Securing data and identities

Mario Kadastik, PhD

Top Systems

mario.kadastik@top-systems.eu

Topics

- Why do we even need encryption?
- What might/should people encrypt?
- What kind of technologies to use?
- Some example products...

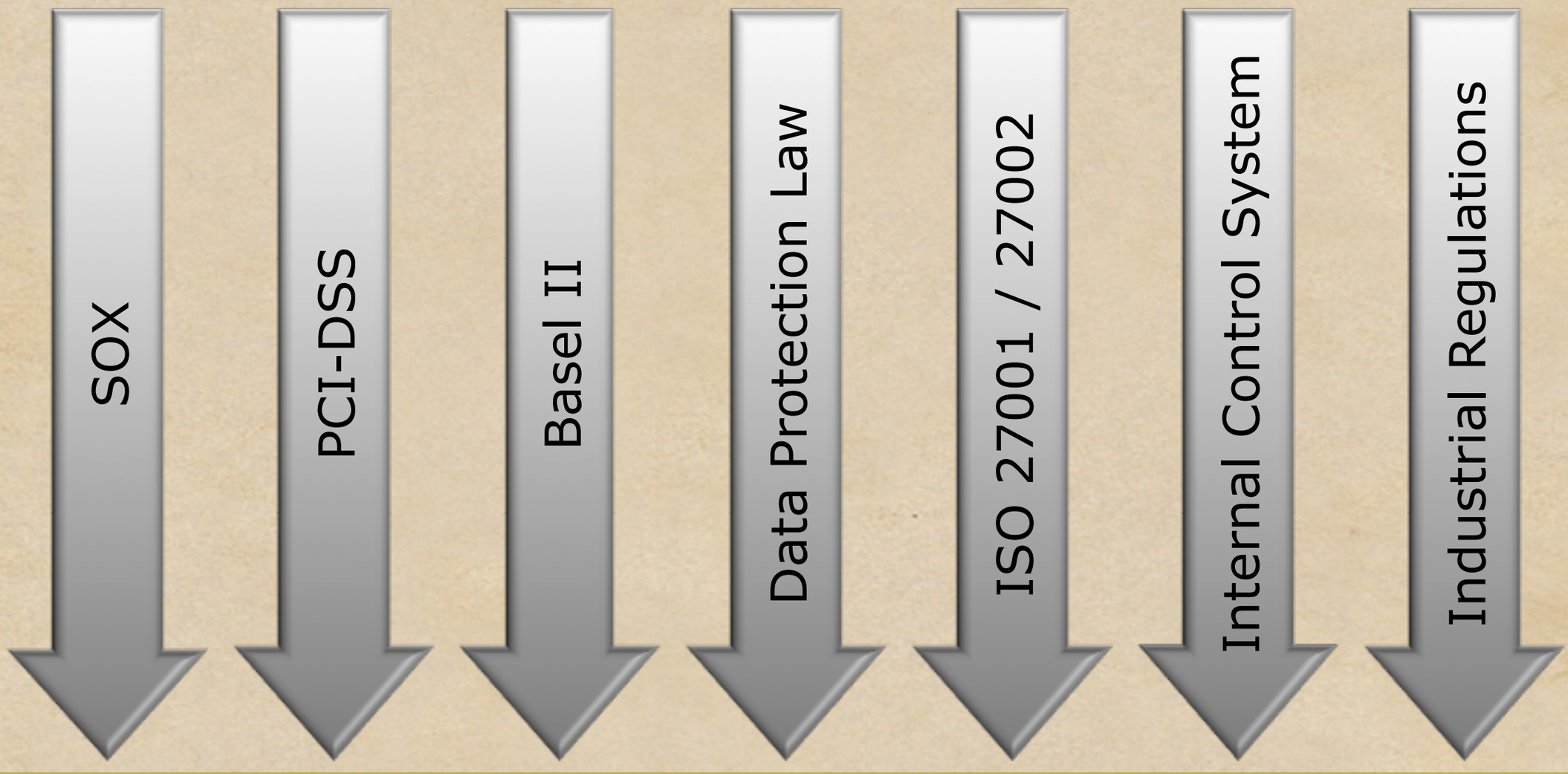
Digital frontier

- We live online
  - e-Government, e-Banking, e-Commerce
- The amount of data that companies have to keep and process about people is huge
- With increased data comes increased responsibility

Why encryption?

- Providing encryption is providing trust
- Encrypted connections allow for safe communication without eavesdroppers
- Encrypted identity information allows one to trust who they are dealing with
- This is also understood by regulatory people as more and more regulations require data encryption for any sensitive information both at rest and in transit

Regulations



Information Security

So where is data?

- We can differentiate two separate classes
  - Data at rest
  - Data in transit
- In both cases there are good implementations and not so good ones

Data at rest

- Any database of information can be misused by a culprit in one way or another
- Gaining access to a system the culprit can steal/alter the content bringing either direct or indirect loss of revenue
- The largest loss however is the loss of trust
- Encrypting key information in databases and files can keep the culprit away

Data at rest

- However often the encryption keys are stored in the same place as the encrypted data...
  - It's like locking your front door and leaving the key under the mat...

