

# Workshop on Security in Distributed Systems

Philipp A. Baer und Thomas Weise

FG Verteilte Systeme  
Universität Kassel

22. Oktober 2007



**VERTEILTE SYSTEME**



Motivation

Themen





























# UNSICHERHEIT

... in Softwaresystemen



# Buffer Overflows

## Beschreibung

*Pufferüberläufe sind eine der häufigsten Attacken auf Rechnernetze. Sie nutzen Pufferüberläufe allgemeine Programmierfehler aus, die besonders in Sprachen wie C sehr schnell auftreten können.*



# Cross-Site Scripting

## Beschreibung

*Deim Cross-Site Scripting (XSS) geht es hauptsächlich darum, dem Besucher einer Internetseite Schadcode unterzuschieben. Dabei wird häufig eine andere, vertrauenswürdige Seite als Deckmantel benutzt. Ein Angreifer kann unter Umständen z.B. auf seiner Webseite einen Link zu einer vermeintlich sicheren Seite stellen, die dann jedoch auf Schadcode verweist.*



# SQL-Injection

## Beschreibung

*SQL-Injection baut auf Schwachstellen in der Auswertung von eingehenden Daten auf der Serverseite aus. Ein Beispiel wäre zum Beispiel ein Login-Formular, bei dem die Eigabedaten nicht überprüft werden. Sind die Daten in einer SQL-Datenbank hinterlegt, kann direkt eine SQL-Abfrage eingegeben werden, zum Beispiel um eine Tabelle zu löschen.*



# Spoofing

## Beschreibung

*Spoofing umfasst alle Arten von Methoden, die genutzt werden, um sich als jemand anderes (Person, Prozess, System, Host, ...) auszugeben. Es gibt viele Spielarten: ARP-, DNS-, DHCP-, IP-, Mac-, Mail- oder URL-Spoofing.*



# Denial-of-Service

## Beschreibung

*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).*



# Sniffng

## Beschreibung

*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.*



# Trojaner

## Beschreibung

*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.*



## Viren

### Beschreibung

*Ein Virus ist ein Programm, welches seinen Kode in (mehrere) andere Programme einfügt und sich somit verbreitet.*



# Würmer

## Beschreibung

*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.*



# Phishing

## Beschreibung

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



# UNSICHERHEIT

... in Kryptosystemen



## Klassische Verfahren

### Beschreibung

*Die klassischen Verfahren der Kryptographie sind wegen der vielen verschiedenen Ansätze, aber vor allem der sich dahinter verbergenden Geschichte interessant. Beispielsweise waren bereits die alten Ägypter in der Lage, Texte oder Informationen zu verschlüsseln. Weitreichenden Einfluss auf den Ausgang von Kriegen hatte die Kryptographie spätestens seit dem ersten Weltkrieg.*



# Security by Obfuscation

## Beschreibung

*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.*



# Security by Obscurity

## Beschreibung

*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.*



## Sicherheit im Mobilfunk

### Beschreibung

*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.*



# SPIONAGE UND FORENSIK

Wie Daten verwertet werden.



## Techniken zum Ausspähen von Daten

### Beschreibung

*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 nur Daten, sondern auch das Verhalten von Benutzern überwachen.*





# EIGENE IDEEN

Sind noch Wünsche offen?