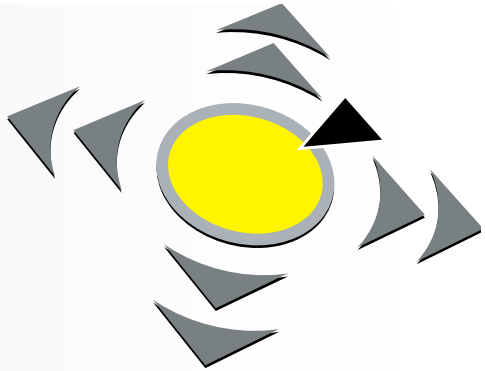
Spring 2010

SIDAR - Graduierten-Workshop über Reaktive Sicherheit

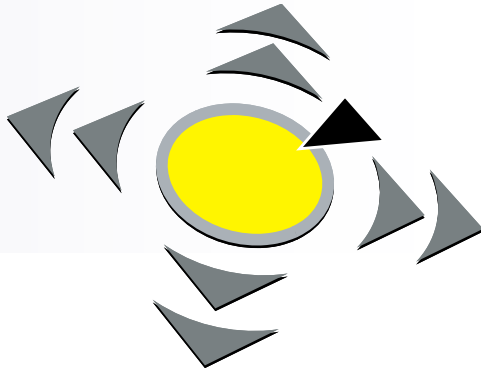
7. Juli 2010 • Bonn, Deutschland



Herzlich willkommen zum Workshop

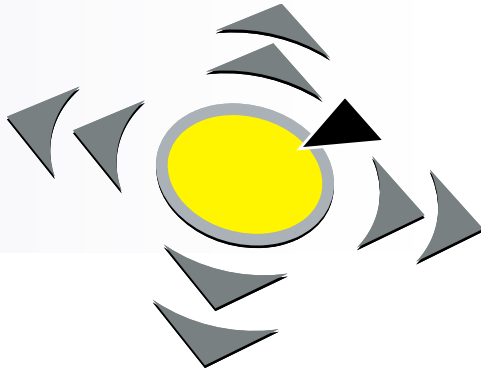
Sebastian Schmerl (BTU Cottbus)
Simon Hunke (Fraunhofer FKIE)

Idee des Spring Workshops



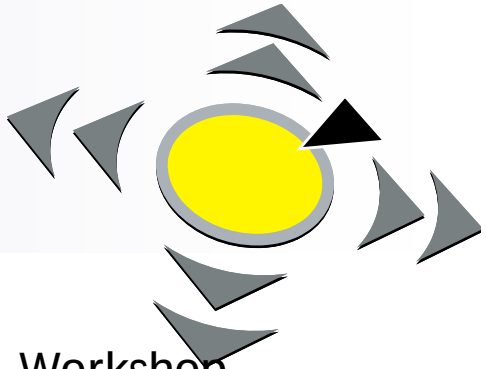
- Ziele:
  - Förderung des wissenschaftlichen Nachwuchses
  - frühzeitige themenbezogene Vernetzung
  - zwanglos Erfahrungen sammeln (Betreuer bleiben draußen ;-)
- Kernmaßnahmen
  - Beiträge: möglichst breiter Überblick
    - auch laufende oder (bald) publizierte Arbeiten
    - Themen aus Abschlussarbeit oder Dissertation
    - keine Papierauswahl
  - Kosten: möglichst viele sollen teilnehmen können
    - keine Teilnahmegebühren (Finanzierung durch SIDAR)
    - Reduktion der Notwendigkeit von Übernachtungen
    - argumentierbarer Reisebedarf: Vortrag und Publikation

