

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Man-in-the-Middle-Angriffe

Praktikum Datenschutz und Datensicherheit Sommersemester 2016

Fabian Uhlmann Diana Irmscher

Fakultät für Informatik und Mathematik

Hochschule für angewandte Wissenschaften München

28. Juli 2016

Begrüßung

Man in the Middle
im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle-
Angriffe im
geswichten
Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmischer

Begrüßung

Man in the Middle
im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle-
Angriffe im
geswichten
Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen



Fabian Uhlmann
Informatik, Bachelor



Diana Irmischer
Informatik, Bachelor

Agenda

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle
im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle-
Angriffe im
geswitchten
Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

1. Begrüßung

2. Man in the Middle im Web

3. Man-in-the-Middle-Angriffe im gewitchten Netzwerk

4. Quellen

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

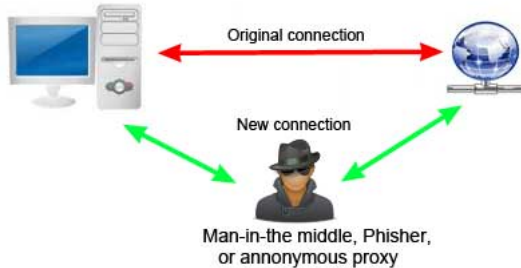
Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

Dell und Lenovo haben demonstriert, dass man mit Man-in-the-Middle Angriffen die Sicherheit eines Systems sehr effizient aushebeln kann. Wie funktioniert ein derartiger Angriff und was kann man tun, um sich zu schützen.

Man in the Middle (MITM)

Man-in-the-middle attack



<http://www.computerhope.com>

Quelle: [2]



Quelle: [1]

Man-in-the-Middle-Angriffe

Fabian Uhlmann,
Diana Irmischer

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken
Schutz

Man-in-the-Middle-Angriffe im geschwitten Netzwerk

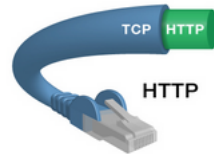
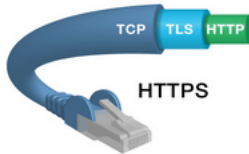
Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

HTTP(s) und Zertifikate

Man-in-the-Middle-Angriffe

Fabian Uhlmann,
Diana Irmischer



Quelle: [3]

Begrüßung

Man in the Middle im Web

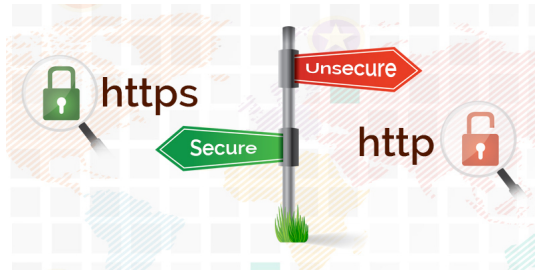
Einführung

Sicherheitslücken
Schutz

Man-in-the-Middle-Angriffe im gewichenen Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen



Quelle: [4]

HTTP(s) und Zertifikate

Man-in-the-Middle-Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

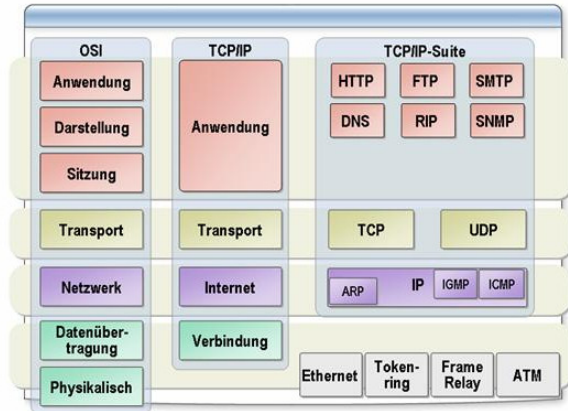
Einführung

Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen



Quelle: [5]

