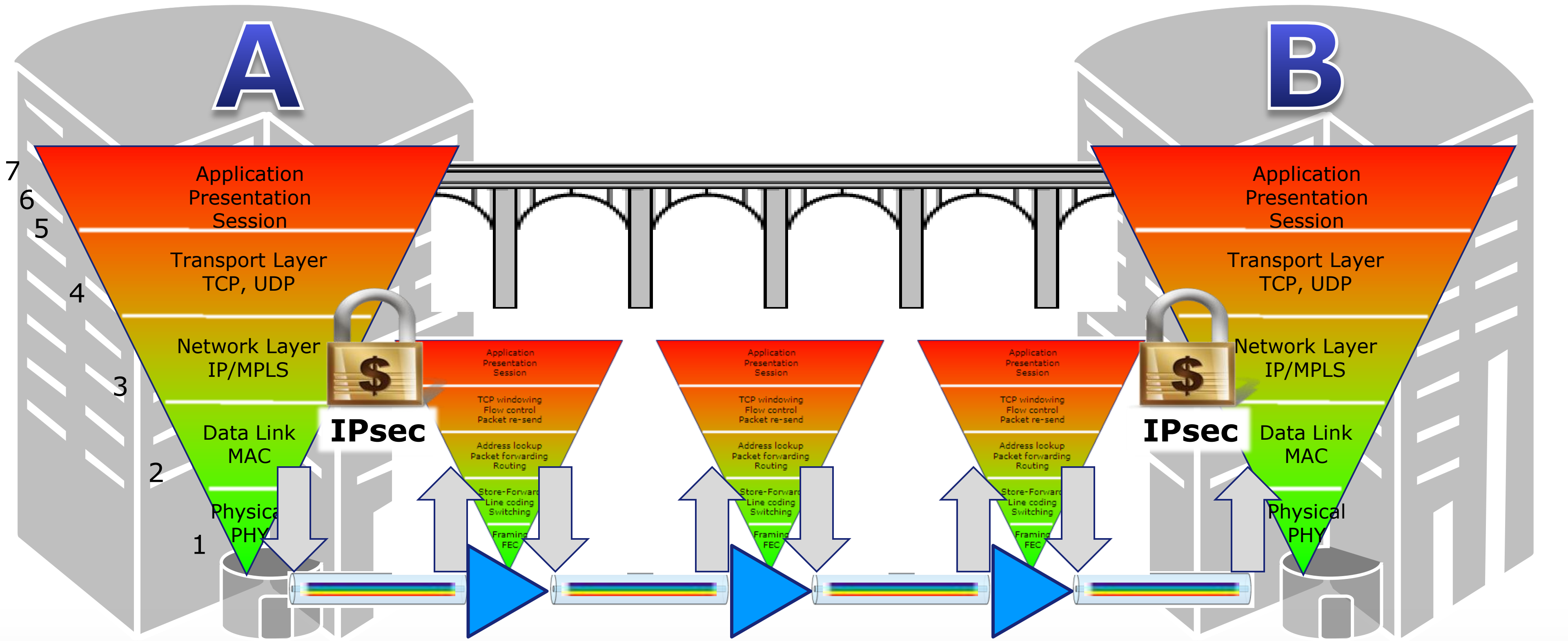
Jim Theodoras

Feb 2014

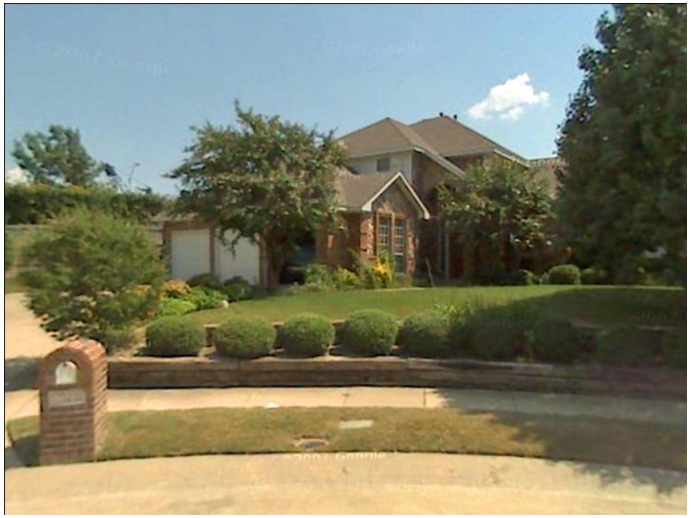
OSI Model


Top of Stack
7
6
5
Application
Presentation
Session
Data
4
Transport Layer
TCP, UDP
Segments
OSI Layer
3
Network Layer
IP/MPLS
Packets
Data Unit
2
Data Link
MAC
Frames
1
Physical
PHY
Bits
Bottom of stack

Getting from Point A to Point B



Home Security Analogy



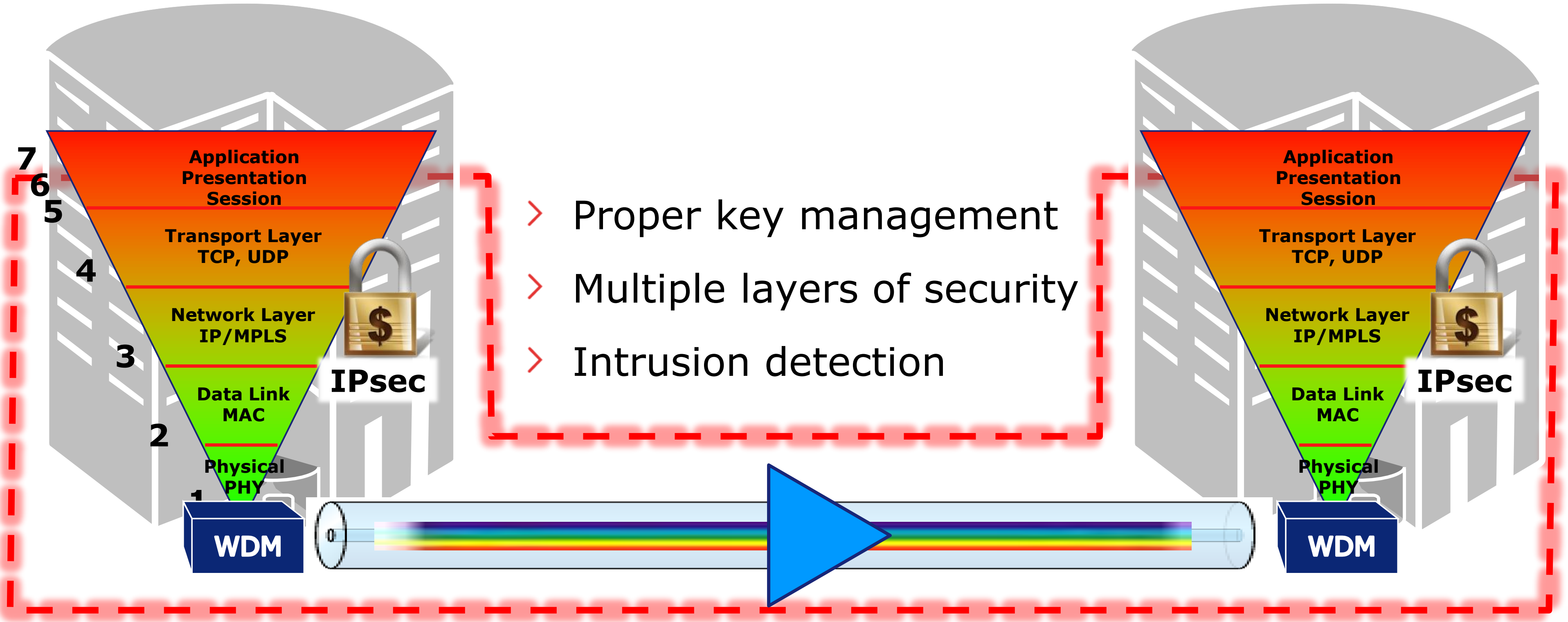
Single layer of security
– a locked front door

