MPLS Security

Enno Rey, erey@ernw.de
CISSP/ISSAP, CISA

1

Agenda

- MPLS Grundbegriffe & Technologie
- MPLS VPNs
- Angriffs-Klassifizierung und -Tools
- „Layer 2 VPNs“/VPLS
- Checkliste & Zusammenfassung

2

Wer ich bin

- "Old-school networker"
- Arbeit auf Layer 2–4 seit den frühen 90ern
- Mit dediziertem Fokus auf Sicherheit seit 1997
- Gründer (2001) and technischer GF der ERNW GmbH, eines hoch-spezialisierten Sicherheits-Dienstleisters mit 12 Mitarbeitern (Sitz in Heidelberg + kleines Büro in Lissabon)
- (Ko-) Autor eines Buch über Penetrations-Tests und regelmässiger Sprecher auf internationalen Sicherheitskonferenzen

3

MPLS Einführung

- *Multiprotocol Label Switching* [RFC 3031 et.al.]
- *Forwarding*-Technologie, basierend auf *Labels*. Pakete können mehrere Labels für unterschiedliche Zwecke tragen.
- Ursprüngliches Ziel: effizienteres *Forwarding* als „klassisches IP-Routing".
- Wird in den meisten Carrier Backbones eingesetzt.
- Bildet die Grundlage verschiedener „*Advanced Services*"

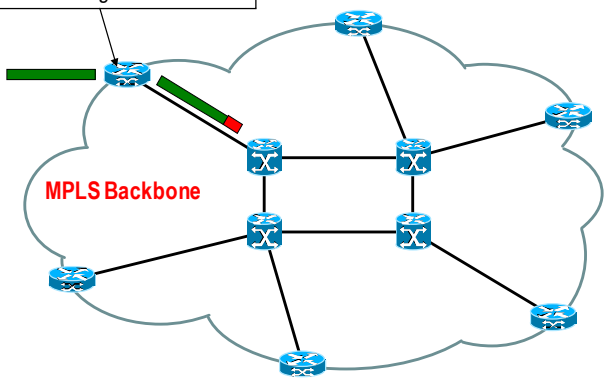
Tag ('Label') = 20 bits
S = Bottom of Stack, 1 bit
COS/EXP = Class of Service, 3 bits
TTL = Time to Live, 8 bits

4

MPLS Grundlagen

ERNW Wir leben IT-Security.

IP Pakete werden klassifiziert und *gelabelt*

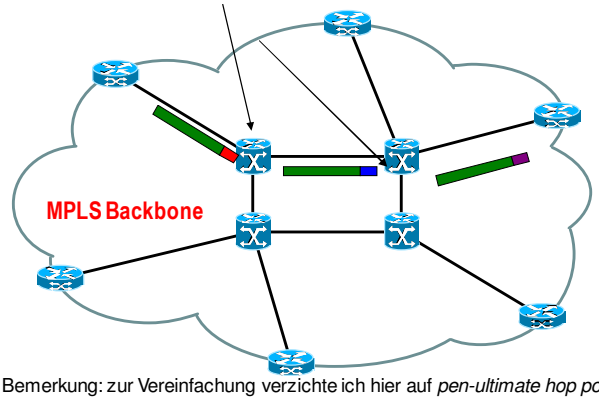


5

MPLS Grundlagen

ERNW Wir leben IT-Security.

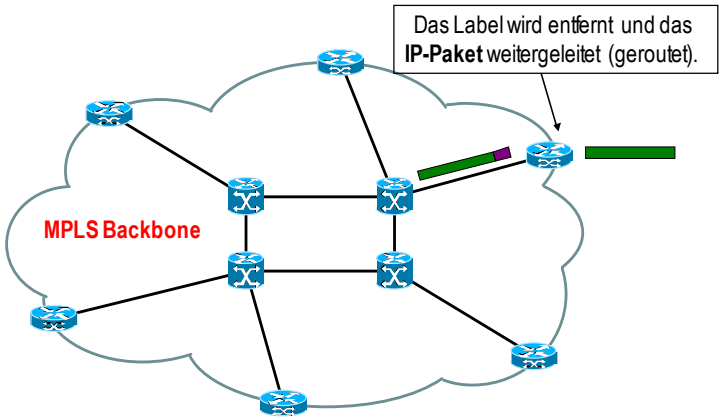
Im Backbone werden Pakete anhand ihrer *Label* weitergeleitet. Das **rote** Label wird gegen ein **blaues** getauscht, das **blaue** gegen ein **lila** Label.



Bemerkung: zur Vereinfachung verzichte ich hier auf *pen-ultimate hop popping*.

6

MPLS Grundlagen



Hier nenne ich die Label „Forwarding Label“ (weil sie genau dazu dienen).

7

Sicherheits-Diskussion

- Das erste, woran Joe Hacker bei einer Diskussion über die Sicherheit einer Forwarding („Routing“) Technologie denkt, sind ... „Spoofing“ oder „Injection“-Angriffe.

