Informationen zum Seminar IT-Sicherheit des Lehrstuhl für Kommunikationssicherheit

Wichtige Termine

Mi. 25.04.2007, 12h:	**Vorbesprechung in Raum IC 4/39**
Fr. 13.07.2007:	**Abgabe der schriftlichen Ausarbeitung**
Di. 24.07.2007, 10-16h:	**Präsentationen aller Seminarteilnehmer in IC 4/39**

Allgemeine Hinweise
Beginnend mit diesem Semester ergeben sich zwei grundlegende Änderungen im Vergleich zu vergangenen Seminaren:

1) alle zu vergebenen Themen werden aus einem Themengebiet stammen. Dieses Semester dürft ihr euch auf **„Security in Mobile Radio“** (Themen s. Seite 2) freuen.
2) erstmalig wird zusätzlich zur schriftlichen Ausarbeitung und der Präsentation ein Wikipedia-Eintrag in englischer Sprache fester Bestandteil der Seminarleistung.

Templates für die schriftliche Ausarbeitung und die Vortrags-Folien 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. Wenn sich mehrere Interessenten für ein Thema finden, entscheidet das Los. Außerdem habt ihr die Möglichkeit weitergehende Fragen zum Ablauf etc. zu stellen.

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). Alle Ausarbeitungen werden auf unserer Webseite veröffentlicht. Wer sich noch nie mit Latex befasst hat findet unter de.wikipedia.org/wiki/LaTeX viele nützliche Hinweise.
Achtung: wer seine Ausarbeitung nicht bis zum 13. Juli seinem Betreuer per eMail geschickt hat bekommt keinen Seminarschein!

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 www.crypto.rub.de/its_seminar_ss07.html verfügbar ist. In die Revision-History bitte stets das folgende Kommentar eingeben: „This contribution is a result of the seminar 'Security in Mobile Radio' which was held at the communication security chair at the Ruhr-University Bochum, Germany“.

Präsentation der Ergebnisse
Die Abschluß-Präsentation setzt sich aus 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.

Sollten noch Fragen bestehen, einfach eine eMail mit Betreff „Seminar-07“ an poschmann@crypto.rub.de schreiben.

Themenliste zum Thema „Security in Mobile Radio“

Thema	Betreuer	Interessent
~~Cryptanalysis of KASUMI~~	~~Andrey~~	~~Oliver Grieb~~
Data Security in 4G Networks	Andrey	Xiaofeng Lou
Cryptanalysis of TIA's "Common Cryptographic Algorithms" (CMEA, ORYX, CAVE)	Andy	Haipeng Wu
Hardware-assisted Attacks on A5/1	Andy	Marc Schober
Location Based Services – Bug or Feature?	Axel	Michael Pridat
Crypto Phones	Axel	Zidu Wang
Security in WAP 1.x and WAP 2.0	Bodo	Chen Zhang
~~Trusted Computing for Mobile Platforms~~	~~Marko~~	
Bluetooth Security & Hacks	Tim	Andreas Becker
~~Security Analysis of Java VM in Cell Phones~~	~~Tim~~	~~Michael Zilbermann~~
Near Field Communication in Cell Phones	Timo	Annika Paus
Cell Phone Forensics	Timo + Marko	Lars Wolleschensky
IMSI Catcher	Thomas	Daehyun Strobel
SIM Card Security	Thomas	Sheng He