HTTP(s) und Zertifikate

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmischer

Begrüßung

Man in the Middle im Web

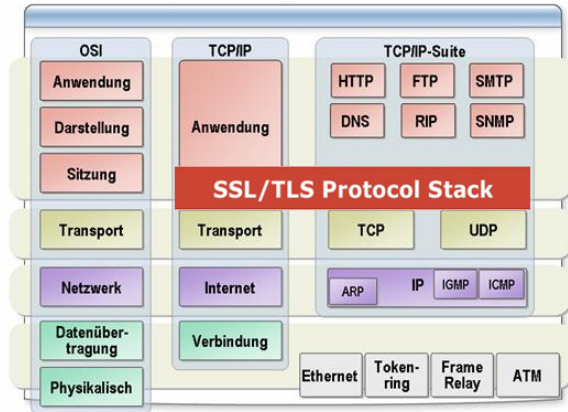
Einführung

Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen



Quelle: [5]

HTTP(s) und Zertifikate

Man-in-the-Middle-Angriffe

Fabian Uhlmann,
Diana Irscher

Begrüßung

Man in the Middle im Web

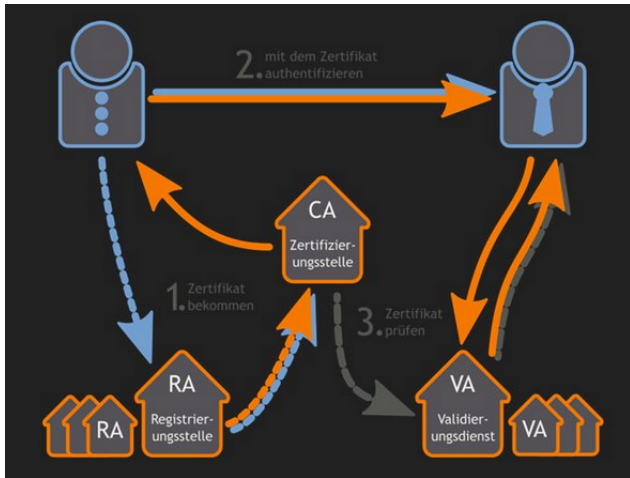
Einführung

Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im gesicherten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen



Quelle: [6]

HTTP(s) und Zertifikate

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web


Einführung

Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

 Zertifikat-Ansicht: "www.dkb.de"

Allgemein Details

Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:

- SSL Client Certificate
- SSL Server Certificate

Ausgestellt für

Allgemeiner Name (CN) www.dkb.de
 Organisation (O) Deutsche Kreditbank Aktiengesellschaft
 Organisationseinheit (OU) OE-56031
 Seriennummer 0E:D7:F4:CF:CF:70:7E:EB:C0:4E:BE:53:75:47:90:0E

Ausgestellt von

Allgemeiner Name (CN) Symantec Class 3 Extended Validation SHA256 SSL CA
 Organisation (O) Symantec Corporation
 Organisationseinheit (OU) Symantec Trust Network

Gültigkeitsdauer

Beginnt mit 19.04.2016
 Läuft ab am 20.04.2018

Fingerabdrücke

SHA-256-Fingerabdruck B5:54:04:AE:CC:25:8E:CB:E8:E1:10:81:E8:93:2F:08:2D:FF:EB:58:64:8F:7D:1C:24:F6:1D:9C:F5:76:2C:0B
 SHA1-Fingerabdruck D4:E6:3D:25:00:19:EA:F3:CC:B1:79:68:25:B7:7F:CE:75:AB:AD:E6

HTTP(s) und Zertifikate

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im gesicherten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

Zertifikat-Ansicht: "www.dkb.de"

Allgemein Details

Zertifikats-hierarchie

- VeriSign Universal Root Certification Authority
 - Symantec Class 3 Extended Validation SHA256 SSL CA
 - www.dkb.de