  Nebenbei: dieser Ansatz ist naiv… oder haben Sie je erfolgreiche „EIGRP Injektions-Angriffe” gesehen?
- Aber: die gerade vorgestellten *Forwarding Labels* haben nur „lokale Bedeutung“.
  Zwei benachbarte Router („Peers“) verständigen sich über ihre Bedeutung mithilfe eines *label distribution protocol*.
- Injektion oder Modifikation solcher Labels würde daher wenig (Angriffs-) Nutzen bringen.
- Diese netten kleinen Labels können jedoch noch für ganz andere Zwecken eingesetzt werden …

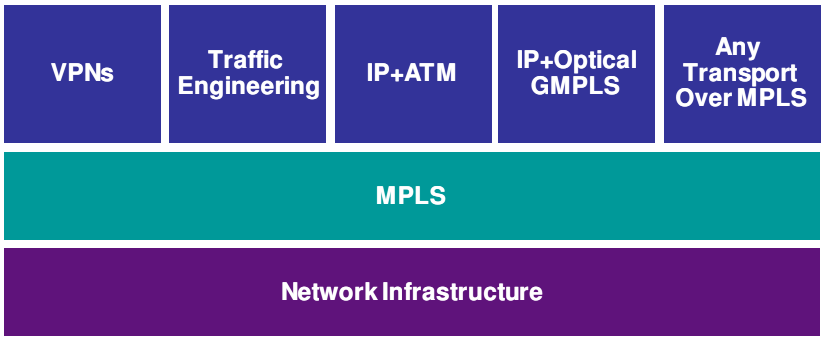
8

MPLS Services

- VPNs („Layer 3“ oder „Layer 2“)
- *Any Transport over MPLS*
- *Virtual Private LAN Service*
- MPLS Traffic Engineering
- *Generalized MPLS* (GMPLS)
- weitere

9

MPLS als Grundlage für „Advanced Services”



10

MPLS Services

- Einige dieser Technologien (etwa Traffic Engineering) sind nur für Backbone-Betreiber/Carrier relevant.
- Andere („Layer 3 VPNs“, „Layer 2 VPNs“) spielen für viele Organisationen (als Kunden) eine grosse Rolle.
- MPLS VPNs werden zunehmend in Enterprise-Netzwerken eingesetzt, zur Traffic-Virtualisierung (vglbar VLANs).

11

MPLS VPNs („Layer 3 VPNs“)

- Eigenständige (jedoch MPLS-basierte) Technologie, RFC 4364
- Vergleichbar Frame Relay/ATM
- Aber hochgradig ‚virtualisiert‘ (VRF-Ansatz, gemeinsamer Backbone).
- Zusätzliche Labels werden verwendet, um logische Pfade für den Traffic einzelner Kunden festzulegen.
- Realisierung unterschiedlicher VPN-Topologien möglich (u.a. mithilfe der *route targets*).

12

MPLS VPNs („Layer 3 VPNs“)

P-Netzwerk (Provider-Netzwerk)

- Backbone-Netzwerk des Service-Providers (SP)

P-Router (Provider-Router)

- Backbone-Router im Provider-Netzwerk

PE-Router (Provider-Edge-Router)

- Router des SPs, der die Verbindung zum CE-Router herstellt

C-Netzwerk (Customer-Netzwerk)

- Netzwerk unter Administrationshoheit des Kunden

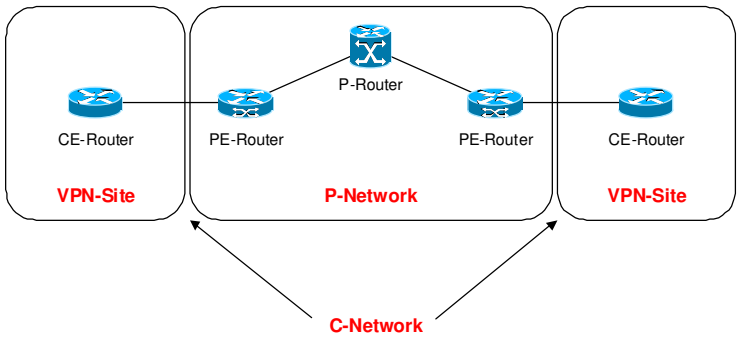
CE-Router (Customer-Edge-Router)

- Kunden-Router, der die Verbindung zum PE-Router herstellt

13

MPLS VPNs („Layer 3 VPNs“)

