

Informatik-Doppelstunde: Sicherheit des Domain Name System

Lehrender:	NN
Mentor:	NN
Ort:	NN
Datum:	20.04.2007
Zeit:	7.45 – 9.20 Uhr
Reihenthema:	Anwendungen und Funktionsweise des Internets
Stundenthema:	Logische Struktur des Internets und DNS-Sicherheit

1 Betroffene Entscheidungen

1.1 Thematischer Zusammenhang

Der Unterricht findet im Rahmen einer neunwöchigen Unterrichtssequenz zum Thema Internetworking statt. In den ersten zwei Woche wurden das Client-Server-Prinzip, Protokolle der Aufbau des Internets und IP-Adressierung thematisiert.

In der dritten Woche geht es um die Adressierung im Internet mit Domainnamen. Dazu sollen folgende Lernziele thematisiert werden:

Die Schülerinnen und Schüler

- S1 können die logische Struktur des Internet, die durch die Namensräume des Domain Name System (DNS) gebildet wird, beschreiben.
- S2 sind sich Angriffsmöglichkeiten, die durch das DNS bestehen, bewusst.

1.2 Ziele der Doppelstunde

Um mögliche Bedrohungen im Internet, die durch das DNS bedingt sind, zu verstehen, ist es notwendig den Ablauf zur Auflösung eines Domainnamens zu verstehen. Grundsätzlich werden dabei rekursive und iterative Anfragen unterschieden. Daran wird deutlich, dass i.d.R. mehrere DNS-Server an diesem Vorgang beteiligt sind. Mit dem wichtigen Konzept des DNS-Caching wird deutlich, dass es ausreicht, die Daten eines Servers zu manipulieren, der in die Namensauflösung involviert ist. Die Vertrauenswürdigkeit eines Abfrageergebnisses hängt also davon ab, ob alle beteiligten Server vertrauenswürdig sind. Es reicht nicht alleine aus, dass der DNS-Server der gesuchten Domain zuverlässige Auskunft erteilt. In der zweiten Stunde geht es daher um folgende Teillernziele:

Die Schülerinnen und Schüler

- L1 können den Ablauf einer DNS-Abfrage beschreiben.
- L2 können DNS-Caching erklären.

1.3 Hausaufgaben

Als Hausaufgabe bekommen die Lernenden den Auftrag, den iterativen Ablauf einer DNS-Namensauflösung mit Caching in einer Grafik darzustellen (Grafik ist zu vervollständigen).

1.4 Geplanter Unterrichtsverlauf

Zeit	Dauer	Phase	Teilziel	Inhalt	Methode	Medien
1. Stunde						
7.45	10'			Besprechung einer Schülerlösung der Hausaufgabe - Anschreiben eines ausgelesenen Domainnamens und Markierung der Lese- richtung im Baum - Ergänzung des Baums um die Domainnamen aus Aufgabenstellung - Ergänzung der Lösung um den Begriff Top-Level-Domain	SV, UG	OHP
7.55	10'			Ausgabe und Besprechung Aufgabe 2, AB4 - Gegenüberstellung hierarchische Strukturierung von Telefonbucheinträgen und DNS an Folie mit Baumdarstellung - Unterscheidung von Blättern und inneren Knoten - Zuordnung von DNS-Servern zu inneren Knoten	UG	AB, OHP
8.05	5'		L2	- Aufgabe 2, AB4 bearbeiten	GA	AB
8.10	5'	Ergebnissi- cherung		Besprechung der Lösung zu Aufgabe 2 (mit FO1) - Beginn mit Top-Level-Domain - verschiedene Auskünfte: Nameserver und IP-Adressen	UG	OHP
8.15	15			Eigenschaften DNS an Tafel sammeln (TB1) - Übersetzung von Domainnamen in IP-Adressen - DNS-Server sind für Bereiche (Domains) verantwortlich - Bereiche (Domains) sind hierarchisch strukturiert Beschreibung zu DNS an Tafel aufschreiben	UG	TA

