Encryption

How To Secure My Data

What to Protect???

DATA

Data At Rest

Data at Rest Examples

Worst Culprits?

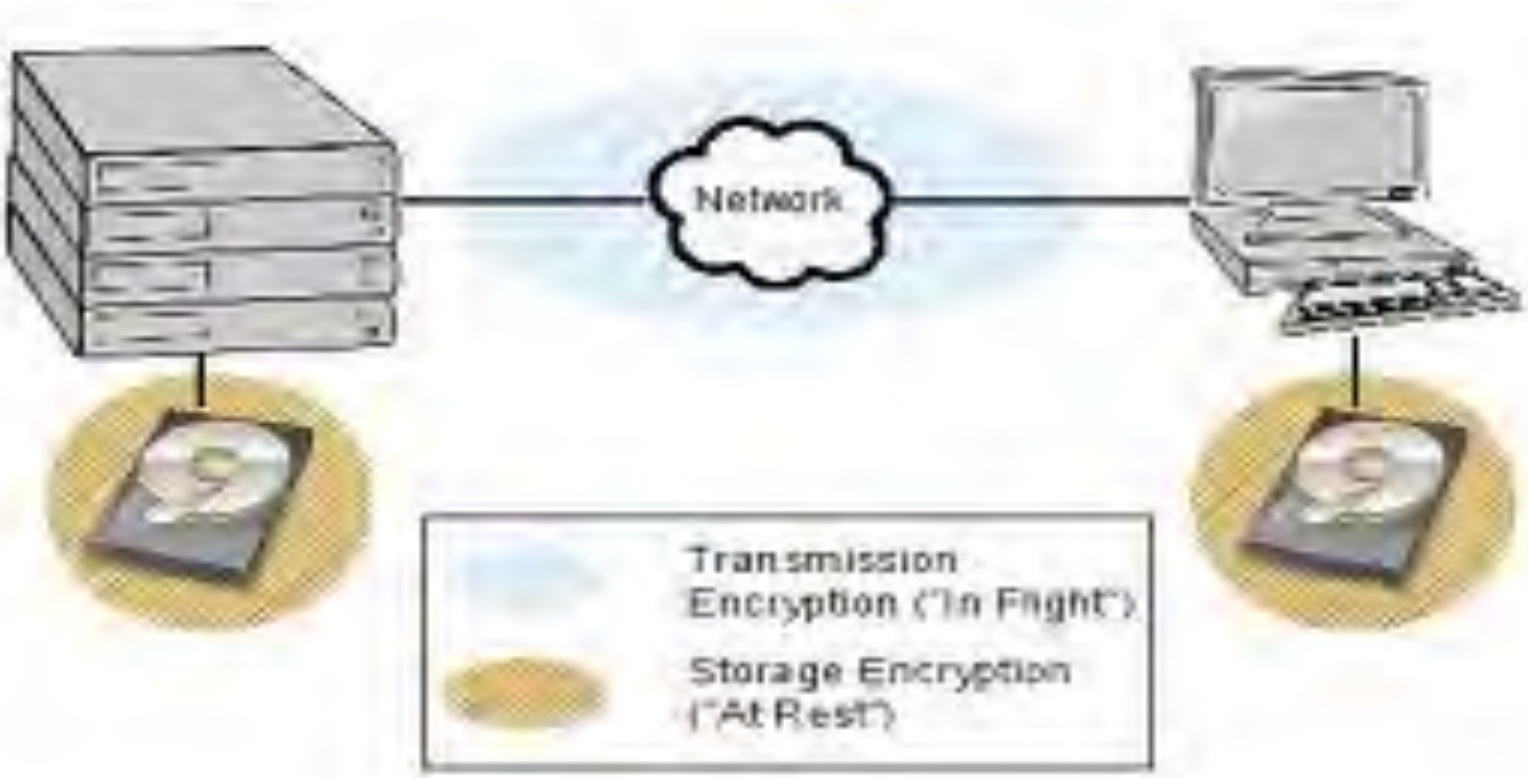
- Lost
- Infected Easily
- Used as ‘Backup’
- Lent to others
- Data Corruptions more common

Worst Culprits?

