Pre-Course Meeting

Proseminar
„Network Hacking & Defense“

Dr. Holger Kinkelin and Nadine Herold

Content

www.fotoila.de

- ❑ **Administrative Issues**
  - ▪ Responsibilities
  - ▪ Learning Targets of the Proseminar
  - ▪ Registration / Topic Selection
  - ▪ Grading
  - ▪ Etc.

- ❑ Overview on Topics

Responsibilities and Basic Information

- Lecturer:
  - Prof. Dr.-Ing. Georg Carle
- Organisation
  - Holger Kinkelin (kinkelin@net.in.tum.de)
  - Nadine Herold (herold@net.in.tum.de)
- Advisors:
  - Nadine, Holger and other members of the Chair
- Overview
  - Main Language: German
  - Extent: 2 SWS (4 ECTS)
  - Course Type: Proseminar (introductory seminar)
  - We offer 16 places

Learning Targets

- Learn how to work scientifically
  - Research information
  - Write a scientific paper
  - Create a presentation/give a talk
  - Perform peer reviews

➔ Training for seminars/BA/MA/…

- Network-related topics
  - Understand threats in networked environments
  - Understand how attacks work
  - Understand how defense mechanisms work

➔ Learn new or refresh knowledge

How to register to the Proseminar (I)

- New TUM-procedure for student admission:
  - Central matching system for courses.
  - Part of TUMonline.

  → We don’t decide who gets a place in the proseminar!

- [19.6. - 22.6.14] Inform yourself in TUMonline about the course offerings for the winter term 2014. ✓
- [23.6. - 4.7.14] Attend pre-course meetings for the courses that interest you. ✓
- [4.7. - 8.7.14] Register for the Hacking proseminar in the appropriate matching system with your TUMonline ID.
- [12.7.14] Log into the matching system and check if you have been assigned to the Hacking proseminar.

How to register to the Proseminar (II)

- ❑ The matching system allows us to give a bonus to those students that joined the pre-course meeting.
  - → It is more likely that you receive a place if you want…

- ❑ So write down your name, student ID number, and mail address to the list of participants of today's meeting.
  - ❑ This is voluntary!

IMPORTANT

Bonus!

How to get a Topic after successful Registration?

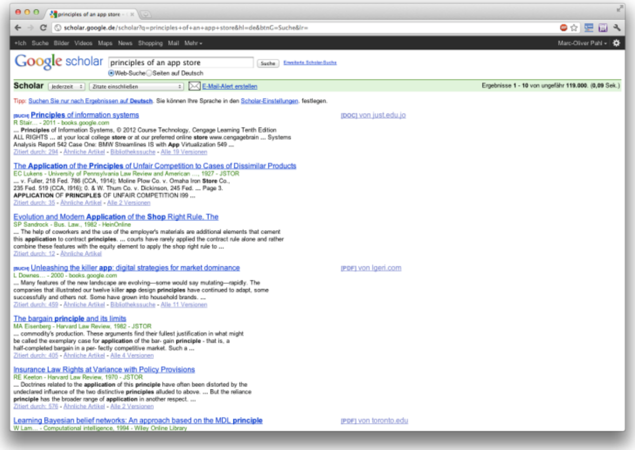
- ❑ Join the Kickoff-Meeting in the 1st week of winter term.
  - ❑ Mandatory!
- ❑ The advisors present all topics in detail.
- ❑ You tell us your favorite 3 topics.
- ❑ We apply another matching system.
- ❑ You receive your topic + contact to the advisor.

Modus might change slightly.

Topic Handling

- From your advisor you may receive some literature.
  - This is just to get you started

- Find appropriate (scientific) sources yourself
  - scholar.google.com
  - acm.org
  - ieee.org
  - You sources' sources
  - (Finding scientific sources is tricky for some hacking related topics…)


principles of an app store
scholar.google.de/scholar?q=principles+of+an+app+store&hl=de&btnG=Suche&lr=
+Ich Suche Bilder Videos Maps News Shopping Mail Mehr
Marc-Oliver Pahl
Google scholar
Suche
Erweiterte Scholar-Suche
Web-Suche
Seiten auf Deutsch
Scholar
Jederzeit
Zitate einschließen
E-Mail-Alert erstellen

principles of an app store

Ergebnisse **1 - 10** von ungefähr **119.000**. (**0,09** Sek.)