SIDAR Themengebiet
Die GI-Fachgruppe SIDAR



- Der Name **SIDAR**
  - Security – Intrusion Detection and Response
  - Erkennung und Beherrschung von Vorfällen der Informationssicherheit
- Themenschwerpunkte **Reaktive Sicherheit**
  - **Verwundbarkeitsanalyse:** z.B.
    - neue Verwundbarkeiten
    - Verwundbarkeits-Scanner
  - **Angriffserkennung:** z.B.
    - Intrusion Detection
    - IT-Frühwarnung
    - Viren-Scanner
    - Wurm-Abwehr
  - **Vorfallsbehandlung:** z.B.
    - Computer Emergency Response Teams (CERTs)
  - **IT-Forensik:** z.B.
    - Spurensicherung und -analyse zur Vorfallsrekonstruktion
    - Angreiferverfolgung

SIDAR – Hintergrund
Dienstleistungen und Aktivitäten

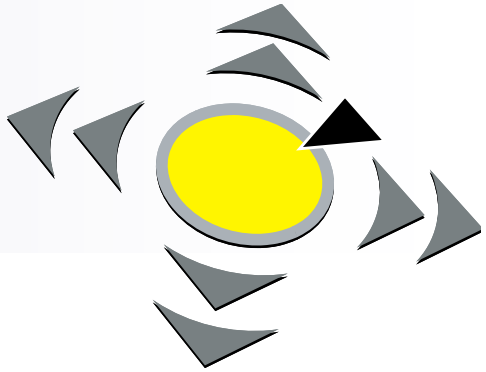


- Tagungen — DIMVA, SPRING, SICK, EC2ND, DFN-Workshop
- Email-Forum — mail.gi-fb-sicherheit.de/mailman/listinfo/sidar

- Web-Portal — www.gi-fg-sidar.de
  - Aktuelles zu SIDAR-Aktivitäten
  - Tagungen
  - Publikationen
  - Themenbezogende Inhalte
  - Ansprechpartner

- Promotionspreis IT-Sicherheit
  - Gestiftet von CAST e.V. ,Gesellschaft für Informatik (GI)
  - Deadline: 31. Juli 2010

Beteiligte
Herzlichen Dank

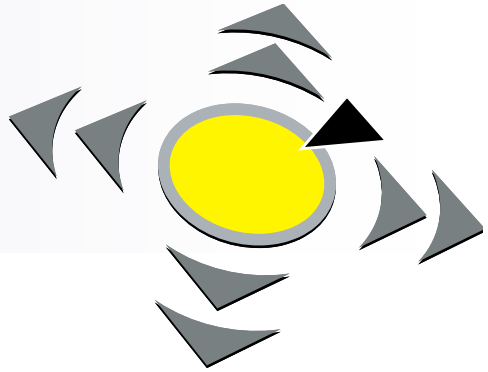


- Autoren
- Teilnehmer
- Tagungsbüro
- Helfer

Organisatorisches
Während der Sektionen und Sitzungen

- Bitte Mobil-Telefone **lautlos** schalten

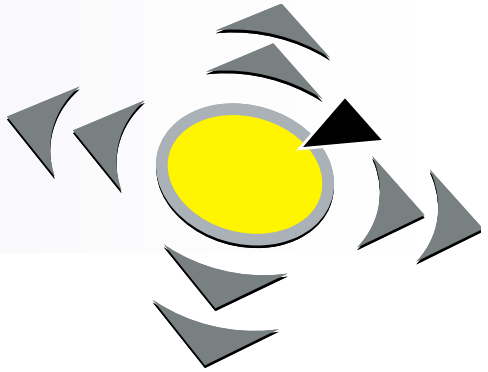
Organisatorisches
Abfrage Teilnehmergruppen



- Für Versicherungszwecke der GI
  - Bitte durch Handzeichen die Zugehörigkeit zu den jeweiligen Gruppen anzeigen (Meldung bei mehreren Gruppen ist möglich).