- Stolen
- Left at airports, on trains etc
- Hard disk corruption common
- Connected to many networks

&

Data in Motion



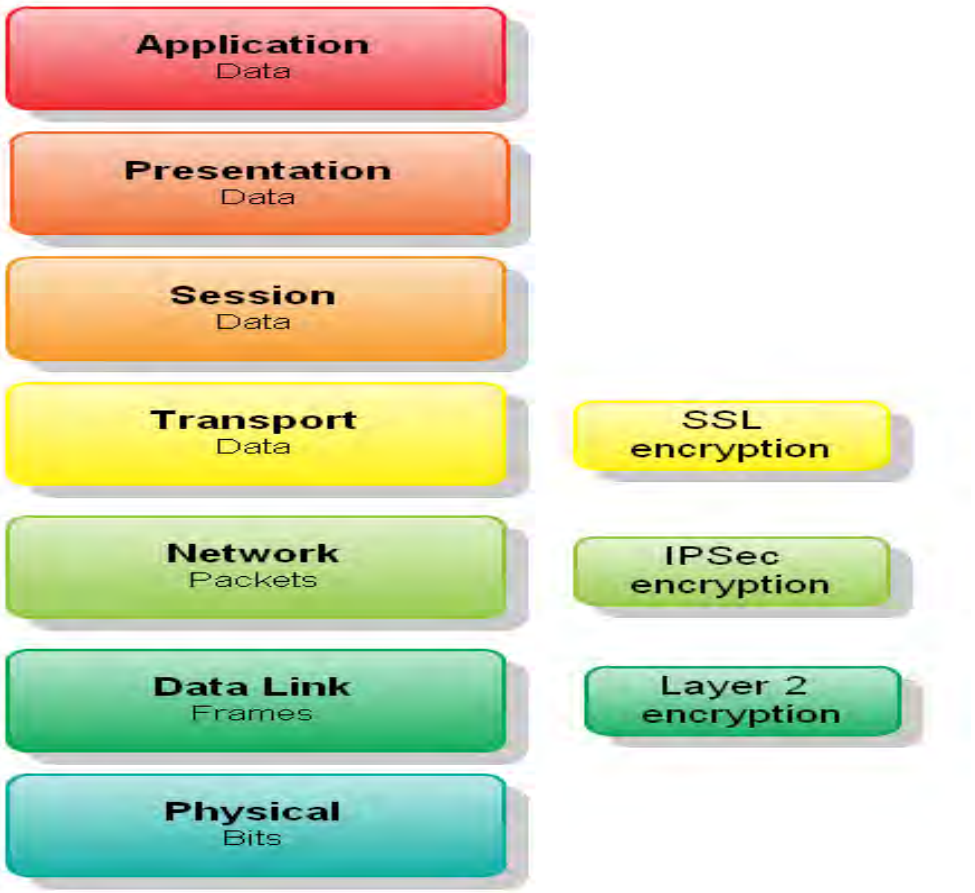
What can we do decrease the Risk?

- Laptops and Memory sticks should never have a unique copy of important information.
- All confidential information should be encrypted.
- Staff informed of good working practises.
- Make Sure Laptops are ‘Patched’

Encryption

- **Encryption** is the conversion of data into a form called a ciphertext that cannot be easily understood by unauthorized people.
- **Decryption** is the process of converting encrypted data back into its original form, so it can be understood

Layers Encryption



In reality, encryption can happen at different layers of a network stack, the following are just a few examples:

- End-to-end encryption happens within applications.
- SSL encryption takes place at the transport layer.
- IPSec encryption takes place at the network layer.
- Layer 2 encryption takes place at the data link layer.

Understanding layer 2 encryption

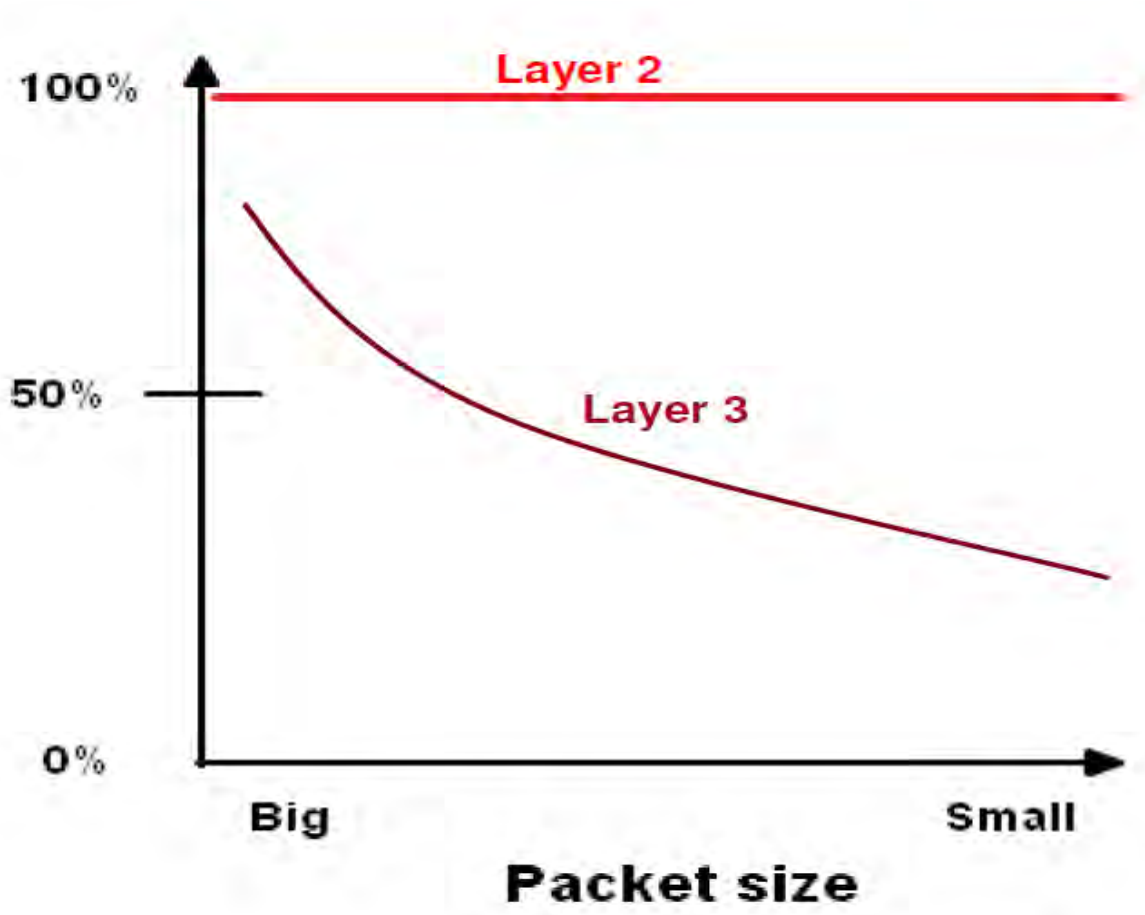
At first glance encryption seems an easy choice; after all why expose confidential information to prying eyes when you can protect it by scrambling?

