Are They Secure?

How to Assess MPLS Providers From a Customer Perspective

Enno Rey, erey@ernw.de
CISSP/ISSAP, CISA, BS 7799 Lead Auditor

Agenda

- **Problem Statement**
- **Approach**
- **Conclusions**

ERNW GmbH

- **Founded in 2001**
- **Based in Heidelberg, Germany (+ small office in Lisbon, Portugal)**
- **Network Consulting with a dedicated focus on IT-Security**
- **Current force level: 12 Experts**
- **Key fields of activity:**
  - Audit/Penetration-Testing
  - Risk-Evaluation & -Management, Security Management
  - Security Research
- **Our typical customers : banks, federal agencies, internet providers/carriers, large enterprises**

Introductory Remarks

- **This talk is based on a (still ongoing) project conducted by one of ERNW's customers, with consulting support from our side. It describes our joint experience and learning curve.**
- **To avoid legal discussions (and because our "sample" evidently was too small to make well-founded judgements about the carriers) and potential NDA violations (e.g. during Q+A session) we decided together not to disclose the name of the customer (hence $COMPANY in the following) or the carriers (mostly). Exception: very positive comments at some points.**
- **If not noted otherwise, throughout the talk the term "we" designates "ERNW + $COMPANY".**
- **Talk scheduled for 30 minutes: 25 min presentation, 5 min Q+A. Slides are numbered, if you've questions pls note no. and ask later.**

$COMPANY

- **Large media/publishing corporation**
- **Revenue 2006 ~ 10 bn US$**
- **Locations in 50+ countries**
- **World wide backbone, mostly Frame Relay based, some “MPLS islands“ already**
- **Planning to build “NGN“ based on MPLS**

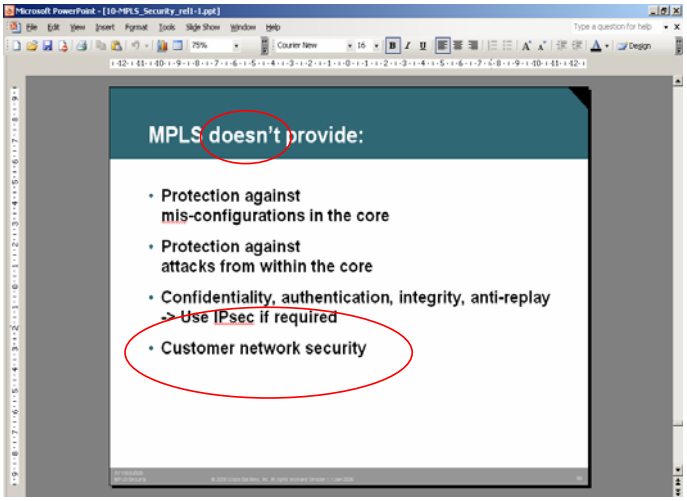
5

Problem Statement

- **New technology**
- **What risks?**
- **Which business reasonable controls?**

6

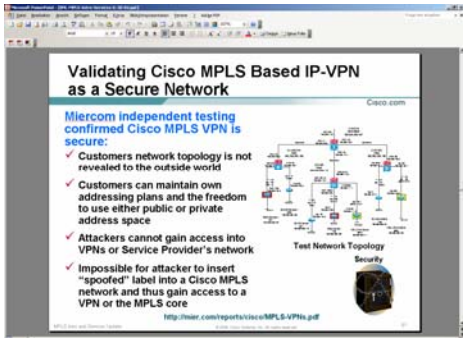
Problem Statement

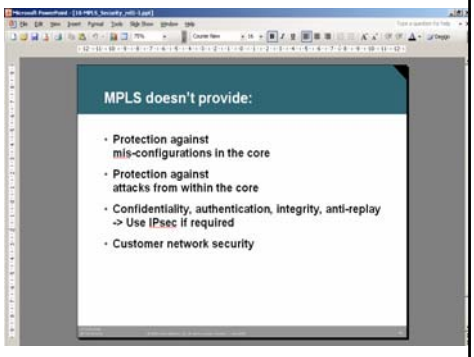


From tutorial *Best Practice Guidelines for Deploying MPLS* given by some *Cisco* people at APRICOT 2006, see [1]

7

Btw: spot the difference...





from [2]

8

From $COMPANY's
Network Security Architecture

ERNW Living Security.