- Vereinfachte Darstellung eines MPLS/VPN-Netzwerks

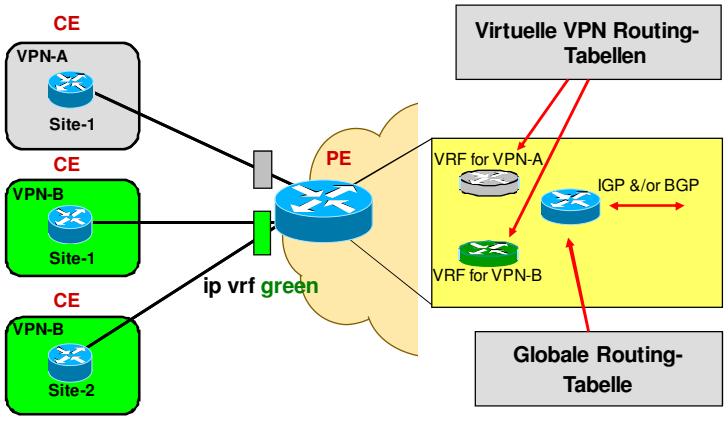


14

MPLS VPNs („Layer 3 VPNs“)

ERNW Wir leben IT-Security.

- Teilung eines Routers durch mehrere VRFs

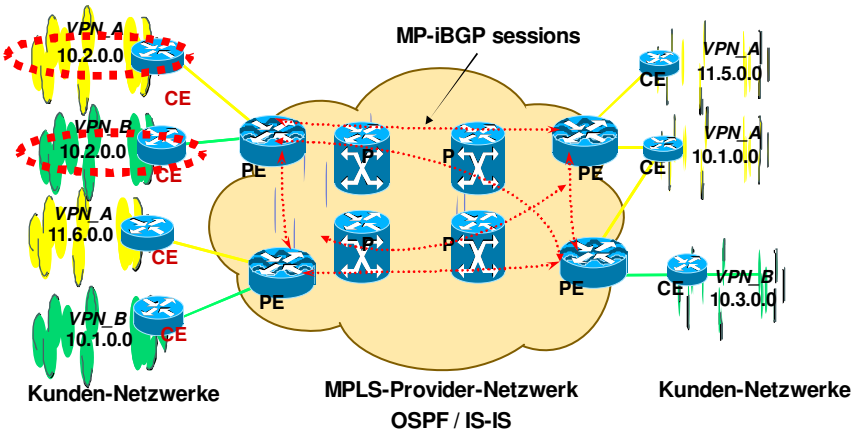


15

MPLS VPNs („Layer 3 VPNs“)

ERNW Wir leben IT-Security.

- ein komplexeres Beispiel für ein MPLS/VPN-Netzwerk



16

Was hier im Detail geschieht

ERNW Wir leben IT-Security.

- **Die PE Routers weisen den Adress-Prefixes der VPNs Label zu (*route distinguisher*).**
- **Die Information (*label, route distinguisher, prefix*) wird dann zwischen den PEs per *Multiprotocol BGP* [RFC 2283] ausgetauscht.**
- **=> damit weiss ein PE, welcher andere PE für ein bestimmtes Prefix in einem bestimmten VPN zuständig ist.**

- **Wenn ein Paket den Ingress-PE in Richtung Backbone verlässt, hat es (mindestens) zwei Label:**
  - ein „Forwarding label" für den Transport zum Egress-PE, durch den Backbone.
  - ein zweites, das das VPN (und Prefix) des Ziels identifiziert.
- **Kurz gesagt: „Die Label regeln hier die VPNs".**

17

Man sollte sich darüber klar sein...

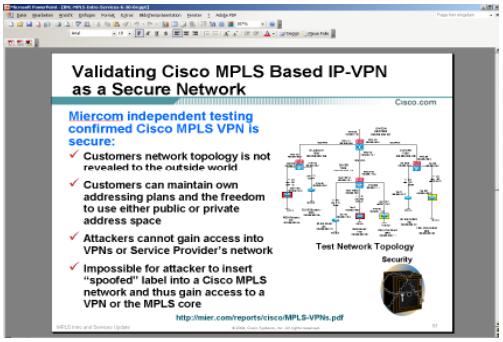
ERNW Wir leben IT-Security.

- Keine Verschlüsselung
- PE-Device wird potentiell mit anderen Kunden geteilt
- Revisions-Anforderungen?
- Generell Risiko-Analyse erforderlich

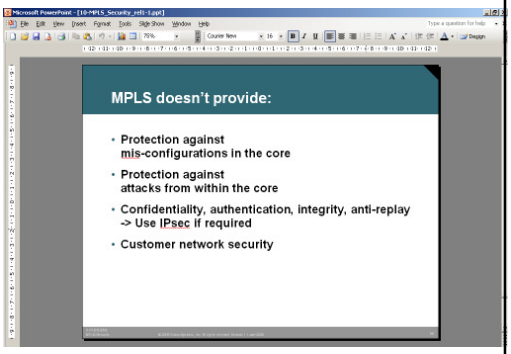
- Sie können eine exemplarische RA (aus Carrier-Sicht) von mir erhalten.