Zertifikats-Layout

- www.dkb.de
 - Certificate
 - Version
 - Serial Number
 - Certificate Signature Algorithm
 - Issuer
 - Validity
 - Not Before
 - Not After
 - Subject
 - Subject Public Key Info

Feld-Wert

PKCS #1 SHA-256 With RSA Encryption

Zertifikats-Layout

- Not After
- Subject
 - Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject's Public Key
- Extensions
 - Certificate Subject Alt Name
 - Certificate Basic Constraints
 - Certificate Key Usage
 - Certificate Policies
 - CRL Distribution Points

Feld-Wert

PKCS #1 RSA Encryption

HTTP(s) und Zertifikate

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmischer

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen



Quelle: [7]

Sicherheitslücke - Lenovo

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmischer

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken

Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

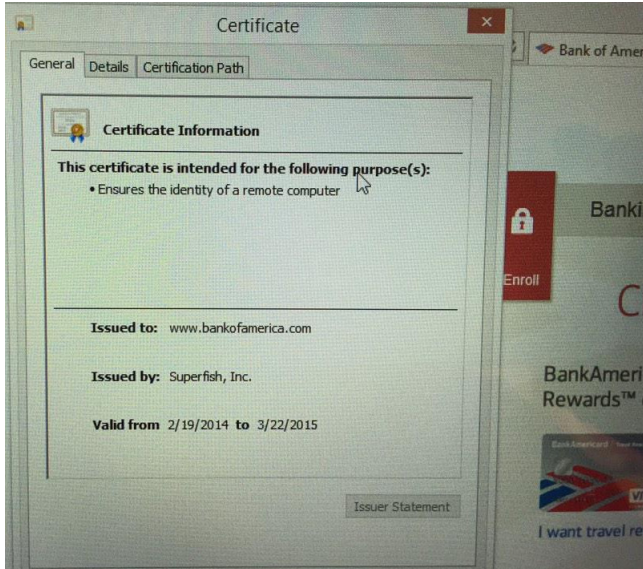
Einführung

Angriffsmöglichkeiten

Werkzeuge

Maßnahmen

Quellen



Quelle: [8]

Sicherheitslücke - Lenovo

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken

Schutz

Man-in-the-Middle- Angriffe im gesicherten Netzwerk

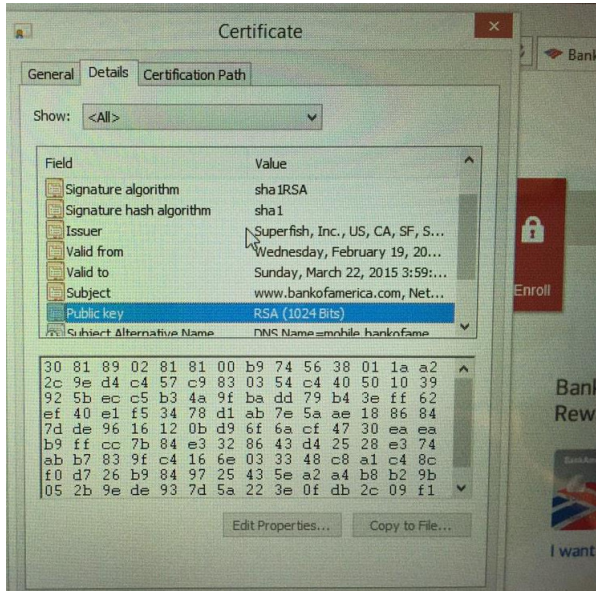
Einführung

Angriffsmöglichkeiten

Werkzeuge

Maßnahmen

Quellen



Quelle: [8]

Sesam öffne Dich

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmischer

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken

Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung

Angriffsmöglichkeiten

Werkzeuge

Maßnahmen

Quellen

```
C:\Windows\system32\cmd.exe

C:\dev>pemcrack super.pem super.dict
--- pemcrack v1.0 - by Robert Graham ---
-> aaas
-> bugi
-> czech
-> ente
-> fuvf
-> hres
-> jdjgj
-> jvjgj
found: komodia

C:\dev>
```