- Encryption has to be implemented wisely and one has to understand the value of encryption keys -> sum value of all the encrypted data

Key protection

- To really protect the encrypted content one has to protect the encryption keys

- Specific hardware exists that performs all the transactions necessary inside a trusted boundary

- Various levels exist for when only evidence of intrusion/ theft is necessary or wether active countermeasures need to be implemented

Data in transit

- In todays world there is constantly private data moving about on "the net"
- Any unencrypted communication can be recorded/changed by ANYONE who manages to connect to a device in the path of the communication
- A common example is ordinary web browsing vs SSL encrypted browsing

Basic data in transit

- In the case of https encryption there are two benefits
  - Client identifies the site
  - No man-in-the-middle attacks possible
- However for it to be safe the SSL keys have to be kept in a secure way
- Loss of corporate web server keys can lead to phishing attacks, MiM attacks and generic loss of trust

More complex data in transit

- Even if people protect their datacenters with armed guards and three tier access systems they forget the data leaving...
- Anyone can open a junction box or crawl into a manhole to install wire tapping equipment
- And it's not expensive! Cloning a fiber with a simple touching device costs less than 1000 eur

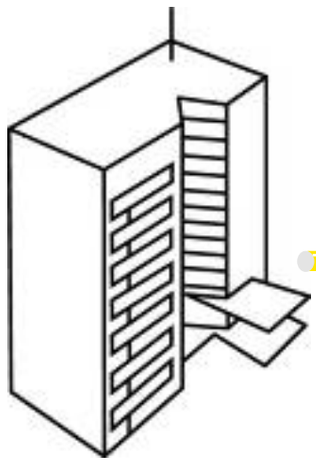
Wiretapping

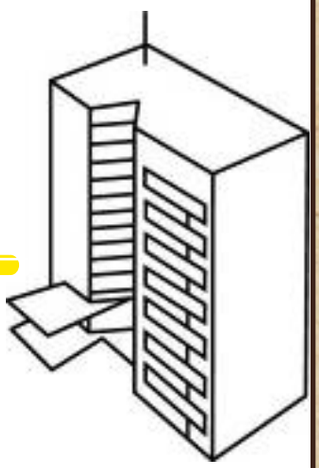
- Myths about wiretapping and encryption
  - Fiber links cannot be tapped
  - Volume of data and multiplexing make it impossible to make sense
  - Fiber Channel protocol is too complex
  - Encryption is too slow / adds complexity