18

Die „offizielle Sicht“ im Wandel der Zeiten



aus [1]



aus [6]

19

MPLS VPNs – Angriffs-Klassizierung

- **Angriffe von ausserhalb der Wolke (von Seiten des/der CEs)**
  - üblicherweise nicht durchführbar
  - das (für einen Angreifer) interessanteste Szenario ergibt sich, wenn der PE-CE Link Layer2-basiert und *shared* (mit anderen Kunden) ist

- **Angriffe von innerhalb der Wolke**

20

Angriffe von innerhalb der Wolke

ERNW Wir leben IT-Security.

Diese können weiter unterteilt werden in

- **Angriffe, die die Kompromittierung eines Carrier-Devices voraussetzen (im folgenden "DC")**
- **Angriffe, die das Einbringen (*Injection*) eines vom Angreifer kontrollierten Device voraussetzen (*Device Injection*: "DI")**
- **Angriffe, die irgendwo im *packet path* einen „Zugriff auf's Kabel" [und damit die Möglichkeit zum Lesen und Modifizieren von Paketen], voraussetzen (Wire Access: "WA")**

21

Zur Klarstellung

ERNW Wir leben IT-Security.

Richtig, alle diese Angriffe benötigen „core access".

Ich überlasse es hier (noch) dem Zuhörer, ob er dies für machbar/wahrscheinlich hält... oder auch nicht.

Bedenken Sie stets... Risiko-Analyse beinhaltet (mindestens) zwei Fragen:

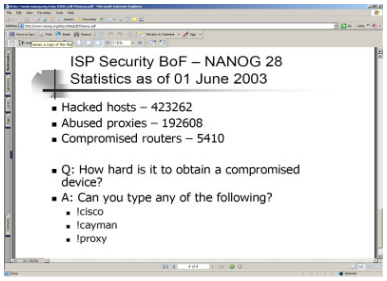
Wie wahrscheinlich ist der Eintritt eines Ereignisses?
Welche *Auswirkung* hat der Eintritt eines Ereignisses?

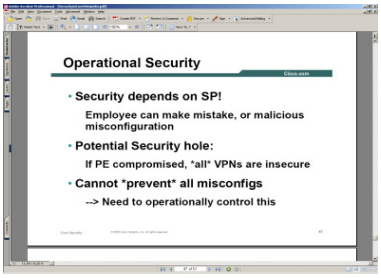
22

Mögliche Szenarien, DC

- Auch Carrier Devices *werden* kompromittiert (dies jedoch selten zugegeben ;-)
- Menschliche Konfigurationsfehler *können* vorkommen
- Devices müssen gemanagt werden (über eine – attackierbare – Mgmt-Infrastr.)
- Note: knowledge of SNMP RW community (and one-way reachability of device) can be considered "DC"

aus [3]





aus [2]

23

Unlängst...

- ... nahm ich im Rahmen eines Projekts an einem *MPLS implementation lab* teil, mit fünf weltweiten MPLS Carriern, die jeweils einen Vertriebsmitarbeiter und einen Techniker entsendet hatten.
- Wir haben den NW-Verkehr gemonitort (wurde im Vorfeld kommuniziert).
- Ein europäischer Top3 Carrier Mitarbeiter versuchte regelmässig, SNMP-Abfragen gegen ein Backbone-Device mit offizieller IP-Adresse durchzuführen...

```
_________________
09/11/06 09:27:41 udp 10.16.12.19.1025 -> 148.115.13.101.161
   (snmp)[version 1]
public
```

24

Mögliche Szenarien, DI

- Angreifer benötigt physischen Zugang zu Carrier-Lokationen.
  Üblicherweise nicht sehr wahrscheinlich, aber...
- Es gibt vereinzelt PEs, die sich in Kunden-Lokationen befinden.
- Es *gibt* Kunden, die eigene PEs haben.
  Diesen wird vom Carrier in einem bestimmten Maß vertraut.
  Vertrauen Sie diesen?
- Es gibt Länder, in denen man der Integrität von Lokationen oder Devices nicht vertrauen sollte, aus unterschiedlichen Gründen.

25

Mögliche Szenarien, WA

- Dies ist üblicherweise das einfachste Szenario für einen Angreifer (im Vergleich zu den anderen)
- Layer 2 Sicherheit wird meist in Carrier-Umgebungen vernachlässgit (nach unserer Erfahrung).
- Angreifer kompromittiert ggf. ein System (oder kontrolliert es sogar völlig legal), installiert L2 Angriffs-Toolkit und erhält so Zugang zu „weiteren Netzteilen“.
- L2 Übergangs-Punkte (IXPs) können Ausgangspunkt für Angriffe sein.
- Allgemein sind Übergangs-Punkte, insbesondere auch die zwischen Carriern (aufgrund der zugrundeliegenden „trust models“) von besonderem Interesse. Denken Sie an RFC 4364 sect. 9 and 10...

26

Unterschiede zwischen FR/ATM und dem MPLS VPNs Zeitalter

ERNW Wir leben IT-Security.

