ERNW
Enno Rey Netzwerke GmbH

ERNW Newsletter 7 / Juli 2005

Liebe Partner, liebe Kollegen,

willkommen zur siebten Ausgabe des ERNW-Newsletters über Layer 2 Sicherheit:

Neue Angriffe auf Layer 2 in Cisco-Netzen

Von: Enno Rey & Peter Fiers.

Der Artikel beschreibt neben einigen bekannten Layer2 Sicherheits-Problemen neue Angriffs-Methoden in Cisco-basierten Netzen.

Sicherheitsprobleme auf der Ebene der Netzwerk-Infrastruktur können erhebliche Auswirkungen haben. So kann etwa die Verfügbarkeit des gesamten Netzwerks gefährdet werden oder ein Angreifer in die Lage versetzt werden, den Verkehr kompletter Segmente mitzulesen oder zu manipulieren. Meist ist es auch nicht möglich, Sicherheitsprobleme auf den Layern 2 und 3 durch Massnahmen auf anderen, höhergelegenen Netzwerk-Schichten zu adressieren (was umgekehrt oft funktioniert, etwa wenn IPsec zur Sicherung von höhergelegenen Dienst-Protokollen eingesetzt wird).

Dennoch wird Angriffen und Sicherheits-Massnahmen insbesondere auf Layer 2 in vielen Netzen nur wenig Bedeutung beigemessen, was möglicherweise darauf zurückzuführen ist, dass die meisten Angriffe die Kontrolle über einen physisch angeschlossenen Knoten voraussetzen (also – vermeintlich – nur durch Innentäter möglich sind, deren Existenz durch Sicherheits-Verantwortliche ja gerne ausgeklammert wird).

Ein weiterer Grund für die Vernachlässigung der Sicherheit auf Layer 2 könnte sein, dass entsprechende Techniken und Tools bislang nur wenig verbreitet waren.

Inzwischen ist Layer 2 Angriffs-Knowhow jedoch einfach verfügbar: seit Anfang des Jahres liegt ein detailliertes Buch zum Thema vor [1] und Ende März wurde ein Tool veröffentlicht [2], das viele – bisher als theoretisch geltende – Angriffe automatisiert.

Ein Szenario, in dem ein Angreifer nach der erfolgreichen Kompromittierung eines Webservers in einer DMZ dieses System nutzt, um grossflächig *interne* Kommunikation mitzulesen, ist mittlerweile problemlos realisierbar, vorausgesetzt, die DMZ ist über ein eigenes VLAN (also nicht einen dedizierten Switch) implementiert, was oft der Fall ist.

Zu den auf Infrastruktur-Ebene attackierbaren und teilweise schon lange diskutierten Protokollen zählen etwa neben dem *Address Resolution Protocol* (ARP, bekannt geworden durch *ARP Spoofing*) in erster Linie DHCP, ICMP, CDP, das *Spanning Tree Protocol* (STP) und Ciscos *Hot Standby Router Protocol* (HSRP).

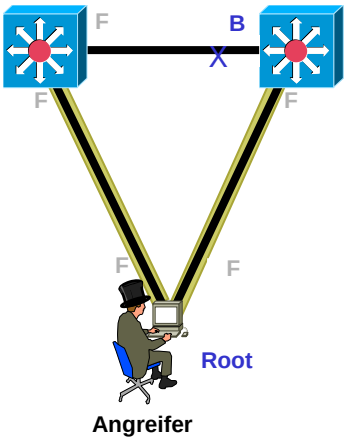
Spanning Tree

Spanning Tree dient der Entdeckung & Vermeidung von Schleifen, wenn redundante Pfade zwischen Switches existieren. Es basiert auf dem IEEE 802.1d Standard. Beteiligte Switches versenden dazu pro *Hello Interval* sogenannte *Bridge Protocol Data Units* (BPDUs) auf allen Ports an die Multicast-Adresse 01-80-c2-00-00-00.

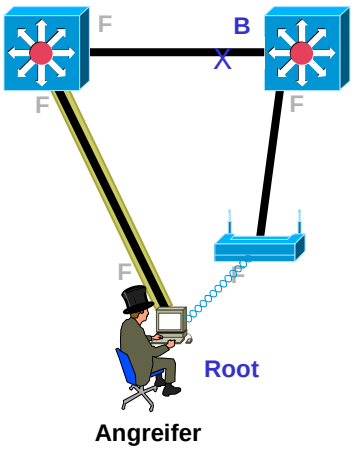
Anhand der ausgetauschten BPDUs bilden die beteiligten Switche (meist pro VLAN) einen logischen Baum, den *Spanning Tree*. Dieser Baum hat eine Wurzel, die *Root Bridge,* gekennzeichnet durch die niedrigste sogenannte *Bridge ID*, die aus einer konfigurierbaren *Priority* und der MAC-Adresse des jeweiligen Geräts besteht. Die Switches deaktivieren temporär redundante Verbindungen innerhalb des Baums. Bei Ausfall eines Gerätes oder einer Verbindung wird die Netzwerktopologie neu berechnet und ggf. eine neue *Root Bridge* gewählt.

