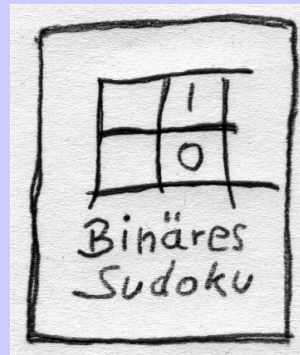




Willkommen zum Seminar





Überblick

Inhalt

1 - Organisatorisches

2 - Themen



1 - Organisatorisches



1 - Organisatorisches

Kapitel 1 - Organisatorisches

- Wann und wo findet das Seminar statt
- Registrierung
- Fragen an mich



1 - Organisatorisches

Wann und wo findet das Seminar statt?

- Es wird einen Termin zur Literaturrecherche geben
- Es wird einen Termin für Fragen und für die Überprüfung des Zwischenstandes geben
- Es wird Termine für die Seminarvorträge geben (einen Block) mit Anwesenheitspflicht !!!
- Falls man zu einem oder mehreren Vorträgen nicht kommen kann ist eine Krankmeldung vorzulegen!

Achtung: Die Dienstagstermine fallen im Gegenzug aus



1 - Organisatorisches

Registrierung?

Bitte registrieren Sie sich zum Seminar unter folgendem Link:

<http://www.informatik.hs-mannheim.de/~fischer/serverprogs/registration/SEM/index.php>



1 - Organisatorisches

Fragen...

- Fragen können gerne auch per Email an mich gerichtet werden oder aber bei Diskussionsbedarf einfach per Mail einen Termin vereinbaren...
- Rückkopplung ist ausdrücklich erwünscht !!!!!



1 - Organisatorisches

Fragen?



2 - Themen



2 - Themen

1 - Das Neuron in der Simulation (Hodgkin/Huxley, Fitzhugh/Nagumo)

Hodgin und Huxley bzw Fitzhugh/Nagumo haben ein vereinfachtes Modell einer Differentialgleichung zur Simulation eines spikenden Neurons aufgestellt. Durch kleine Änderungen an diesem Modell erzeugt Eugene M. Izhikevich einen schnellen und trotzdem realistischen Algorithmus zur Simulation von Neuronen. Wie funktioniert's?



2 - Themen

Themen: J.Fischer

2 - Fraktale grundlegendes zur Theorie

Vielleicht haben viele schon von Mandelbrot bzw. Apfelmännchen oder Juliamengen gehört. Was steckt dahinter? Was heisst fraktal?



2 - Themen

Themen: J.Fischer

3 - Chaos und Berechnung des Lyapunovexponenten

Was heisst Chaotisch im Sinne der Physik? Was ist ein Orbit, was ein Attraktor?

Wann ist ein Zustand stabil, wann instabil? Was heisst periodisch und quasiperiodisch. Was ist ein Fixpunkt?



2 - Themen

Themen: J.Fischer

4 - Was bedeutet Information, was bedeutet Entropie?

Der Begriff Information ist eng verwandt mit dem Begriff der Entropie. Aber wie misst man die Information einer Menge an Daten? Was hat das mit Ordnung im System zu tun? Im Sinne dieser „Ordnung“: Kann man in einem geschlossenen System mehr „Ordnung“ machen?



2 - Themen

Themen: J.Fischer

5 - Deep Belief Networks

Eines der State of the Art Neuronalen Netze sind Deep Belief Netzwerke. Wie funktionieren die? Wofür sind sie geeignet? (Mathematische/Statistik-Kenntnisse vorausgesetzt)



2 - Themen

Themen: J.Fischer

6 - Support Vector Machines

Es heisst immer Neuronale Netze sind unvorhersehbar und werden wenig eingesetzt, weil man im Grunde nicht weiss wie diese Abbildung funktioniert. eine Support Vector Machine ist eine Abstraktion eines Neuronalen Netzes, bei der man all das im Griff hat und das ohne Dutzende von Parametern als Experte einstellen zu müssen.



2 - Themen

Themen: J.Fischer

7 - Echo-State-Netzwerke

Herbert Jäger (IUB Bremen) hat ein rekurrentes Netzwerk erfunden, welches die Gewichte eines rekurrentes Neuronales Netz mit Hilfe eines Gleichungssystems berechnet. Das Netzwerk ist "State Of The Art" und ermöglicht eine Abbildung mit Gedächtnis!



2 - Themen

Themen: J.Fischer

8 - Gleichungssysteme und dünn besetzte Matrizen

Gleichungssysteme zu lösen bedarf mit dem Gaußalgorithmus $O(N^3)$

Rechenschriffe. Nun gibt es viele Systeme in der Natur, bei denen zur Simulation Gleichungssysteme mit dünn besetzten Matrizen berechnet werden müssen. Wie kann man das Problem angehen?