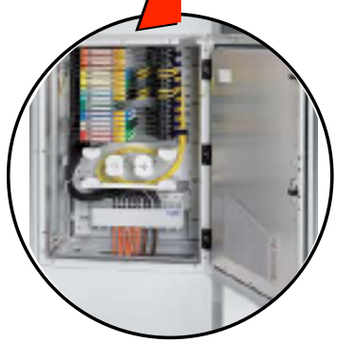
Myth 1 - impossible to tap

Y-Bridge for service operations

Clip-on coupling device

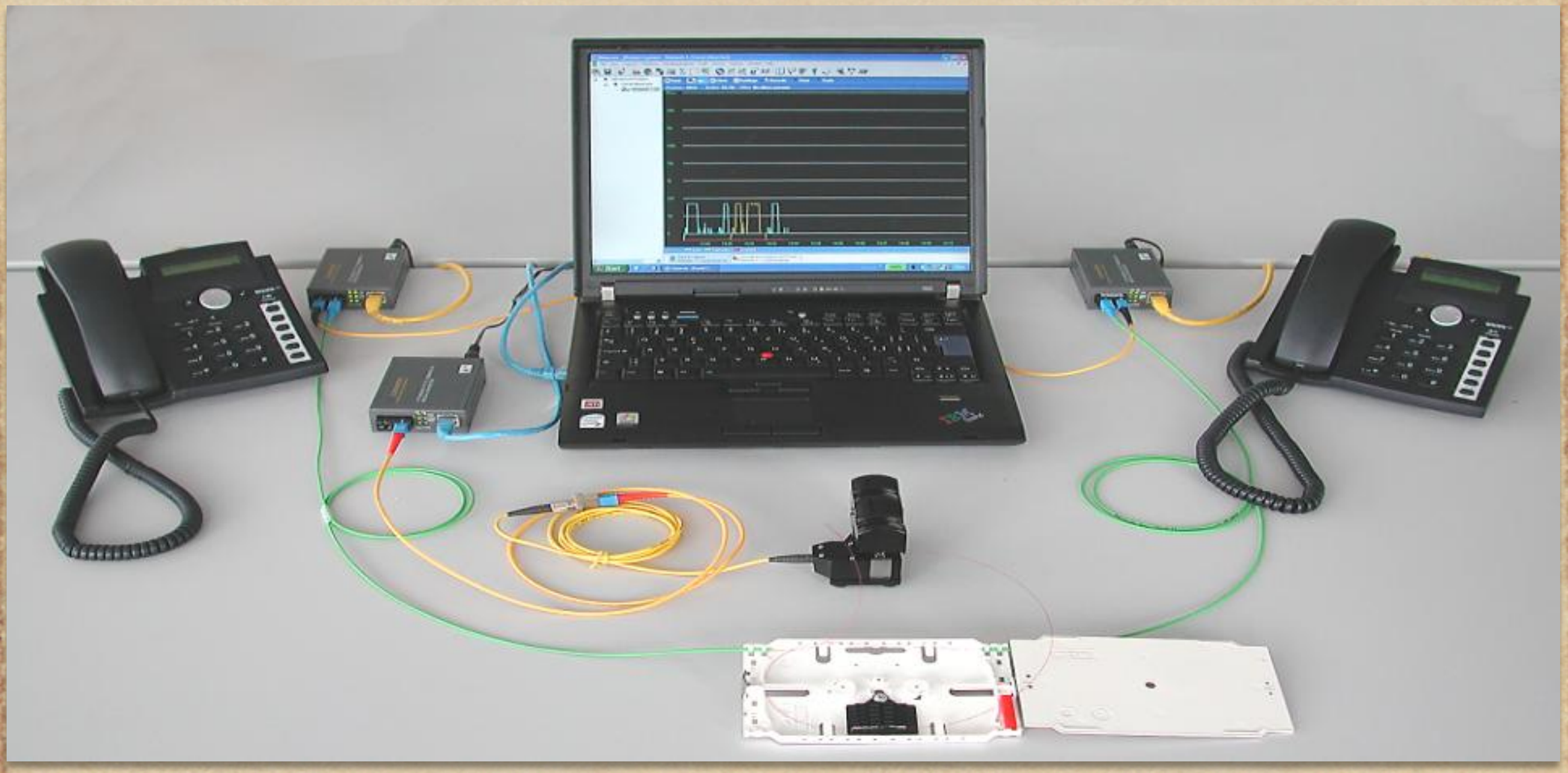






Junction box with splicing boxes
outdoor / inhouse / channel

Simple VOIP listening setup



Myth 2 - Volume and DWM

- Gigabit data analyzers are easily and freely available also as software
- *WDM analyzers are readily available allowing excellent wavelength separation throughout the used ranges
- Software applications for ethernet, sonet, FC analyzing are available both free and commercially

Myth 3 - FC too complex

File Edit View Histogram Tools Window Options Help

00:05.130_379_192 | All Ports

Icon	mm:ss.ms_us_ns (R	Port	Count - Type	Count - Type	Summary	Bytes	Destinat	Source	LUN	OX_Id
FR	00:05.123_959_824	FC Port(1,1,1)	1 - FC4SData		FC4SData; SCSI FCP; Offset = 0x00001800; Len = 0x800;	2084	011500	010900		00D6
FR	00:05.130_213_752	FC Port(1,1,2)		1 - FC4Status	Good Status;	60	010900	011500		00D6
FR	00:05.130_275_644	FC Port(1,1,1)	1 - FC4Cmd		Write(10); LUN = 0x0002; LBA = 0x005E607F; FCP_DL = 0x(	68	011500	010900	0002	00E1
FR	00:05.130_370_880	FC Port(1,1,2)		1 - FC4XRdy	DATA_RO = 0x00000000; BURST_LEN = 0x00001000;	48	010900	011500		00E1
FR	00:05.130_379_192	FC Port(1,1,1)	1 - FC4SData		FC4SData; SCSI FCP; Offset = 0x00000000; Len = 0x800;	2084	011500	010900		00E1
FR	00:05.130_384_228	FC Port(1,1,1)	1 - FC4SData		FC4SData; SCSI FCP; Offset = 0x00000800; Len = 0x800;	2084	011500	010900		00E1
FR	00:05.135_282_736	FC Port(1,1,2)		1 - FC4Status	Good Status;	60	010900	011500		00E1
FR	00:05.135_321_216	FC Port(1,1,1)	1 - FC4Cmd		Write(10); LUN = 0x0002; LBA = 0x005E606F; FCP_DL = 0x(	68	011500	010900	0002	00F3
FR	00:05.135_410_384	FC Port(1,1,2)		1 - FC4XRdy	DATA_RO = 0x00000000; BURST_LEN = 0x00001000;	48	010900	011500		00F3
FR	00:05.135_418_932	FC Port(1,1,1)	1 - FC4SData		FC4SData; SCSI FCP; Offset = 0x00000000; Len = 0x800;	2084	011500	010900		00F3
FR	00:05.135_423_968	FC Port(1,1,1)	1 - FC4SData		FC4SData; SCSI FCP; Offset = 0x00000800; Len = 0x800;	2084	011500	010900		00F3
FR	00:05.139_213_964	FC Port(1,1,2)		1 - FC4Status	Good Status;	60	010900	011500		00F3

