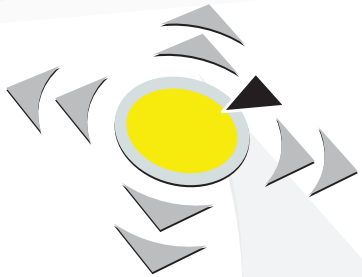
SPRING

GI FG SIDAR Graduierten-Workshop über Reaktive Sicherheit

Ulrich Flegel

Gesellschaft für Informatik e.V.· Fachbereich Sicherheit
Fachgruppe **Security** · **Intrusion Detection and Response**

14.–15. September 2009



Idee von SPRING

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

Idee von SPRING

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

Idee von SPRING

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

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

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

Themengebiets-Ansprechpartner

Verwundbarkeitsanalyse

- Thomas Biege — thomas@novell.com

Intrusion Detection

- Ulrich Flegel — ulrich.flegel@sap.com
- Michael Meier — michael.meier@udo.edu

Malware

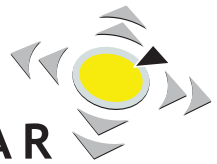
- Toralv Dirro — toralv_dirro@mcafee.com
- Christian Gorecki — christian.gorecki@informatik.uni-mannheim.de
- Thorsten Holz — thorsten.holz@informatik.uni-mannheim.de
- Michael Meier — michael.meier@udo.edu

Vorfallsbehandlung

- Sandra Frings
- Dirk Schadt

IT-Forensik

- Christian Gorecki — dirk.schadt@spot.net
- Dietmar Mauersberger — dietmar.mauersberger@polizei.bayern.de
- Holger Morgenstern



Dienstleistungen und Aktivitäten

- Tagungen
- Email-Forum
- Web-Portal
  - Aktuelles zu SIDAR-Aktivitäten
  - Tagungen
  - Publikationen
  - Themenbezogener Inhalt
  - Ansprechpartner

Dienstleistungen und Aktivitäten

- Tagungen
- Email-Forum
- Web-Portal
  - Aktuelles zu SIDAR-Aktivitäten
  - Tagungen
  - Publikationen
  - Themenbezogener Inhalt
  - Ansprechpartner

Dienstleistungen und Aktivitäten

- Tagungen
- Email-Forum
- Web-Portal
  - Aktuelles zu SIDAR-Aktivitäten
  - Tagungen
  - Publikationen
  - Themenbezogener Inhalt
  - Ansprechpartner

Herzlichen Dank!

- Redner
- Autoren
- Moderatoren
- Fraunhofer IAO

Programm Tag 1

Neue Bedrohungen

Moderation: *Philip Trinius*

Malwareanalyse und Korrelation

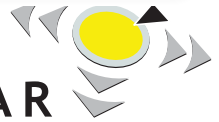
Moderation: *Michael Meier*

Smartphone-Malware

Moderation: *Jan Göbel*

Ausnutzung von Kontext

Moderation: *Ulrich Flegel*



Programm Tag 1

Neue Bedrohungen

Moderation: *Philip Trinius*

Malwareanalyse und Korrelation

Moderation: *Michael Meier*

Smartphone-Malware

Moderation: *Jan Göbel*

Ausnutzung von Kontext

Moderation: *Ulrich Flegel*

Programm Tag 1

Neue Bedrohungen

Moderation: *Philip Trinius*

Malwareanalyse und Korrelation

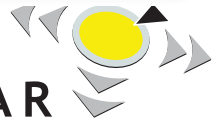
Moderation: *Michael Meier*

Smartphone-Malware

Moderation: *Jan Göbel*

Ausnutzung von Kontext

Moderation: *Ulrich Flegel*



Programm Tag 1

Neue Bedrohungen

Moderation: *Philip Trinius*

Malwareanalyse und Korrelation

Moderation: *Michael Meier*

Smartphone-Malware

Moderation: *Jan Göbel*

Ausnutzung von Kontext

Moderation: *Ulrich Flegel*

Programm Tag 2

Netzbasierte Erkennungsverfahren

Moderation: *Jan Göbel*

Signaturgenerierung für Intrusion und Fraud Detection

Moderation: *Peter Wurzinger*

Verwundbarkeitsanalyse und Datenflußkontrolle

Moderation: *Ulrich Flegel*

Programm Tag 2

Netzbasierte Erkennungsverfahren

Moderation: *Jan Göbel*

Signaturgenerierung für Intrusion und Fraud Detection

Moderation: *Peter Wurzinger*

Verwundbarkeitsanalyse und Datenflußkontrolle

Moderation: *Ulrich Flegel*

Programm Tag 2

Netzbasierte Erkennungsverfahren

Moderation: *Jan Göbel*

Signaturgenerierung für Intrusion und Fraud Detection

Moderation: *Peter Wurzinger*

Verwundbarkeitsanalyse und Datenflußkontrolle

Moderation: *Ulrich Flegel*

Bitte Mobiltelefone **lautlos** schalten

SIDAR

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

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

Abfrage Teilnehmergruppen

Für Versicherungszwecke der GI

Bitte durch Handzeichen die Zugehörigkeit zu den jeweiligen Gruppen anzeigen (Meldung bei mehreren Gruppen ist möglich).