Some of the traditional objections to encryption include loss of performance and the complexity of managing encryption keys.

Today however modern hardware and software systems have whittled away these issues to the extent that it is now possible to deploy hardware encryption to secure information at full line rates up to 10Gbps and with simple fully automatic key management.

Benefits of layer 2 encryption

Layer 2 encryption is often referred to as a “bump in the wire” technology. The phrase conveys the simplicity, maintainability and performance benefits of layer 2 solutions that are designed to be transparent to end users with little or no performance impact on network throughput.


100%
Layer 2
50%
Layer 3
0%
Big
Small
Packet size

In a recent study by the Rochester Institute of Technology (RIT), it was determined that Layer 2 encryption technologies provide superior throughput and far lower latency than IPSec VPNs, which operate at Layer 3.

The RIT study concludes:

Enterprises that need to secure a point-to-point link are likely to achieve better encryption performance by shifting from traditional encryption with IPSec at Layer 3 to the overhead-free encryption of frame payloads at Layer 2.”

Layer 2 Encryption

- Only Layer 2 encryption solution worldwide with 100% data throughput rates of up to 10 gigabits per second without overhead
- scalable encryption solutions and optional upgrades
- Easy to integrate into existing point-to-point, point-to-multipoint and multipoint-to-multipoint networks
- Encrypts unicast, multicast and broadcast, supports class of service, VLAN-ID and tagging

Maximum performance and minimum latency

The outstanding performance with 100% encryption throughput of up to 10 gigabits per second and the extremely low latency in the microsecond range allow the equipment to be used even in time-critical applications and connections subject to heavy loads. The Layer 2 approach guarantees a simple configuration, bump-in-the-wire integration and minimal maintenance.

additional advantages of encrypting at Layer 2

- Lowest impact on network performance
- Reduced complexity (bump in the wire)
- Transparent to media (voice, data, video etc.)
- Little or no configuration
- Operates at wire speed up to 10Gbps.
- Introduces no overhead. In contrast, Layer 3 IPSec typically adds significant overhead (over 40% of available bandwidth for smaller packets)
- Implementation of Layer 2 encryption devices is simple

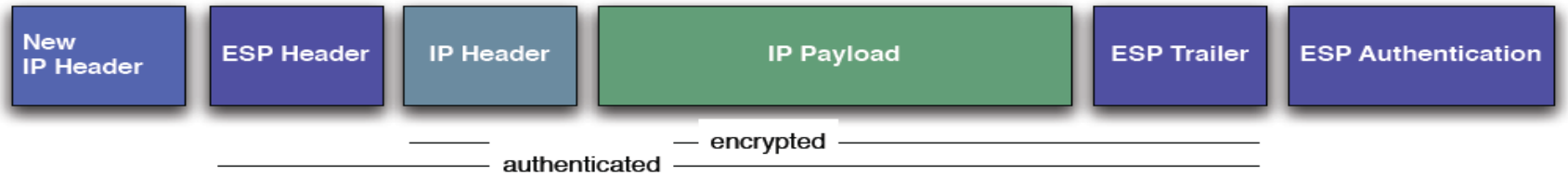
additional advantages of encrypting at Layer2

Outsourcing of routing tables is also seen as a weakness of Layer 3 VPN services because many corporations don't want to relinquish control or even share their routing schemes with anyone, not even their service provider. They prefer Layer 2 network services, such as Ethernet, Frame Relay or ATM as these are simpler in architecture and allow customers to retain control of their own routing tables.