- MPLS ist IP-basiert, die zugrundliegende Infrastruktur zunehmend Ethernet => typische IP/Ethernet Angriffe (e.g. ARP basierte) können auftreten.
- MPLS ist eine stark "virtuelle Technologie"... mit allen Vor-/Nachteilen solcher
- WA Szenarien existieren (praktisch) nicht im FR/ATM Umfeld.
- FR/ATM benötigt dedizierte Hardware, mit dediziertem Mgmt etc.
- (Früher) keine automatisierten Angriffstools erhältlich , kein „libnet for ATM"
- Üblicherweise keine "technology transition points" zwischen Carrier, hinsichtlich FR/ATM

27

MPLS Angriffs-Tools

ERNW Wir leben IT-Security.

- Thorsten Fischer von *irmplc* hat erste Tools implementiert.
- Erhältlich unter [4], noch sehr „experimentell".
- Wir arbeiten zusammen an einer Weiterentwicklung.

- Das „grosse Layer2 Angriffstool" (*yersinia*) soll um MPLS-Funktionalität erweitert werden (auch hier sind wir mit den Autoren in Kontakt/gemeinsamer Arbeit).

- Auf der Shmoocon07 wurde in einem Vortrag explizit nach Mitarbeitern für ein „MPLS Fuzzing" Tool gesucht.

28

Beispiel: *label bruteforcing tool*

ERNW Wir leben IT-Security.

```
mpls-lbf(1)


NAME
       mpls-lbf - a MPLS LSP label brute-forcer

SYNOPSIS
       mpls-lbf  -m hw_addr -d hw_addr -s IP -t IP -p port -o port -l maxlabel
       [-l maxlabel]

DESCRIPTION
       mpls-lbf is a small tool which sends a series of TCP SYN packets  to  a
       specified  port  on  a specified (fixed) host, and labels these packets
       with MPLS labels. The labels are encoded in the TCP sequence number  in
       such a way that the expected SYN ACK or RST reply can be used to recon-
       struct the labels along the LSP traversed by the TCP SYN packets.

       If the this label enumeration is carried out from the core, it might be
       used  as  an information gathering tool, which can then be used in con-
       junction with mpld-fwd to forward  MPLS-labelled  traffic  outside  the
       core.

       It  makes  sense to set up a sniffing device that receives this traffic
```

29

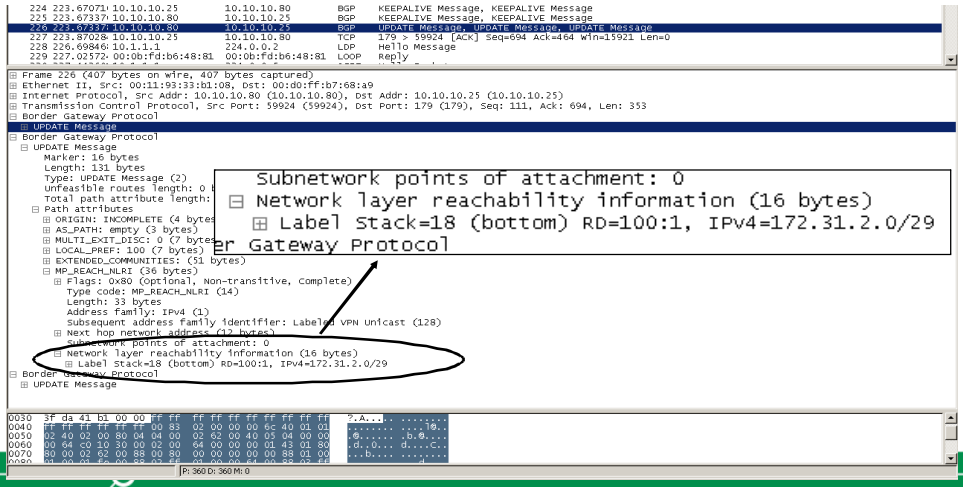
Aussichtsreichste Angriffspfade (WA vorausgesetzt)

ERNW Wir leben IT-Security.

- **Modifikation des MP-BGP Austauschs**
- **Modifikation von VPN Labeln**

30

MP-BGP Sitzung



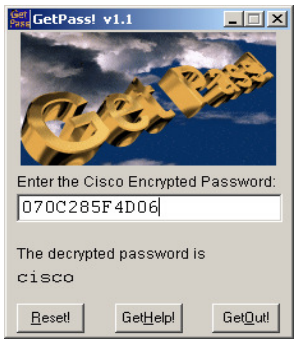
31

Angriffe gegen MP-BGP

- **MP-BGP Modifikation ermöglicht *Traffic Redirection* auf „Prefix-Eben“ oder sogar Hinzufügung von „bogus prefixes/networks“.**
  => „*x1* Verkehr“ kann aus „*x2* network“ gelesen/geändert werden
- **Gegenmassnahmen:**
  MD5-gesichertes BGP zwischen PEs beugt Modifikation vor.
  Die Fähigkeit „unsolicited TCP ACKs“ in x1 zu entdecken, kann hilfreich sein (=> Monitoring/IDS).
- **In den meisten Carrier-Netzen wird (zumindest teilweise...) MD5 gesichertes BGP eingesetzt ... aber nicht in allen (e.g. ATT ist höchstwahrscheinlich eine Ausnahme)...**