Quelle: [9]

```
C:\Windows\system32\cmd.exe

C:\dev>openssl rsa -in super.pem -text
Enter pass phrase for super.pem:
Private-Key: (1024 bit)
modulus:
  00:e8:f3:4a:18:76:5f:19:3f:b1:cf:58:e9:7f:43:
  07:09:95:80:35:c5:0f:fe:71:31:27:81:99:12:26:
  20:a5:df:8f:6a:fc:42:55:39:ee:09:38:89:d9:e0:
  36:c4:ac:01:82:5b:d5:39:e6:f9:8f:07:88:df:fe:
  ee:f6:a1:14:ce:a9:74:45:d8:fd:f0:17:57:2a:82:
  e1:7a:2e:12:93:5a:ac:8a:d7:15:63:d1:b7:9b:55:
  80:0f:58:bc:1c:49:ed:20:62:dd:b6:4c:a5:3a:eb:
  1c:3d:a0:ff:7a:71:a6:d3:10:78:33:ae:4b:c2:1c:
  fd:92:4a:a1:c3:e7:41:a4:2d
publicExponent: 65537 (0x10001)
privateExponent:
  00:a7:a9:5b:5e:09:ec:5e:5e:d2:9a:5a:f3:0b:ce:
  71:45:3b:9d:e0:95:69:f2:87:03:8a:dc:a3:10:45:
  f2:df:8f:ed:48:62:31:57:e7:ee:e4:22:16:4d:83:
  2b:c8:17:c8:aa:4b:70:47:51:6f:b2:bb:08:8f:b7:
  8b:c4:64:a1:74:d1:0c:46:54:e5:73:cc:26:76:6c:
  13:92:d6:80:d4:3e:a6:2d:c7:c0:c1:1d:47:4b:c3:
  d8:8c:af:bc:81:f7:b6:ae:a6:34:a8:03:bb:eb:e8:
  ce:6f:03:5a:c1:0f:f7:a8:eb:85:56:e8:d5:4d:6b:
  cf:21:2d:5f:8e:9a:7e:8e:fd
prime1:
  00:fd:55:da:9c:66:aa:8f:8b:9a:12:ca:9f:63:a9:
  ff:ef:e3:13:9b:88:8f:38:ce:ea:7e:8c:88:e0:4a:
  69:25:76:64:95:cf:c5:6d:c5:76:94:08:d8:d8:99:
  7d:53:a5:fb:5a:7a:82:3e:7f:bf:ce:0e:38:ea:52:
  96:4e:78:40:6b
prime2:
  00:eb:66:8b:a9:f0:f1:68:d8:ea:ec:97:66:8b:04:
  ff:4a:f8:4a:44:92:a3:6d:04:25:b0:42:25:c8:1d:
  a1:f2:93:f9:50:86:07:88:69:87:a5:f0:19:d9:6c:
  d1:c6:be:a9:ae:59:13:56:b5:f7:a7:69:c3:05:6b:
  7b:48:66:f3:c7
```

Quelle: [9]

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmischer

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken

Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

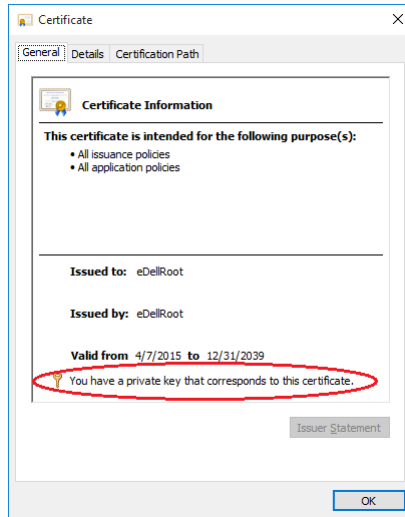
Einführung

Angriffsmöglichkeiten

Werkzeuge

Maßnahmen

Quellen



Quelle: [10]