Ein Angreifer, der ein Device mit niedriger(er) *Bridge ID* konnektieren kann – sei es durch Anschluss eines Devices mit niedriger *Priority*, sei es durch Verwendung eines Tools, das STP-Pakete generiert –, kann unter Umständen den Verkehr eines ganzen VLANs insgesamt oder teilweise zu sich umleiten. Wenn er seine Priorität in kurzen zeitlichen Abständen wechselweise afu einen höheren und einen niedrigeren Wert setzt, kommt dies (aufgrund der stetigen Neu-Berechnungen des Baums mit Konnektivitäts-Verlust) meist einem *Denial-of-Service* Angriff gleich.

Verfügt der Angreifer über zwei physische Konnektierungs-Punkte auf unterschiedlichen Switches (im gleichen VLAN), kann er den Verkehr nach einer solchen Umleitung weiterleiten und somit eine *Man-in-the-middle* Position (MITM) einnehmen. Er könnte dann den gesamten umgeleiteten Verkehr mitlesen.



Üblicherweise verfügt ein Angreifer aber nicht über physische Konnektivität zu zwei Switches (etwa innerhalb eines Raums), so dass dieser Angriff oft nicht möglich ist. Dies ändert sich jedoch, sobald Wireless LANs im Einsatz sind, da dann regelmässig Kabel-gebundener Anschluss (Dose im Büro) und Funk-Anschluss (per AP an einen [Backbone-] Switch) auf unterschiedlichen Switches terminieren:

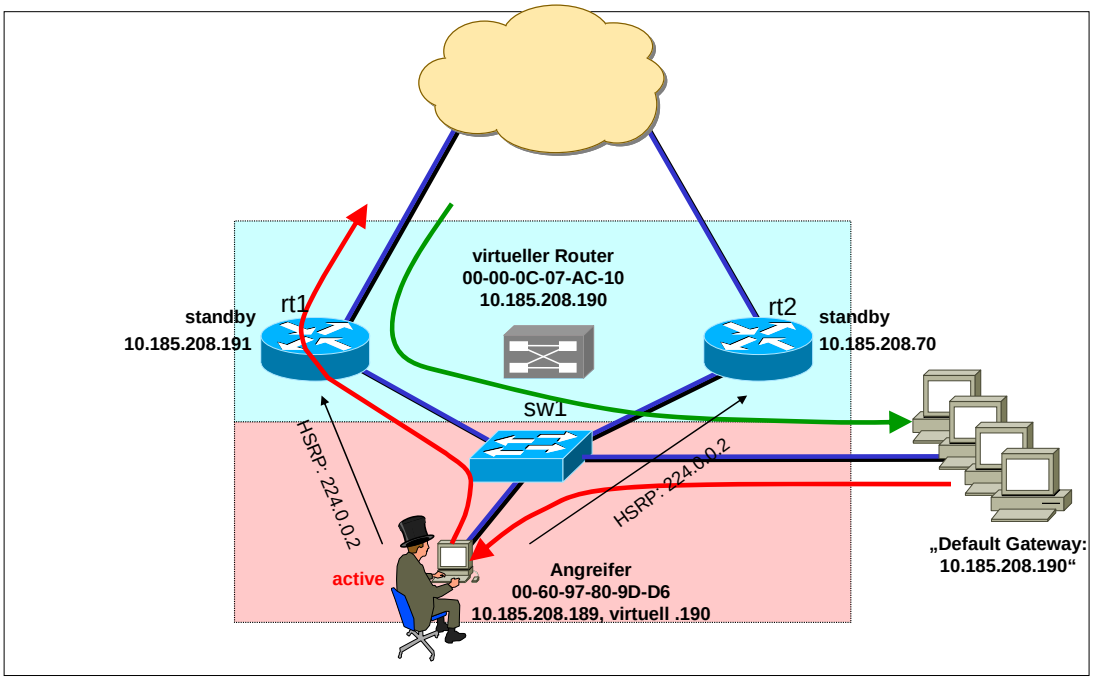


Verfügt der Angreifer über eine Trunk-Verbindung (siehe dazu unten), können ggf. sogar alle VLANs beeinflusst werden. Die konkrete Auswirkung aller STP-Angriffe hängt jedoch stets vom jeweils aktuellen Spanning Tree und dem Standort eines Angreifers ab. Die Auswirkungen des ersten Angriffs werden beim Einsatz von *Rapid Spanning Tree* potentiell deutlich verringert. Darüber hinaus können an vielen Switches Ports so konfiguriert werden, dass sie entweder überhaupt keine BPDUs entgegennehmen (*BPDU Guard* Feature bei Cisco) oder sich hinter dem jeweiligen Port keine STP Root befinden darf (*Root Guard* bei Cisco). Das *Port Security* Feature kann wiederum gegen den MITM-Angriff verwendet werden, weil dann der umgeleitete Verkehr nicht mehr von den Switches entgegengenommen würde.

HSRP

Das *Hot Standby Router Protocol* [HSRP, RFC 2281] ist ein initial von Cisco entwickeltes Protokoll, das den redundanten Betrieb mehrerer Router ermöglicht, die dabei zusammen unter einer virtuellen IP-Adresse (und MAC-Adresse) erreichbar sind. Dazu tauschen die Router periodisch *Hello*-Nachrichten aus, die an die *All Routers on this Subnet* Multicast-Adresse (224.0.0.2) geschickt werden. Die höchste dabei übermittelte *Priority* bestimmt, welcher Router der sog. *Active* Router wird, also den Verkehr tatsächlich entgegennimmt/weiterleitet.

Die anderen Router gehen dann in den inaktiven *Standby* Modus.Ein Angreifer, der HSRP-Pakete mit einer höheren Priorität als der der vorhandenen HSRP-Teilnehmer injizieren kann, kann so alle HSRP-Systeme seines Subnetzes in den *Standby* Status zwingen. Damit kann entweder ein *Denial-of-Service* Angriff durchgeführt werden (wenn der Verkehr danach nicht weitergeleitet wird) oder der aus dem Segment fliessende Verkehr über das Angreifer-System umgeleitet werden.



Im Gegensatz zu *Spanning Tree* sind hier Gegen-Massnahmen oft deutlich schwieriger zu realisieren. Cisco empfiehlt entweder den Einsatz von IPsec, um den HSRP-Verkehr zu verschlüsseln (was auf Layer3-Switches, die HSRP implementieren, keine Option ist) oder die Verwendung von HSRP-Authentifizierung, wobei hier meist das Kennwort im Klartext übertragen wird und so einem motivierten Angreifer bekannt sein sollte. Die sicherere MD5 Authentifizierung von HSRP ist erst auf neueren Releases möglich (bei Routern ab IOS 12.3(2)T) und auch der Einsatz von IGMP-Filtern ist eher selten anzutreffen.

Während die genannten Angriffe gegen STP und HSRP durchaus bekannt sind und schon seit geraumer Zeit entsprechende Tools vorliegen (etwa irpas [7]), sind inzwischen zwei weitere Protokolle in den Blickpunkt gerückt, für die erstmals im Rahmen des neuen Tools *yersinia* automatisierte Angriffe (mit gravierenden Folgen) implementiert sind.
Es handelt sich dabei um zwei Cisco-proprietäre Protokolle: das *Dynamic Trunking Protocol* (DTP) und das *VLAN Trunking Protocol* (VTP).

DTP

Mit dem *Dynamic Trunking Protocol* können Trunk-Verbindungen zwischen Switches ausgehandelt werden. Im Gegensatz zu Access Ports, über die einzelne Stationen an Switches konnektiert sind, verbinden Trunk Ports mehrere Devices untereinander (Switches mit anderen Switches oder Routern). Ein Trunk Port ist per default Mitglied aller VLANs eines Switches, d.h. es wird potentiell der Verkehr aller VLANs darüber transportiert (dies kann jedoch durch die sog. *allowed vlans* eingeschränkt werden).

Die VLAN-Zugehörigkeit einzelner Frames wird dabei durch ihr jeweiliges *VLAN Tag* mit-übertragen. Welche Ports eines Switches Trunk-Ports sind oder werden, kann (und sollte) der jeweilige Sysadmin manuell konfigurieren. Dies kann jedoch auch zwischen Switches dynamisch ausgehandelt werden, eben mithilfe von DTP, das auf den meisten Plattformen inzwischen implementiert ist (Ausnahme etwa 2900XL/3500XL).

Switches sollen so in die Lage versetzt werden, selbständig zu erkennen, wo sie mit anderen Switches verbunden sind, um die jeweiligen Ports dann in den Trunk Status zu versetzen.