Tipp: Suchen Sie nur nach Ergebnissen auf **Deutsch**. Sie können Ihre Sprache in den Scholar-Einstellungen. festlegen.

[BUCH] **Principles** of information systems — [DOC] von just.edu.jo
R Stair... - 2011 - books.google.com
… **Principles** of Information Systems, © 2012 Course Technology, Cengage Learning Tenth Edition ALL RIGHTS … at your local college **store** or at our preferred online **store** www.cengagebrain … Systems Analysis Report 542 Case One: BMW Streamlines IS with **App** Virtualization 549 …
Zitiert durch: 294 - Ähnliche Artikel - Bibliothekssuche - Alle 19 Versionen

The **Application** of the **Principles** of Unfair Competition to Cases of Dissimilar Products
EC Lukens - University of Pennsylvania Law Review and American …, 1927 - JSTOR
… v. Fuller, 218 Fed. 786 (CCA, 1914); Moline Plow Co. v. Omaha Iron **Store** Co., 235 Fed. 519 (CCA, I916); 0. & W. Thum Co. v. Dickinson, 245 Fed. … Page 3. **APPLICATION** OF **PRINCIPLES** OF UNFAIR COMPETITION I99 …
Zitiert durch: 35 - Ähnliche Artikel - Alle 2 Versionen

Evolution and Modern **Application** of the **Shop** Right Rule, The
SP Sandrock - Bus. Law., 1982 - HeinOnline
… The help of coworkers and the use of the employer's materials are additional elements that cement this **application** to contract **principles**. … courts have rarely applied the contract rule alone and rather combine these features with the equity element to apply the shop right rule to …
Zitiert durch: 12 - Ähnliche Artikel

[BUCH] Unleashing the killer **app**: digital strategies for market dominance — [PDF] von lgeri.com
L Downes... - 2000 - books.google.com
… Many features of the new landscape are evolving—some would say mutating—rapidly. The companies that illustrated our twelve killer **app** design **principles** have continued to adapt, some successfully and others not. Some have grown into household brands. …
Zitiert durch: 459 - Ähnliche Artikel - Bibliothekssuche - Alle 11 Versionen

The bargain **principle** and its limits
MA Eisenberg - Harvard Law Review, 1982 - JSTOR
… commodity's production. These arguments find their fullest justification in what might be called the exemplary case for **application** of the bar- gain **principle** - that is, a half-completed bargain in a per- fectly competitive market. Such a …
Zitiert durch: 405 - Ähnliche Artikel - Alle 4 Versionen

Insurance Law Rights at Variance with Policy Provisions
RE Keeton - Harvard Law Review, 1970 - JSTOR
… Doctrines related to the **application** of this **principle** have often been distorted by the undeclared influence of the two distinctive **principles** alluded to above. … But the reliance **principle** has the broader range of **application** in another respect. …
Zitiert durch: 576 - Ähnliche Artikel - Alle 2 Versionen

Learning Bayesian belief networks: An approach based on the MDL **principle** — [PDF] von toronto.edu
W Lam... - Computational intelligence, 1994 - Wiley Online Library

Just presenting the given literature is NOT enough

Paper procedure

- First version of your paper
  - Agree on the content with your advisor
  - Use the supplied paper template from the webpage
  - Keep in touch with your advisor
  - Try to finish well in time so you advisor can give you feedback

- Write reviews
  - You will be given two papers of your fellow students

- Final version of your paper
  - Use the received reviews to improve your paper
  - You will also receive some feedback from your advisor

Talks and Papers
can be in
German or English!