IP Packet

IP Packet IP Sec Transport Mode

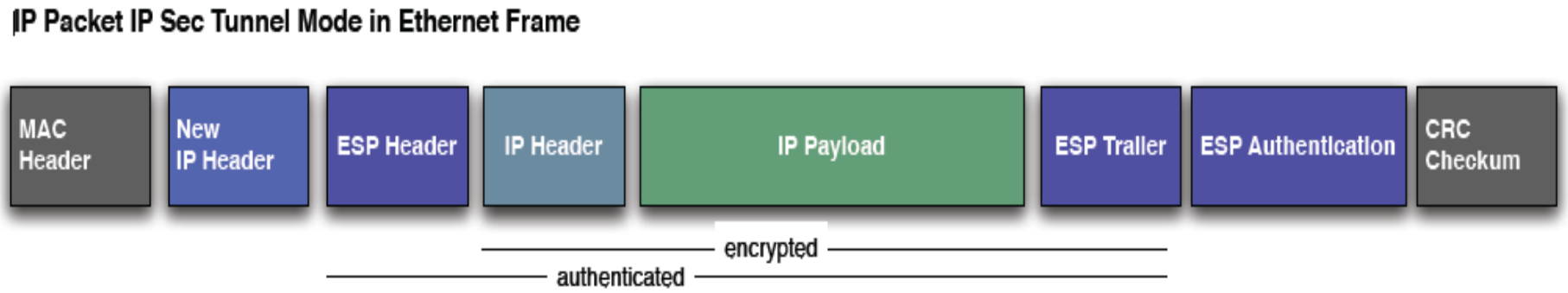
IP Packet IP Sec Tunnel Mode



Let’s start with a packet the way it is transported on layer 3: It consists of an IP header and the payload. IPSec ESP transport mode adds an ESP Header, an ESP trailer and ESP authentication. In transport mode only the payload is encrypted while the IP header remains unprotected. The established way to encrypt site-to-site traffic with IPSec is the tunnel mode. A new IP Header is added, so that the entire

IP packet (header and payload) can be encrypted without sacrificing network compatibility.

For the transport over an Ethernet network the encrypted IP packet gets a MAC header and a CRC checksum.



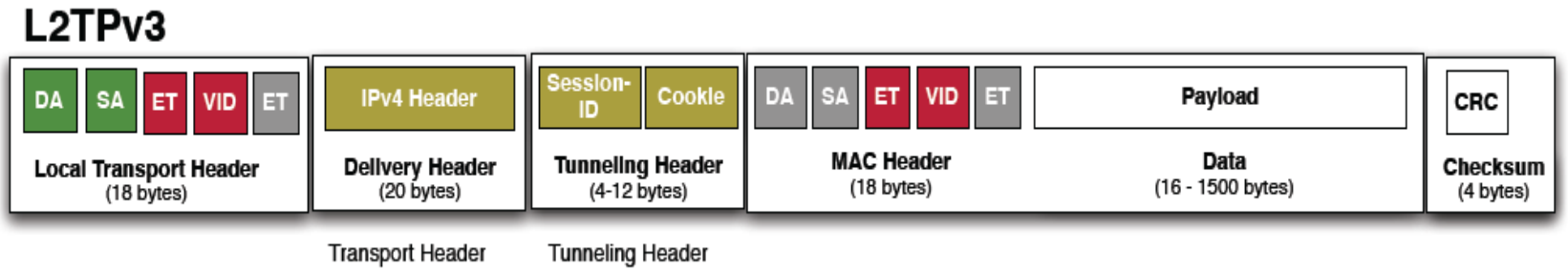
For Ethernet the entire IP packet encrypted with IPSec ESP Tunnel Mode is pure payload. Accordingly a transport mode encryption at layer 2 can provide the same protection as IPSec ESP Tunnel Mode without generating packet overhead. The encryption can encrypt the entire IP packet without introducing packet overhead. IPSec ESP Mode features Encapsulating Security Payload, which provides confidentiality, data origin authentication, connectionless integrity and an anti-replay mechanism. To maintain comparable layer-specific security, equivalent features need to be implemented at layer 2. Some of the overhead that would have been generated at layer 3 thus moves down to layer 2. Properly implemented it will cause less overhead and be much more flexible in terms of network functionality than IPSec at layer 3.

At layer 3 it also matters if you encrypt IPv4 or IPv6. Both are using IPSec as encryption standard, but the differences between IPv4 and IPv6 make it a completely different story.