- 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

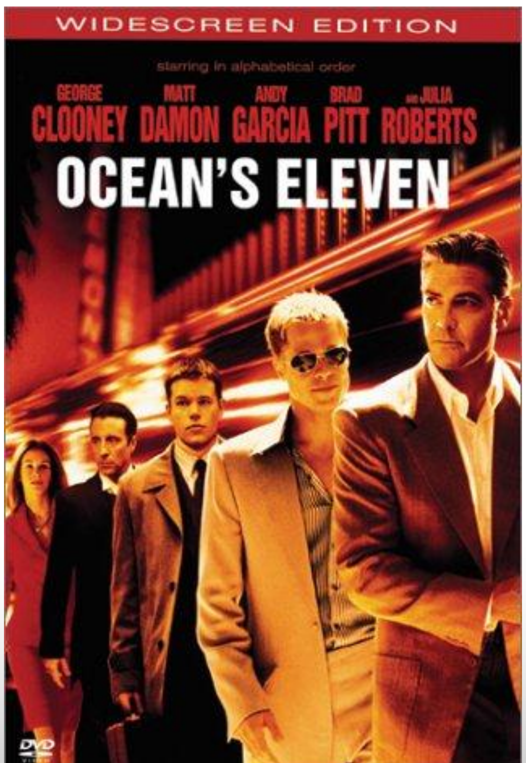
Secure End-to-End Data Transport

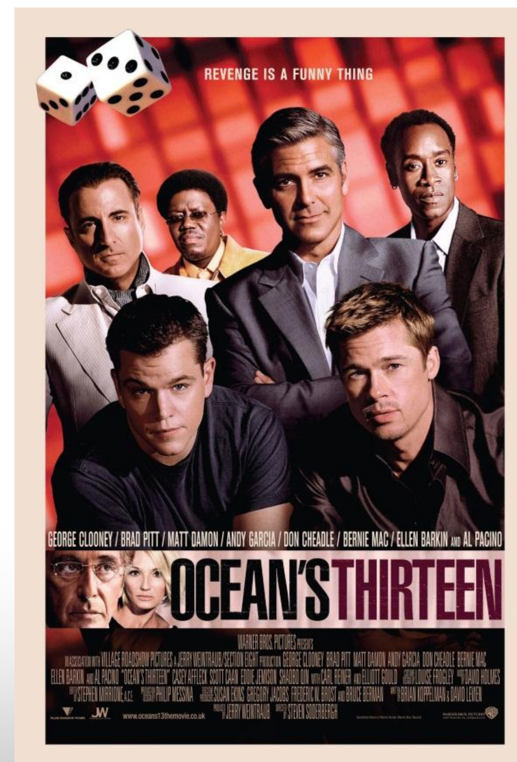


- Proper key management
- Multiple layers of security
- Intrusion detection

Layers of Security

- Layered security is not just a Hollywood plot device.
- Layered and tiered security works.





Sideways Attacks

Mathematical Sleight-of-Hand

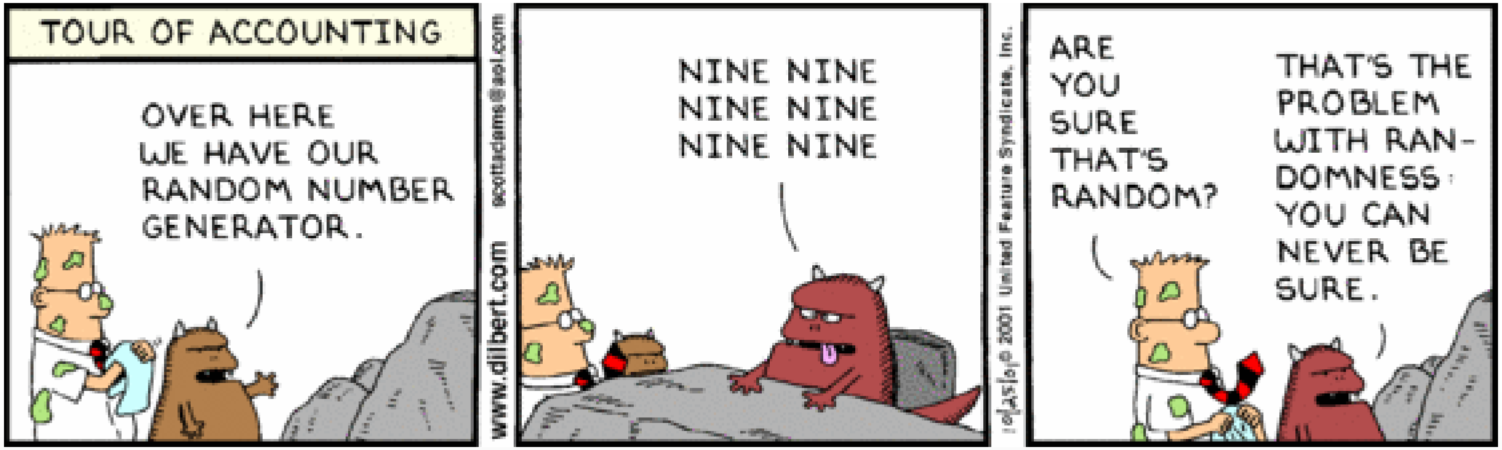
- 64,000 possible combinations
- A "sideways attack" reduces that to 100 possible combinations.
- A "backdoor" renders the lock useless.

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.

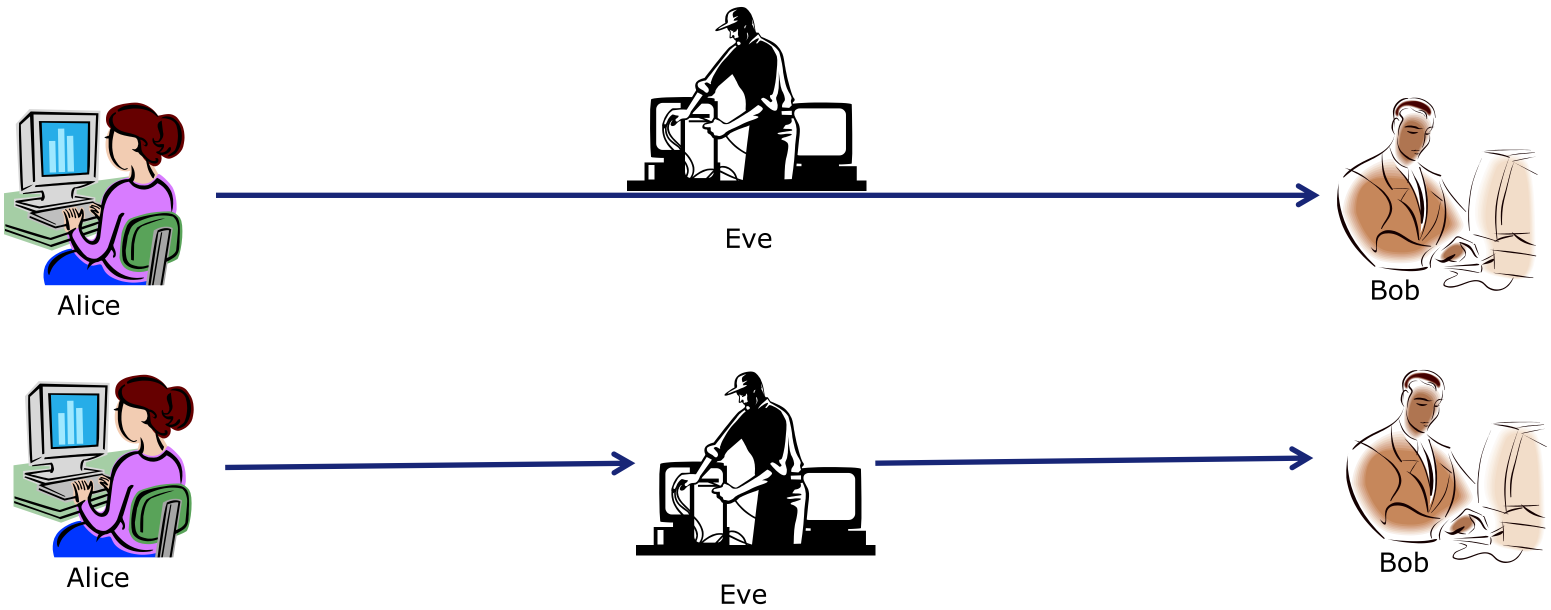
F2o<fa!7S7052C5JavW%G.@uQc/0JymD>CA:lsLZ"P+fU3Js6l@]ie9<A{$L3Nh

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.