2 - Themen

Themen: J.Fischer

9 - TD Gammon (Ein selbstlernender Backgammon Algorithmus)

Eines der Highlights der Künstlich lernenden Systeme war TD-Gammon, ein selbstlernender Reinforcement Algorithmus, der kombiniert mit einem Neuronalen Netz lernt, indem er Backgammon-Partien gegen sich selbst spielt. Mittlerweile spielt das Programm auf Weltmeisterniveau.



2 - Themen

Themen: J.Fischer

10 - Weboptimierung: Javascript Befehlssatz, der just in Time Compiliert wird

Was muss man tun, um Programme im Web bis ins Letzte zu optimieren?

Was passiert mit dem JavaScript Befehlssatz, der gleich in Maschinensprache umgesetzt wird...



2 - Themen

Themen: J.Fischer

11 - Benchmarks im Bereich maschinelles Lernen

In der Forschung kocht jeder sein eigenes Süppchen... Welche Möglichkeiten der Vergleiche verschiedener Algorithmen für's Maschinelle Lernen gibt es?
Welche Standard Benchmarks finden Sie?



2 - Themen

Themen: J.Fischer

12 - Evolution Neuronaler Netze für Laufroboter (auf Rough Terrain)

Was gibt es an Literatur, was sind die Highlights...



2 - Themen

Themen: J.Fischer

13 - Funktionale Programmierung in Beispielen (Java/C++)

Mittlerweile sind sowohl in C++ als auch in Java Elemente der funktionalen Programmierung implementiert. Was für Vorteile bringen diese? Wie funktioniert es? (Wie wird das intern umgesetzt z.B. das übergeben einer Funktion an eine Prozedur) Erläutern sie das an Beispielen.



2 - Themen

Themen: J.Fischer

14 - Physically Based Rendering

Es werden Beispielsweise bei Lichtreflexionen die physikalischen Gesetze genauer simuliert....

Wie funktioniert es?



2 - Themen

Themen: J.Fischer

15 - Deferred Shading

Lichtberechnung und Geometrieverarbeitung einer Szene werden getrennt...

Wie funktioniert's genau?



2 - Themen

Themen: J.Fischer

16 - Continuous Collision Detection

Wenn eine Kugel in einem Spiel auf eine Wand geschossen wird, so kann es vorkommen, dass sie durch die Wand tunnelt... Wie vermeidet man das?



2 - Themen

Themen: S.Paulus

1 - Anwendung des OWASP Risk Rating bei Threat Modeling

Threat Modeling ist eine Technik, um vor dem Erstellen von Code auf der Basis von Software-Entwurfsbeschreibungen Schwachstellen und Angriffsvektoren zu identifizieren und zu bewerten. Die Bewertung sollte dabei möglichst vergleichbar sein. Eine einheitliche Methodik ist durch das OWASP Risk Rating, welche eigentlich für existierende Schwachstellen in Code entwickelt wurde, gegeben. Diese Methodik und ihr Nutzen soll erläutert und an einem Threat Modeling Beispiel demonstriert werden.



2 - Themen

Themen: S.Paulus

2 - Unterschied zwischen ISO 27001 und BSI IT-Grundschutz

ISO 27001 und der IT-Grundschutz des BSI sind zwei Standards, um Informationssicherheit in einem Unternehmen zu etablieren. Dabei erfreuen sich beide Standards einer großen Beliebtheit, und sind sich in der Vorgehensweise sehr ähnlich - unterscheiden sich aber auch in wichtigen Aspekten. Die grundsätzliche Funktionsweise eines Informationssicherheitsmanagementsystems soll erläutert, und die Unterschiede zwischen den beiden Standards sollen überblicksartig dargestellt werden.



2 - Themen

Themen: S.Paulus

3 - Session Management und Single Sign-On für föderierte Web-Anwendungen

Es gibt immer mehr Web-Anwendungen, die immer mehr Anmelde-Informationen von uns wollen. Darauf versucht das Konzept der „föderierten Identitäten“ eine Antwort zu geben. Föderierte Identitäten (Stichworte sind etwa Liberty Alliance, OpenID, OAuth, SAML,...) versuchen, die Anzahl der erforderlichen Authentifizierenden zu reduzieren. Wie funktionieren diese Techniken, welche Auswirkungen haben sie auf das Session Management, und wo setzt man sie am besten ein?



2 - Themen

Themen: S.Paulus

4 - COBIT

„Control OBjectives for Information Technology“ ist ein Standard der internationalen Vereinigung der IT-Auditoren. Diese prüfen die Ordnungsmäßigkeit und Effektivität von IT-Systemen nach gemeinsamen, über Jahre gesammelten Best Practices. Seit der Version 5 deckt COBIT aber nicht nur diese beiden Ziele ab, sondern stellt einen Bauplan für eine zukunftssichere IT-Organisation und deren Dienstleistungen. COBIT soll beschrieben werden, und an einem Beispiel demonstriert werden.



