

Informatik-Einzelstunde: Signatur und Zertifikate

Lehrender:	NN
Mentor:	NN
Ort:	NN
Datum:	06.06.2007
Zeit:	11.25 – 12.10 Uhr
Reihenthema:	Anwendungen und Funktionsweise des Internets
Stundenthema:	Zertifikate

1 Betroffene Entscheidungen

1.1 Thematischer Zusammenhang

Die Schülerinnen und Schüler

- S1 können mit Hilfe der elektronischen Signatur authentische E-Mails versenden.
- S2 können die Authentizität einer signierten Nachricht bewerten.
- S3 verstehen wie Autorisation mit Hilfe von Zertifikaten im Kontext von DRM umgesetzt wird.

1.2 Ziele der Einzelstunde

Die Schülerinnen und Schüler

- L1 können erklären, was ein Zertifikat ist.
- L2 können den Aufbau eines Zertifikats erklären.

1.3 Hausaufgaben

1.4 Geplanter Unterrichtsverlauf

Zeit	Dauer	Phase	Teilziel	Inhalt	Methode	Medien
------	-------	-------	----------	--------	---------	--------

1. Stunde						
	5'	Einleitung		<p>Wiederholung: Zusammensetzung einer signierten Nachricht</p> <p>In der vorangegangenen Stunde wurde aufgezeigt, wie vertrauliche Kommunikation durch den Man-in-the-middle-Angriff kompromittiert werden kann. In dieser Stunde soll es darum gehen, ob die Authentizität in ähnlicher Weise kompromittiert werden kann.</p> <p>Außerdem wollen wir uns ansehen, welche Möglichkeiten es gibt, diesen Man-in-the-middle-Angriff auszuschließen.</p>	UG	TA
	5'	Erarbeitung		Bearbeitung einer Aufgabe zum Man-in-the-middle-Angriff mit digitaler Signatur (Aufgabe 1)	EA	AB
	10'			Besprechung der Aufgabe und Erarbeitung Begriff Zertifikat mit Analogie Ausweis	UG	OHP
	10'			Begriffsverallgemeinerung Authentizität und Vertraulichkeit	UG	TA
	5'	Ergebnissi-		Überleitung zur Authentizität von Webseiten	LV	

	15'	cherung	Bearbeitung einer Aufgabe zu Zertifikaten für Hypertext Transfer Protocol Secure (HTTPS) Untersuchen der zwei folgenden Webseiten auf Ihre Authentizität: - https://www.elster.de - http://vu.fernuni-hagen.de mögliche Fragen: <ul style="list-style-type: none"> • Wie bewertet der Webbrowser die Sicherheit dieser Webseiten? • Welche Angaben sind in den Zertifikaten aufgeführt? • Sehen Sie sich die Zertifikate an, die vom Webbrowser gespeichert werden und suchen Sie das Zertifikat von VeriSign. Wie lange ist es gültig? 	DE / UG	CO
--	-----	---------	--	---------	----

Methoden:

DE: Demonstrationsexperiment
 SE: Schülerexperiment

EA: Einzelarbeit
 SV: Schülervortrag

GA: Gruppenarbeit
 UG: Unterrichtsgespräch

LV: Lehrervortrag

Medien:

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 Thema der digitalen Unterschrift oder elektronischen Signatur und das Thema Zertifikat begegnen einem Anwender immer wieder im Umgang mit vernetzten Informatiksystemen. Bei der Installation von Software wird darauf hingewiesen, wenn die Software nicht durch Microsoft zertifiziert wurde. Beim Besuch von Webseiten, die eine Authentisierung des Servers im Zusammenhang mit vertraulicher Datenübertragung unterstützen, wird danach gefragt, ob das Zertifikat akzeptiert werden soll. Es kann aber auch vorkommen, dass ein Zertifikat stillschweigend durch den Webbrowser akzeptiert wird, weil es durch bereits akzeptierte Zertifikate verifiziert werden konnte. Bei der Erzeugung eines Schlüsselpaares für die vertrauliche Kommunikation per E-Mail wird gefragt, ob ein Widerrufszertifikat erzeugt werden soll. Es ist möglich, den öffentlichen Schlüssel eines Bekannten zu verifizieren, indem die Angaben und der Schlüssel signiert werden. Auch im Kontext von Digital Rights Management werden Zertifikate eingesetzt. Um eine begründete Entscheidung treffen zu können, ob beim Webseitenabruf ein Zertifikat akzeptiert wird oder nicht, ist es notwendig zu verstehen, was sich dahinter verbirgt.

2.3 Begründung des Lernweges

Voraussetzung für ein Gespräch über Autorisation mit DRM sind folgende Fachkonzepte:

- elektronische Signatur,
- Zertifikat,
- asymmetrische Verschlüsselung,
- symmetrische Verschlüsselung,
- Client-Server-Architektur,
- Rechtevergabe.

Client-Server-Architektur, Verschlüsselungsverfahren und elektronische Signatur werden in vorhergehenden Unterrichtsstunden behandelt. Als neue Konzepte bleiben das Zertifikat und die Rechtevergabe. Eine zusätzliche Schwierigkeit besteht darin, dass Verschlüsselungsverfahren und elektronische Signatur erst einführend im Kontext von E-Mail behandelt wurden. Es muss also ein Transfer erfolgen, wobei die Inhalte den Lernenden noch nicht sehr vertraut sind.

Aus den verschiedenen Bezeichnungen für die elektronische Signatur wurde dieser Begriff gewählt, weil er auch in den deutschen Gesetzestexten verwendet wird:

„Die Begriffe digitale und elektronische Signatur sind weitgehend synonym. In der englischsprachigen Fachliteratur wird der Begriff „Digital Signature“ benutzt (siehe auch DSS). Im Signaturgesetz wird nur der Begriff "elektronische Signatur" verwendet. In der EU-Richtlinie

und im Signaturgesetz wurden die Begriffe einfache und fortgeschrittene elektronische Signatur eingeführt.“ [http://de.wikipedia.org/wiki/Elektronische_Signatur, 08.06.2006]

Zudem wird bei der elektronischen Unterschrift nicht darauf eingegangen, dass in der Praxis ein Hash-Wert der Nachricht signiert wird. Das Prinzip der Authentizität wird auch an dieser vereinfachten Darstellung deutlich.

3 Literatur

[Bless et al., 2005] R. Bless, S. Mink, E.-O. Blaß, M. Conrad, H.-J. Hof, K. Kutzner, M. Schöller: Sichere Netzwerkkommunikation. Grundlagen, Protokolle und Architekturen. Springer, Heidelberg, 2005.

[RFC2440] Request for Comments „OpenPGP Message Format“. 1998. URL: <http://www.ietf.org/rfc/rfc2440.txt> – geprüft: 29.05.2006

[Schneier, 2001] B. Schneier: Secrets & Lies. IT-Sicherheit in einer vernetzten Welt. dpunkt, Heidelberg, 2001.

[Schneier, 2006] B. Schneier: Angewandte Kryptographie. Pearson Studium, München, 2006.