DTP ist dazu üblicherweise auf allen Ports zunächst *aktiviert* („The key thing to remember about DTP is the default mode on most switches is *Auto." [3]*) und die nachfolgende, vielfach anzutreffende exemplarische Konfiguration ändert auch diesen (Verhandlungs-bereiten) Status eines Ports *nicht*:

```
interface FastEthernet0/2
switchport access vlan 27
spanning-tree portfast
```

Es können daher normalerweise sogar auf (vermeintlichen) Access Ports Trunk-Verbindungen verhandelt werden. Gelingt es einem Angreifer, einen Trunk auszuhandeln, ist meist sofort folgendes möglich:

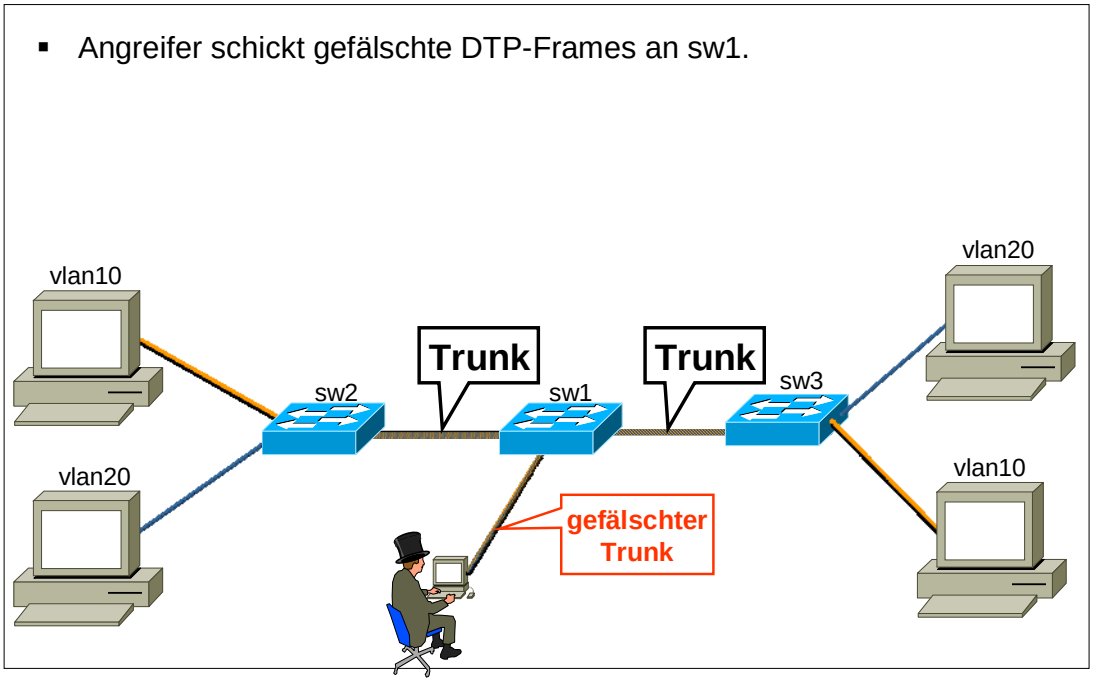
- Das Mitlesen des Broadcast- und Multicast-Traffics *aller VLANs* (sonstige Default-Konfiguration ohne Einschränkung der *allowed VLANs* und ohne *VTP Pruning* vorausgesetzt, was sehr häufig der Fall ist).

- Teilnahme am *VLAN Trunking Protocol* (siehe dazu unten) und dadurch oft die Möglichkeit, die VLAN-Konfiguration zu verändern (etwa VLANs zu erzeugen oder *zu löschen*).

