Seminar Kommunikation und Multimedia

"Network Security"
"Advanced Network Security"

Institut für Betriebssysteme und Rechnerverbund
Technische Universität Braunschweig

14.04.2010

Ablauf

Organisation

- 12 – 15 Seiten Ausarbeitung
- 20 Minuten Vortrag
- Jeder Teilnehmer muss zwei andere Arbeiten begutachten
- Zu jeder Arbeit werden zwei Gutachten erstellt
- Gutachten dienen zur Verbesserung der eigenen Arbeit
- Mailingliste aller Teilnehmer (`skm@ibr.cs.tu-bs.de`)

Reviews - Gutachten

- Verbreitete Qualitätssicherungsmaßnahme in der Wissenschaft
- Feedback, Verbesserungsvorschläge, Lob, Kritik
- Gutachten werden anonym erstellt
- Optional: Gutachter gibt Scan/PDF mit Anmerkungen ab
- Arbeiten zur Begutachtung können optional anonymisiert eingereicht werden
- Gutachten haben keinen Einfluss auf die Bewertung der Arbeit

Zeitplan

26.04.2010, 16:00 Uhr	Abgabe einer ersten Gliederung
17.05.2010, 16:00 Uhr	Abgabe der ersten vollständigen Ausarbeitung
31.05.2010, 12:00 Uhr	Abgabe der vollständigen Ausarbeitung
31.05.2010, 17:00 Uhr	Ausgabe Ausarbeitung für die Reviews an die Teilnehmer
07.06.2010, 12:00 Uhr	Abgabe der Reviews durch die Teilnehmer
07.06.2010, 17:00 Uhr	Ausgabe der Reviews an die Teilnehmer
21.06.2010, 16:00 Uhr	Abgabe der finalen Ausarbeitung
28.06.2010, 16:00 Uhr	Abgabe einer ersten Version der Folien
05.07.2010, 16:00 Uhr	Abgabe der finalen Folien
07.07.2010, 08:30 Uhr	Blockveranstaltung mit Vorträgen (IZ Raum 105)

Ausarbeitung (1/3)

Gliederung

- Titel
- Kurzfassung
- Einleitung
- Weitere Kapitel der Arbeit
- Zusammenfassung
- Literaturverzeichnis

Ausarbeitung (2/3)

Layout

- DIN A4
- 12 - 15 Seiten
- Schriftgröße 11 - 12 pt, Text 1-zeilig, Blocksatz
- Ränder nicht unter 2 cm
- Kapitel nummeriert
- Seitenzahlen auf jeder Seite
- Keine separate Titelseite, kein Inhaltsverzeichnis
- Wenn LaTeX, dann Style `article` oder `scrartcl`
- Abgabe als PDF-Dokument

Ausarbeitung (3/3)

Mindestanforderungen

- Verständliche und korrekte deutsche oder englische Sprache
- Klare und sinnvolle Struktur
- Eigene Formulierungen
- Keine kopierten oder übersetzten Passagen!!!
- Layout gemäß Anforderungen

Ausarbeitung (3/3)

Mindestanforderungen

- Verständliche und korrekte deutsche oder englische Sprache
- Klare und sinnvolle Struktur
- Eigene Formulierungen
- Keine kopierten oder übersetzten Passagen!!!
- Layout gemäß Anforderungen

Arbeiten, die diese Mindestanforderungen nicht erfüllen, nehmen nicht am Review-Prozess teil und und können nicht gewertet werden.

Präsentation

- 20 Minuten Vortrag
- 5 – 10 Minuten Fragen und Diskussion
- Aktive Teilnahme an Diskussionen
- Folienvorlagen auf der Webseite
- Vorlagen nicht zwingend

Wo finde ich Quellen und Literatur?

- ACM Digital Library - `http://www.acm.org/dl`
- IEEE Xplore - `http://ieeexplore.ieee.org`
- Citeseer - `http://citeseer.ist.psu.edu`
- Google Scholar - `http://scholar.google.com`

Weiteres Vorgehen

- Einlesen in die Literatur
- Recherche nach weiteren Quellen
- Aufstellen einer ersten Gliederung
- Absprache mit dem Betreuer

Mailingliste: `skm@ibr.cs.tu-bs.de`

Weitere Informationen unter

http://www.ibr.cs.tu-bs.de/courses/ss10/skm-ba

http://www.ibr.cs.tu-bs.de/courses/ss10/skm-ma

Fragen?

