**Spring 2011**
**SIDAR - Graduierten-Workshop über Reaktive Sicherheit**
**21.-22. März 2011 • Bochum, Deutschland**


# Herzlich willkommen zum Workshop

Sebastian Uellenbeck (HGI/RUB)

# Idee des Spring Workshops

Horst Görtz Institut für IT-Sicherheit

- 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 FG SIDAR und FG Angewandte Kryptographie)
    - Argumentierbarer Reisebedarf: Vortrag und Publikation

# Besonderheit Spring 2011



- Kooperation mit Kryptotag (Aktivität der GI FG Angewandte Kryptographie)
- Kryptotag und Spring zeitgleich und am gleichen Ort (nur ein Raum weiter)
  - Sektionen und Pausen immer gleichzeitig
  - Wechsel der Veranstaltung nach persönlichen Vorlieben möglich
  - Mittagessen und Abendveranstaltung gemeinsam mit Kryptotag-Teilnehmern

# SIDAR Themengebiet
# Die GI-Fachgruppe SIDAR



- Der Name **SIDAR**
  - **S**ecurity - **I**ntrusion **D**etection **A**nd **R**esponse
  - 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
- E-Mail-Forum:
  `mail.gi-fb-sicherheit.de/mailman/listinfo/sidar`
- Web-Portal: `www.gi-fg-sidar.de`
  - Aktuelles zu SIDAR-Aktivitäten
  - Tagungen
  - Publikationen
  - Themenbezogene Inhalte
  - Ansprechpartner