$COMPANY security domains are defined as:

<u>Blue</u> - The "core" domain. Owned and managed by the $COMPANY business unit. Verified to be in compliance with baseline $COMPANY and business unit security requirements. […] This network will be verified to be in compliance with the $COMPANY Corporate Trust Security Model.

<u>Red</u> - Systems which are not owned and managed by the $COMPANY business unit, or with unknown or non-compliant controls for security. Generally, Red domains should be considered untrusted and hostile.

9

From $COMPANY's
Network Security Architecture

ERNW Living Security.

- **"If network traffic between domains must traverse other domain types, the control measures in place must match the requirements for the least trusted domain in the route. For example, connecting two sites of the same business unit via a third party network is seen as Blue-to-Red-to-Blue. This would require the controls for a Red-to-Blue connection."**
- **Simply speaking this mandates for encryption if traversing "untrusted" (red) networks.**

10

But…

ERNW Living Security.

- **Using encryption means...**
  costs, effort (= costs), (key) management/operations etc.
- **And this would immediately inspire a painful retrospective question (bringing politics into game):**
  “Why did we trust the frame relay network so far?“
- **Or, the other way round: “if we trusted that one, why should we mis-trust MPLS?“**
- **=> structured approach needed**
  => goal: find sth measurable to rate trustworthiness

The big question

ERNW Living Security.

- **Why trust the carriers?**

- **They don‘t trust us (e.g. some were absolutely unwilling to share information about their operational procedures).**
- **SLAs usually focused on availability, not “security“ [which is perfectly fine... as long as one is aware of it]**

Steps

ERNW Living Security.

- ***Request For Information*** **(RFI) submitted to carriers**
- **Lab**
- **Background Research (google etc.)**
- **Questionnaire(s)**
- **Site Visits**

RFI

ERNW Living Security.

Contents

RFI, Security Requirements (Excerpt)

ERNW Living Security.

4.6 Separate backbones – mandatory that the carrier's Internet service and private VPN services are carried on separate backbones. Note: if that is not implemented at physical level, Vendor is required to provide convincing information to $COMPANY that security is at the same level as if the backbones were physically separate.

4.7 Please provide complete details of the internal security program that is in place that will assure $COMPANY that its data is protected from unauthorized disclosure or other misuse

4.8 Please describe your cryptographic management practices, including; primitive generation, admin vetting, authentication, shared secrets, key rotation, key escrow and any other pertinent elements. Are all cryptographic modules utilized in this IP services network FIPS 140-2 Level 2 certified?

4.9 Are you subject to CALEA or any other legislation that obligates you to provide $COMPANY clear text digital assets to stated authorities?

4.10 Will you provide an SLA that attests to your intent to protect $COMPANY's digital assets from unauthorized access? Describe how this would be measured.

4.11 What financial liability will you accept for such a breach?

4.12 What access controls are in place to insure only authorized employees can access the physical facilities and locations that contain management control plane terminals, systems or network elements that process $COMPANY's data?

15

RFI Results

ERNW Living Security.

- **Submitted to 21 vendors**
- **Seven declined to participate (=> 14 left)**
- **During RFI process some mergers => reducing number to twelve**
- **Of these twelve, six "global", six "regional"**
- **Four passed security review**
- **Four provide network services over shared infrastructure supporting both Public and Private networks => out**
- **One did not support Multi-VRF (VRF-Lite) => out**

16

Lab

ERNW Living Security.

