



# 2<sup>nd</sup> Kassel Student Workshop on Security in Distributed Systems

## KaSWoSDS'09

Thomas Weise and Philipp A. Baer  
FG Verteilte Systeme  
Universität Kassel  
2008-10-21



# Contents

- Einführung
- Themen



# Einführung

- Zweiter Workshop der "KaSWoSDS-Serie"
- Seminar [lat. "Pflanzschule"], das

*Hochschulwesen: Lehrveranstaltung, in der die Studierenden sich an der Diskussion beteiligen, Referate anfertigen und zum Teil Klausuren schreiben; in der Regel Proseminar für Studienanfänger, Mittel- und Hauptseminar als Examensvoraussetzung und Oberbeziehungsweise Doktorandenseminar.*



# Einführung

- Es stehen verschiedene Themen zur Auswahl, jeder Teilnehmer wählt sich ein passendes aus. Dann folgen vier Phasen:
  - 1) Thema verstehen
  - 2) Exploit für ein Beispiel der Sicherheitslücke entwickeln
  - 3) Ausarbeitung schreiben (auch Gegenmaßnahmen)
  - 4) Einreichen, Begutachten, Korrigieren von Ausarbeitungen.
  - 5) Erstellen einer Präsentation und Vortrag auf dem Workshop.

**Alle Ausarbeitungen werden am Ende gebunden und als technischer Report veröffentlicht.**



# Einführung

- Das Seminar wird als Workshop (Blockveranstaltung) abgehalten
- Vorbereitung auf internationale Workshops und Konferenzen
- Am Ende steht eine zitierbare Publikation  
(wenn genug Teilnehmer zusammenkommen)
- **Das macht mehr Spaß als ein normales Seminar!**



# Themen

- 1) **Übersicht**
- 2) **Unsicherheit in Softwaresystemen**
- 3) **Unsicherheit in Kryptographiesystemen**
- 4) **Spionage und Forensik**



# Themen - Übersicht

## 1. Übersicht

Die grundlegenden Angriffspunkte in einem Rechnernetz dienen als Einführung. Dazu zählen Schwachstellen in der Software und den Datenkanälen, aber auch Sicherheitsgefährdungen die aus unsachgemäßem Umgang resultieren.



# Themen - Unsicherheit in Softwaresystemen

## 2. Denial-of-Service

Denial-of-Service-Attacken (DoS) haben das Ziel, einen oder mehrere Dienste auf dem angegriffenen Host funktionsunfähig zu machen. Dies wird meistens erreicht, indem das entsprechende System mit Netzwerkpacketen überlastet wird. Bei einem DoS-Angriff, der parallel von verschiedenen Quellen ausgeführt wird spricht man von Distributed DoS (DDoS).



# Themen - Unsicherheit in Softwaresystemen

## 3. Sniffing

Sniffer sind Programme, die den Datenverkehr auf einem LAN mithören. Sie können zur Datenanalyse verwendet werden, aber auch um beispielsweise das Surfverhalten von Internetnutzern aufzuzeichnen oder um Informationen abzuhören.



# Themen - Unsicherheit in Softwaresystemen

## 4. Trojaner

Trojaner sind Programme, die einer nützlichen Applikation gleichen aber in Wirklichkeit Schadcode beinhalten. Sie werden z.B. erzeugt, indem man ein vorhandenes, nützliches Programm durch Umlinken mit einem anderen Programm verbindet, das den Schadcode enthält.



# Themen - Unsicherheit in Softwaresystemen

## 5. Würmer

Ein Wurm ist ein Programm, das sich über ein Netzwerk von Computern verbreitet. Es nutzt dazu höherwertige Ressourcen, Protokolle, Netzwerkdienste oder Benutzerinteraktionen. Würmer können auch dazu benutzt werden, Trojaner auf dem Zielsystem abzusetzen.



# Themen - Unsicherheit in Softwaresystemen

## 6. Phishing

Beim Phishing wird versucht, über gefälschte Internetadressen oder gefälschte Emailabsender an persönliche Daten eines Benutzers zu kommen. Dabei wird der Webaufttritt bzw. die Email-Adresse z.B. einer Bank täuschend echt nachempfunden. Es werden auch aktiv Nachrichten verbreitet, die Benutzer dazu verleiten soll, persönliche Informationen wie PINs preiszugeben.