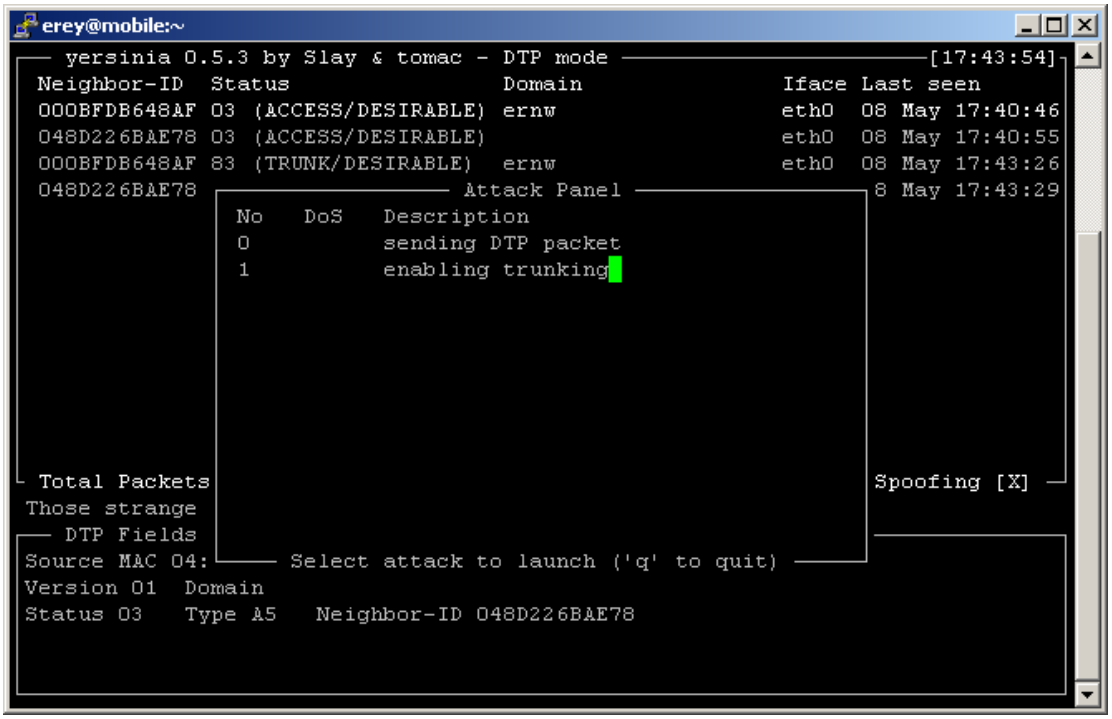
- ARP-Spoofing gegen Systeme *in anderen VLANs* (und somit Mitlesen von deren Verkehr!).

Schematisch sieht ein solcher Angriff in etwa so aus:

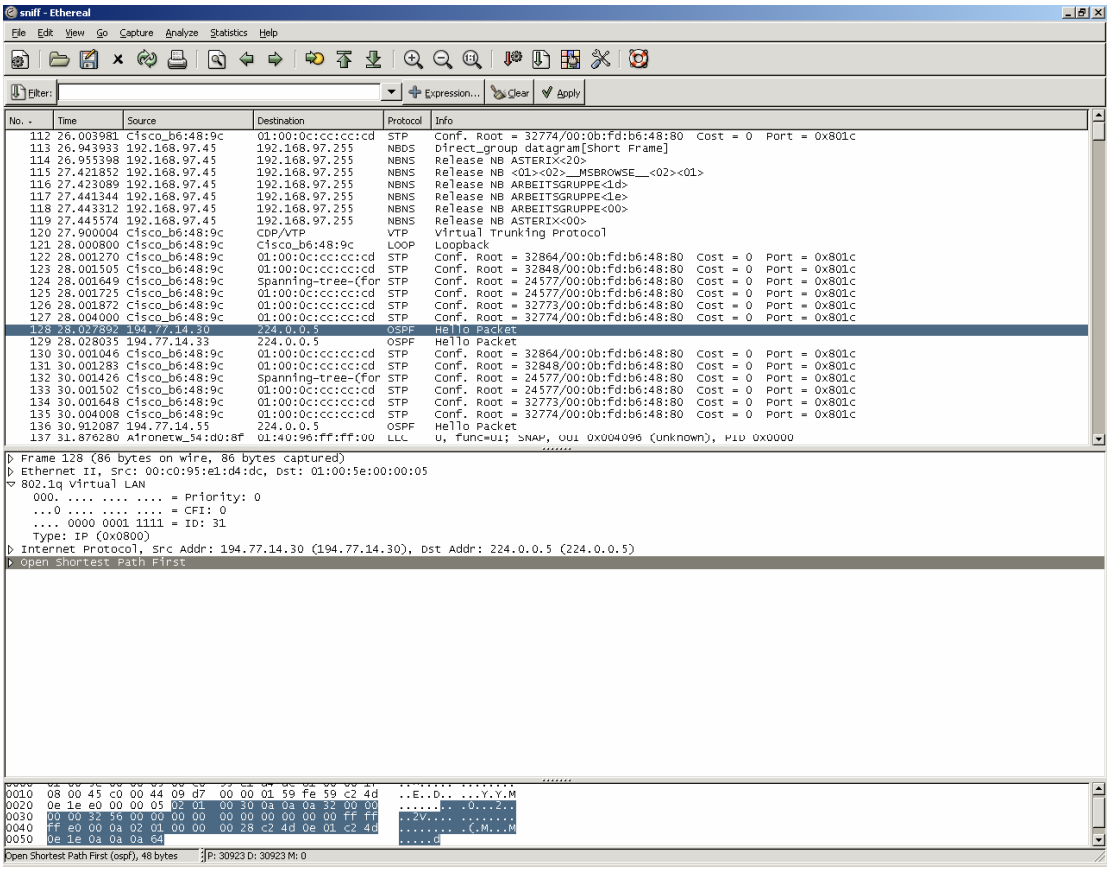
Aufbau einer gefälschten Trunk-Verbindung