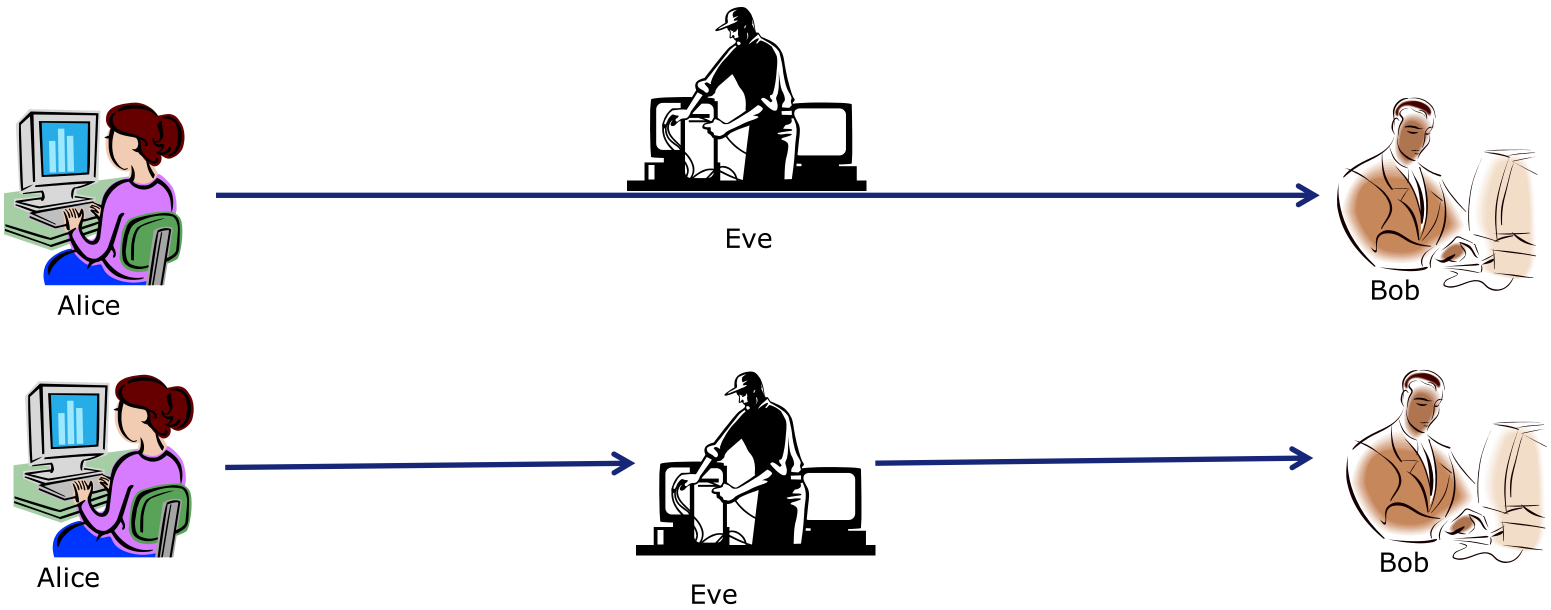
Encryption Basics
Cryptographic Goals



Alice wants to send Bob a message.

Eve is either listening or is directly intercepting the line and can manipulate all messages to Bob.

Encryption Basics
Cryptographic Goals

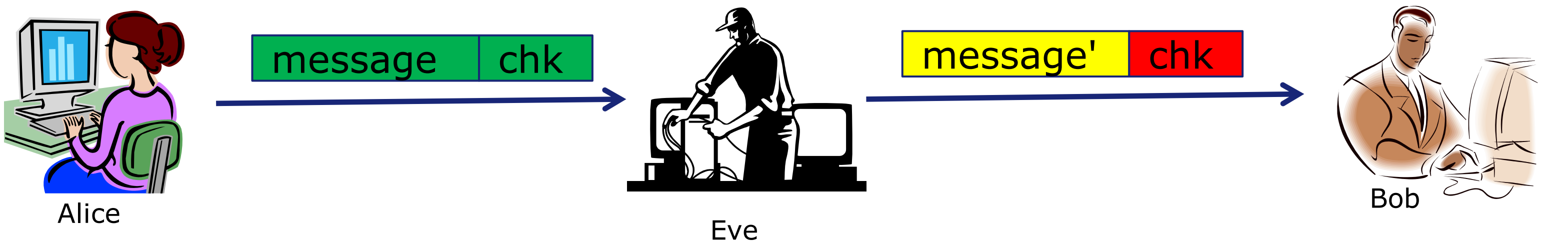


Confidentiality (privacy) - "Encryption"

- 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.

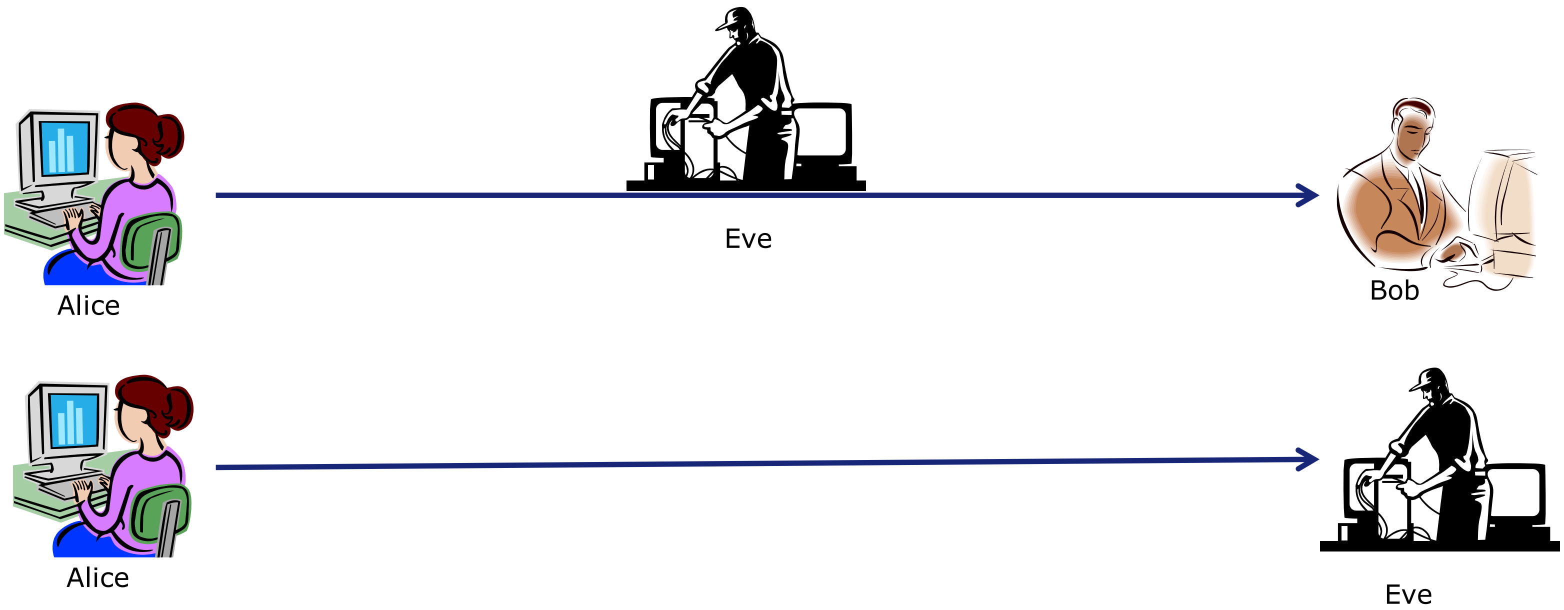
Encryption Basics
Cryptographic Goals



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"