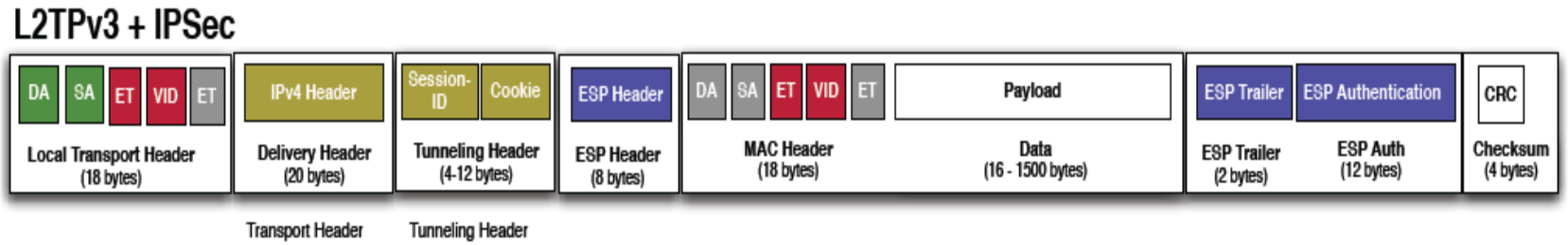
At layer 2 though, it does not make any difference if the payload to be encrypted consists of IPv4 or IPv6.

Using IPSec for Ethernet encryption

It is possible to encrypt Ethernet using IPSec. In order to do so the Ethernet frame has to be fork lifted up to layer 3 to become IP payload. As soon as the Ethernet frame is IP payload it can be encrypted at layer 3 with IPSec. As IP is transported over Ethernet the result is Ethernet transported over IP over Ethernet. It is as inefficient as it sounds. If e.g. L2TPv3 is used to transport Ethernet over IP the overhead generated by encapsulation is 50 bytes.



IPSec encryption will add another 38-53 bytes. The security overhead and the security are limited as only transport mode can be used in this scenario.



Native Ethernet encryption at layer 2

Let's start again with an IP packet the way it is transported on layer 3: It consists of an IP-header and the payload. For the transport on layer 2 on Ethernet the packet is framed with a MAC header and a CRC checksum. For Ethernet it doesn't make a difference if the IP packet is encrypted or not, it is just payload.

IP Packet (Header and Payload)

IP Packet (Header and Payload) inside Ethernet Frame

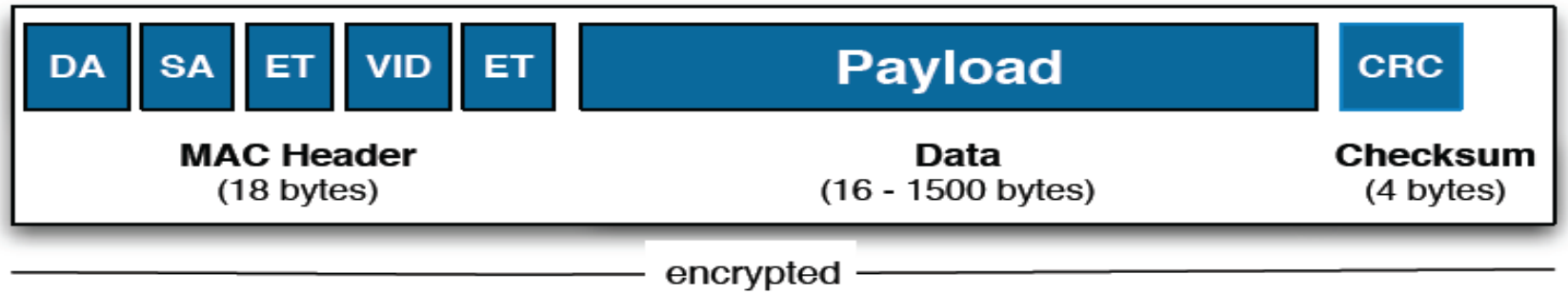
IP Packet as Ethernet Payload

A transport mode encryption at layer 2 will encrypt the entire IP packet including the IP header without requiring any tunneling. Tunneling alone generates 20-40 bytes of avoidable overhead and adds noticeable latency.