Themenvorstellung Bachelor

5 Themen

B1: Sicherheitsaspekte in Body-Area-Networks

BAN nimmt Vitalparameter auf

- EKG, Temperatur, Blutdruck, etc.
- Daten privat und intim
- Daten Sicherheitsrelevant, z.B. Alarm bei Herzstillstand

In dieser Seminararbeit:

- Grundlegende Datenschutzanforderungen und - Möglichkeiten in BANs aufzeigen
- Mögliche Einschränkungen erläutern
- Beispiele aus der Praxis vorstellen

B2: Sicherheit in eduroam

eduroam

- EDUcation ROAMing
- ermöglicht weltweites WLAN Roaming an allen teilnehmenden Einrichtungen (derzeitig hauptsächlich in Europa und Asien)

In dieser Seminararbeit:

- Funktionsweise des eduroam
- Betrachtung der Sicherheitsaspekte
  - Zugangsauthentifizierung (RADIUS, 802.1x)
  - Zertifikate, Verschlüsselungen, ...
  - Besucher im lokalen Netz
  - Zugriff auf Heimatnetzwerk

B3: Sicherheit durch Zeitsynchronisation

- Sicherheitsmechanismen zur Wahrung von Authentizität und Privatsphäre
- Häufig von synchronisierten Uhren abhängig
- Angriff auf die Mechanismen zur Synchronisierung

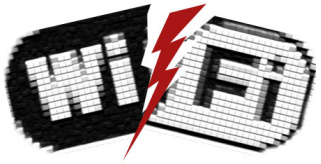
In dieser Seminararbeit:

- Betroffene Sicherheitsmechanismen vorstellen
- Vor- und Nachteile dieser Designentscheidung
- Mögliche Angriffszenarien

B4: Bluetooth vs. ZigBee

- Vorstellung Bluetooth
- Schwerpunkt Sicherheit
- Gibt es Schwachstellen / Angriffsmöglichkeiten ?
- Vorstellung ZigBee
- Vergleichbar mit Bluetooth?
- Sicherheit bei ZigBee

B5: Security and threats in WiFi network (Jian Li)



- The security technologies used in current WiFi networks: WEP, WPA, WPA2,...
- Do they security enough to protected the WiFi network? What kind of weakness do they have.
- Currently how to crack a WiFi protected by these security technologies.
- How to increase the security of WiFi network.

Themenvorstellung Diplom/Master

4 Themen

M1: Sicherheit in unterbrechungstoleranten Netzen

Delay Tolerant Networks (DTNs)

- Robust gegen Unterbrechungen
- Keine Ende-zu-Ende Verbindung
- Store-and-Forward
- Sehr hohe Latenzen möglich

In dieser Seminararbeit:

- Funktionieren aktuelle Sicherheitsmechanismen bei sehr hoher Latenz?
- Welche Alternativen gibt es?
- Welche neuen Angriffszenarien entstehen in DTNs?

M2: Artificial Immune Systems

Artifical Immune Systems

- Bilden Mechanismen des menschlichen Immunsystems ab, um Angriffe auf Netzwerke zu erkennen.

In dieser Seminararbeit:

- Überblick über AIS Ansätze
- Codierung von Detektoren
- Detektorgenerierung, Schwerpunkt: Negative Selection
- Matchingverfahren (r-contiguous bits-matching)

M3: GSM considered harmful today?

- GSM hat weltweit mehr als 800 Mio. Benutzer
- Basis für viele sicherheitskritische Anwendungen (Banking, mTAN, Internet, etc.)
- GSM wird von vielen als "sicher" angesehen

- A5/1 gilt als unsicher
- GSM hat verschiedene Schwachstellen
- Mobiltelefone verlassen sich auf korrekte Funktion des Netzes

In dieser Seminararbeit:

- Überblick über Arbeiten zum Thema GSM Sicherheit
- Welche Sicherheitsprobleme gibt es auf Netzseite?
- Welche Sicherheitsprobleme gibt es in Mobiltelefonen?

M4: Sicherheit in drahtlosen Sensornetzen

- Wie sicher sind drahtlose Sensornetze?
  - Ad-hoc Kommunikation
  - Unbekannte Struktur und Umgebung
  - Unbekannte Kommunikationspartner
  - Finden vertrauenswürdiger Routen
  - Schutz vor manipulierten Knoten
- Sicherheitsanforderungen drahtloser Sensornetze
- Lösungsvorschläge
- EU Projekt AWISSENET: http://www.awissenet.eu/

Fragen?

Themenvergabe

Ablauf der Themenvergabe

Verlosung

- Nummer auf dem Los = Reihenfolge bei der Auswahl
- Verbindliche Anmeldung durch Eintrag in Liste

1. Master/Diplom-Themen (mit Online-Anmeldung!)
2. Vergabe Bachelor-Themen (mit Online-Anmeldung!)
3. Vergabe restlicher Themen (ohne Online-Anmeldung)