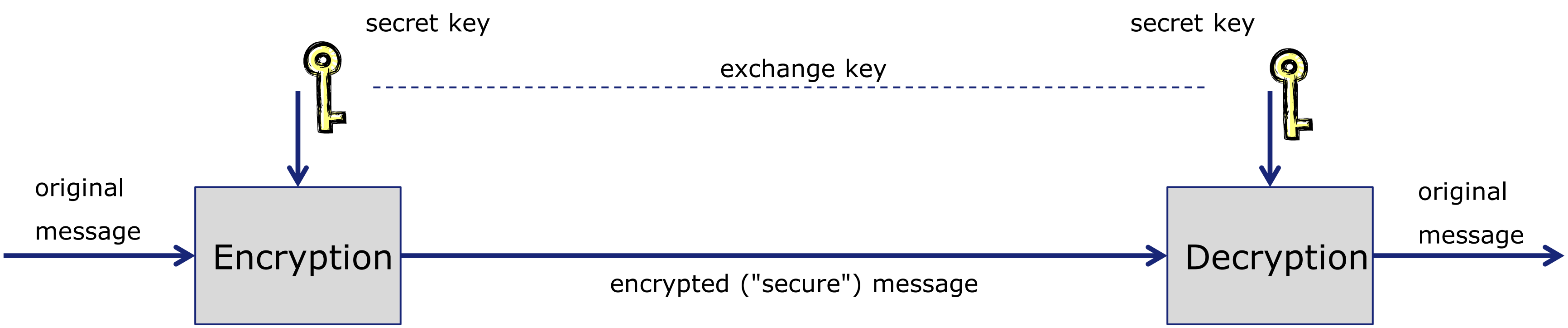
- Alice and Bob can detect, whether they are connected.

Encryption Basics

Encryption Basics
Symmetric Encryption

Symmetric Encryption:

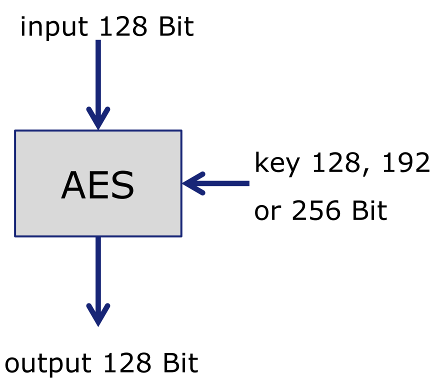
- Alice and Bob use the same algorithm
- Alice and Bob use the same secret key

