THALES

Data Transmission Security

Securing The Blurry Line Between Classified and Unclassified Data

Mark Saunders
Sales Engineering Network Security
Thales eSecurity

Data Proliferation Continues to Flourish

Today, we require data “everywhere”

- Situational Awareness
- Orders
- Unmanned vehicle controls
- Live Voice and Video
- Intelligence
- More…

Methods for delivering data have come a long way

The rise of high speed virtual networks

Security for the transmission of data has lagged

We need to be smarter

New Classifications of Data are Emerging

Secret and Top Secret methods for data security are well established

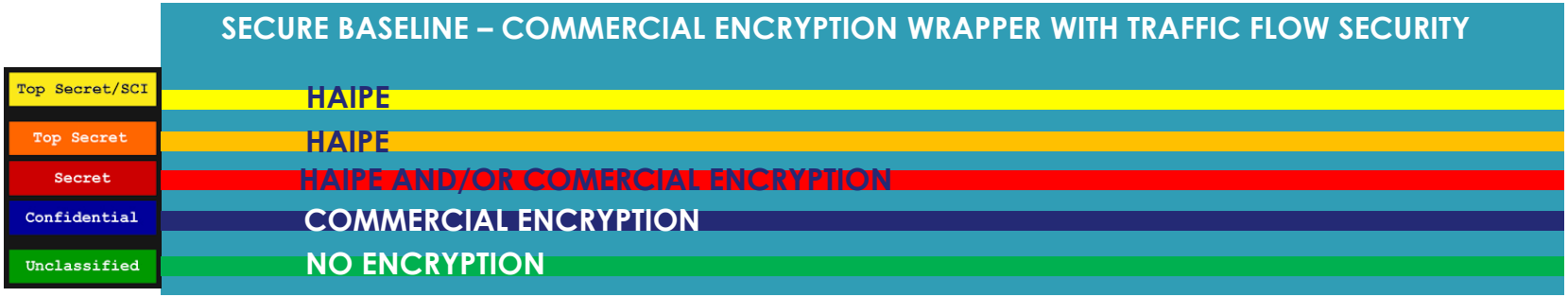
New data classifications are emerging

- The sheer volume of data required
- The influence of timeliness and longevity value of the data such a situational awareness
- Sheer volume of data creating needs for securing certain classifications of data

New methods for securing data transmissions must be implemented

An Efficient and Secure Network Baseline Must Be Established

- Protect against compromises for all data types (sensitive and benign)
- Preserve the integrity of existing secure protocols (secret and top secret)
- Provide a baseline for the protection of new data classifications via double commercial encryption
- The above requirements must be met at near 100% network efficiency



Encryption Alone Does NOT Constitute Security

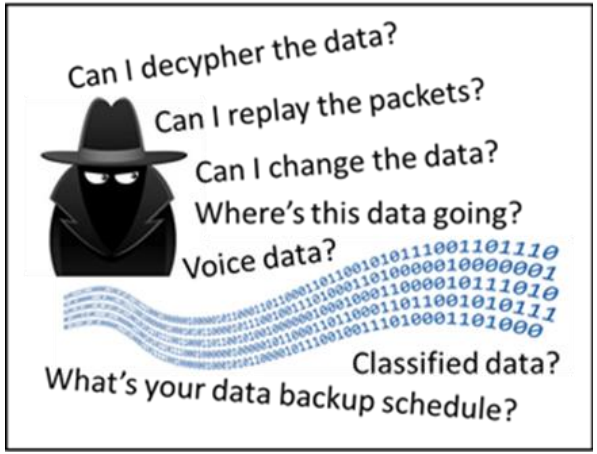
- Encryption secures data content
- Encryption does NOT necessarily secure data transmission
- Data Security and Transmission Security are two separate topics
- Both combine to solve the holistic problem of Data Transmission Security

	Data Security
+	Transmission Security
=	Total Data In Motion Security

So You Think Your Information Is Secure?