32

Während eines Audits...
MD5 ‚gesichertes' BGP



- **Implementierung gemäss Setup-Guide eines *grossen* Netzwerk-Consulting Unternehmens**

⇒ **Andere Kunden werden dieselbe Konfig haben...**

- **Übrigens: *OSPF authentication key* (im Guide und in Praxis) war der String... ‚*highsecure*'**

33

MD5 ‚secured' BGP,
Aus einem internen Dok eines Carriers

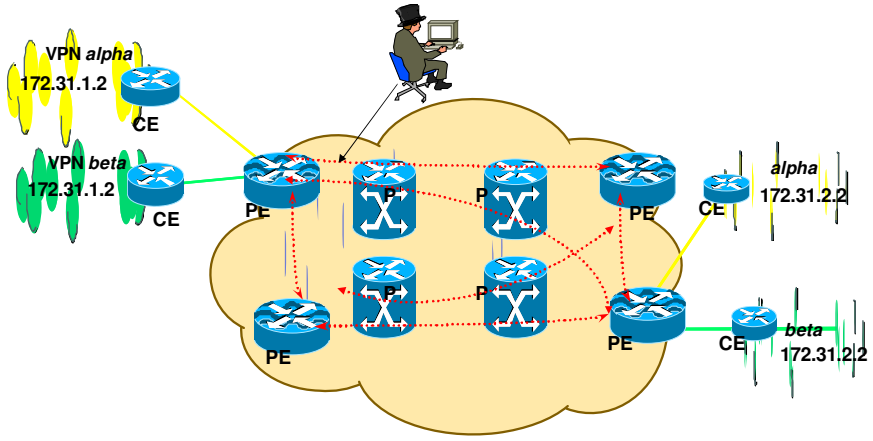
The other challenge with MD5 is that, though good in theory, it is difficult to implement effectively. The security of authentication is only as good as the key management. It requires extensive administrative systems to securely store passwords, track changes and allow quick changes if compromised, but the most difficult part is probably synchronizing the customer's administrative system with the carrier's. Both ends need the password changed at the same time or "chained" and without resetting BGP to prevent extended downtime. These capabilities are not generally available.

Some carriers may never change the password and others have used the default "cisco" key.

34

Modifikation von *VPN Labels*

ERNW Wir leben IT-Security.



35

Modifikation von *VPN Labels*

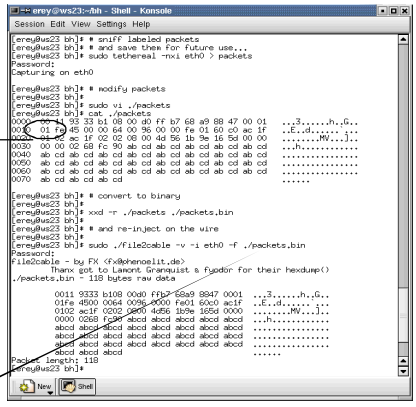
ERNW Wir leben IT-Security.

(1) Die Labels eines der PEs

```
pe_7204vxr>sh ip vp vpnv4 vrf alpha labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (alpha)
   20.20.20.21/32   10.10.10.25     nolabel/17
   20.20.20.40/32   172.31.2.2      19/nolabel
   172.31.1.0/29    10.10.10.25     nolabel/18
   172.31.2.0/29    0.0.0.0         17/aggregate(alpha)
   192.168.5.0      10.10.10.25     nolabel/19

pe_7204vxr>sh ip bgp vpnv4 vrf beta labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 100:2 (beta)
   172.31.1.0/29    10.10.10.25     nolabel/20
   172.31.2.0/29    0.0.0.0         16/aggregate(beta)
```

(2) Pakete von VPN *alpha* werden gesnifft + ‚re-labeled' mit VPN *beta*



(3) Hier *tcpdump* eines Systems in VPN *beta,* das zunächst ‚normal' gepingt wird und dann ein re-labeled Ping aus VPN *alpha* erhält

```
01:55:45.993783 IP 172.31.1.2 > 172.31.2.2: icmp 40: echo request seq 17408
01:55:45.993815 IP 172.31.2.2 > 172.31.1.2: icmp 40: echo reply seq 17408
01:55:46.995175 IP 172.31.1.2 > 172.31.2.2: icmp 40: echo request seq 17664
01:55:46.995211 IP 172.31.2.2 > 172.31.1.2: icmp 40: echo reply seq 17664
01:55:47.996723 IP 172.31.1.2 > 172.31.2.2: icmp 40: echo request seq 17920
01:55:47.996756 IP 172.31.2.2 > 172.31.1.2: icmp 40: echo reply seq 17920

01:59:14.136855 IP 172.31.1.2 > 172.31.2.2: icmp 80: echo request seq 5725
01:59:14.136906 IP 172.31.2.2 > 172.31.1.2: icmp 80: echo reply seq 5725
```