To get a better understanding how layer 2 encryptors encrypt at layer 2 it is best to look at the different encryption modes:

Native Ethernet Encryption Modes

A- Bulk Mode

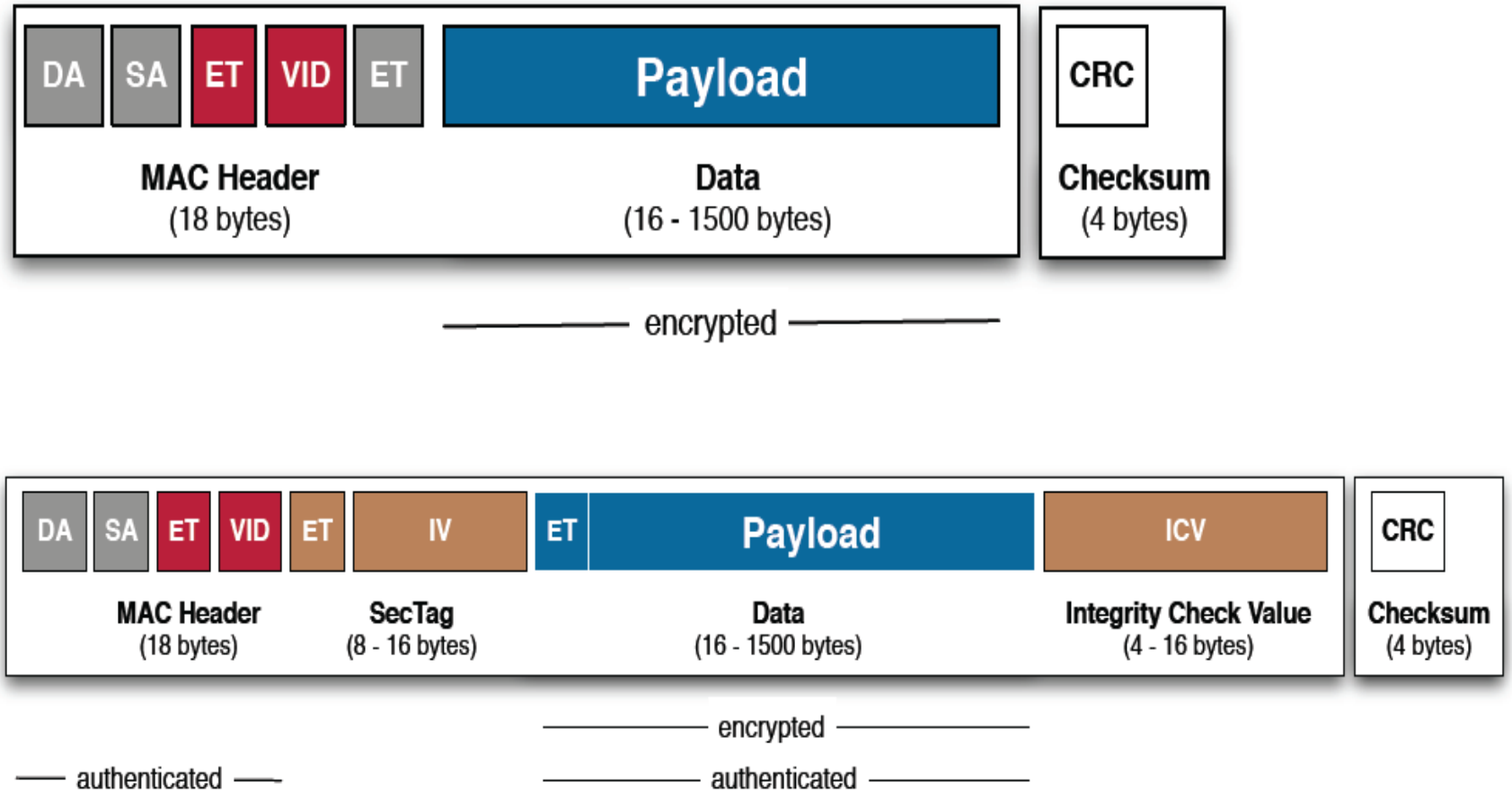


Bulk Mode (also known under the terms Frame Encryption and Link Encryption) encrypts the entire Ethernet frame between the Preamble and the Interframe Gap. To reach the same coverage when encrypting the frame with a layer 3 encryptor, the entire Ethernet frame would have to be lifted up to layer 3, encapsulated and then encrypted with IPSec ESP Tunnel Mode. This would cause massive and unnecessary overhead. The Bulk Mode on layer 2 limits the available usage scenario to Hop-to-hop, as all relevant addressing info is encrypted