# Organisatorisches
# Während der Sektionen



- Bitte Mobil-Telefone lautlos schalten

# Organisatorisches
## Vorträge

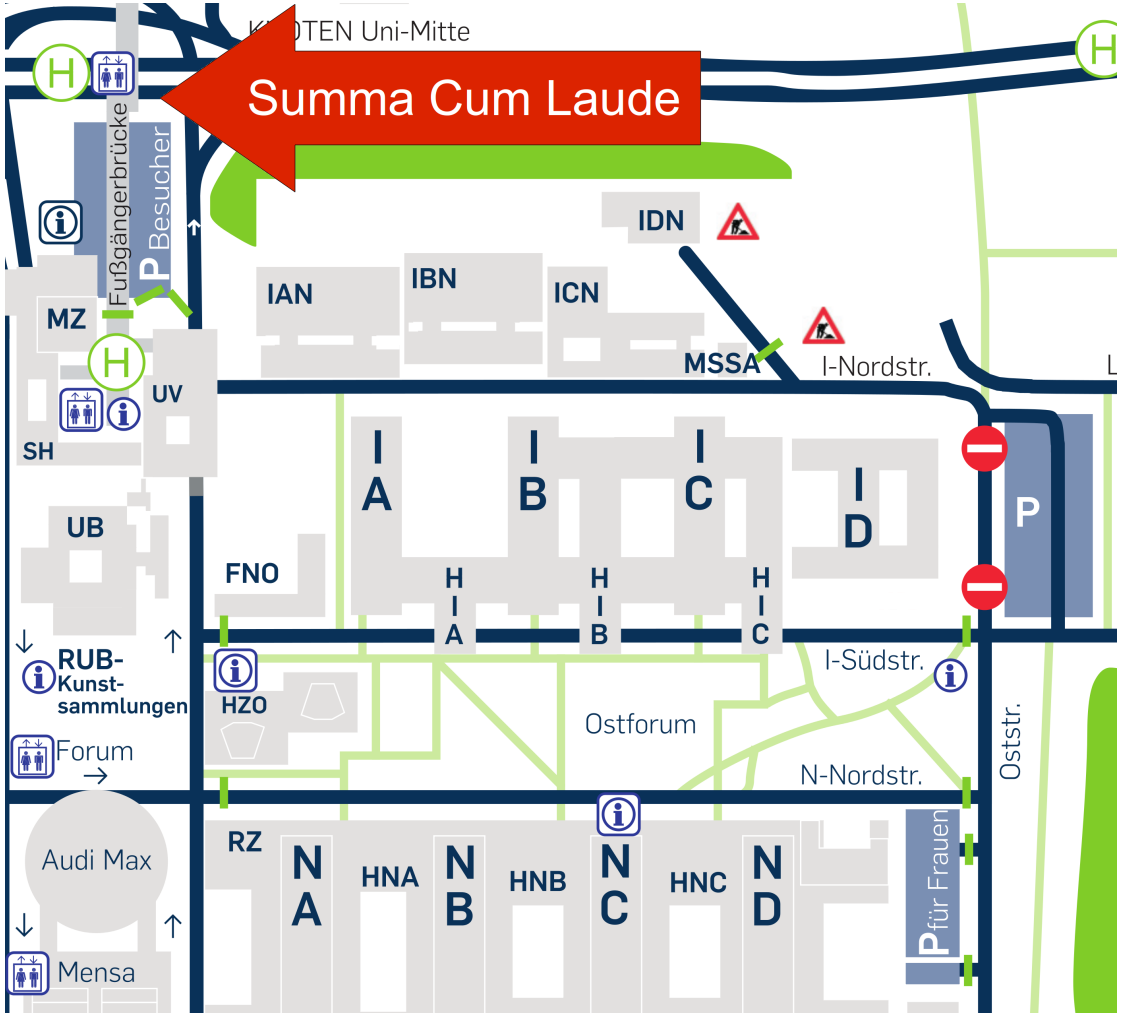
Horst Görtz Institut für IT-Sicherheit

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

# After-Work-Meeting
# Summa Cum Laude

Horst Görtz Institut für IT-Sicherheit

- Summa Cum Laude **ab 19:00**
  - Im Unicenter
  - Querenburger Höhe 283
  - 44801 Bochum
  - 0234 / 9789100
- Fußball **ab 20:15** Bochum - Cottbus
  - im Summa Cum Laude oder
  - im Stadion



# Programm

Horst Görtz Institut für IT-Sicherheit

- Montag
  - Sektion 1: Entdeckung von schadhaftem Verhalten
    Moderation: Sebastian Uellenbeck (Ruhr-Universität Bochum)
  - Sektion 2: Betriebssysteme und Informationsfreiheit
    Moderation: Ralf Hund (Ruhr-Universität Bochum)
  - Sektion 3: Forensik
    Moderation: Johannes Hoffmann (Ruhr-Universität Bochum)
- Dienstag
  - Sektion 1: Smartphone Security Teil 1
    Moderation: Michael Meier (Uni Bonn, TU Dortmund, Fraunhofer FKIE)
  - Sektion 2: Smartphone Security Teil 2
    Moderation: Sebastian Uellenbeck (Ruhr-Universität Bochum)

# Programm 21. März, Sektion 1: Entdeckung von schadhaftem Verhalten

Horst Görtz Institut für IT-Sicherheit

- Verschleiernde Transformationen von Programmen
  *Michael Rex* – Technische Universität Dortmund
- Erkennung von bösartigen Netzwerkverbindungen mittels Verhaltensgraphenanalyse
  *Ralf Hund* – Ruhr-Universität Bochum
- SEODisc: Ansatz zur Erkennung von SEO-Attacken
  *Matthias Meyer* – Technische Universität Dortmund

# Programm 21. März, Sektion 2: Betriebssysteme und Informationsfreiheit

Horst Görtz Institut für IT-Sicherheit

- Evaluating Ring -3 Rootkits
  *Patrick Stewin* – TU Berlin / T-Labs
- OS Agnostic Sandboxing Using Virtual CPUs
  *Matthias Lange* – TU Berlin / Deutsche Telekom Laboratories
- Practical P2P-Based Censorship Resistance
  *Benjamin Michéle* – TU-Berlin / Deutsche Telekom Laboratories