36

Bewertung

- Label Modifikation & nachfolgendes „VPN hopping“ sind möglich.
- Es können sogar bi-direktionale Verbindungen aufgebaut werden (wenn Angreifer den Verkehr in beide Richtungen modifiziert).
- NB: dieser Eingriff kann in VPN *alpha* nicht bemerkt werden, da keine Checksumme o.ä.
- MP-BGP Modifikation kann zu Verkehrs-Umleitung auf Standort-Ebene oder zum Auftreten von „bogus prefixes/sites“führen.
- Gegen diesen Angriff gibt es Gegenmassnahmen:
  MD5 BGP zwischen PEs beugt MP-BGP Modifikation vor.
  Fähigkeit, „unsolicited TCP ACKs“ in VPN *alpha* zu entdecken, kann hilfreich sein.

37

MPLS „Layer 2 VPNs“

- Terminus bezeichnet meist *Any Transport over MPLS* [AToM]
- AToM: „Technology for transport of different layer 2 protocols (e.g. ATM, Frame Relay, Ethernet, PPP, HDLC) over MPLS backbone“.
- Kann aus unterschiedlichen Gründen sehr interessant für Carrier und/oder Kunden sein.
- Arbeit mit *Pseudo Wires* = logischen Pfaden, die zwischen MPLS fähigen Devices im Backbone etabliert werden.

38

MPLS „Layer 2 VPNs“

- Zugrundeliegende Mechanismen ähnlich wie bei *Layer 3 VPNs*:
  Pakete haben (mindestens) zwei Label, eines zu Forwarding-Zwecken,
  ein weiteres zur Identizierung des Kunden/logischen Pfades.
- Modifikation von Labels ermöglicht „VPN hopping“ wie oben beschrieben.
- Zwei Varianten verdienen besonderes Interesse:
  Ethernet over MPLS [EoMPLS]
  Virtual Private LAN Service [VPLS]

39

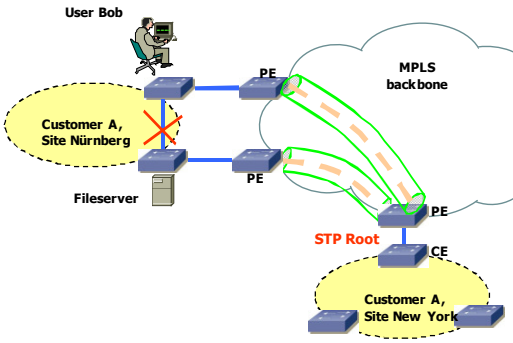
EoMPLS / VPLS

- **„Transparenter“ Transport von Ethernet über MPLS Wolke**
- **Relativ neue Technologie**
- **Sicherheits-Auswirkungen scheinen vielen unklar zu sein**

  … sogar teilweise den Herstellern…

40

Beispiel möglicher Probleme



„Normales“ Netzwerk-Verhalten?

Womöglich… aber…

Weiss CorpITSec, dass Bobs Zugriff auf den Server einen Carrier-Backbone durchläuft?

In einem anderen Land…

wo *Carnivore/DCS 1000* zuschlägt (oder es ein ‚anderes Verständnis von intellectual property‘ gibt)…

Unverschlüsselt!

41

Angriffe im Zeitalter von VPLS

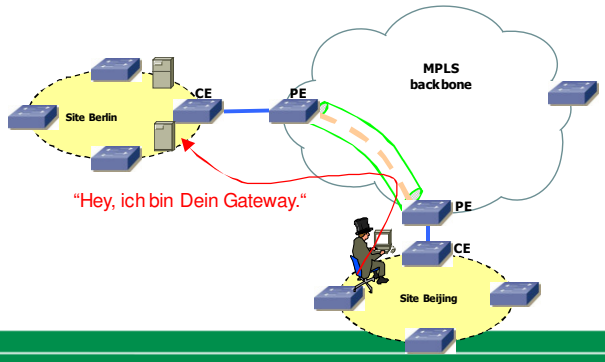
Können unterteilt werden:

- **Angriffe “über die Wolke“**
- **Angriffe gegen VPLS-performing Devices**

42

Attacken „über die Wolke“

- Hängen hochgradig vom Transparenz-Grad der „VPLS Wolke“ ab.
- Bei voller Transparenz (wie in einem *Juniper*-basierten Lab das uns zur Verfügung stand)…
- … kann man jeden beliebigen Layer2-Angriff über die Wolke ausführen.
- Erfolgreiche Tests mit *yersinia*.
- Sehr cool (?): vom Standort Beijing aus kann man Systeme in Berlin arp-spoofen/sniffen…



43

Attacken gegen VPLS-performing Devices

- Hängen hochgradig von deren Funktionen ab.
- Üblicherweise nehmen diese nicht am STP oder anderen Infrastruk-Protokollen teil.
- Die meisten Layer2-Angriffe sind daher nicht möglich.
- Aber diese Devices lernen (und speichern) MAC-Adressen.
- Sie hielten *MAC table flooding* für einen veralteten Angriff?