Native Ethernet Encryption Modes

B- Transport Mode

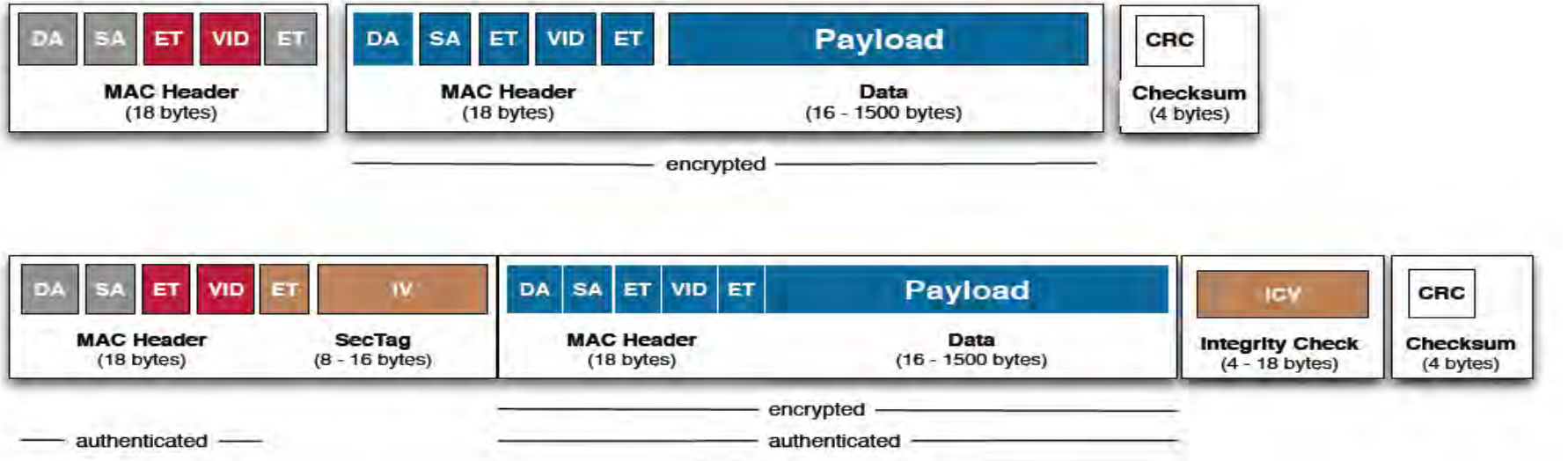
The most widely used encryption mode is the transport mode. The reason behind this is the full network compatibility ensured by limiting the encryption to the payload.


DA
SA
ET
VID
ET
Payload
CRC
MAC Header
(18 bytes)
Data
(16 - 1500 bytes)
Checksum
(4 bytes)
encrypted
DA
SA
ET
VID
ET
IV
ET
Payload
ICV
CRC
MAC Header
(18 bytes)
SecTag
(8 - 16 bytes)
Data
(16 - 1500 bytes)
Integrity Check Value
(4 - 16 bytes)
Checksum
(4 bytes)
encrypted
authenticated
authenticated

Native Ethernet Encryption Modes

C- Tunnel Mode

Tunnel mode is also an option on layer 2, but only used if the entire original frame must be encrypted and the encryption needs to support a multi-hopscenario. Tunneling adds overhead and processing time.



Weaknesses & Solutions

What are Weaknesses ??

How To Solve??

level Vulnerabilities

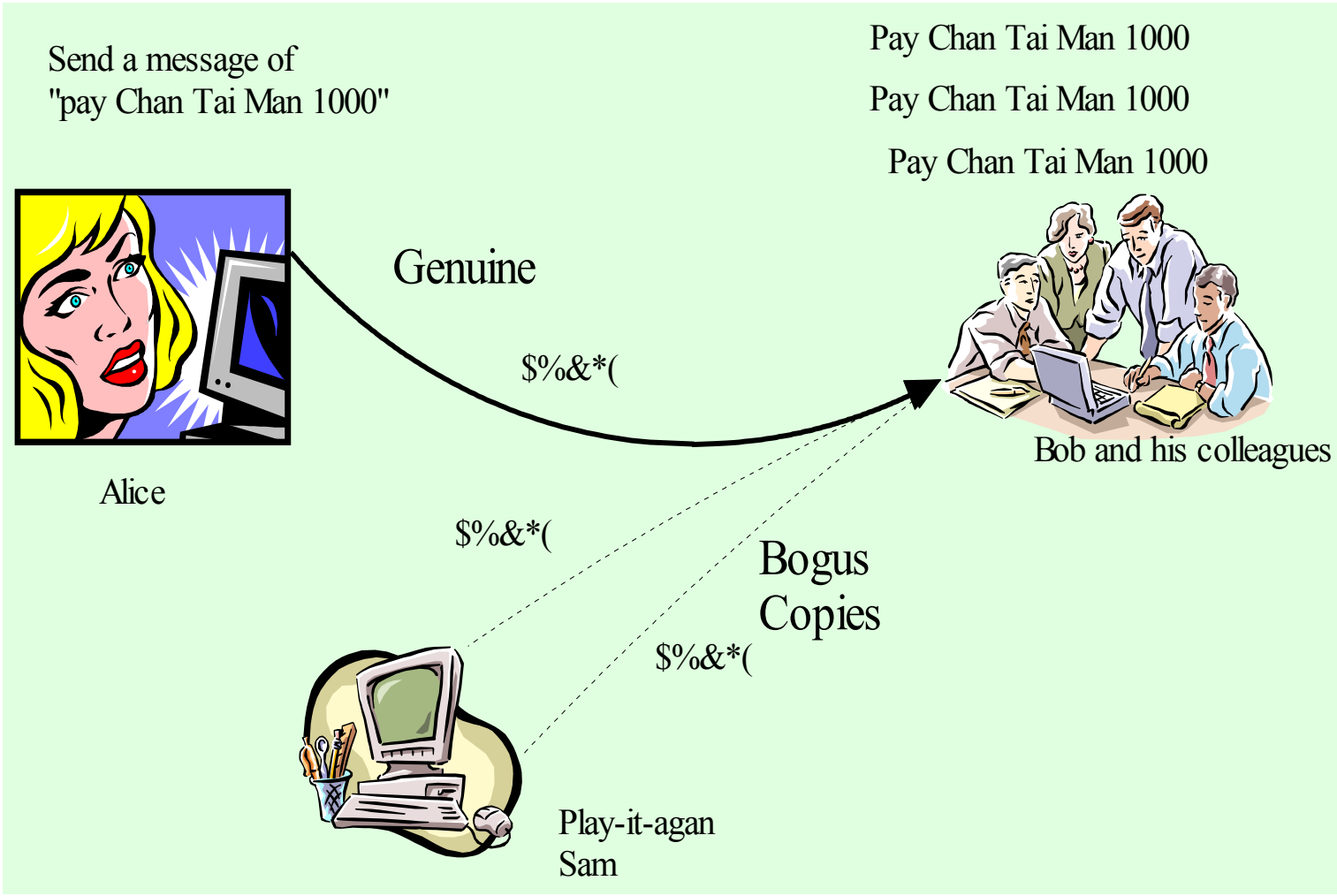
There are a few attacks, Below are some of them:

- Replay Attacks
- Rewrite Attacks
- Convert Signalling Attacks

Replay Attacks –

- If the message is an encrypted, why should we care about replay?
- The reason is that:
  - If an outsider captures the encrypted message and re-send it, he/she might attack the system

Example of Replay Attacks

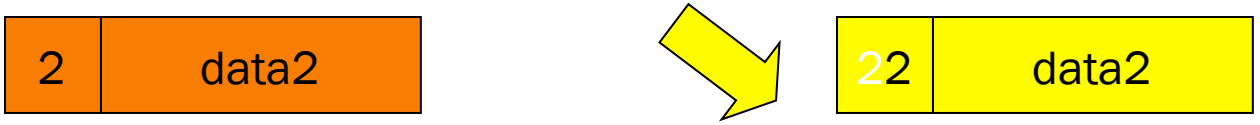


Example of Replay Attacks - Explanation

- Alice sends a message of “pay Chan Tai Man” to Bob. She sends one genuine (true) message.
- Play-it-again **Sam** captures the encrypted message and re-sends twice to Bob.
- Bob and his colleagues will then pay Chan Tai Man three times.
- Of course, Sam will have certain benefits of doing this.

How to solve this? – Replay attack

- Each plaintext message must have an extra information such as message number.
- If the receiver receives a duplicated message, it is discarded.



This will solve it in TCP/IP (layers 3 & 4). It has this feature to solve this problem

Rewrite Attacks

- If an hacker knows the contents, he/she can modify the encrypted message.
- Say for example, the encrypted message of pay 1000 is 89^&**o**iu, he/she can modify 89^&**a**iu by changing o to a. The resulting plaintext message is 9000. (This assumes that 89^&aiu will produce 9000.)

How to resolve this? - rewrite

There are many methods. Below are some of them

1. Avoid products using other modes. Always use block ciphers techniques. (crude rewrite attacks are still possible with block mode.); or
2. Insert a random number into each packet, include it in the packet checksum and encrypt the resulting packet; or
3. Use digital signature to authenticate the source of data. (the message is signed)

Digital signatures

- A **digital signature** is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is **authentic**. Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.

Digital signatures

- Digital signatures rely on certain types of **encryption** to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures.

Encryption and digital signatures can be used together, or separately.

- a message may be encrypted, but not digitally signed (only people with the key can read it,
  but the reader cannot be certain who actually wrote it)
- a message may be digitally signed, but not encrypted (everyone can tell who wrote it, and
  everyone can read it)
- a message may be encrypted first, then digitally signed (only someone with the key can read
  it, but anyone can tell who wrote it)
- a message may be digitally signed first, then encrypted (only someone with the key can read
  it, and only that same reader can be sure who sent the document)

Your employees are your biggest security challenge. Constant education of users is crucial. When they join the company, a proper orientation should be held to explain the importance of information security, what it entails, what they should and should not be doing.

Jack Loo


Think Twice
Before Sending!


Caught by phishers...
Don't take the bait!


If you
don't know
the person
on the other end,
mind what
you say


Contents
Unknown
UNSOLICITED
EMAIL!

Thank You

Mohammad Jarrar