# Programm 21. März, Sektion 3: Forensik

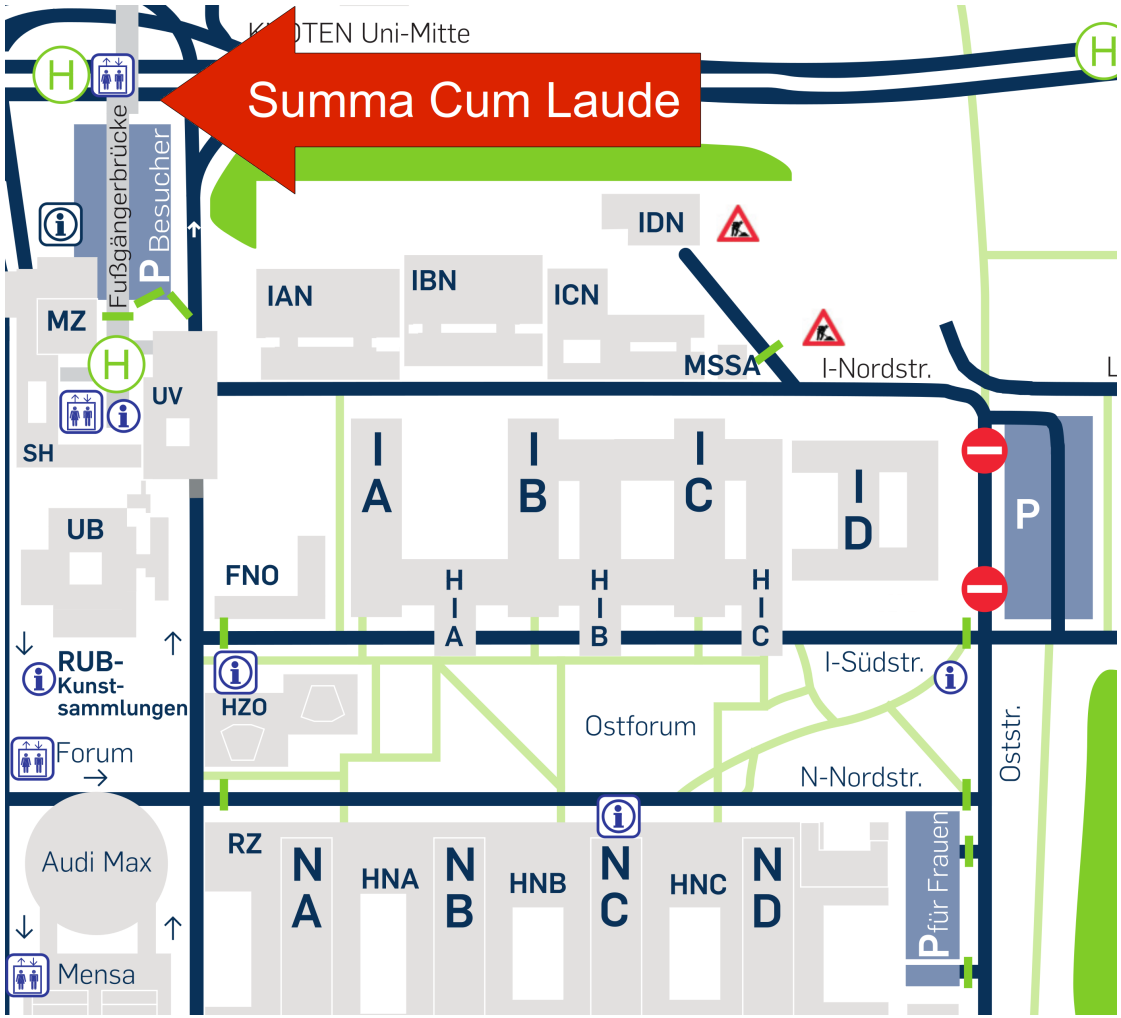
Horst Görtz Institut für IT-Sicherheit

- Tools and Processes for Forensic Analyses of Smartphones and Mobile Malware
  *Michael Spreitzenbarth* – University of Erlangen-Nuremberg
- Security Aspects of Piecewise Hashing in Computer Forensics
  *Frank Breitinger* – Hochschule Darmstadt
  *Harald Baier* – Center for Advanced Security Research Darmstadt

# Abschluss Tag 1
# Summa Cum Laude

Horst Görtz Institut für IT-Sicherheit

- Summa Cum Laude **ab 19:00**
  - Im Unicenter
  - Querenburger Höhe 283
  - 44801 Bochum
  - 0234 / 9789100
- Fußball **ab 20:15** Bochum - Cottbus
  - im Summa Cum Laude oder
  - im Stadion



# Programm 22. März, Sektion 1: Smartphone Security Teil 1

Horst Görtz Institut für IT-Sicherheit

- Antiforensik auf mobilen Endgeräten
  *Stefan Lambertz* – FH Aachen
- Smartphone Honeypots
  *Collin Mulliner* – TU-Berlin / Deutsche Telekom Laboratories

# Programm 22. März, Sektion 2: Smartphone Security Teil 2

Horst Görtz Institut für IT-Sicherheit

- Taming the Robot: Efficient Sand-boxing of the Android OS
  *Steffen Liebergeld* – TU Berlin / Deutsche Telekom Laboratories
- Android Security
  *Daniel Bußmeyer* – Ruhr-Universität Bochum

# Nachlese und Ausblick



- Kurzbeiträge und Präsentationen:
  `www.gi-fg-sidar.de/spring`
- Feedback:
  `spring@gi-fg-sidar.de`
- Spring 2012
  Lust zu organisieren?
- Nächste SIDAR-Veranstaltung:
  - 10.-12. Mai 2011, Stuttgart: IMF 2011

    IT Security Incident Management & IT Forensics

# Beteiligte
# Herzlichen Dank

Horst Görtz Institut für IT-Sicherheit

- Autoren
- Moderatoren
- Teilnehmer
- Helfer

# Abschluss
# Bleibt nur noch zu wünschen

Horst Görtz Institut für IT-Sicherheit

Viel Spaß in Bochum

bzw.

Gute Heimreise