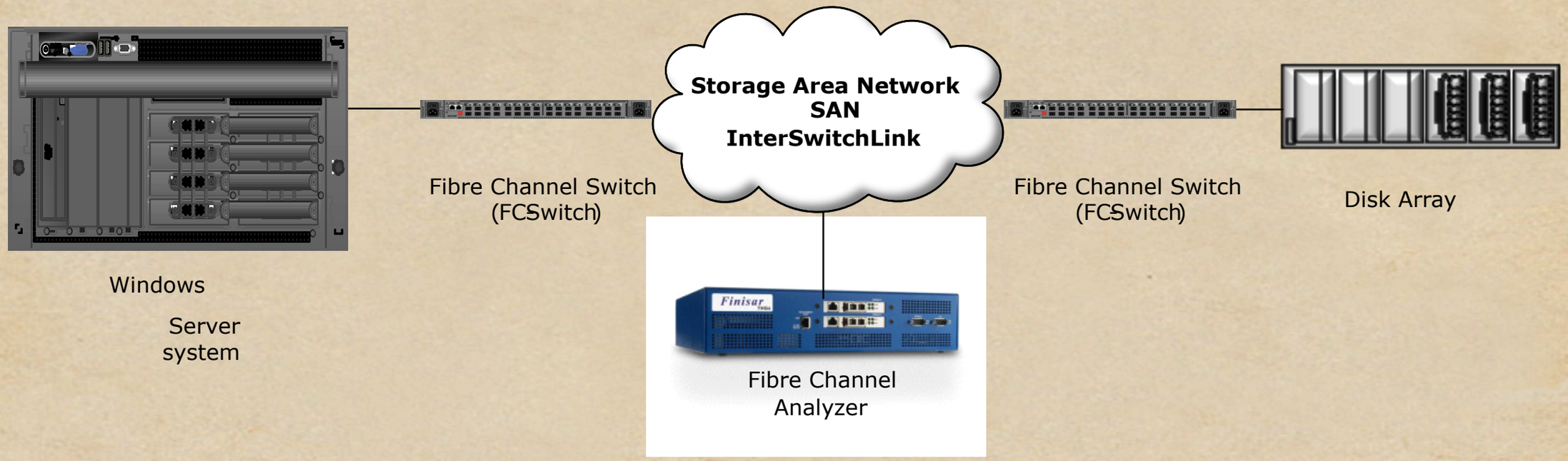
General | 10 Bit | Tree

Index	Hex	Ascii
04D0	00 00 00 00 1B 00 01 00 28 00 00 00 28 00 04 00 18 00 00 00 0D 00 00 00 0D 00 00 00	........[...[..............
04EC	00 00 00 00 00 00 00 00 50 15 74 D1 03 00 00 00 9C 54 00 01 0D 00 00 00 0D 00 00 00	........P.tÑ....œT..........
0508	00 00 00 00 00 00 00 00 00 00 00 00 48 01 00 00 00 00 00 00 01 00 00 00 1B 00 00 00	............H..............
0524	00 00 00 00 00 00 00 00 07 00 07 00 28 00 85 00 B8 [illegible] 1B 00	............[illegible] ...
0540	04 00 00 00 07 00 00 00 00 00 00 00 07 00 0C 00 00 [illegible] 23 23	...................[illegible]########
055C	23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 [illegible] 23 23	################[illegible]########
0578	23 23 0D 0A 56 49 53 41 20 43 41 52 44 0D 0A 54 48 [illegible] 4C 44	##..VISA CARD..THOMAS SCHELD
0594	0D 0A 34 32 33 32 20 35 38 35 32 20 33 36 36 30 20 [illegible]	..4232 5852 3660 XXXX 11/200
05B0	39 20 30 31 39 0D 0A 23 23 23 23 23 23 23 23 23 23 [illegible] 23 23	9 019..########[illegible]##
05CC	23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 23 00 00 00 00 00 00 00 00 00 00 00	################[illegible]----------
05E8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	----------
0604	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00	----------

FC-Frames contain readable information!

