

Informatik-Doppelstunde: Signatur und Zertifikate

Lehrender:	NN
Mentor:	NN
Ort:	NN
Datum:	01.06.2007
Zeit:	7.45 – 9.20 Uhr
Reihenthema:	Anwendungen und Funktionsweise des Internets
Stundenthema:	Signatur und Zertifikate

1 Getroffene Entscheidungen

1.1 Thematischer Zusammenhang

In der vorhergehenden Woche wurden symmetrische und asymmetrische Verschlüsselungsverfahren zur Gewährleistung der Vertraulichkeit eingeführt. Der Sicherheitsdienst Vertraulichkeit wurde im Kontext der Internetanwendung E-Mail mit OpenPGP eingesetzt. Das Problem der Authentizität der verwendeten öffentlichen Schlüssel wurde bisher nicht thematisiert. Ein weiteres Thema der vorangegangenen Wochen war die Problematik, dass die Authentizität von E-Mails nicht durch die verwendeten Protokolle gewährleistet werden kann.

In dieser Woche geht es darum, die asymmetrische Verschlüsselung durch die elektronische Signatur mit dem Problem der Authentifizierung zu verknüpfen. Dies wird zunächst im Kontext der Internetanwendung E-Mail weitergeführt. Dazu wird zunächst der Einsatz der asymmetrischen Verfahren für eine elektronische Signatur betrachtet. Daran schließt sich mit der Frage der Authentizität der öffentlichen Schlüssel die Thematik Zertifikate an. Im Rahmen des dritten Grobziels geht es dann darum, die Thematik der Authentifizierung mit Zertifikaten auf den Bereich der digitalen Rechteverwaltung zu übertragen. Zusätzlich geht es um die Rechteverwaltung und damit insgesamt um das Thema Autorisation.

Die Schülerinnen und Schüler

- S1 können mit Hilfe der elektronischen Signatur authentische E-Mails versenden.
- S2 können die Authentizität einer signierten Nachricht bewerten.
- S3 können Autorisation mit Hilfe von Zertifikaten im Kontext der digitalen Rechteverwaltung erklären.

1.2 Ziele der Doppelstunde

In der Doppelstunde sollen die Schülerinnen und Schüler lernen, wie eine authentische E-Mail mit Hilfe von elektronischer Signatur versendet werden kann und außerdem sollen Sie die Authentizität bewerten können. Dazu müssen sie eine E-Mail signieren können. Wichtiger Unterschied zur symmetrischen Verschlüsselung ist die Verwendung eines privaten und eines öffentlichen Schlüssels. Wie diese Schlüssel zur Gewährleistung von Vertraulichkeit und Authentizität verwendet werden ist notwendig, um die Verfahren sicher anwenden zu können

Um die Authentizität einer elektronisch signierten E-Mail bewerten zu können, müssen die Lernenden erst einmal ein Bewusstsein dafür bekommen, dass die Authentizität gefährdet sein kann. Ein Beispiel dafür ist der so genannte Man-in-the-middle-Angriff. Außerdem müssen

Gestaltung: S. Freischlad

sie mit Zertifikaten einen Lösungsansatz des Problems der Authentizität öffentlicher Schlüssel kennen lernen.

Die Schülerinnen und Schüler

- L1 können eine E-Mail signieren.
- L2 können erklären, wie asymmetrischer Verschlüsselungsverfahren zur Gewährleistung der Vertraulichkeit und Authentizität eingesetzt werden.
- L3 können den Ablauf beim Man-in-the-middle-Angriff erklären.

1.3 Hausaufgaben

1.4 Geplanter Unterrichtsverlauf

Zeit	Dauer	Phase	Teilziel	Inhalt	Methode	Medien
1. Stunde						
	15'	Ergebnissicherung		<ul style="list-style-type: none"> - Besprechung Aufgabe 1 zum Ablauf der Ver- und Entschlüsselung einer vertraulichen Nachricht mit asymmetrischem Verschlüsselungsverfahren - Tabelle mit Eigenschaften symmetrische/asymmetrische Verschlüsselung 	SV / UG	OHP, TA
	5'	Zielorientierung		Außerdem haben wir gesehen, dass es im Prinzip einfach ist, eine Absenderadresse zu fälschen. Wie gewährleistet man, dass ein Brief nicht mit einem falschen Absender verschickt wird? → mit Unterschriften	UG	
	10'	Erarbeitung		Digitale Signatur als Umkehrung der asymmetrischen Verschlüsselung	UG	
	25'			Versand einer signierten Nachricht (Aufgaben 1, 2)	EA	CO
2. Stunde						
	10'			Besprechung Aufgabe 2	UG	FO
	5'	Zielorientierung		Angriffsmöglichkeit Vertauschen des Schlüssels	UG	
	15'	Erarbeitung		Rollenspiel zum Man-in-the-middle-Angriff	SE	
	10'			Bearbeitung zu Aufgaben „Man-in-the-middle-Angriff“ (Aufgabe 3)	EA	AB

	10'	Ergebnissicherung		Besprechung Aufgabe 3	UG	FO
--	-----	-------------------	--	-----------------------	----	----

Methoden:

DE: Demonstrationsexperiment

EA: Einzelarbeit

GA: Gruppenarbeit

LV: Lehrervortrag

SE: Schülerexperiment

SV: Schülervortrag

UG: Unterrichtsgespräch

Medien:

AB: Arbeitsblatt

CO: Computer

CP: Computerprojektion

FO: Folien

OHP: Overhead-Projektor

TA: Tafel

TB: Tafelbild

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

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. Gestaltung: S. Freischlad