Sicherheitslücke - DELL

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken

Schutz

Man-in-the-Middle- Angriffe im gesicherten Netzwerk

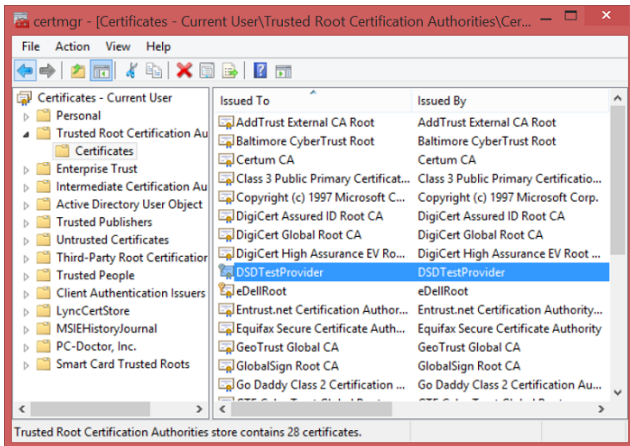
Einführung

Angriffsmöglichkeiten

Werkzeuge

Maßnahmen

Quellen



Quelle: [11]

Sicherheitslücke - DELL

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmischer

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken

Schutz

Man-in-the-Middle- Angriffe im gesicherten Netzwerk

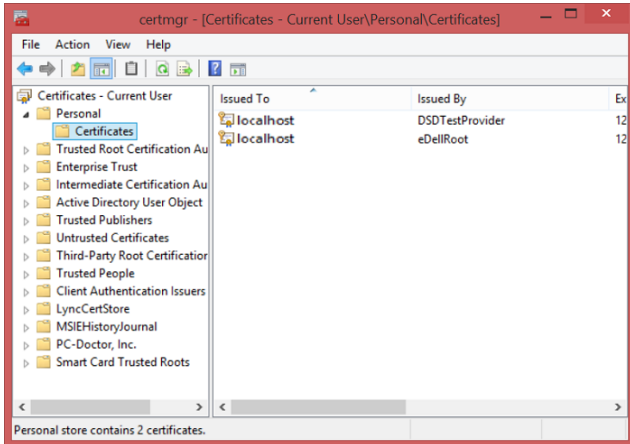
Einführung

Angriffsmöglichkeiten

Werkzeuge

Maßnahmen

Quellen



Quelle: [11]

Organize				
Name	Publisher	Installed On	Size	Version
Dell Foundation Services	Dell Inc.	6/1/2016		3.1.3300.0

Quelle: [11]

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher



SSL Report: dkb.de (212.34.75.193)

Assessed on: Wed, 27 Jul 2016 23:30:53 UTC | [HIDDEN](#) | [Clear cache](#)

[Scan Another >](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO >](#)

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken

Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

Quelle: [12]

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken

Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung

Angriffsmöglichkeiten

Werkzeuge

Maßnahmen

Quellen

Authentication

Server Key and Certificate #1

Subject	www.dkb.de Fingerprint SHA1: d4e63d250019eaf3ccb1796825b77fce75abade6 Pin SHA256: aFa3/x2yjWfdzcNeDJoJU4L5j1lIAaQ+GIDRLzKI@o=
Common names	www.dkb.de
Alternative names	apps.dkb.de www.dkb.de dkb.de
Valid from	Tue, 19 Apr 2016 00:00:00 UTC
Valid until	Thu, 19 Apr 2018 23:59:59 UTC (expires in 1 year and 8 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Symantec Class 3 Extended Validation SHA256 SSL CA AIA: http://sh.symcb.com/sh.crt
Signature algorithm	SHA256withRSA

Quelle: [12]

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Schutzmöglichkeiten:

Begrüßung

- neuer Rechner ohne BS

Man in the Middle im Web

- Kontrolle Zertifikate

Einführung Sicherheitslücken Schutz

- inhaltliche Überprüfung Zertifikatsspeicher
- inhaltliche Überprüfung aktueller Programmliste

