



openHPI – Sicherheit im Internet Adressverfälschung im Internet – Spoofing

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Adressverfälschung im Internet – Spoofing

Spoofing (dt. vortäuschen, manipulieren)

- Bezeichnet im Internet das Vortäuschen jeder Art gefälschter Adressen
- Dient meist zur Vorbereitung für weiterführende Angriffe

Anwendung

- Datenpakete versenden mit **gefälschter Absenderadresse**, um Angriff zu vertuschen oder unter falscher Identität Zugriff auf ein geschütztes System zu erlangen
- **Agieren mit der Zieladresse** eines Dritten, um an Daten zu kommen, die für diesen Dritten bestimmt sind
 - z.B. bei Man-in-the-Middle-Angriffen

IP-Spoofing bezeichnet den Einsatz gefälschter IP-Adressen bei Sendungen an Dritte

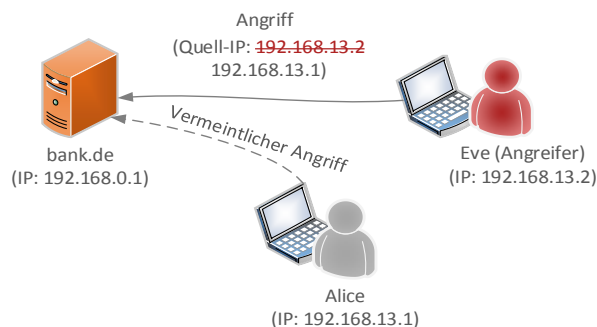
- Angreifer erzeugt und versendet Datenpakete mit verfälschter IP-Absenderadresse, um gegenüber seinem Opfer einen vertrauenswürdigen Absender vorzutäuschen

Einschränkung

- Funktioniert meist nur bei verbindungslosen Protokollen (z.B. UDP, ICMP), bei denen keine Rückantwort erwartet wird
 - Rückantwort wird an im empfangenen Paket genannte Absenderadresse gesendet ...
- IP-Spoofing funktioniert bei verbindungsorientierten Protokollen nur, wenn Zugriff auf ein Zwischensystem möglich ist
 - Dort kann Antwortpaket vom Angreifer abgefangen werden ...

Angriffsszenario: Angreifer versteckt sich

- Angreifer verfälscht seine Adresse, damit es so aussieht, als würde jemand anderes den Angriff durchführen
- Einsatz z.B. bei DDoS-Angriffen, damit Opfer den eigentlichen Ursprung nicht feststellen kann



Gegenmaßnahmen

- Einrichten guter **Filterregeln** auf einer Firewall
 - Sperrung von Paketen aus externem Netzwerk, die vorgeben, aus internem Netz zu stammen
- Einsatz **verbindungsorientierter Protokolle**
 - verbindungsorientierte Protokolle wie TCP erwarten Aufbau einer Ende-zu-Ende Verbindung
 - Angreifer mit gefälschter IP kann in der Regel keine Rückantwort erhalten bzw. geben
- **Authentifizierung**
 - Verwendung von sicherer Authentifizierungsverfahren, z.B. Einsatz von IPSEC verhindert Absenderfälschung

DNS-Spoofing bezeichnet das Vortäuschen einer falschen Zuordnung zwischen DNS-Name (Computername) und IP-Adresse

- Falscher Eintrag im DNS-System leitet legitime DNS-Adresse auf IP-Adresse des Angreifers um