44

Erfahrungen aus dem Lab

- **Eine Runde *Juniper M7i Router* (nb: „schweres Eisen“).**
- **Die nur im Lab konnektiert waren und nichts zu tun hatten.**

```
lab@JESSICA# run show chassis cfeb
CFEB status:
  State                          Online
  Intake Temperature          27 degrees C / 80 degrees F
  Exhaust Temperature         34 degrees C / 93 degrees F
  CPU utilization              2 percent
  Interrupt utilization        0 percent
  Heap utilization             8 percent
  Buffer utilization          26 percent
  Total CPU DRAM             128 MB
  Internet Processor II          Version 1, Foundry IBM, Part number
164
  Start time:                    2006-01-20 08:34:29 CET
  Uptime:                      4 hours, 10 minutes, 21 seconds
```


Erfahrungen aus dem Lab

```
lab@JESSICA# run show chassis cfeb
CFEB status:
  State                          Online
  Intake Temperature          27 degrees C / 80 degrees F
  Exhaust Temperature         35 degrees C / 95 degrees F
  CPU utilization             11 percent
  Interrupt utilization        0 percent
  Heap utilization             9 percent
  Buffer utilization          26 percent
  Total CPU DRAM             128 MB
  Internet Processor II          Version 1, Foundry IBM, Part number
164
  Start time:                    2006-01-20 08:34:29 CET
  Uptime:                      4 hours, 12 minutes
```

(1) Mac flooding with *macof* [default mac address maximum of 512 applied].

(2) Mac flooding with *macof* [mac address maximum set to 65000].

Note:
- ‚schweres Eisen‘
- aktuell *nichts* weiter zu tun
- Angriff von einem ‚Kunden‘
- Box soll tausende von Kunden konnektieren…

```
lab@JESSICA# run show chassis cfeb
CFEB status:
  State                          Online
  Intake Temperature          28 degrees C / 82 degrees F
  Exhaust Temperature         35 degrees C / 95 degrees F
  CPU utilization             25 percent
  Interrupt utilization        1 percent
  Heap utilization            40 percent
  Buffer utilization          27 percent
  Total CPU DRAM             128 MB
  Internet Processor II          Version 1, Foundry IBM, Part number
164
  Start time:                    2006-01-20 07:34:29 UTC
  Uptime:                      5 hours, 1 minute, 13 seconds
```

Checkliste

- ***Request for Information*** **vor Carrier-Auswahl**
- **Lab / eigene Recherche (google...)**

- **Vertragliche Gestaltung**
- **Technische Rahmenbedingungen (*public/private services* über gleiche Infrastruktur? MD5 BGP zwischen PEs? etc.)**
- **Fragebögen zur Bewertung von *Trust***

- **Beispiele/Templates vom Referenten erhältlich (erey@ernw.de)**

47

Zusammenfassung

- **MPLS ist nicht nur eine Forwarding-Technologie, sondern bildet auch die Grundlage für eine Reihe weiterer Dienste.**
- **Zu diesen zählen verschiedene „VPN Technologien“.**
- **Unter bestimmten Bedingungen können diese angegriffen werden oder Sicherheitsprobleme auftreten**
  => Risiko-Analyse notwendig.
- **Zunehmend werden MPLS-basierte „Ethernet-Dienste“ angeboten, vor allem *Virtual Private LAN Service*.**
- **Die dadurch entstehende Verschmelzung von Layer2 und Layer3 wird zu ganz neuen Sicherheitsprobleme führen.**

48

Fragen?

ERNW Wir leben IT-Security.

49

Danke für Ihre Aufmerksamkeit!

ERNW Wir leben IT-Security.

50

Quellen

[1] Präsentation *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

[2] http://www.nanog.org/mtg-0306/pdf/thomas.pdf

[3] Cisco Präsentation *Security in Core Networks*:
http://www.cisco.com/global/HU/rendezvenyek/presentations/SecurityinCoreNetworks.pdf

[4] MPLS attack tools: www.irmplc.com/Tools/irm-mpls-tools-1.0.tar.bz2

[5] Michael H. Behringer/Monique J. Morrow: MPLS VPN Security (Indianapolis 2005)

[6] http://www.apricot.net/apricot2006/slides/tutorial/monday/MPLS_Tutorial.zip

- Allgemeiner Literaturhinweis zu Angriffstechniken (auch gegen Devices):
  Dominick Baier/Enno Rey/Michael Thumann: Mehr IT-Sicherheit durch Pen-Tests [Vieweg-Verlag, ISBN 3528058390].

51