Ready | Filters | OS | SF | SH | Overlap | 4

Myth 3 - FC too complex

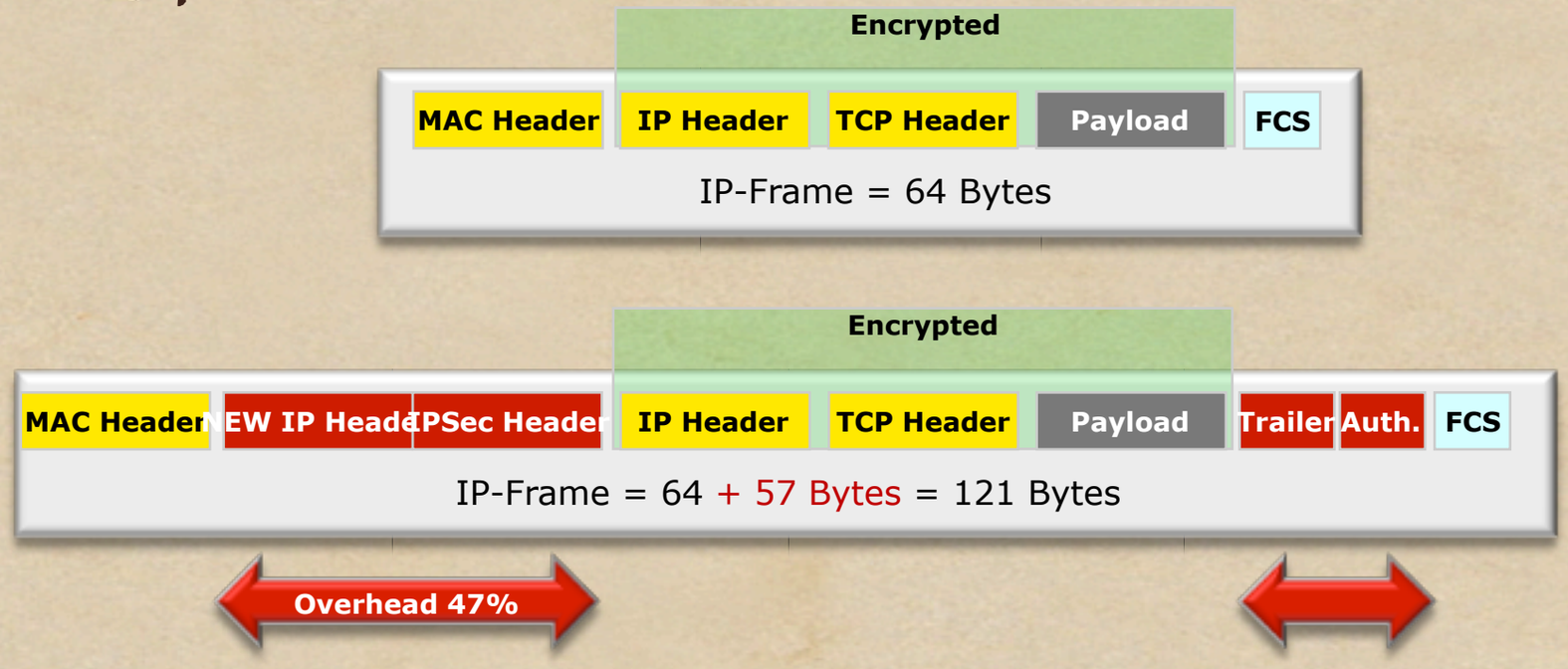


Reconstruction of a complete disk

- **FC-analyzer records all data traffic between Server and Disk Array,** including all SCSI-commands, Logical Block Addresses, and read – write Commands – *information now readable in this format*
- **Export from FC-analyzer** – to a CSV-file and convert into a binary file by means of a simple pearl script
- **Create a mirrored copy** Mount binary file using "ImDisk" in Windows-Explorer, recorded data appears as an additional disk in Windows-Explorer

Myth 4 - too slow/complex

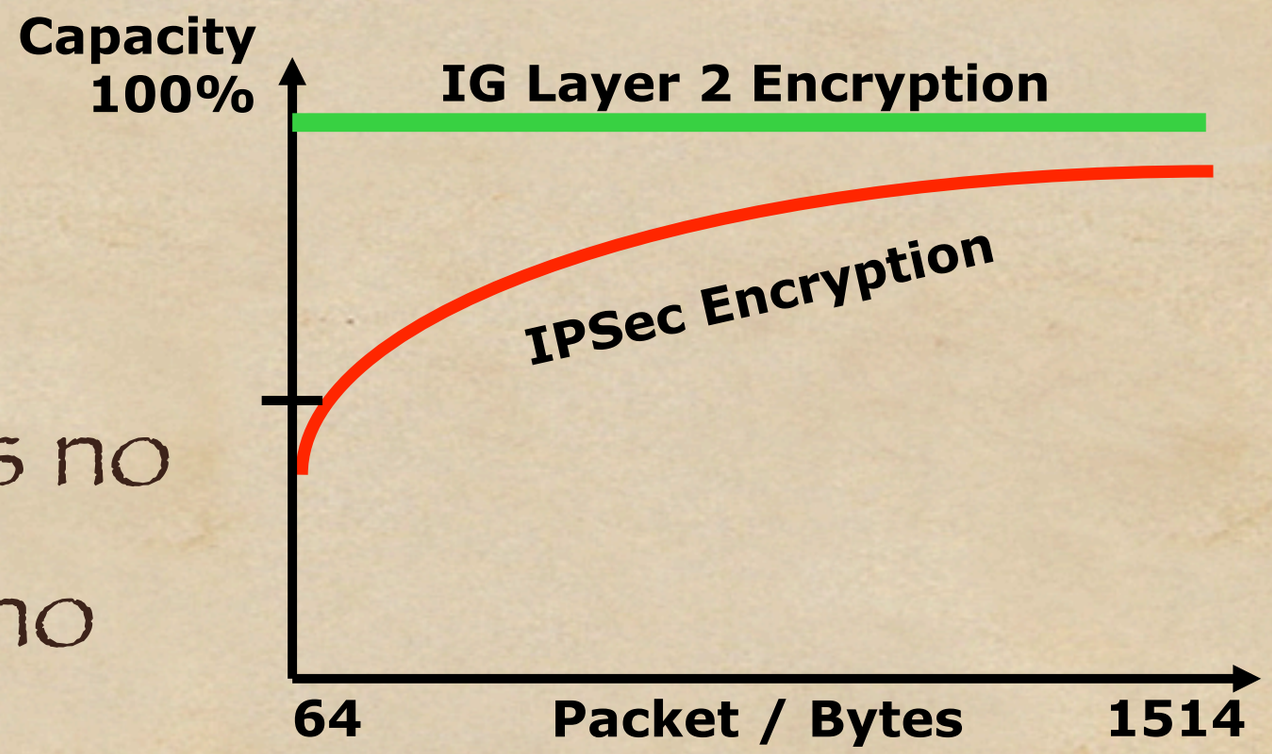
- Using layer-3 encryption or pseudo layer-2 encryption this is true



