Informationen zum Seminar „IT-Sicherheit“ des Lehrstuhls für Embedded Security

Wichtige Termine

Do. 06.11.2008, 16h:	**Vorbesprechung in IC 4/161**
Fr. 05.12.2008:	**Abgabe des Expose**
Mi. 11.02.2009:	**Endversion der schriftlichen Ausarbeitung**
Mi. 25.02.2009:	**Finale Endversion der schriftlichen Ausarbeitung**
Di. 10.03.2009:	**Wikipedia-Eintrag**
Mi. 11.03.2009, 10-16h:	**Präsentationen aller Seminarteilnehmer in IC 4/39**

Allgemeine Hinweise
Dieses Semester hat das ITS-Seminar das folgende Überthema:

„Modes of Operation for Block Ciphers and Hash Functions“.

Zusätzlich zur schriftlichen Ausarbeitung, der Präsentation und einem Wikipedia-Eintrag wird das Expose zum festen Bestandteil der Seminarleistung. Das Seminar wird dieses Semester etwas strukturierter ablaufen.

Templates für die schriftliche Ausarbeitung und die Vortragsfolien sind unter www.crypto.rub.de verfügbar. Dort findet ihr auch einige von uns zusammengestellte Tipps, u.a. zum Schreiben in englischer Sprache und dem Halten von Vorträgen.

Vorbesprechung
Während der Vorbesprechung stellen die Betreuer ihre Themen kurz vor. Anschließend werden die Themen (und damit auch die Betreuer) Interessenten zugeordnet. Jeder Interessent bekommt zuerst eine individuelle Nummer. Mithilfe eines Zufallszahlengenerators werden die verteilten Nummern in einer zufälligen Reihenfolge aufgelistet. In dieser Reihenfolge können die entsprechenden Interessenten dann jeweils ein Thema aus der vorgegebenen Themenliste auswählen.

Expose
4 Wochen nach der Vorbesprechung (also spätestens am **05.12.2008**) müssen alle Teilnehmer ein schriftliches Expose bestehend aus

a) einseitigem Abstract in dem eine Übersicht über das Thema und den Bezug zum Oberthema gegeben werden soll,
b) Grobgliederung der Ausarbeitung,
c) Literaturangaben

an den jeweiligen Betreuer abgeben. Dieses Expose wird bewertet und geht mit *10%* in die Endbewertung ein. Sollte der Termin nicht eingehalten werden, so hat der entsprechende Seminarist eine weitere Woche Zeit (bis **12.12.2008**) das Expose nachzuliefern, allerdings bekommt er hierfür **0 Pt**. Bei Nicht-Einreichung bekommt der Teilnehmer keinen Schein.

Schriftliche Ausarbeitung
Die Ausarbeitung soll in Latex angefertigt werden, einen Umfang von ca. 15 Seiten haben und in *englischer* Sprache geschrieben sein (deutsch nur in Ausnahmefällen). Wer sich noch nie mit Latex befasst hat, findet unter de.wikipedia.org/wiki/LaTeX viele nützliche Hinweise. 4 Wochen vor dem Blockseminar-Termin (also spätestens am **11.02.2009**) muss die Endversion der schriftlichen Ausarbeitung abgegeben werden. Dies ist ein fixer Termin. Bei Nicht-Einreichung erhält der Teilnehmer keinen Schein. Die schriftliche Ausarbeitung muss an den jeweiligen Betreuer per E-Mail gesendet werden. 2 Wochen vor dem Blockseminar-Termin (also spätestens am **25.02.2009**, bei Nicht-Einreichung bekommt der Teilnehmer keinen Schein) ist die finale Endversion der schriftlichen Ausarbeitung fällig, in welcher der Seminarteilnehmer die Kommentare seines/ihres Betreuers zu der Endversion adressieren muss. Diese finale Endversion muss an den jeweiligen Betreuer und Andrey Bogdanov (abogdanov@crypto.rub.de) per E-Mail geschickt werden. Wer diesen Termin nicht einhält oder die Kommentare des Betreuers nicht einarbetet, bekommt keinen Schein. Diese finale Endversion der schriftlichen Ausarbeitung wird vom Betreuer bewertet und geht mit *50%* in die

Endbewertung ein.

Wikipedia-Eintrag
Eine Kurzfassung (ca. eine DIN-A4 Seite, auf jeden Fall in englisch) der schriftlichen Ausarbeitung soll ins englische Wikipedia eingepflegt werden. Dazu bitte einen Benutzernamen anlegen und alle Änderungen mit diesem Benutzernamen vornehmen. Als weiterführende Literatur bitte stets eure Seminarausarbeitung angeben, die auf unserer Webseite unter http://www.crypto.rub.de/its_seminar_ws0809.html verfügbar ist. In die Revision-History bitte stets das folgende Kommentar eingeben: „This contribution is a result of the seminar 'Modes of Operation for Block Ciphers and Hash Functions' which was held at the chair for communication security at the Ruhr-University Bochum, Germany“. Der Wikipedia-Eintrag muss bis zum **10.03.2009** gemacht worden sein und geht mit *10%* in die Note ein, sonst bekommt der Teilnehmer keinen Schein.

Präsentation der Ergebnisse
Die Abschluß-Präsentation setzt sich aus ca. 20 Minuten Vortrag und anschließenden 5 Minuten für Fragen zusammen. Bitte mit Eurem Betreuer einen Termin für den Probevortrag absprechen. Auf den Folien bitte unbedingt den Weblink für den Wikipedia-Eintrag angeben. Der Vortrag wird vom jeweiligen Betreuer bewertet und geht mit *30%* in die Note ein.

Wer weniger als *75%* hat, bekommt keinen Schein.

Sollten noch Fragen bestehen, einfach eine eMail mit Betreff „ITS-Seminar WS0809“ an abogdanov@crypto.rub.de schreiben.

Themenliste

Thema	Betreuer	Interessent
Building Stream Ciphers From Block Ciphers and Their Security (CTR, OFB, CFB, etc.)	Axel Poschmann	Christoph Hudde
CBC Mode and Its Security (Content Leak, Data Modification Leak, etc.)	Timo Kasper	Armand Ngaleu
Authenticated Encryption Modes of Block Ciphers, Their Security and Implementation Properties (GCM, CCM*, etc.)	Axel Poschmann	Hequn Chen
Message Authentication Codes Using Hash Functions, Their Security and Implementation Properties (HMAC, NMAC, etc.)	Markus Kasper	Dennis Ptasik
Pseudorandom Number Generators Using Block Ciphers and Hash Functions, Their Security and Implementation Properties (BSI AIS20, ANSI X9.17, etc.)	Timo Kasper	Daniel Höttges
Building Hash Functions from Block Ciphers, Their Security and Implementation Properties (Davies-Meyer, Miyaguchi-Preneel, Hirose, etc.)	Thomas Eisenbarth	Timo Bartkewitz
Symmetric Key Management: Key Derivation and Key Wrap	Thomas Eisenbarth	Özlem Sönmez