- **Five vendors invited to two weeks of lab testing at $COMPANYs premises**
- **Goals: test promises of RFI & get an impression of**
  - their professionalism
  - their technical capabilities
  - the maturity of their operational procedures
  - their willingness to share their knowledge and to work together with each other
- **Additional goal: define working CE template**
- **Given the lab‘s location the outgoing network traffic was subject to $COMPANY‘s IDS systems (they knew in advance).**

17

Lab, some observations

ERNW Living Security.

- **One technician‘s laptop constantly tried to poll data from internal system with SNMP community “public“ => generated IDS alarms. Not very cool.**
- **One vendor obviously not used/not willing to cooperate with others (maybe due to some kind-of-monopoly of this vendor in particular regions of the world).**
- **We got pretty good insight who has mature operational procedures and who not.**

18

Background research (google etc.)

ERNW Living Security.

- **Found some pictures of $SOME_CARRIERS‘s NOC (where cameras explicitly prohibited) on contractor‘s web site.**
- **At $SOME_OTHER_CARRIER found a certificate retrieval web-gui with source code containing lots of customer names.**
- **Side note: some looking glass servers still reveal lots of interesting information.**

19

Site visits, again some observations

ERNW Living Security.

- **Visit of data center in Beijing:**
  - probably “the worst possible place“
  - security of site/equipment untrusted (China...)
  - cages not locked, cables hanging freely/ accessible
- **At $SOME_CARRIER *instant messaging* to internet on mgmt stations**
- **Conducted interviews and asked for testation proof where appropriate**
  => turned out to be difficult.
  They couldn‘t/wouldn‘t share (despite NDA).

20

Assessment Questionnaires

ERNW Living Security.

Dimension *IP Remote Access*
Rationale: Remote Access must be secured appropriately, see ISO 18028-4 and ISO 17799:2005, sect 11.7
Scope:

			Yes	No	Score	Adjusted
Q5.1	Is there remote access to the organisation's network?		x		5	5
Q5.2	Is the access controlled/managed via centralised facilities?	80%	x		-0.25	-0.125
Q5.3	Is an appropriate Access Control Solution implemented?	80%	x		-0.5	-0.25
Q5.4	Is traffic limited to a necessary minimum, according to risk analysis and req	80%	x		-1	-0.5
Q5.5	Is logging/auditing activated? Are records properly archived?	80%		x	0	0
Q5.6	Are logging/audit alarms and alerts reviewed periodically?	80%		x	0	0
Q5.7	Are IDS/IPS devices in place and regularly updated?	80%	x		-1	-0.5
Q5.8	Are their logs reviewed on a regular basis?	80%	x		-0.5	-0.25
		Cost:			3.50	6.75

Comments: Juniper elements. No automatic log mining in place.

Question we tried to answer in parallel: CE managed or unmanaged?

ERNW Living Security.

- **Unmanaged CE would mandate additional controls.**
- **We used very formal risk analysis approach here.**
- **However no decision so far from business.**

Definition of CE template

- **In general good collaboration with carriers in that area.**
- **Turned out to be “technically possible“...**
  but regarded as custom ($$$) solution from carrier side...

Last Stage: Risk Assessment

- **Provided information to business to see if they‘re comfortable with results.**
- **Ongoing process, no final decision so far.**

What we learned

- **The carriers are not used to that approach.**
- **Most of them expect to face increasingly such stuff though.**

- **Question that came up: How do others do this?**
- **Answer:**
  - Banks: encrypt anyway.
  - Government: very specific requirements
  => custom solutions

- **Obviously we were the first commercial customers using such a methodology.**

What would we do differently?

- **Treat the carriers as “red“ from the beginning?!**

Questions?

ERNW Living Security.

27

Thanks for your attention!

ERNW Living Security.

28

References

- **[1] http://www.apricot.net/apricot2006/slides/tutorial/monday/MPLS_Tutorial.zip**
- **[2] Presentation *MPLS Basics and In-Depth*: http://www.rhic.bnl.gov/RCF/UserInfo/Meetings/Technology/Archive/06-30-04-CISCO/BNL-MPLS-Intro-Services-6-30-04.ppt**