2 - Themen

Themen: S.Paulus

5 - HTML5 Digital Rights Management in Browsern

Seitdem alle Anwendungen „always on“ sind, und „permanent beta“, ist es erforderlich, dass digitale Inhalte wie Musik, Filme oder auch Texte auch im Browser abgespielt / gezeigt werden können, ohne dass ich ein weiteres Programm / Executable benötige. HTML5 bietet die entsprechende Möglichkeit. Erläutern Sie die Funktionsweise und die Möglichkeiten, die sich dadurch den großen Herstellern bietet - und welche Bedeutung der Browser für die Umsätze im Internet bekommt.



2 - Themen

Themen: S.Paulus

6 - Access Governance

Sicherheit im Umgang mit elektronischen Informationen bedeutet auch immer, sicherzustellen, dass nur der an die Daten herankommt, der dies auch darf. Doch wer entscheidet darüber, wer etwas darf, und wie kommt man an seine Rechte? Welche Technologien sind erforderlich, um dies durchzusetzen? Der Vortrag soll einen Überblick über den Themenbereich des Access Governance geben, und mit Beispielen aus der Hochschule Mannheim demonstrieren.



2 - Themen

Themen: S.Paulus

7 - Security Response: was ist das und warum braucht man das?

Software ist nie 100% sicher, kein Entwickler der Welt schafft es, Code zu schreiben, der nicht doch mal einen Fehler enthält, oder einem Angreifer eine Schwachstelle anbietet. Deswegen ist es wichtig, dass man als Hersteller weiss, wie man mit dieser Situation umgeht, und sich darauf vorbereitet. Dieser Prozess der „Security Response“ soll dargestellt werden, die verschiedenen Optionen diskutiert, und Empfehlungen für KMUs gegeben werden.



2 - Themen

Themen: S.Paulus

8 - SSL Heartbleed

Die „Heartbleed“ Schwachstelle im SSL Protokoll hat die gesamte Internet-Gemeinde Anfang dieses Jahres stark verunsichert - war es doch möglich, ein korrekt konfiguriertes und aktuell gepatchtes SSL anzugreifen. Der Vortrag soll die Vorgehensweise von SSL erläutern, die Implementierungsschwierigkeiten diskutieren, und erklären, wie es zu der Heartbleed-Schwachstelle kommen konnte. Ideal wäre eine Demonstration mit einem Packet Sniffer.



2 - Themen

Themen: S.Paulus

9 - Security Patterns in der Software-Entwicklung

Security Patterns sind etablierte, implementierungsunabhängige Lösungskonzepte für wiederkehrende Sicherheitsprobleme, etwa „SSL“ für die Sicherheitsanforderung „authentische und vertrauliche Kommunikation“. Erläutern Sie das Konzept der Security Patterns, und stellen Sie beispielhaft Security Patterns in den folgenden Themenbereichen vor: Benutzerverwaltung, Session Management, Auditierbarkeit, Sichere Speicherung von Passwörtern, und elektronische Urkunden.



2 - Themen

Themen: S.Paulus

10 - Messbarkeit von Sicherheit

Um die IT und im Speziellen Software professioneller zu machen, ist es erforderlich, Kennzahlen einzuführen, etwa um den Fortschritt über die Zeit messen zu können, oder nachvollziehbare Ziele setzen zu können. Im Sicherheitsbereich ist dies etwas schwieriger, da Sicherheitseigenschaften oft viel schwerer zu messen sind, als „Unsicherheitseigenschaften“. Erläutern Sie, wie man Sicherheit messen kann, welche Ansätze es gibt und welche Probleme man sich dadurch schafft.



2 - Themen

Themen: S.Paulus

11 - Datenschutz bei Big Data: Probleme und Lösungsansätze

Big Data bezeichnet die Auswertung von sehr großen Mengen von Daten, um bestimmte Profilinformationen zu gewinnen, die auf statistischer Basis Vorhersagen von Trends erlauben - bis hin zur Vorhersage individueller Entscheidungen, die der Betroffene selbst noch gar nicht kennt. Inwiefern bestehen in diesem Kontext Probleme mit dem Datenschutz? Sind solche Auswertungen erlaubt? Sollten sie erlaubt sein? Wo ist die Grenze? Beschreiben Sie den aktuellen Stand der Datenschutz-Diskussion im Big-Data-Umfeld und nehmen Sie Stellung.



2 - Themen

Themen: S.Paulus

12 - Internet of Things: wie verändert sich die Bedrohungslage?

Als Internet of Things wird der Trend bezeichnet, nicht nur beliebige Datenquellen (z.B. Sensoren) auszuwerten, sondern darüber hinaus die Steuerungsmöglichkeiten von elektronischen Bauteilen zu nutzen, um auf Basis von IT-gestützten oder gar automatisierten Entscheidungen Prozessabläufe und Umgebungsgestaltung zu verändern. Welche Risiken sind damit verbunden, und in welcher Form sind diese anders als die heutigen Risiken der Informationssicherheit?