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

- auf aktuellem Stand bleiben

→ Verwendung fachspezifischer Foren, Newsletter oder Zeitschriften

Einführung Angriffsmöglichkeiten Werkzeuge Maßnahmen

→ Information über verwendete HW u. SW

Quellen

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

Es gibt Man-in-the-Middle-Angriffe nicht nur gegen SSL/TLS-Verbindungen, sondern auch gegen "normale" Netzwerkverbindungen. Sie werden von Angreifern eingesetzt, um in einem geswitchten Netz zu sniffen.

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

- stellt Verbindungskomponente in einem Netzwerk dar
- arbeitet auf Schicht 1 des ISO-/OSI-Schichtenmodells
- nicht zielorientiert
- sendet Bits an alle Teilnehmer, die an Hub angeschlossen sind
- wurde in Netzwerken hauptsächlich aus Kostengründen eingesetzt
- wurde mittlerweile fast vollständig von Switches verdrängt, da diese mittlerweile günstig geworden sind

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

- arbeite auf Schicht 2 des ISO-/OSI-Schichtenmodell
- zwei Typen:
 - einfacher Switch : leitet Pakete mit Hilfe von MAC-Adressen von Quelle zu Ziel weiter; verwendet dafür Switch-Tabelle
 - Layer-3-Switch : zusätzlich zur oben genannten Funktion noch Überwachungsfunktionen möglich, z.B. IP-Filterung, Routing (Schicht 3)

Einsatz eines Switches bringt wesentliche Vorteile zum Vorgänger Hub

- erhöhte Datensicherheit
- geringere Netzwerklast

Funktion Switch-Tabelle

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

Adresse	Interface	Zeit
62-FE-F7-11-89-A3	1	9:01
7C-BA-B2-B4-91-10	3	9:12
...

Switch-Tabelle ermöglicht wesentlichen Punkt der Funktionsweise:

- Switch verfügt über Ein- und Ausgänge, sogenannte Ports
- können unabhängig voneinander empfangen und senden
- an Ein- und Ausgängen sind einzelne Netzwerkteilnehmer angeschlossen
- für jeden Port MAC-Adresse des Teilnehmers hinterlegt

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmischer

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

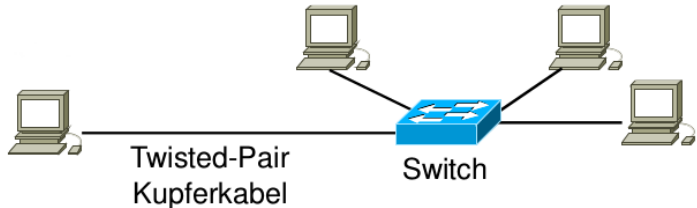
Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

Store-und-Forward-Prinzip

- 1 Switch empfängt gesamtes Frame, berechnet CRC, wenn CRC nicht stimmt, wird Frame verworfen
- 2 überprüfen, ob Quell-Adresse in Switch-Tabelle, wenn nicht, Eintrag zusammen mit Port in Switch-Tabelle
- 3Ziel-Adresse mit Einträgen in Switch-Tabelle vergleichen, wenn vorhanden, wird an Teilnehmer mit passenden Port weitergeleitet, ansonsten Weiterleitung an alle Ports

Was ist ein geschwitchtes Netzwerk



- Auslastung des Netzwerkes stark reduziert
- Frame nur noch an einen Teilnehmer, wenn dieser bekannt
- Switch kann Teilnehmer auch in Gruppen aufspalten und unterscheiden, an welche Gruppe Frame gesendet wird
- nahezu jeden Netzwerk verfügt heute über mindestens einen Switch

Mehrere Switches in einem Netzwerk

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

- natürlich möglich
- kann man nicht einfach miteinander verbinden, da sonst eine Schleife gelegt wird, gesamter Netzwerkverkehr kommt zum Erliegen
- Vorkehrungen treffen, spezielle Kabel