Encryption protects data at rest

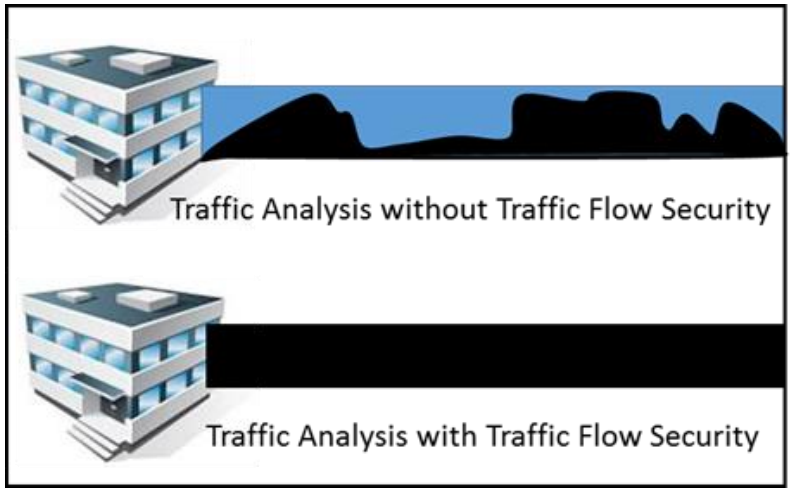
Even encrypted data has vulnerabilities when set into motion



- Data Integrity compromises
  - Packet level authentication.
- Packet Replay attacks
  - Secured by Galois Counter Mode (GCM)
- Data Analysis – how much data, when, where, what type?
  - Secured by Traffic Flow Security (TFS)

Masking Data Patterns with Traffic Flow Security

- Traffic patterns and data types can be determined through analysis
- Random data can be generated to mask downtime
- An eavesdropper sees a constant frame size 24 hours a day, 7 days a week



- An eavesdropper cannot differentiate between highly classified data, unclassified data, or no data at all

Are We Secure Yet?

Data protected with encryption

Transmission protected from man in the middle attacks

Analysis of data protected by Traffic Flow Security

What else could possibly go wrong?

Let's Talk About Efficiency

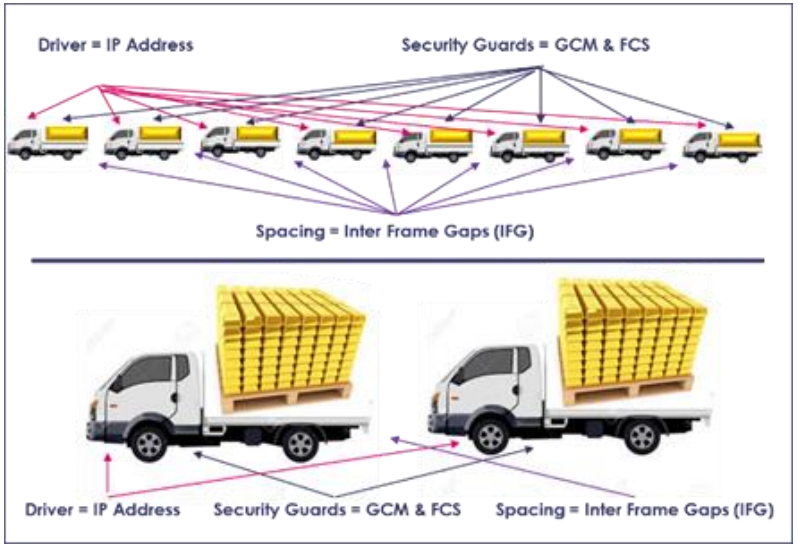
- Transporting a packet from point A to point B is quite complex
- Overhead is required to route, prioritize, and secure the data
- Data types (e.g. voice, data, jumbo frames) vary in size
- Overhead is constant while data packets vary
- It is possible that overhead is greater than data

Solving the Problems of Efficiency

- Move many encrypted packets into a larger, secure transmission "container"
- Significantly reduce the burden of overhead

Actual Test Data Yields
98% Efficiency
With
Full Data Encryption
And
Total Transmission Security

Moving The Gold



Are We There Yet?

Data protected with encryption

Transmission protected from man in the middle attacks

Analysis of data protected by Traffic Flow Security

98% Network Efficiency

Yes, We're There!

Conclusion

- **A secure, encrypted infrastructure can be achieved with 98% efficiency**
- **Existing classified protocols can seamlessly tunnel through**
  - Provides an additional layer of commercial encryption for data
  - Provides complete protection for data in motion
  - Provides TFS to mask traffic patterns and classified protocols
- **Unclassified benign communications are completely masked**
- **New classifications can use a simple encrypted VPN to achieve double commercial encryption with no additional effort**
- **All data is protected – from Top Secret to Funny Cat Videos**

Further Reading

- Further reading.
- Please download the full paper at http://go.thalesesecurity.com/rs/480-LWA-970/images/Data_Transmission_Security.pdf
- Mark.saunders@thales-esecrutiy.com