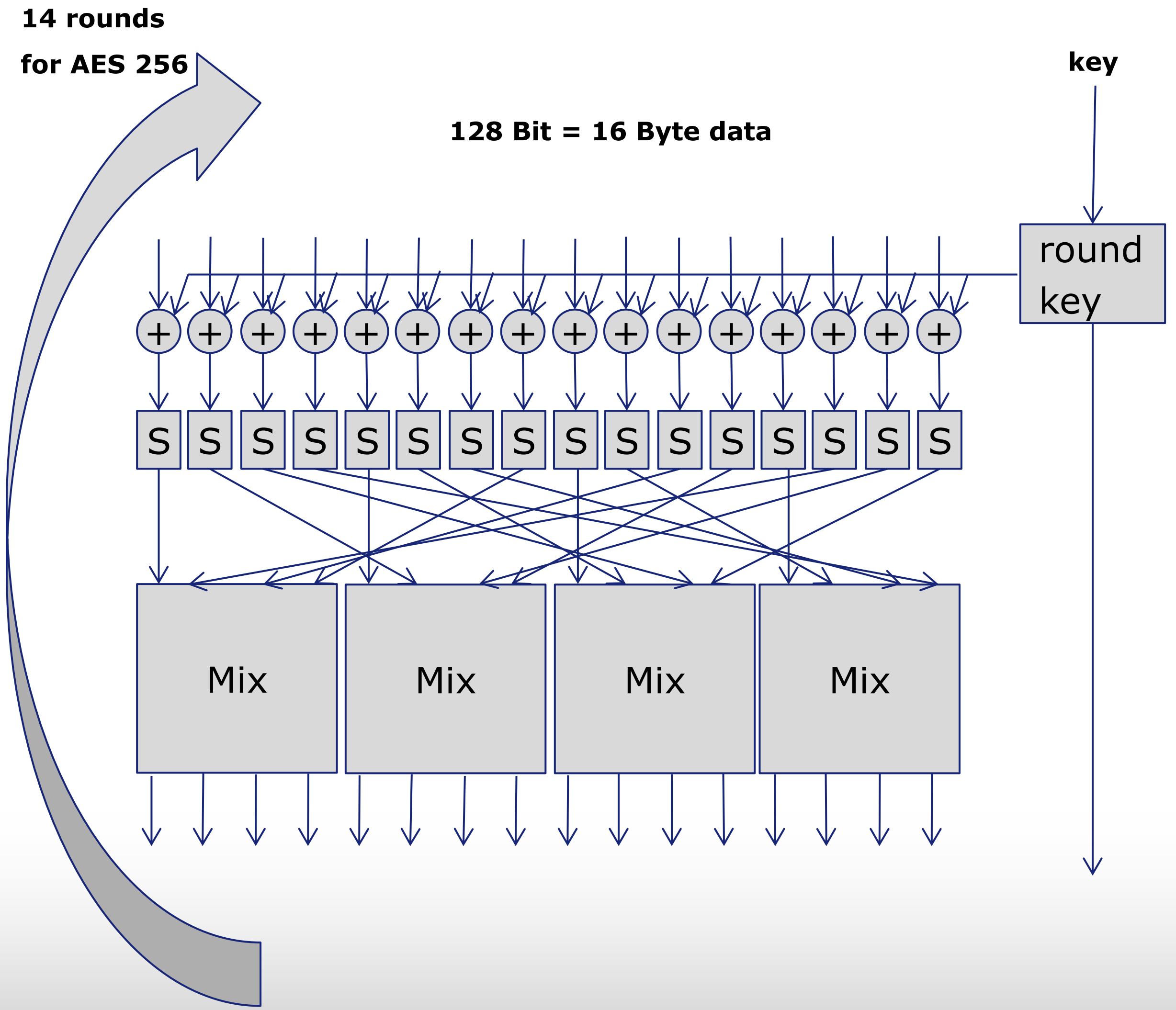


Disadvantage

- Alice and Bob must exchange the secret key and must keep it secret

Encryption Basics
Symmetric Encryption with AES

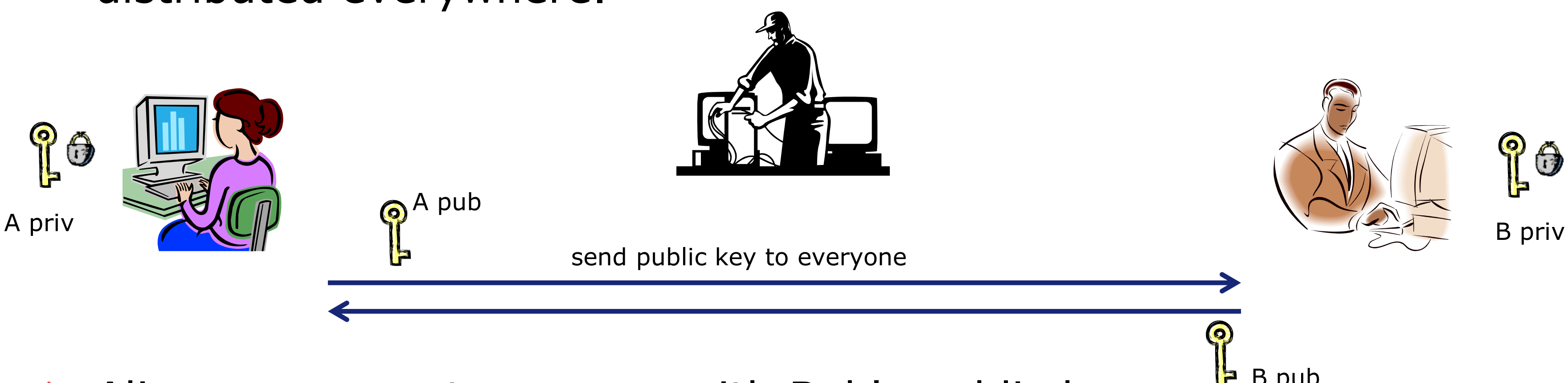




Encryption Basics
Asymmetric Encryption

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

public key g^{rA}

public key g^{rB}

random number r_B

$(g^{rB})^{rA} = g^{(rA\ rB)}$

g^{rA} g^{rB}

$(g^{rA})^{rB} = g^{(rA\ rB)}$

Eve must 1x calculate logarithm

to get the same result

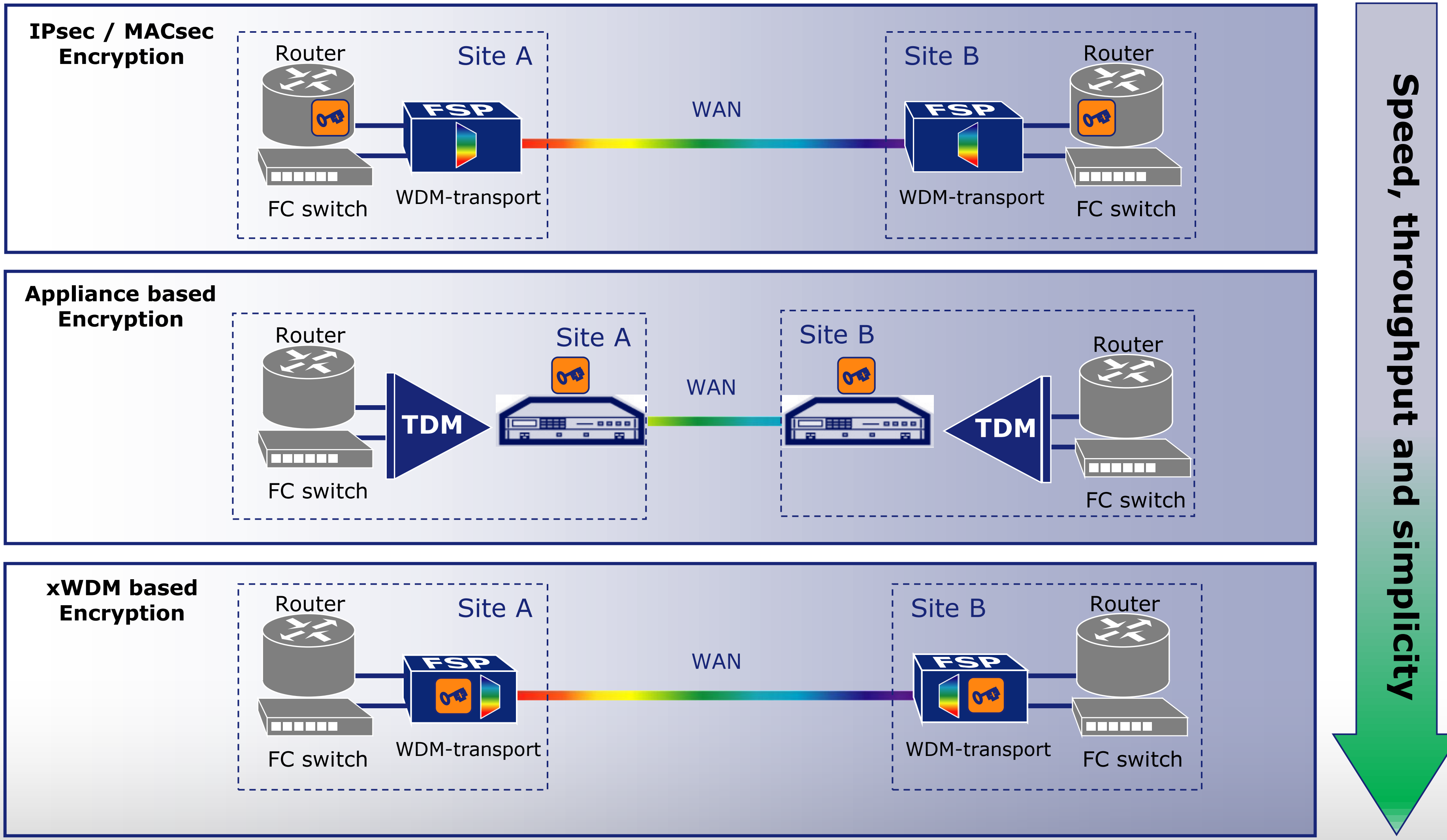
Encryption Basics
Symmetric vs. Asymmetric Encryption

	Asymmetric Encryption	Symmetric Encryption
Requires secure channel for key-exchange	☺ No	☹ Yes
Is very slow	☹ Yes	☺ No
Can be implemented in hardware (FPGA)	☹ No (only partially)	☺ Yes
Encrypt large amount of data	☹ No	☺ Yes
Combine both methods?	☺	☺

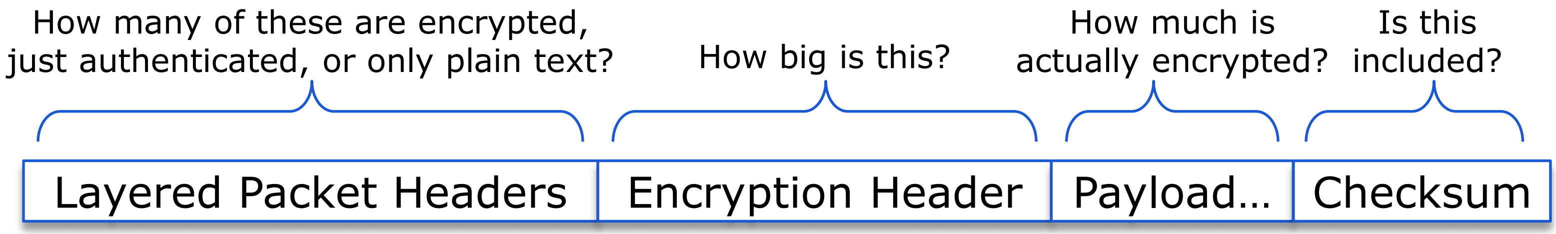
Hybrid approach uses asymmetric method for generation of encryption key ("Diffie-Hellman") and symmetric method for encryption ("AES")