2. Stunde						
8.35	15'	Zielorientierung		Raumwechsel DNS-Spoofing / Anzeigen einer falschen Webseite bei Eingabe eines bekannten Domainnamens (Manipulation der Datei c:\windows\system32\drivers\etc\hosts) „Wie kann es sein, dass unter dem Domainnamen die falsche Webseite angezeigt wird?“ → In dieser Stunde geht es darum, wie der Ablauf zur Bestimmung eines Domainnamens im Internet aussieht. - Demonstration zur Verwendung von nslookup	LV	CO
8.50	20'	Erarbeitung	L3, L4	- Experimente mit nslookup Raumwechsel	SE, GA	AB, CO
9.00	10'			- Besprechung der Ergebnisse (mit grafischer Darstellung des Ablaufs) - Unterschied zwischen angezeigtem Pfad zur Domainnamensauflösung und manueller Auflösung - Was ist lokaler, autoritativer DNS-Server? → DNS-Caching	SV	OHP
<i>voraussichtliches Ende des Unterrichts</i>						
	10'	Ergebnissicherung	L3, L4	Als Hausaufgabe bekommen die Lernenden den Auftrag, den iterativen Ablauf einer DNS-Namensauflösung mit Caching in einer Grafik darzustellen (Grafik ist zu vervollständigen).	EA	AB

Methoden:

DE: Demonstrationsexperiment

EA: Einzelarbeit

GA: Gruppenarbeit

LV: Lehrervortrag

SE: Schülerexperiment

SV: Schülervortrag

UG: Unterrichtsgespräch

Medien:

Gestaltung: S. Freischlad, P. Stupperich, S. Warkentin

AB: Arbeitsblatt
OHP: Overhead-Projektor

CO: Computer
TA: Tafel

CP: Computerprojektion
TB: Tafelbild

FO: Folien

2 Begründung zentraler didaktischer Entscheidungen

2.1 Lerngruppe

Der Kurs besteht aus 3 Schülerinnen und 21 Schülern. In diesem Schuljahr hat der Informatikkurs begonnen. Bisher wurde objektorientierte Programmierung mit Java und dem Konzept zu „Stiften und Mäusen“ und BlueJ im Unterricht behandelt. Dazu wurden bereits Klassendiagramme mit verschiedenen Beziehungen behandelt. Außerdem wurde eine Unterrichtsreihe zum Thema endliche Automaten durchgeführt. In einer Stunde wurden zudem Kenntnisse zum Binärsystem wiederholt.

2.2 Begründung der Inhalte

Das Domain Name System stellt einen wichtigen Teil des Internets dar, der durch den Anwender sichtbar ist. Durch die verteilte Datenbank, die als ein sehr wichtiger Vorzug des DNS anzusehen ist, bietet insbesondere DNS-Caching eine besondere Gefährdung. Ein Angriff muss nicht zwingend auf die Manipulation einer bestimmten Datenbank erfolgen. Vielmehr reicht es häufig aus, die Daten eines DNS-Servers zu manipulieren, um das System zu kompromittieren.

2.3 Begründung des Lernweges

Die Stunde beginnt damit, dass ein bekannter Domainname in einem Webbrowser eingegeben wird. Es erscheint aber nicht die erwartete Webseite sondern eine offensichtlich falsche Seite. Um diese Beobachtung erklären zu können, ist es notwendig, den Ablauf zur Auflösung eines Domainnamens etwas genauer zu untersuchen.

Die Schülerinnen und Schüler beschreiben dazu eine Hypothese, wie die Auflösung eines Domainnamens zu einer IP-Adresse abläuft und führen ein Experiment mit nslookup durch. Dazu sollen sie gezielt durch die Abfrage von Datensätzen des Typs NS bzw. A die Auflösung verschiedener Domainnamen manuell durchführen. Im daran anschließenden Unterrichtsgespräch werden iterative und rekursive Anfragen sowie der Einsatz lokaler DNS-Server besprochen.

3 Literatur

- [BSI] Bundesamt für Sicherheit in der Informationstechnik: Beispiele für Gefährdungen im Internet. DNS-Spoofing.
URL: <http://www.bsi.de/fachthem/sinet/gefahr/vulner/index.htm> (06.03.2007).
- [Claus/Schwill, 1997] Claus, V.; Schwill, A.: Schülerduden Informatik. Ein Lexikon zum Informatikunterricht. 3. Auflage, Dudenverlag, Mannheim, 1997.
- [Kurose/Ross, 2002] Kurose, J. F.; Ross, K. W.: Computernetze. Pearson Studium, München, 2002, S. 137-148.
- [Peterson/Davie, 2004] Peterson, L. L.; Davie, B. S.: Computernetze. Eine systemorientierte Einführung. Deutsche Ausgabe der 3. amerikanischen Auflage, dpunkt, Heidelberg, 2004, S. 636-642
- [Schneier, 2004] Schneier, B.: Secrets & Lies. IT-Sicherheit in einer vernetzten Welt. dpunkt.verlag, Heidelberg, 2004, S. 173f.