DuD
Datenschutz und Datensicherheit

Spoofing

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

IP-Spoofing

Unter „*spoofing*" (wörtlich: „Schwindeln") werden Angriffe verstanden, die darauf beruhen, daß einem Kommunikationspartner etwas vorgetäuscht wird, beispielsweise eine falsche internet protocol (IP) Adresse des Absenders. Dies ist möglich, weil die IP-Adresse sehr leicht in der Rechnerkonfiguration geändert werden kann (*IP spoofing*). Die Knotenrechner des Internet sorgen allerdings dafür, daß die Antwortpakete an den richtigen Rechner zurückgeleitet werden. Es sind jedoch wirkungsvolle „blinde" Angriffe möglich [Bell_96]. Solche, auch Maskerade genannte Angriffe (siehe z.B. [DaFS_96]) nutzen das Fehlen wirksamer Authentizitätsmechanismen zum Nachweis der Identität der Gegenstelle in den verwendeten Kommunikationsprotokollen – ein zentrales Sicherheitsproblem im Internet.

Eine besonders wirkungsvolle Klasse von *spoofing*-Angriffen sind solche, die nicht die IP-Adresse fälschen, sondern eine falsche als vermeintlich korrekte Adresse unterschieben. Ein solcher Angriff ist möglich auf Dienste wie WWW und FTP, die statt der IP-Adresse einen leichter zu merkenden symbolischen Namen, z.B. „www.dud.de" verwenden.

Diese Dienste nutzen den *domain name service* (DNS) des Internet, der dem symbolischen Namen eines Internet-Rechners dessen weltweit eindeutige, numerische IP-Adresse, z.B. „193.189.250.196", zuordnet. DNS-Anfragen richtet das Anwendungsprogramm (z.B. ein WWW-Browser) an den in der TCP/IP-Konfiguration des Rechners eingestellten *name server* (DNS-Server). DNS-Server sind im Internet verteilt; sie dürfen nur für ihren eigenen Bereich (Domäne) eine verbindliche Zuordnung vornehmen. Anfragen nach einem entfernten Rechner leiten sie an den zuständigen DNS-Server weiter. Dessen Antwort wird in der Regel für eine begrenzte Zeit in einem *Cache* gespeichert, damit bei weiteren Anfragen keine erneute Weiterleitung erforderlich ist.

DNS-Spoofing

Weil Authentizitätsmechanismen fehlen, können Antworten auf DNS-Anfragen gefälscht werden (*DNS spoofing*). In dem abgebildeten Beispiel fälscht eine Angreiferin Alice den *Cache*-Eintrag der Adresse „www.y.de" bei einem ausgewählten DNS-Server (bspw. dem eines großen Online-Providers) der Domäne „x.de", indem sie eine DNS-Anfrage stellt und die Weiterleitung an den zuständigen DNS-Server selbst (falsch) beantwortet, bevor dieser reagieren kann. Verspätete Antworten werden von DNS-Servern ignoriert. Bis zur Löschung des *Cache* werden nun Zugriffe auf „www.y.de" von jedem Rechner, der diesen DNS-Server verwendet (z.B. Bob), an die falsche IP-Adresse (d.h. an Alice) umgeleitet, ohne daß es dem „Web-Surfer" auffällt.

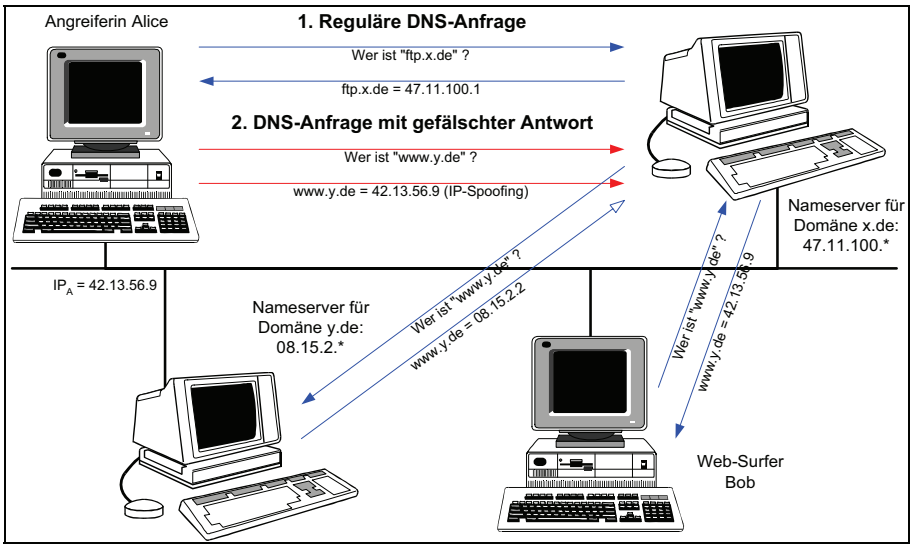

Abb.: Ablauf eines *DNS spoofing*-Angriffs

Im Internet gibt es derzeit keine Gewähr, daß die WWW-Seiten, die man mit seinem Browser sieht, auch tatsächlich vom angegebenen WWW-Server stammen. Auch eine Firewall vor dem DNS-Server hilft nicht, da die Antwort von Alice nicht von der des richtigen DNS-Servers unterschieden werden kann.

Eine einfache Abhilfe ist die Angabe der IP-Adresse statt des symbolischen Namens als URL (z.B. „http://193.189.250.196/dud/dud.htm" statt „http://www.dud.de"). In der Regel kennt man aber die IP-Adresse eines WWW-Servers nicht verläßlich. Auf authentische IP-Adressen wird man warten müssen, bis sich z.B. die Anfang 1997 vorgeschlagenen Erweiterungen des DNS-Protokolls um digitale Signaturen zur Authentisierung der DNS-Antworten durchgesetzt haben [EaKa_97].

Literatur

[Bell_96] Bellovin, S. M.: *Defending Against Sequence Number Attacks*. RFC 1948, May 1996, S. 1-6.

[DaFS_96] Damker, H.; Federrath, H.; Schneider, M. J.: *Maskerade-Angriffe im Internet*. DuD 5/96, S. 286-294.

[EaKa_97] Eastlake, D.; Kaufmann, C.: *Domain Name System Secury Extensions*. RFC 2065, January 1997.