Encryption Methods

Optical transmission security
Principles of encryption

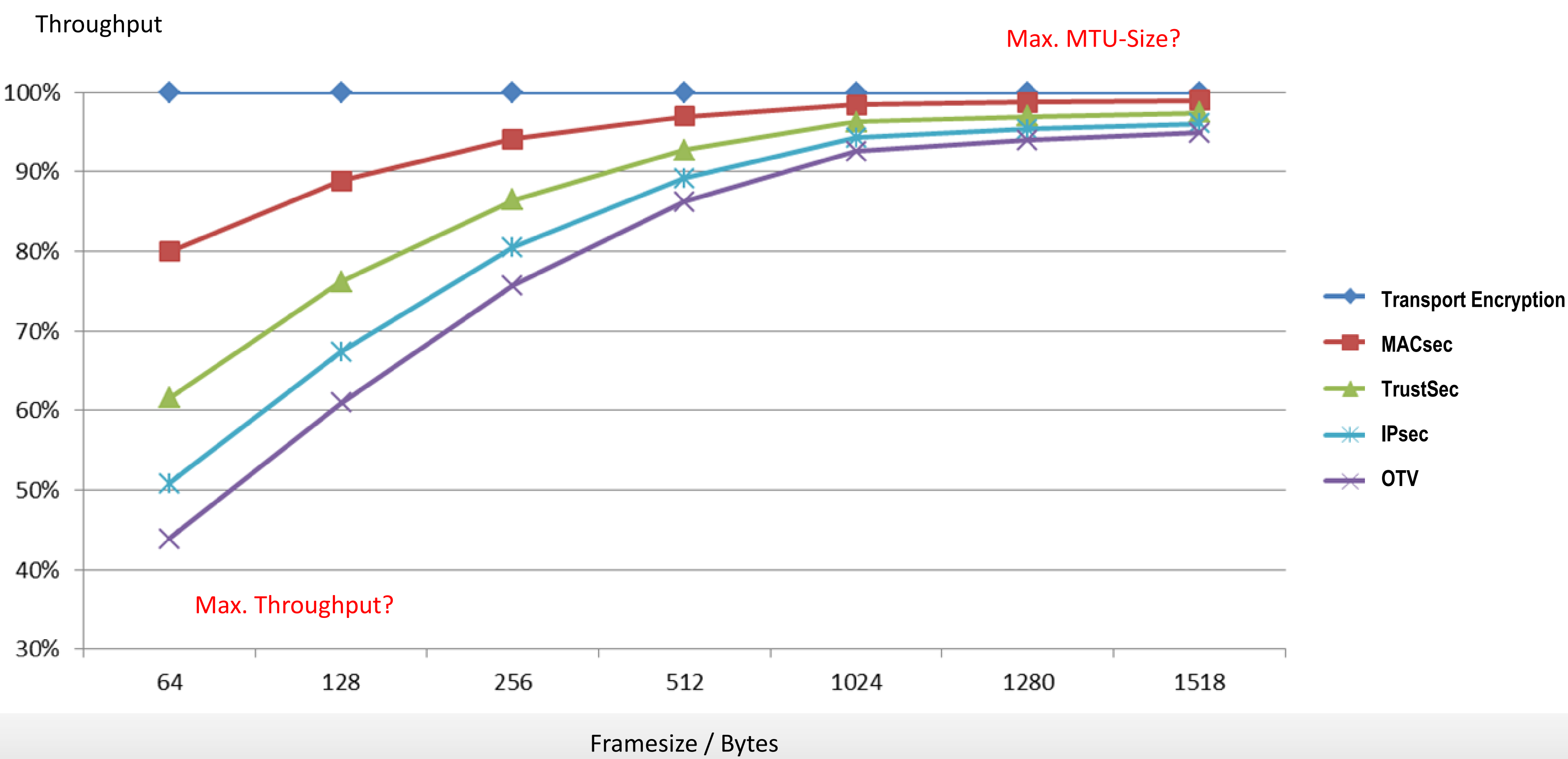


Encryption Method vs Layer

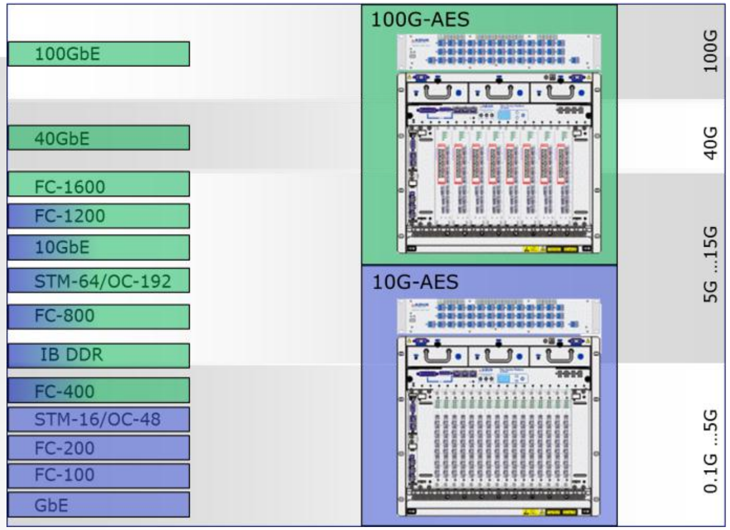


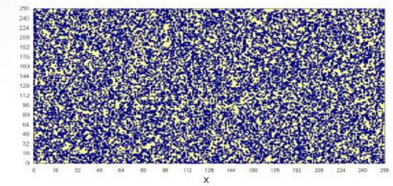
- Overlay Transport Virtualization (OTV)
  - Traditionally used for VPN services
  - 82 Bytes overhead
  - Only select Bytes in header encrypted and authenticated.
- MACsec/TrustSec
  - Point-to-Point Ethernet encryption
  - 32/40 Bytes overhead, respectively
  - Only select Bytes in header encrypted 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