Dieses Problem an sich ist nicht neu. Da Cisco jedoch die Spezifikation von DTP nie publiziert hat, galt dieser Angriff lange als theoretisch und nur mithilfe aufwendig manuell erstellter Pakete als machbar (auch [1] beschreibt noch diese Methode). Mithilfe des neuen Tools *yersinia* kann der Angriff aber problemlos Menü-gesteuert durchgeführt werden:

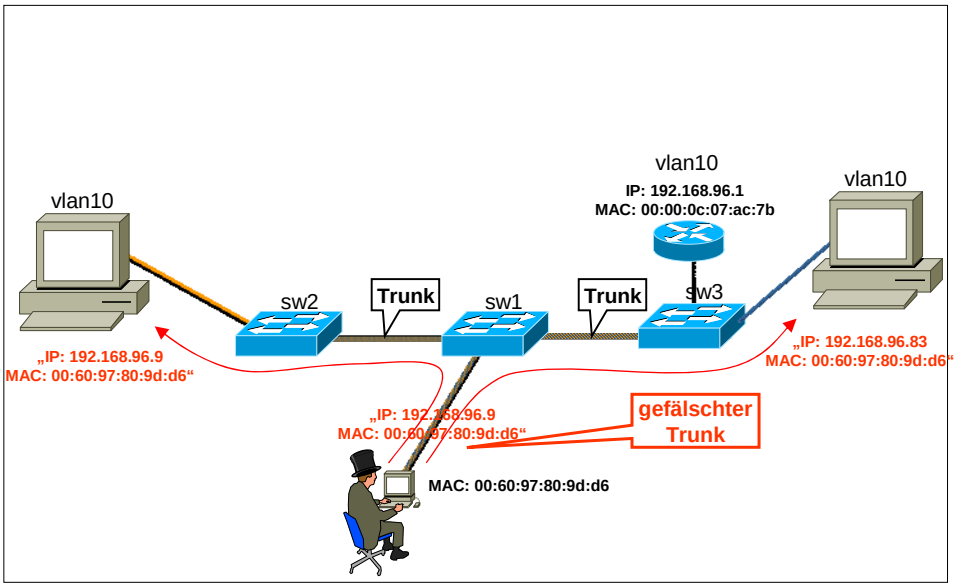


Nach der sofort erfolgreichen Verhandlung eines Trunks sieht der Angreifer dann den darüber transportierten Verkehr, darunter alle Infrastruktur-Protokolle, die über Trunks übertragen werden (v.a. VTP, mehr dazu unten) und den gesamten Multicast- und Broadcast-Traffic des Netzes, etwa üblicherweise auch die Routing-Protokolle (hier OSPF).



Des weiteren ist es anschliessend möglich, in *beliebige* VLANs Pakete einzuschleusen (da der Trunk ja an allen VLANs teilnimmt), d.h. der Angreifer kann gewissermassen Verkehr *entfernter* Netze zu sich umleiten. Die folgende Skizze verdeutlicht diesen Angriff:

ARP-Spoofing über VLAN-Grenzen hinweg



Auch dieser Angriff ist Menü-gesteuert im Tool *yersinia* implementiert und konnte von den Autoren ohne jegliche Probleme erfolgreich getestet werden.

Die häufig (auch von den Autoren) ausgesprochene Empfehlung, Netze zum Schutz vor *ARP Spoofing* zu segmentieren, wird damit obsolet. Ein Angreifer, der ein einziges an einen beliebigen Switch konnektiertes System kontrolliert, kann damit potentiell den Verkehr *aller VLANs aller Switches* mitlesen, sofern die Switches untereinander verbunden sind. Dies gilt allerdings nur, solange weitgehend eine Default-Konfiguration der Devices vorhanden ist. Die einfachste Massnahme, den beschriebenen Angriff zu verhindern, besteht darin, Access-Ports mit User-Zugang tatsächlich auch statisch als solche zu konfigurieren (IOS-basierte Devices: `switchport mode access`, CatOS-Devices: `set trunk` *`mod/port`* `off`).