- However using true layer-2 encryption adds minimal latency and is invisible in the topology

Myth 4 - speed

- 65% of worldwide traffic is small packets
- True layer-2 encryption adds no padding hence no speed loss



So which technologies?

- To protect data at rest and digital identities the first priority is protection of encryption keys
  - Specialized hardware security modules exist to do exactly this
- To protect data in transit it has to be encrypted before it leaves the safe confines of the datacenter
  - Either using encrypted protocols and protecting the keys
  - Or using special encryption devices that encrypt traffic on the fly

HSM's

- Specialized equipment designed to be tamper safe and to perform encryption operations
- Private keys/encryption keys never leave the device unencrypted themselves
- In case of tampering two main levels of safety exist
  - Tamper detection and alerting
  - Tamper prevention in which case keys are destroyed from operating memory
- Technology wise low speed USB to network connected ultra high speed IRU devices exist based on needs

Network encryption

- Clear distinction has to be made on what the goals of encryption are
- Is the data only migrating to a backup site or is it used in a live configuration?
- Is speed an issue?
- The choice between software encryption and various forms of hardware encryption depend on the use cases and customer needs

Layer-2 encryption

- For true intra datacenter communications on main communication lines only a full wire speed layer 2 encryption solution fits
- The units should conform to tamper protection, not just detection

How can we help...

- Top Systems has been operating in encryption business since turn of the century...

- We represent two of the largest and best known encryption providers, both with a long history in the field...

Encryption = trust!

- Remember, encryption is all about trust
- Our partners have been doing this for decades and their origins are in encryption business
- InfoGuard is the private sector front end of Crypto AG that has been doing military encryption for over 80 years
- Thales ISS (ex nCipher Ltd) has been the market leader in HSM technology for over 15 years, their products are used widely in the world in various sectors

Some examples...

nShield Connect 6000

- New network HSM certified with FIPS 140-2 level2-3 and CC EAL 4+
- 3 different models