  - GI-Mitglieder
  - Studierende
  - Ausländische Teilnehmende

Organisatorisches
Workshop-Unterlagen

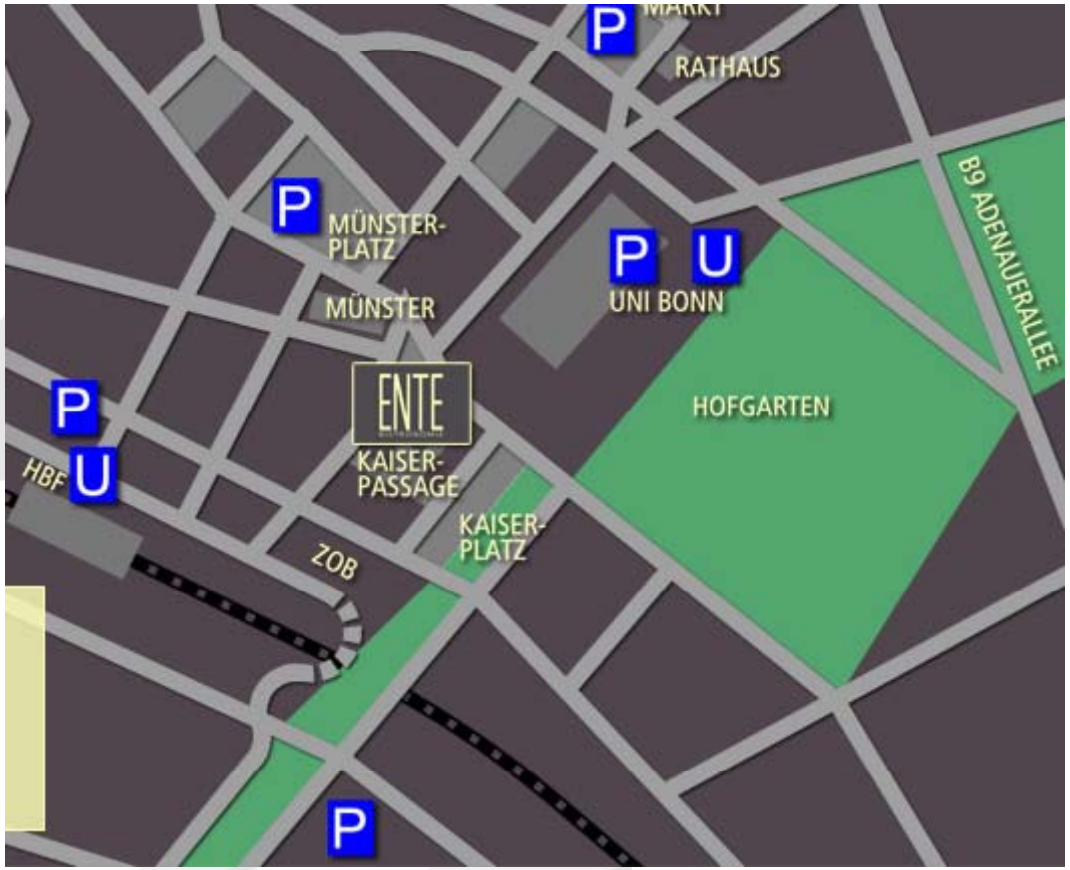


- Abtractsammlung
- Teilnehmerliste (Stand 03.07.2010)
- Programm
- Informationsblätter
  - After-Show-Standort-Info
  - SIDAR – Flyer
- Namensschild

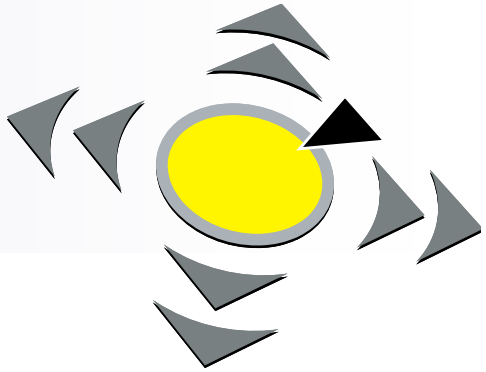
  ⇨ sichtbar tragen

After-Work-Meeting
Gemeinsamer Abend: Die Ente

- Fußball?
- After-Show-Location:
  - Die Ente
  - Martinsplatz 2a
  - 53113 Bonn
  - 0228 / 63 93 22
- Uhrzeit: 18.00 Uhr