VTP

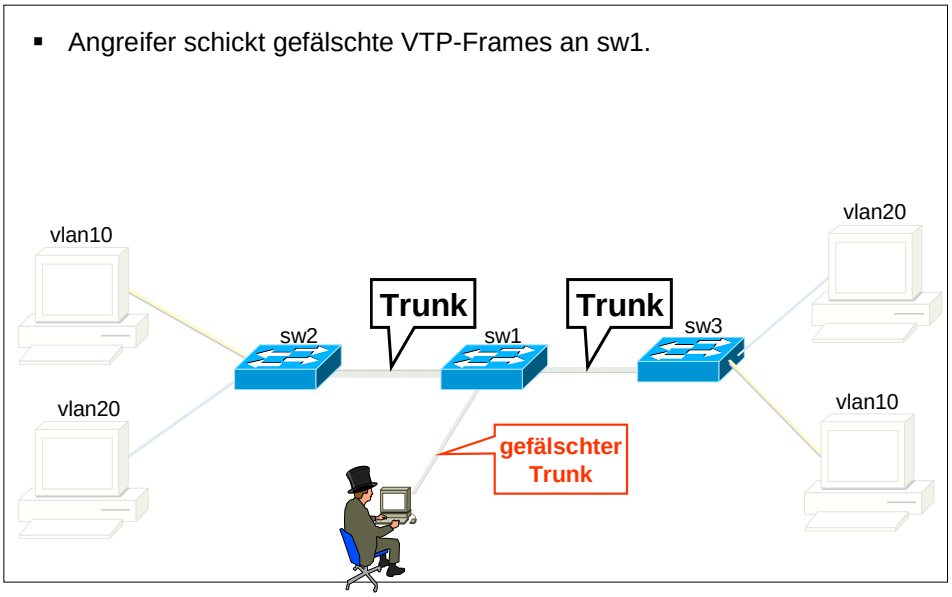
Während *VLAN Tagging* dazu verwendet wird, einzelne Frames den richtigen VLANs zuzuordnen, dient das *VLAN Trunking Protocol* (VTP) dazu, VLAN-Informationen an sich zwischen verschiedenen Switches auszutauschen (also etwa welche VLANs es gibt, wie ihre Namen sind u.ä.). Die Switches versenden dazu über Trunk-Ports VTP-Pakete, wobei funktionierende VTP-Kommunikation nur zwischen Switches derselben sog. *VTP Domain* möglich

ist. Sie können dann mit VTP ihre VLAN-Datenbanken synchronisieren und verwenden dabei eine Revisions-Nummer, die bei auftretenden Synchronisations-Konflikten autorisierende Wirkung hat. Cisco Switches können in drei verschiedenen *VTP Modi* arbeiten: *Server* (kann globale VLANs erstellen/löschen, dies ist die Default-Einstellung!), *Client* (kann keine VLANs ändern) und *Transparent* (kann lokale VLANs erstellen/löschen, ignoriert aber VTP Updates).