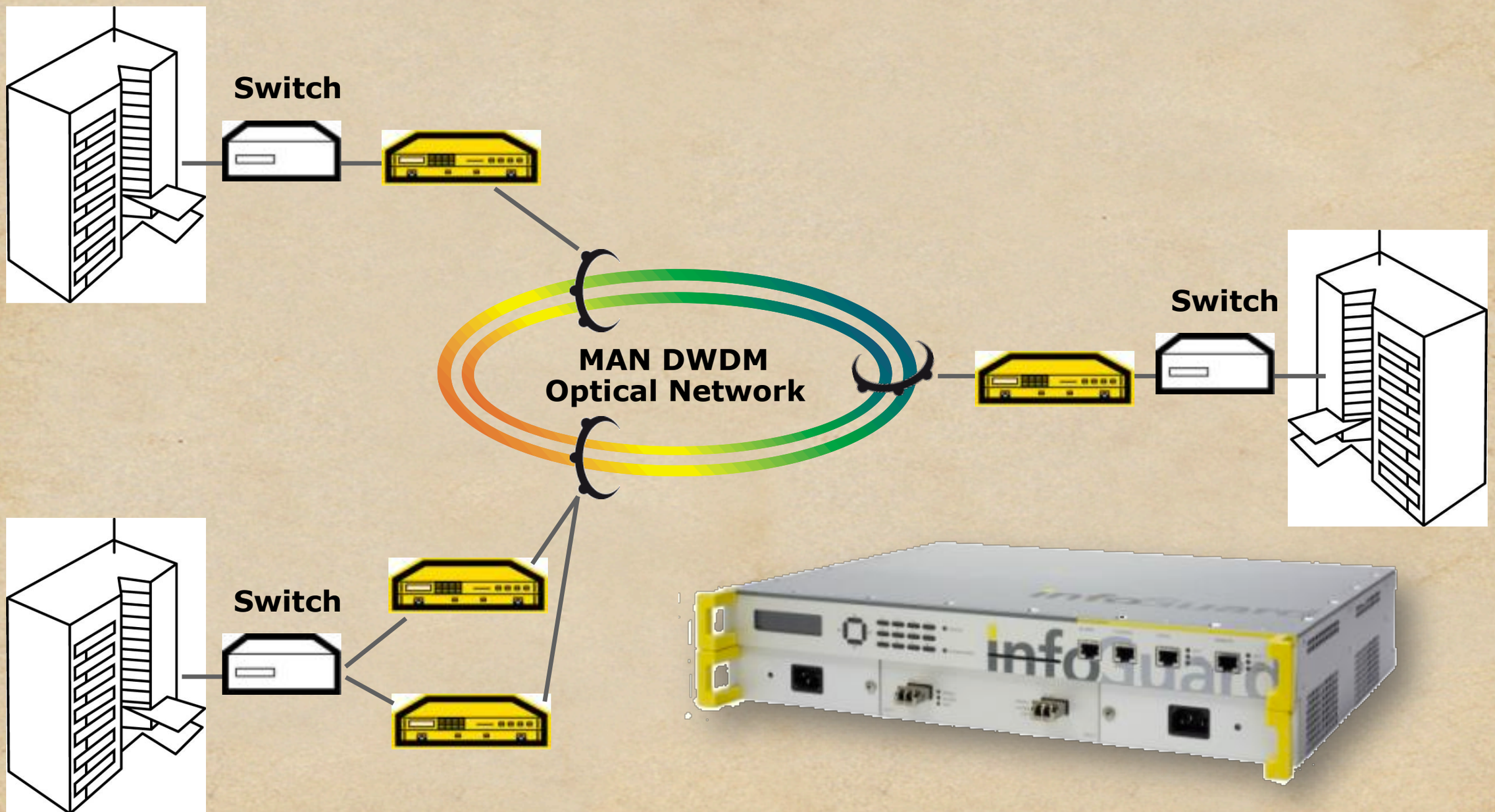
	nShield connect 500	nShield Connect 1500	nShield Connect 6000
RSA 1024bit	500	1500	6000
RSA 2048bit	150	500	3000
RSA 4096bit	65	150	500

- 'Dual' and 'hot-swap' power supply and fans
- Shared with upto 100 clients
- Automatic backup and key sharing.
- Load balancing and fail over by default.
- Various optional API libraries and embedded options.

nShield Solo's

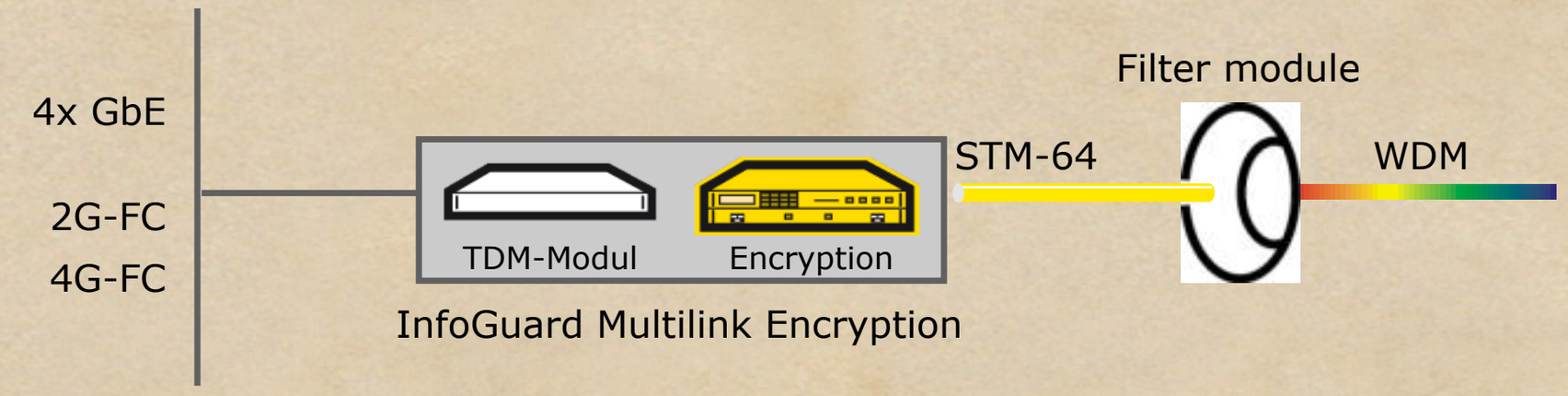
Model	Interface	FIPS 140-2	Common Criteria	CodeSafe-ready
nShield 500 F2/F3	PCI/PCI-X	Level2 Level3	EAL 4+	No/Yes
nShield 500 e F2/F3	PCI Express	Level2 Level3	EAL 4+	No/Yes
nShield 2000 F2/F3	PCI/PCI-X	Level2 Level3	EAL 4+	No/Yes
nShield 4000 F2/F3	PCI/PCI-X	Level2 Level3	EAL 4+	No/Yes
nShield 6000e F2	PCI Express	Level2 Level3	EAL 4+	No/Yes