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

- MAC-Flooding
- MAC-Spoofing
- ARP-Spoofing

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

- Speicher in Switch-Tabelle ist begrenzt
- Switch wird mit gefälschten MAC-Adressen überhäuft, bis Speicher in der Tabelle voll
- wenn Tabelle voll, verhält sich Switch bei neuen Adressen wie Hub, weil diese unbekannt sind
- einige Switches haben Schutzmaßnahmen dagegen, z.B. List mit zugelassenen Ports anlegen

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

- Quell-Adresse mit Adresse des Angreifers ersetzen
- Antwort des Empfängers wird an Angreifer gesendet
- Angreifer wird dabei allerdings in Switch-Tabelle eingetragen
- Schutzmaßnahme: Liste mit erlaubten MAC-Adresse für jeweiligen Port

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

Dieser Angriff macht sich Schwachstelle des ARP-Protokolls zunutze.

Funktionsweise ARP:

- Auflösung IP zu Hardware-Adresse
- jeder Rechner hat ARP-Tabelle
- in ARP-Tabelle alle bekannten Teilnehmer des lokalen Netzwerkes hinterlegt
- damit Einträge nicht veralten, regelmäßig ARP-Request

ARP-Schwächen im Protokoll

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

- jede ARP-Response wird ausgewertet, auch ohne ARP-Request
- Identität des Teilnehmers wird nicht überprüft

ARP-Spoofing Beispiel

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken

Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung

Angriffsmöglichkeiten

Werkzeuge

Maßnahmen

Quellen

Netzwerkteilnehmer

- Diana
- Fabian
- X
- Y Angreifer

ARP-Spoofing Beispiel

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

APR-Tabellen-Einträge mit entsprechenden Werkzeugen manipulieren, sodass in bei den Netzwerkteilnehmern falsche Angaben hinterlegt sind

ARP-Tabelle von Fabian

IP-Adresse Diana	:	MAC-Adresse von Y
IP-Adresse X	:	MAC-Adresse von X
IP-Adresse Y	:	MAC-Adresse von Y

ARP-Tabelle von Diana

IP-Adresse Fabian	:	MAC-Adresse von Y
IP-Adresse X	:	MAC-Adresse von X
IP-Adresse Y	:	MAC-Adresse von Y

ARP-Spoofing Beispiel

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

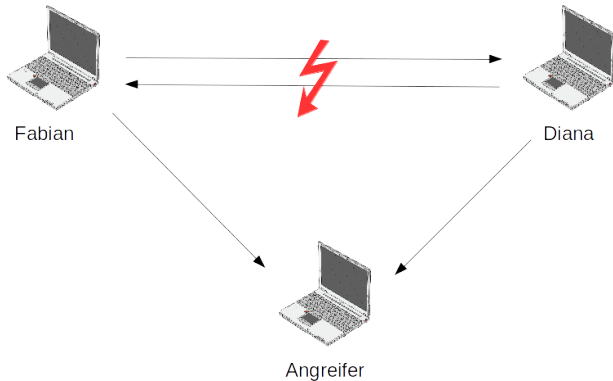
Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geschwittenen Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen



ARP-Spoofing Beispiel

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmischer

Begrüßung

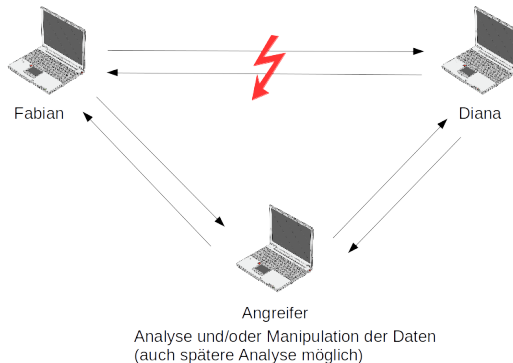
Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geschwitten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen



Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

mehrere Werkzeuge, die sich dafür eignen:

- Ettercap NG : umfangreiche Sammlung von Tools
- Arp-sk : Erzeugen einfacher ARP-Nachrichten
- ARP0c : Spoofing-Tool, händlet selbst den Versand von ARP-Nachrichten
- Dsniff : Sammlung von Tools

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle- Angriffe im geswitchten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

- Passwort-Sniffer dsniff : filtert unverschlüsselte Passwörter im Netzwerk
- arpspoof : leitet Pakete vom Zielhost, welchen in einem Netzwerk zu einem anderen Host gesendet werden sollen, um, indem die ARP-Antworten (ARP-Replies) vom Angreifer gefälscht werden.
- weitere spezielle Sniffer wie z.B. urlsniff und mailsniff

Man-in-the-Middle-Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung
Sicherheitslücken
Schutz

Man-in-the-Middle-Angriffe im geschützten Netzwerk

Einführung
Angriffsmöglichkeiten
Werkzeuge
Maßnahmen

Quellen

- einzig sichere Maßnahme ist manuelle Verwaltung von Ip- und zugehörigen MAC-Adressen; im privaten Netzwerk zu Hause gut umsetzbar
- bringt allerdings einen hohen Arbeitsaufwand mit sich, wenn viele Netzwerkteilnehmer
- in Netzwerk mit vielen wechselnden Geräten nicht umsetzbar
- weitere Maßnahme wäre Überwachung des Netzwerkes, um eine erhöhte Anzahl an ARP-Nachrichten aufzudecken
- Arpwatch ist Programm, dass ARP-Nachrichten im Netzwerk überprüft
 - alle bekannten Adressen in arp.dat hinterlegt
 - taucht eine nicht bekannte Adresse auf, wird Nachricht in syslog hinterlegt
 - hat sich Zuordnung von MAC- zu IP-Adresse geändert,

Man-in-the-Middle- Angriffe

Fabian Uhlmann,
Diana Irmscher

Begrüßung

Man in the Middle im Web

Einführung

Sicherheitslücken

Schutz

Man-in-the-Middle- Angriffe im gesicherten Netzwerk

Einführung

Angriffsmöglichkeiten

Werkzeuge

Maßnahmen

Quellen

- ❶ <http://hackerspace.kinja.com/how-to-defend-yourself-against-mitm-or-man-in-the-middle-1461796382> (Abrufdatum: 26.07.2016)
- ❷ http://blog.agupieware.com/2013_10_01_archive.html (Abrufdatum: 26.07.2016)
- ❸ https://kaazing.com/doc/xmpp/3.5/security/c_sec_https_wss.html (Abrufdatum: 26.07.2016)
- ❹ <http://www.vijaywebsolutions.com/Blog.aspx> (Abrufdatum: 26.07.2016)
- ❺ <http://d.pcnews.at/ins/pcn/103/003000/main.htm> (Abrufdatum: 26.07.2016)
- ❻ <http://slideplayer.org/slide/855695/> (Abrufdatum: 26.07.2016)
- ❼ <http://thehackernews.com/2012/09/crime-new-sslts-attack-for-hijacking.html> (Abrufdatum: 26.07.2016)
- ❽ <http://marcrogers.org/2015/02/19/lenovo-installs-adware-on-customer-laptops-and-compromises-all-ssl/> (Abrufdatum: 26.07.2016)
- ❾ <http://blog.erratasec.com/2015/02/extracting-superfish-certificate.html> (Abrufdatum: 26.07.2016)
- ❿ <http://joenord.blogspot.de/2015/11/new-dell-computer-comes-with-edellroot.html> (Abrufdatum: 26.07.2016)
- ❾ <http://www.dell.com/support/article/us/en/19/SLN300321> (Abrufdatum: 26.07.2016)
- ❿ <https://globalsign.sslabs.com/> (Abrufdatum: 26.07.2016)