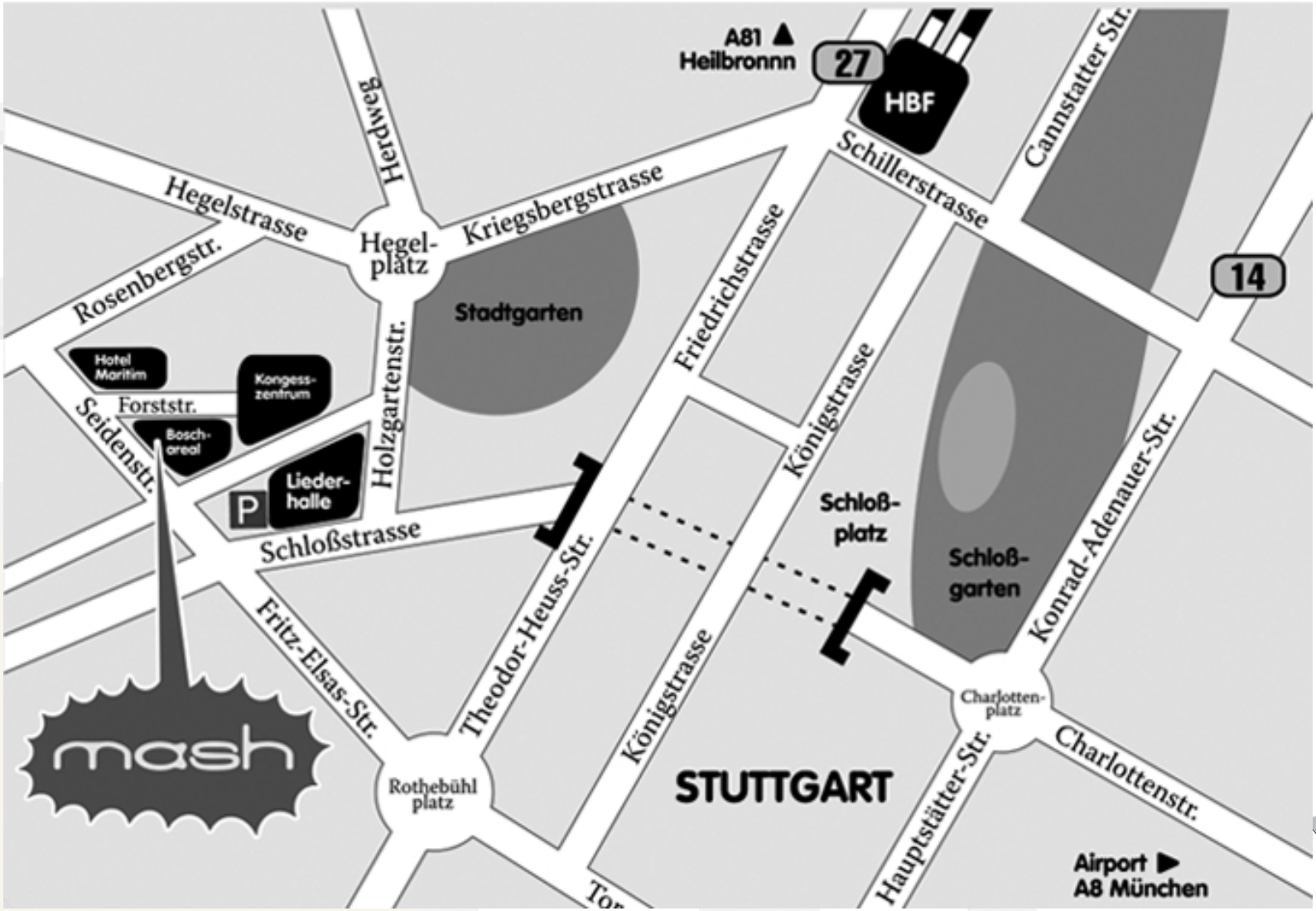
- GI-Mitglieder
- Studierende
- Ausländische Teilnehmende

Workshop-Unterlagen

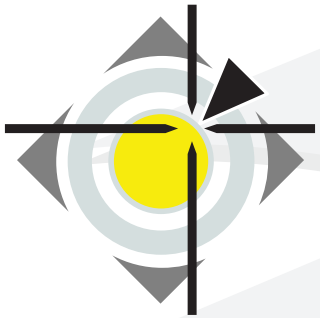
- Namensschild
- Programm
- Abstractsammlung
- Teilnehmerliste (Stand: 07. August)
- Informationsblätter:
  - After-Show-Standort-Info (ASSI)
  - Fachbereich Sicherheit – Schutz und Zuverlässigkeit
  - Fachgruppe SIDAR
  - GI und Studierende in der GI
  - GI-Infotelegramm
  - GI-Sticker

Gemeinsamer Abend: Mash

Forststrasse 7 · Tel 0711/1209330 · www.mash-stuttgart.de



weitere SIDAR-Veranstaltungen



IMF 2009, 15.–17. September, Stuttgart

- internationale Tagung
- Themen: Incident Management, IT-Forensik
- Hauptvorträge internationaler Experten
- Tutorials

DIMVA 2010, Juli, Bonn

- internationale Tagung
- Themen: Intrusion Detection, Malware-Bekämpfung, Verwundbarkeitsanalyse
- Hauptvorträge internationaler Experten
- Rump-Session: Aktuelles und Amüsantes
- Rittermahl auf einer Burg

Bleibt nur noch zu wünschen

Viel Spaß in Stuttgart!

bzw.

Eine gute Heimfahrt!

Overview