Encryption from 10Gb/s to 100Gb/s

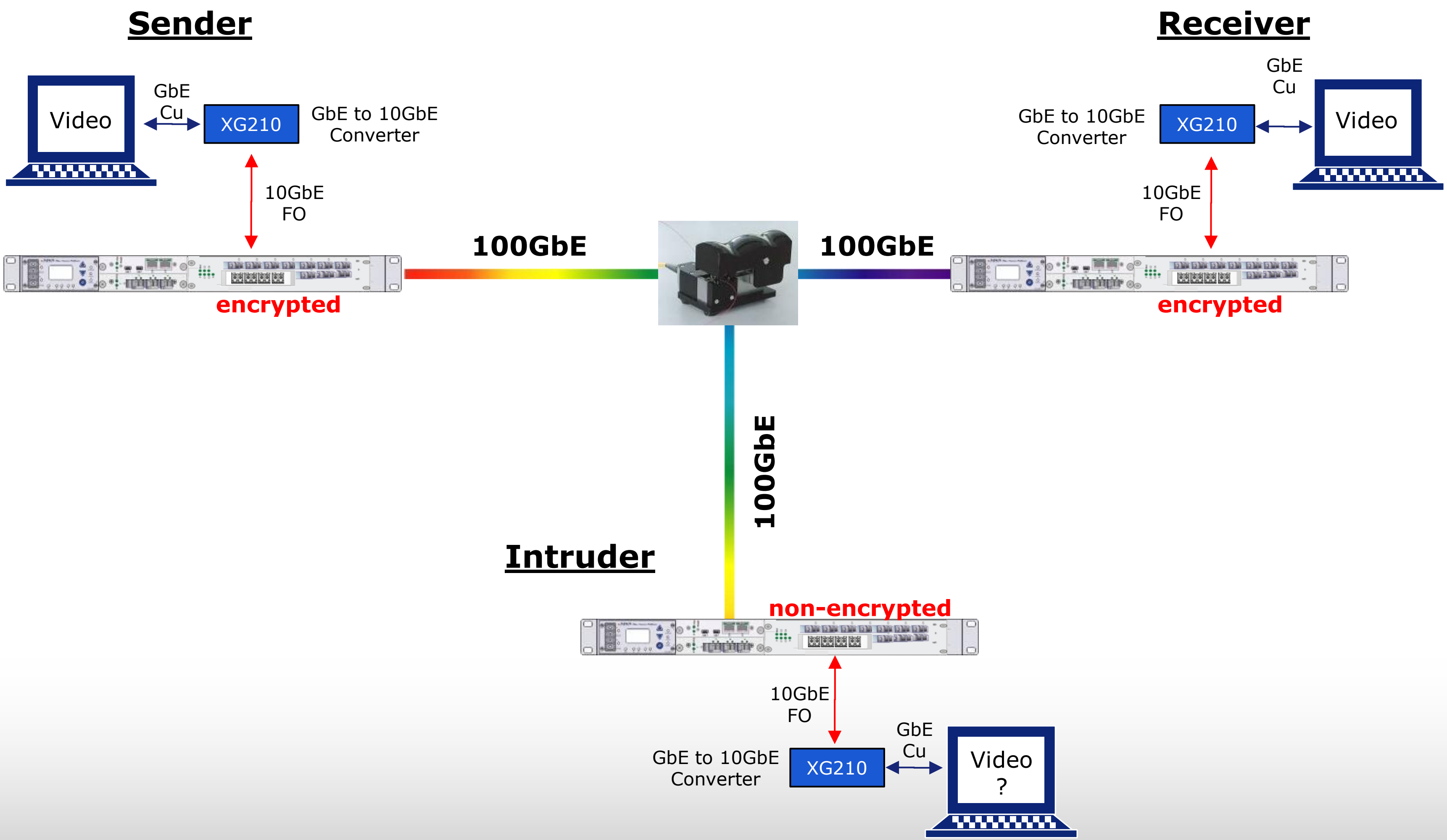




White Noise for key generation

- 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

100G Encryption – Live Demo



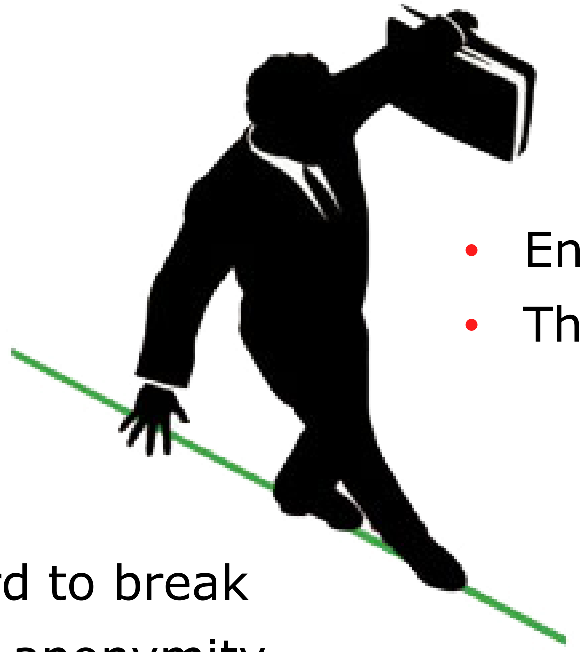
Quantum Key Distribution?

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

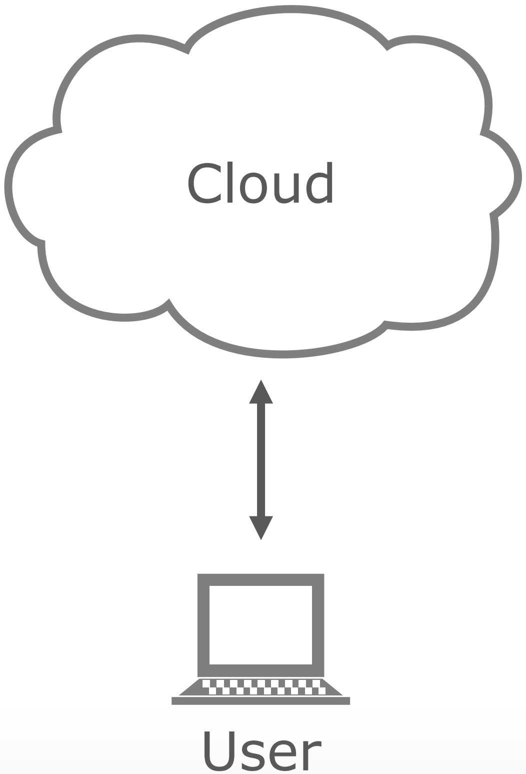


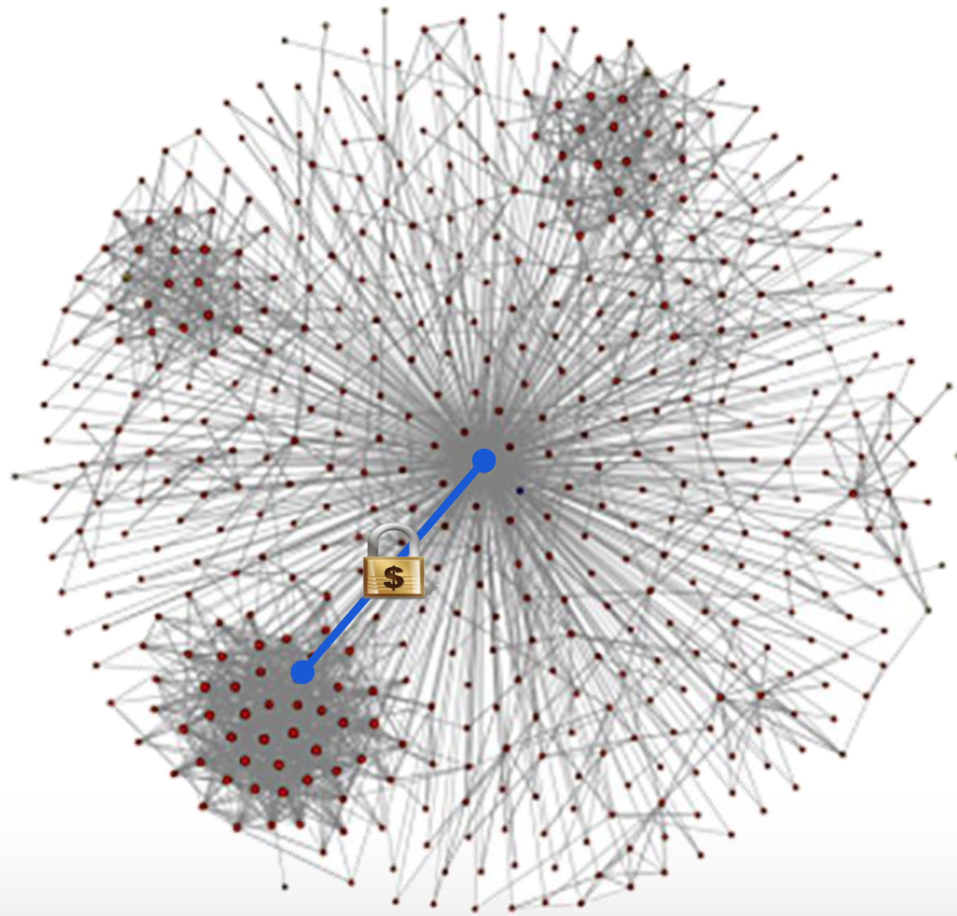
- Encryption too easy to break
- Threats have access to all data

- Encryption too hard to break
- Threats have total anonymity

The Reality of Cloud Connectivity

- While in our heads, we envision connecting to the cloud in one way, the reality is much different.