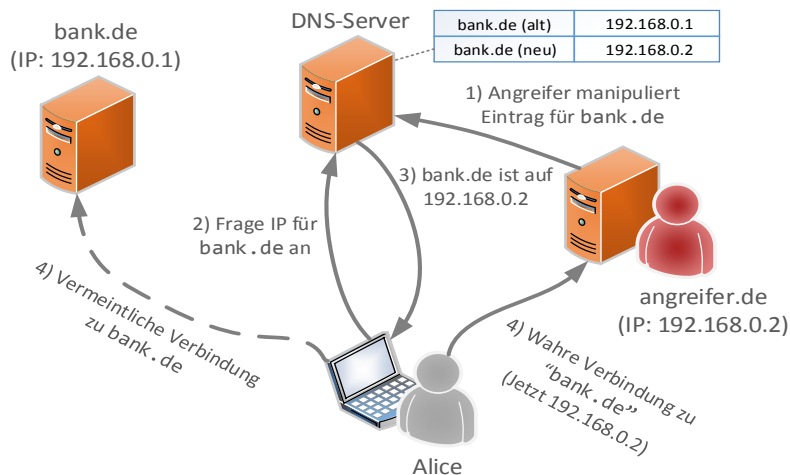
Angriffsmethoden

- Manipulation des DNS-Zwischenspeichers beim Opfer
- **Timing Angriff:** Gefälschte Rückantwort auf DNS-Anfrage des Opfers bevor richtige Antwort vom legitimen DNS-Server bei Opfer ankommt
 - erste Antwort gilt (First-Come-First-Serve)
- ...

Gegenmaßnahmen

- Einspielen von **Updates** für DNS-Server-Software
 - Große Anfälligkeit für DNS-Spoofing wegen vieler Schwachstellen in DNS-Serversoftware
- Verwendung von **DNSSEC**
 - Kommunikation zwischen IP und DNS wird über Signaturen beglaubigt
- Überprüfung des **digitalen Zertifikats** des eigentlichen Ziel-Servers
 - Zertifikat sollte für DNS-Name ausgestellt sein
 - Nach Verbindungsaufbau zu einem zertifikatbasierten SSL-Dienst (z.B. HTTPS) kann Gültigkeit des digitalen Zertifikats für angegebene Domäne überprüft werden

DNS-Spoofing (3/3)



Email-Spoofing bezeichnet das Versenden von Emails mit vorgetäuschten oder gefälschten Absenderadressen

- Verwendung gefälschter Adressen beim Versand von Spam- und Phishing-Emails, um Vertrauen des Nutzers zu erwecken
- Emails enthalten häufig Schadsoftware, die wiederum zum Versand gespoofter Emails verwendet wird

Grundproblem:

- Identität des Absenders wird auf Email-Server nicht überprüft
- Email-Empfänger hat keine Möglichkeit, die Absenderadresse nachträglich zu überprüfen

Angriffsmethoden (1/2)

■ **Ändern des angezeigten Absenders**

- Email-Protokoll (SMTP) erlaubt das Setzen eines Anzeigenamens für den Absender
- Anzeigenamen wird auf vertrauenswürdigen Namen gesetzt, z.B.
 - hinter **OpenHPI [info@open.hpi.de]** versteckt sich **angreifer@domain.de**
- richtige Email-Adresse wird nicht in jedem Email-Programm angezeigt (aber: Überprüfung des tatsächlichen Absenders im Email-Programm immer verbreiteter)

Angriffsmethoden (2/2)

■ **Versand über offene Email-Server (Open-Relay-Server)**

- Email-Server akzeptiert das Versenden von Emails mit jeder Absenderadresse ohne Überprüfung der Identität des Senders

→ Falsche Serverkonfiguration

- Solche Server werden jedoch relativ schnell von Email-Providern geblockt („Blacklisting“)

■ **Verwendung sehr ähnlich aussehender Domänenamen**

- Bössartiger Versender registriert Email-Domäne, die einer vertrauenswürdigen Domäne zum Verwechseln ähnlich sieht, z.B.
 - uni-potsdarn.de anstatt uni-potsdam.de

■ ...

Gegenmaßnahmen

■ **Signieren** von Emails

- Nur legitimer Sender besitzt privaten Schlüssel für Erzeugung von Signatur und kann so mit Hilfe seines öffentlichen Schlüssels erkannt werden

■ **Misstrauen** gegenüber Nachrichten aus unbekannter Quelle, insbesondere bei Aufforderung ...

- zum Öffnen einer Datei
- zur Eingabe von Nutzerdaten