# Themen - Unsicherheit in Softwaresystemen

## 7. Cross Site Request Forgery

Cross Site Request Forgery<sup>6</sup> ist ein Angriff bei dem der Browser (oder das Client-Programm) eines Opfers ohne dessen Wissen und Einverständnis kompromittierende Anfragen/Kommandos an eine Website schickt. Oftmals sind Aktivitäten, die ein Benutzer auf einer Website ausführen kann, an bestimmte URLs geknüpft. Gelingt es einem Angreifer, einen eingeloggten User dazu zu bringen, die von ihm gewünschten Links zu besuchen, so wird dieser die vom Angreifer geplanten Aktivitäten durchführen.



# Themen - Unsicherheit in Kryptosystemen

## 8. Security by Obfuscation

Obfuscation, zu deutsch verdunkeln oder verwirren, wird im Kontext von Sicherheit oft als Ansatz verwendet, um Programmcode unkenntlich zu machen, der dann aber trotzdem noch ausführbar bleibt. Die Programmiersprache Perl ist in diesem Zusammenhang besonders hervorzuheben, da sie diese Technik implizit unterstützt.



# Themen - Unsicherheit in Kryptosystemen

## 9. Security by Obscurity

Security by Obscurity bedeutet im Prinzip, Sicherheit darauf beruhen zu lassen, dass ein Angreifer nicht weiß, mit was er es zu tun hat. In der Kryptographie wird also zum Beispiel das eigentliche Verfahren geheim gehalten. Dieses Prinzip ist sehr umstritten und garantiert nicht für Sicherheit, da, sobald das Prinzip des zugrundeliegenden Algorithmus' bekannt geworden ist, das Verfahren nicht mehr eingesetzt werden kann.



# Themen - Unsicherheit in Kryptosystemen

## 10. Sicherheit im WLAN



# Themen - Unsicherheit in Kryptosystemen

## 11. Sicherheit im Mobilfunk

Sicherheit im Mobilfunk ist ein recht aktuelles Thema, denn eigentlich jede oder jeder besitzt (zumindest) ein Mobiltelefon. Da die Datenübertragung zwischen Mobiltelefon und dem Mobilfunksendesysteme kabellos vonstatten geht, ist hier ein möglicher Ansatzpunkt für Angriffe wie zum Beispiel das Abhören von Gesprächen.



# Themen - Spionage und Forensik

## 12. Techniken zum Ausspähen von Daten

Spyware bezeichnet eine Kategorie von Computerprogrammen, die Daten in einem Computer ausspäht und zum Beispiel an den Urheber der Software (oder an andere Personen/Programme) weiterleitet, ohne dazu berechtigt zu sein. Durch Spyware kann nicht Daten, sondern auch das Verhalten von Benutzern überwachen.



# Themen - Spionage und Forensik

## 13. Auswertung der Ausgespähten Daten

Das Thema Daten- oder Computerforensik beschreibt die Aufgabe, komplexe Zusammenhänge aus vormals unzusammenhängenden Datenmengen abzuleiten. Dies ist vergleichbar mit den forensischen Aufgaben von Ermittlern bei Sicherheitsbehörden



# Themen - Spionage und Forensik

## 14. Datensicherheit in Social Networks (evtl. 2 Vorträge)

Zum einen sind konkrete Statistiken: Welche Benutzergruppe nutzt welches System und speichert/veröffentlicht welche Daten wie?

Welche konkreten Maßnahmen zum Ausspähen dieser Daten gibt es? Kann man diese automatisieren? Kann man Sichtbarkeitsbeschränkungen umgehen? Wie kann man die Daten verschiedener Quellen verbinden? Was kann man alles rausbekommen?



# Themen

Eigene Vorschläge sind willkommen

# Evolutionary Optimization

*Automated solving of complicated problems in the same way nature does*

- Optimization Framework in Java: 

- Genetic Programming: 

- Free Electronic Book: 

<http://www.it-weise.de/projects/book.pdf>

Thomas Weise, [weise@vs.uni-kassel.de](mailto:weise@vs.uni-kassel.de), Raum 1408b