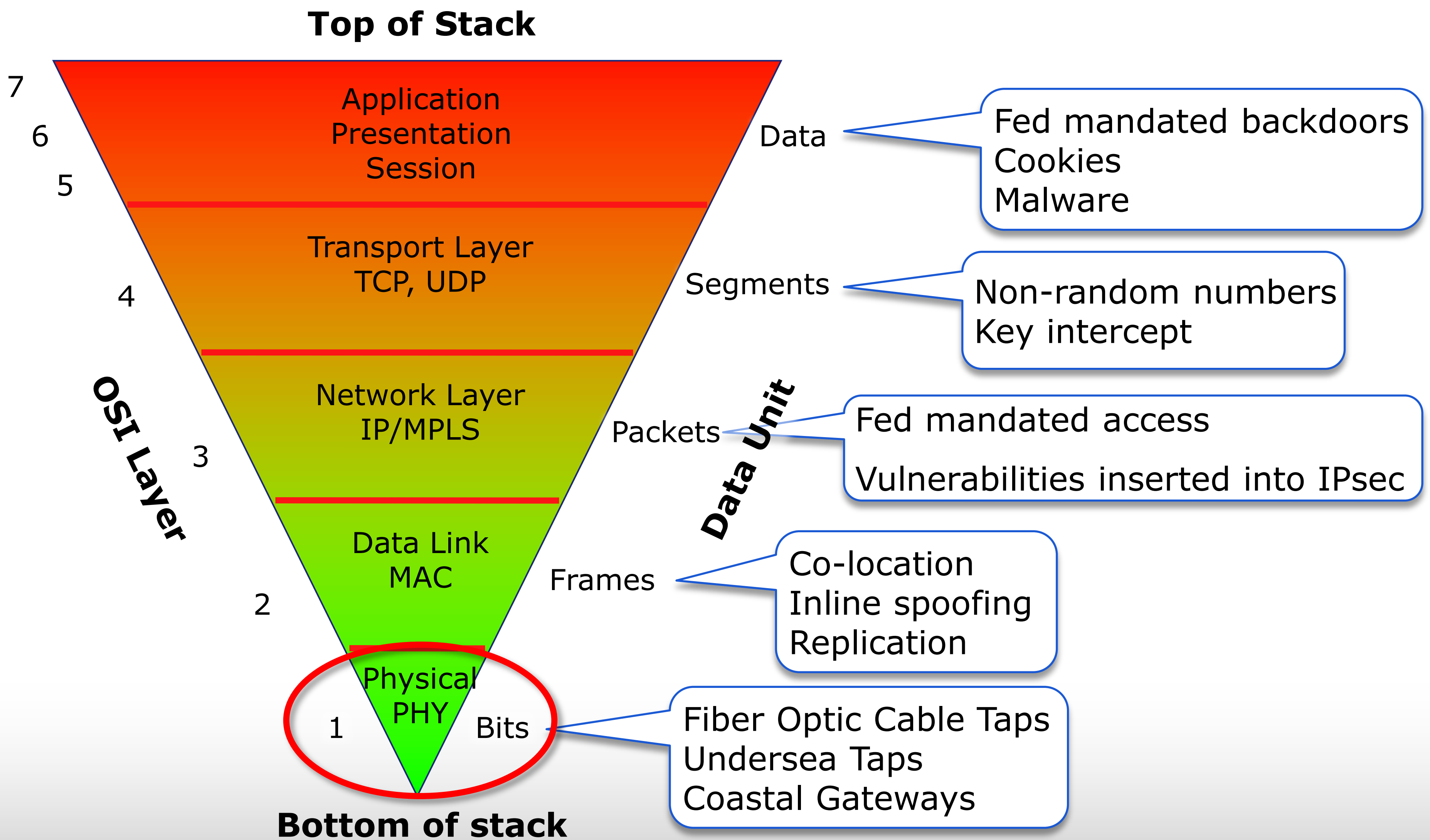




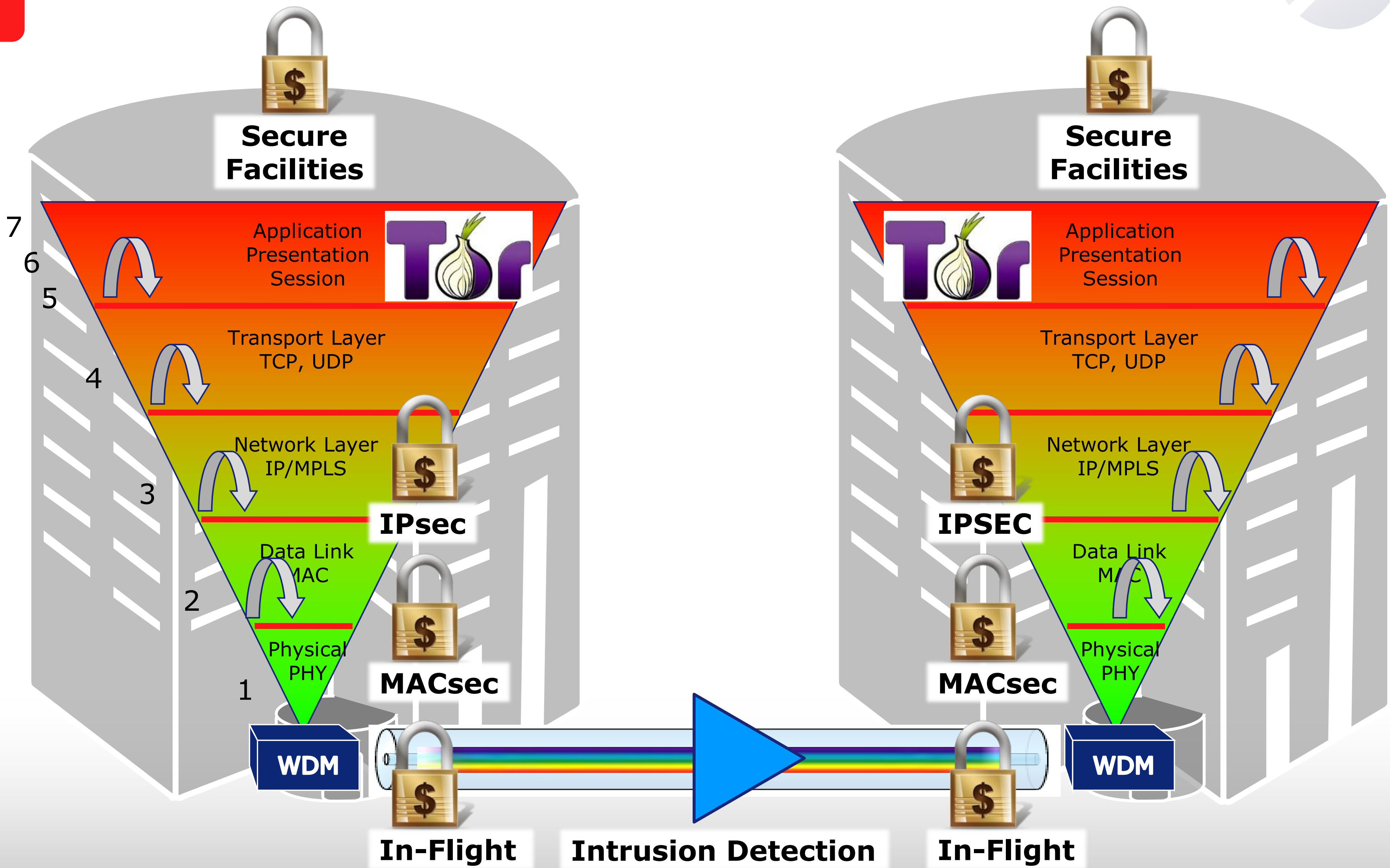
IPsec Compromised from Day 1

- 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 *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



Secure End-to-End Data Transport



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

ADVA™
Optical Networking

Thank you

info@advaoptical.com