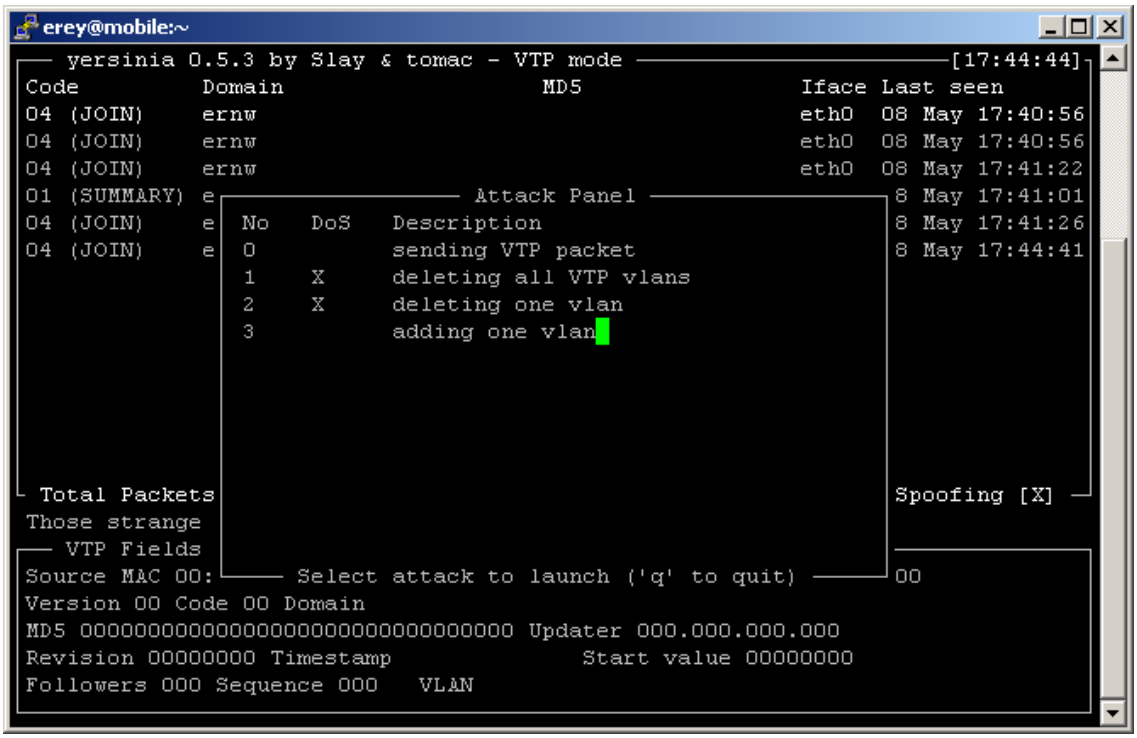
Ein Angreifer, der ein VTP-Paket mit höherer Revisions-Nummer injizieren kann (durch Anschluss eines Devices mit höherer Revisions-Nummer an das Netz oder durch Senden eines entsprechenden Netzwerk-Pakets; Voraussetzung ist jeweils eine bestehende Trunk-Verbindung zu einem Device, das *vtp-server* ist), kann die VLAN-Informationen der gesamten *VTP domain*/des gesamten Netzes löschen. Dies kommt faktisch einem umfassenden *Denial-of-Service* Angriff gleich. Da es sich bei VTP um Layer2-Pakete handelt (ähnlich CDP, hier aber mit SNAP HDLC 0x2003), muss der Angreifer dazu ein System mit physischen Zugang zu einem der Segmente kontrollieren. Entscheidend ist die Konnektierung an einen Port eines Devices und – wie oben beschrieben – die Möglichkeit, dort eine (‚gefälschte') Trunk-Verbindung aufzubauen.

Schematisch sieht der Angriff in etwa so aus:

Löschen aller VLANs durch injizierte VTP-Frames



Auch dieser Angriff galt in erster Linie wegen der Voraussetzung des bestehenden Trunks) bisher als theoretisch; auch hier existiert jetzt mit dem Tool *yersinia* ein „geeignetes Werkzeug“ zur voll-automatischen Ausführung:



Die wichtigste Massnahme zum Schutz vor VTP-basierten Sicherheits-Problemen ist die korrekte Konfiguration von Access-Ports (siehe oben) und damit Unterbindung unautorisierter Trunks. Weiterhin kann ein *VTP Password* konfiguriert werden, das in einen *MD5 Digest* der VTP-Pakete Eingang findet (also nicht im Klartext übertragen wird).

Fazit und Zusammenfassung

Die hier gezeigten Angriffe können gravierende Auswirkungen auf die Verfügbarkeit oder Stabilität bzw. die Vertraulichkeit der übertragenen Daten haben. Viele Netze sind dagegen nicht ausreichend geschützt.

Bislang galten allerdings viele Angriffe als theoretisch und es waren kaum Angriffs-Tools verfügbar. Inzwischen ist das Angriffs-Knowhow aber besser dokumentiert und es liegt ein neues, sehr mächtiges Tool vor.

Sysadmins von Netzen mit Cisco-Switches sollten daher auch auf Layer 2 Sicherheits-Massnahmen implementieren. Einen Anhaltspunkt bieten hier die unter [4], [5] und [6] genannten Dokumente.

Quellen

[1] Aurand, Andreas: LAN-Sicherheit, Heidelberg 2005 (dpunkt-Verlag).
[2] Tool *Yersinia*: http://yersinia.sourceforge.net.
[3] Cisco Packet Magazine, Artikel „Layer 2 -- The Weakest Link“: http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac222/about_cisco_packet_feature09186a0080142deb.html
[4] NSA Guide Switch Security: http://www.nsa.gov/snac/os/switch-guide-version1_01.pdf
[5] Cisco SAFE Blueprint Layer 2 Security: http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008014870f.shtml
[6] Catalyst Secure Template: http://www.cymru.com/gillsr/documents/catalyst-secure-template.htm
[7] IRPAS (Internetwork Routing Protocol Attack Suite): http://www.phenoelit.de/irpas/

Enno Rey (CISSP, CISA) ist technischer Geschäftsführer des Security-Dienstleisters ERNW GmbH.

Für Anregungen oder Kommentare erreichen Sie ihn unter erey@ernw.de.

Peter Fiers (pfiers@ernw.de) ist Security Consultant bei ERNW.