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

27. Juli 2016

Vorstellung

Fabian Uhlmann
Informatik, Bachelor

Diana Irmscher
Informatik, Bachelor

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN MÜNCHEN

Agenda

1. Begrüßung
2. Man in the Middle im Web
3. Man-in-the-Middle-Angriffe im geswitchten Netzwerk

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN MÜNCHEN

Aufgabenstellung

Aufgabenstellung

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.

Hub

- 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

Switch

- 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 Switchtes bringt wesentliche Vorteile zum Vorgänger Hub

- erhöhte Datensicherheit
- geringere Netzwerklast

Funktion Switch-Tabelle

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

Funktion Switch-Tabelle

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
3. Ziel-Adresse mit Einträgen in Switch-Tabelle vergleichen, wenn vorhanden, wird an Teilnehmer mit passenden Port weitergeleitet, ansonsten Weiterleitung an alle Ports

Was ist ein geswitchtes 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

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

Angriffsmöglichkeiten

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

MAC-Flooding

- 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

MAC-Spoofing

- 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

ARP-Spoofing

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

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

ARP-Beispiel

Netzwerkteilnehmer

- Diana
- Fabian
- X
- Y Angreifer

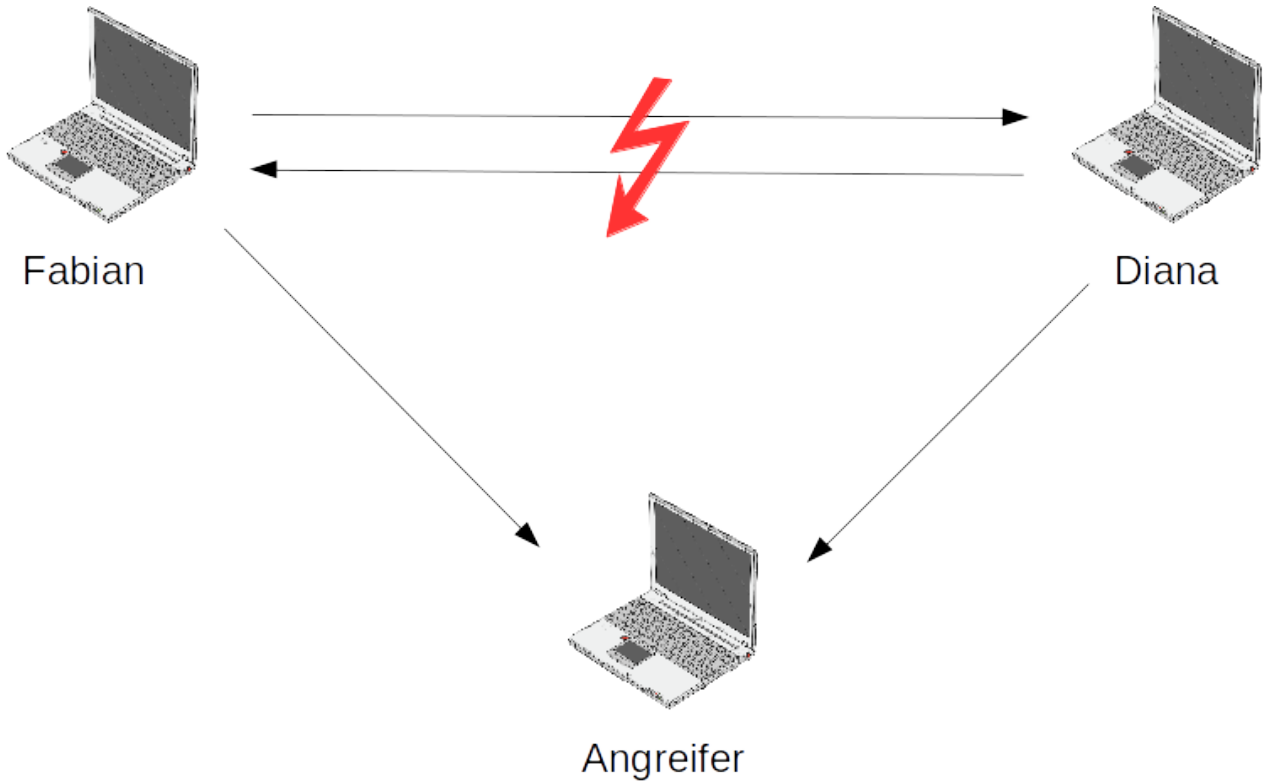
ARP-Beispiel

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

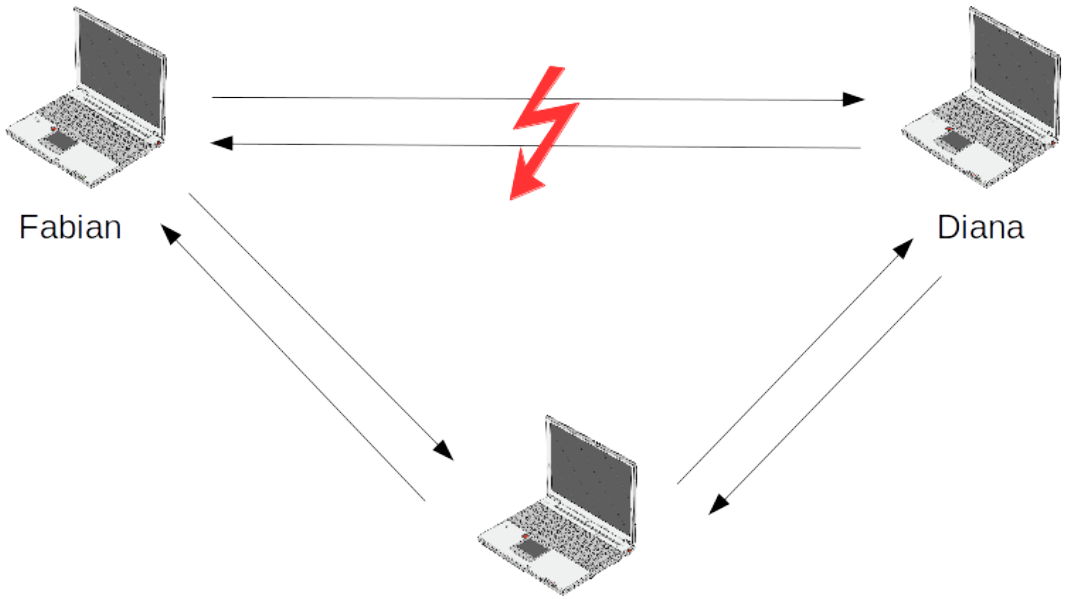
ARP-Tabelle von Fabian		
IP-Adresse Diana	:	MAC-Adresse von Y
IP-Adresse X	:	MAC-Adresse von X
IP-Adresse Y	:	MAC-Adresse von Y

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-Beispiel



ARP-Beispiel



Werkzeuge

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN MÜNCHEN

Schutzmaßnahmen