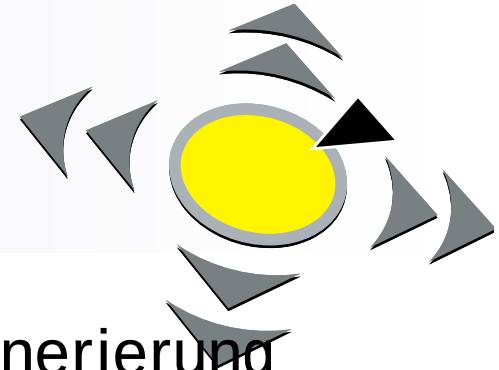


Organisatorisches
Vorträge



- Vortragslänge: ca. 20 Minuten
- Diskussion & Fragen: ca. 5 Minuten
- Vortragsfolien als PDF
- Bilder

Programm



- Sektion 1: Malware-Analyse und Signaturgenerierung

  Moderation: Sebastian Schmerl (BTU-Cottbus)

- Sektion 2: Angriffstechniken

  Moderation: Michael Meier (TU-Dortmund)

- Sektion 3: Bot-Netze

  Moderation: Michael Vogel (BTU-Cottbus)

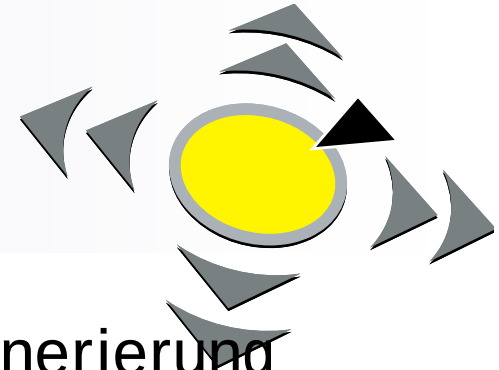
- Sektion 4: Robuste Betriebssysteme

  Moderation: Felix Leder (UNI-Bonn)

- Sektion 5: Kollaborative Intrusion Detection

  Moderation: Simon Hunke (Fraunhofer FKIE)

Programm



- Sektion 1: Malware-Analyse und Signaturgenerierung

  Moderation: Sebastian Schmerl (BTU-Cottbus)

- Sektion 2: Angriffstechniken

  Moderation: Michael Meier (TU-Dortmund)

- Sektion 3: Bot-Netze

  Moderation: Michael Vogel (BTU-Cottbus)

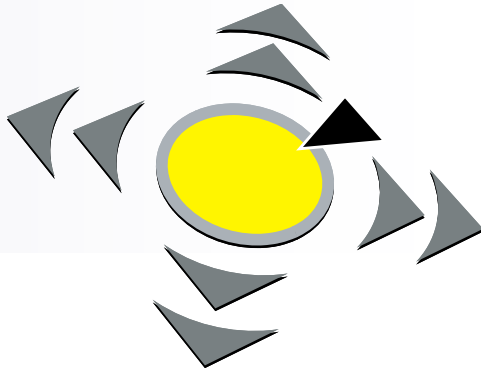
- Sektion 4: Robuste Betriebssysteme

  Moderation: Felix Leder (UNI-Bonn)

- Sektion 5: Kollaborative Intrusion Detection

  Moderation: Simon Hunke (Fraunhofer FKIE)

Nachlese und Ausblick



- Kurzbeiträge und Präsentationen:

  www.gi-fg-sidar.de/spring

- Feedback:

  spring@gi-fg-sidar.de

- Spring 2011

  Lust zu organisieren?

- Nächste SIDAR-Veranstaltung: 8.Juli 2010

  DIMVA 2010 - Detection of Intrusions and Malware & Vulnerability Assessment

  Oktober: EC2ND 2010 (Berlin), SICK 2010 (Denver), Sicherheit 2010 (Berlin)

Abschluss
Bleibt nur noch zu wünschen:

- Viel Spaß in Bonn
- Gute Heimreise

- After-Show-Location:
  - Die Ente
  - Martinsplatz 2a
  - 53113 Bonn
  - 0228 / 63 93 22
- Uhrzeit: 18.00 Uhr