Seminar »Aktuelle Entwicklungen in der Kryptographie«

Prof. Johannes Köbler Sebastian Kuhnert

Sommersemester 2010

Die Kryptographie ist ein hoch dynamisches Feld: Die eingesetzten Verfahren werden beständig weiterentwickelt, um ihre Sicherheit und ihren Ressourcenverbrauch zu verbessern. Diese Entwicklung wird nicht zuletzt durch immer bessere Angriffe erforderlich – und auch stimuliert. So haben beispielsweise neue Angriffe auf MD5 und SHA-1 sowie die SHA-2-Familie die Suche nach neuen sicheren Hashfunktionen angestoßen. In diesem Seminar werden wir uns mit Kandidaten für SHA-3 beschäftigen, die derzeit in einem öffentlichen Verfahren geprüft werden.

Einen weiteren Schwerpunkt des Seminars werden kryptographische Protokolle bilden. Dabei werden wir der Frage nachgehen, wie aus persönlichen Interaktionen gewohnte Sicherheitseigenschaften durch Kryptographie auch für digitale Kommunikation realisiert werden können. Mit modernen Verfahren können dabei sogar Ziele erreicht werden, die in der analogen Welt unerreicht bleiben.

Themengebiete für Referate

1. **Angriffe auf MD5 und SHA-1**
   Diese weit verbreiteten Hashfunktionen haben sich als unsicher herausgestellt.

   Inhalt: Welche allgemeinen Angriffe auf Hashfunktionen sind bekannt? Wie funktionieren MD5 und SHA-1, und wie sehen die besten bekannten Angriffe aus?

   Literatur: http://dx.doi.org/10.1007/11535218_26
   http://eprint.iacr.org/2006/105.pdf
   http://dx.doi.org/10.1007/11535218_2

2. **Kandidaten für SHA-3**
   Derzeit läuft der Wettbewerb für einen neuen Standard für sichere Hashfunktionen.

   Inhalt: Einige der Kandidaten vorstellen. Wie arbeiten sie? Worauf stützt sich ihre Sicherheit?

   Literatur: http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

3. **Kryptographische Protokolle**
   Von vielen kryptographischen Protokollen ist bekannt, dass sie sich unter bestimmten Annahmen mithilfe anderer Protokolle realisieren lassen.

   Inhalt: Was sind Einwegfunktionen? Was ist Oblivious Transfer? Wie lassen sich kryptographische Protokolle aufeinander reduzieren? Welche unterschiedlichen Welten sind in Hinblick auf die Existenz kryptographischer Protokolle möglich?

   Literatur: http://eccc.hpi-web.de/report/2009/123/

Ablauf

- In der ersten Woche stellen wir euch die Referatsthemen vor und ihr wählt euer Thema aus. Außerdem geben wir euch Hinweise zur Gestaltung von Referaten und Ausarbeitungen.
- Im Lauf des Semesters haltet ihr **Referate**
  - Die Referate haben das Ziel, dass ihr (a) euch ein Thema erarbeitet, (b) euer Thema den anderen vermittelt, (c) von den Referaten der anderen lernt und (d) Vortragspraxis sammelt.
  - Einerseits sollen eure Referate *anschaulich* sein: Ihr führt die anderen in euer Thema ein. Bitte setzt dabei nicht mehr voraus, als sie schon wissen. Mit Beispielen und Bildern könnt ihr euren Zuhörern das Verstehen erleichtern. Eine gute Richtschnur für gute Erklärungen ist die Frage »Was hat mir selbst geholfen, das zu verstehen?«
  - Andererseits sollen eure Referate auch *präzise* sein: Klare Definitionen und die Details von Konstruktionen und Algorithmen gehören auch dazu.
  - Für euer Referat stehen euch ca. 90 Minuten zur Verfügung. Bitte plant Zeit für Rückfragen ein!
- **Vorbereitung** des eigenen Referats:
  - Ihr arbeitet euch in das Thema ein, indem ihr die angegebene (und ggf. weitere) Literatur lest. Literatur, die es nicht in der Bibliothek oder im Netz gibt, kann bei uns kopiert werden.
  - Vor der Vorbereitung des Vortrags lest ihr am besten [Tan07, Abschnitt 5] – das lohnt sich auch dann, wenn ihr nicht LaTeX verwendet.
  - Eine Woche vor dem Referat kommt ihr in unsere Sprechstunde, um letzte Verständnisfragen zu stellen und den Ablauf des Referats durchzusprechen.
- Es ist ein zentrales Element eines Seminars, auch von den Referaten der anderen zu lernen. Deshalb solltet ihr möglichst immer **anwesend sein**. Wenn ihr mehr als einmal fehlt, zeigt uns bitte unaufgefordert ein Attest.
- Nach dem Referat fertigt ihr noch eine schriftliche **Ausarbeitung** zu eurem Thema an.
  - Die Ausarbeitungen haben das Ziel, (a) das im Seminar gesammelte Wissen zusammenzufassen, (b) Interessierten einen Einstieg in euer Thema zu ermöglichen und (c) euch die Gelegenheit zu geben, wissenschaftliches Schreiben zu üben (Vorbereitung auf Studien- und Diplomarbeit).
  - Wir werden eure Ausarbeitungen auf der Webseite des Seminars veröffentlichen, wenn ihr damit einverstanden seid.
  - Eure Ausarbeitung sollte ungefähr 10-20 Seiten umfassen.
  - Hinweise zum wissenschaftlichen Schreiben findet ihr unter [Böt06] und [Mit07].

Literatur

[Böt06] Martin Böttcher. *Einführung in das wissenschaftliche Arbeiten.* Universität Leipzig. 2006. URL: http://bis.informatik.uni-leipzig.de/de/Lehre/0506/SS/SemASKE/files?get=einfuehrung_in_das_wiss_arbeiten.pdf (besucht am 12. Apr. 2010).

[Mit07] Roland Mittermair. *Hinweise für korrektes Zitieren.* Institut für Informatik-Systeme, Universität Klagenfurt. 2007. URL: http://www.uni-klu.ac.at/tewi/downloads/Zitierhinweise.pdf (besucht am 12. Apr. 2010).

[Tan07] Till Tantau. *The* BEAMER *class.* Version 3.07. 2007. URL: http://mirror.ctan.org/macros/latex/contrib/beamer/doc/beameruserguide.pdf (visited on Apr. 12, 2010).