1-10 Gb/s encryption

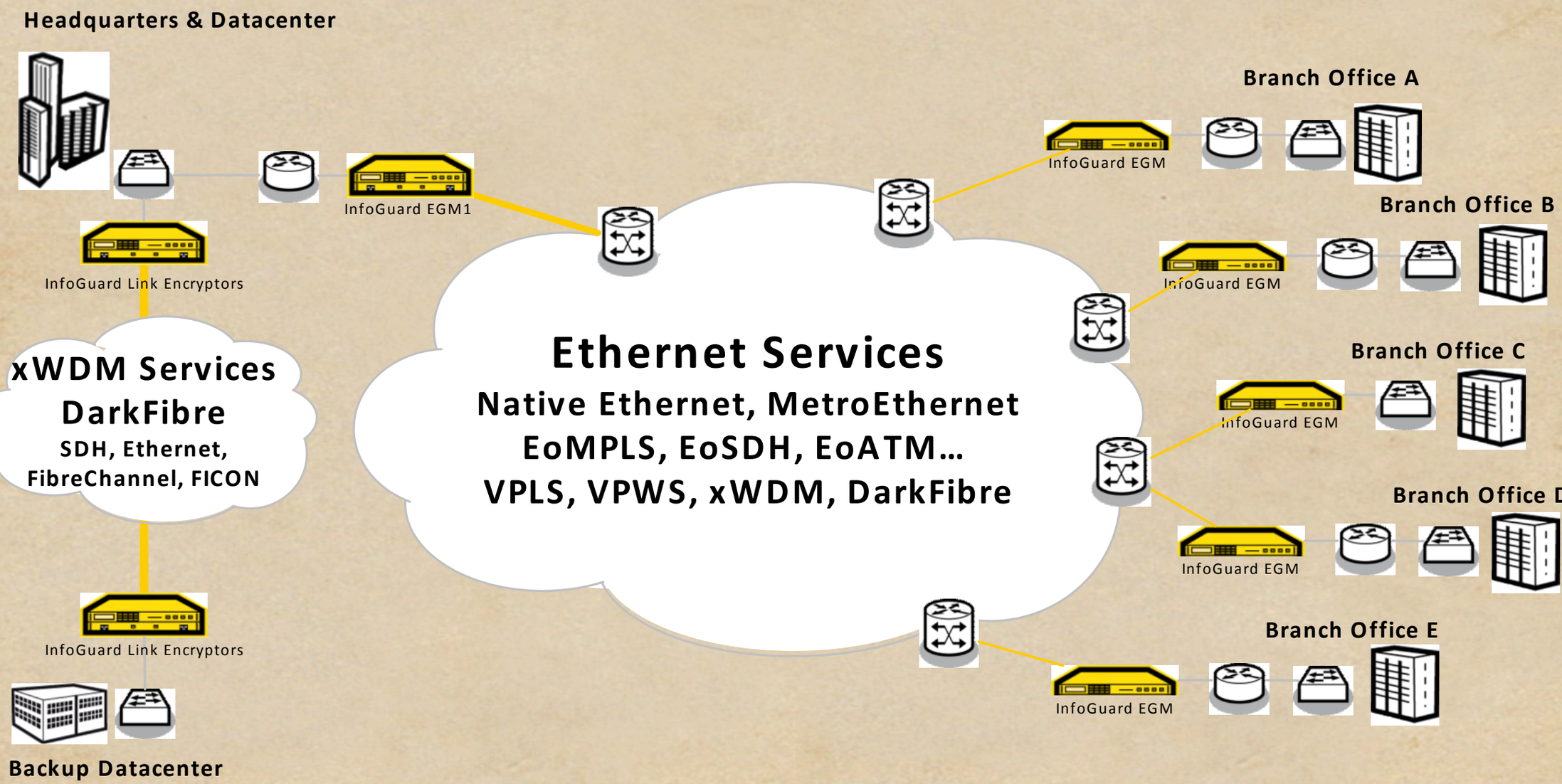


10Gb/s any protocol

- Combination of TDM and encryption device
- Allows any combination of GbE, and FC up to a total of 10Gb



Multiple location encryption



Conclusions

ENCRYPTION ≈ TRUST

There are a lot of newcomers to the field, but they are only starting, would you trust your keys to a child?