Talk procedure

- Prepare your talk
  - Finished slides must be discussed with advisor 1 week before the talk
  - Advisors usually offer the opportunity of test talks
- Give your talk
- Session chair for one talk
  - Introduce the talk
  - Lead the discussion after the talk
  - Ask at least one question
- Mandatory attendance on all sessions

Talks and Papers can be in German or English!

Further Information

- Webpage of the Proseminar: http://www.net.in.tum.de/de/lehre/ws1415/seminare/proseminar-network-hacking/
  - Slides: How to write a paper
  - Slides: How to write a review
  - …
  - Hint: Webpage is not online yet.

Grading

Grading parts:

1. Both of your paper submissions (6 (full) to max. 8 pages ACM) (50%)
   - 1st Version: 37,5%
   - 2nd Version: 12,5%

2. Your talk (20–25min, following discussion and feedback) (25%)
   - Content is graded
   - Personal presentation style is not

3. Your reviews of papers from other seminar participants (12.5% each)

Review quality is Nr. 1 reason for not getting a good grade!

Grading – influencing factors

- Observe the deadlines
  - Advisor meetings are compulsory
  - Use the upload form on our webpage for your submissions
  - 0.3 degrading per day for missed deadlines
- No submission
  - Grade 5 for the concerning part
  - (But you still can continue with the Proseminar!)
- Write the paper yourself
  - Plagiarism → disqualification → Grade 5
  - In doubt ask your advisor!

Seminar Schedule and Deadlines

Given dates might change slightly
(except date of kickoff meeting!)

Required Action	Dates
Kickoff Meeting (room 03.07.023)	Fr. 10.10.2014
Receive literature from advisor personally or per mail	Until Fr. 17.10.2014
Personal meeting with advisor to structure work, e.g., discussion of received literature**. Be prepared!**	Until Fr. 31.10.2014
Hand in **detailed** structure of paper and talk per mail	Fr. 21.11.2014
Hand in **pre-final** presentation slides per mail. (Advisor decides whether it is necessary to have another meeting to refine slides or not!)	Until 1 week before your talk
Upload paper (1. Version)	Fr. 19.12.2014
Upload Reviews	Fr. 09.01.2015
Seminar talks	Fr. 14.11.2014 - Fr. 23.01.2015
Upload paper (2. Version) and final slides	Fr. 30.01.2015

?
R

Content

www.fotoila.de

- ❑ Administrative Issues
  - ▪ Responsibilities
  - ▪ Learning Targets of the Proseminar
  - ▪ Registration / Topic Selection
  - ▪ Grading
  - ▪ Etc.
- ❑ **Overview on Topics**

Caveat Lector!

The following selection of topics is not final yet.

For each topic you need to present not only the attack but also remedies/how to fix/prevent the attack!

We encourage you to integrate a demonstration into your talk. Please do only attack your own infrastructure!

Attacks on Networks and the Infrastructure

- Footprinting, Scanning and Enumeration
  - How does an attacker prepare attacks on networks?
- "Classic" attacks on networks
  - What can an attacker do with insecure protocols, such as ARP, IP, TCP, …?
  - Cryptography for authentication/confidentiality
- Attacks on DNS
  - How can a hacker mess with name resolution?
  - DNSSec?
- Attacking BGP
  - What happens if an attacker messes with routing?

Attacks on Cryptography

- Cryptography for communication
  - Get to know different variants of crypto protocols. Learn about their differences and individual problems.
- Defending WLANs
  - Learn why WEP was such a bad protection for WLANs.
  - Is WPA2 better? And are we safe now? Really?
- Padding Oracles
  - Learn how a weakness of Block Ciphers in conjunction with padding and a specific operational mode works.
- Cold Boot Attacks
  - Even when full disc encryption is used, data is endangered as it is possible to extract the encryption key from memory…

Attacks on the Web 2.0 and Online Services

- ❑ SQL Injection
  - Hackers are able to insert unwanted SQL statements via badly implemented interfaces of web sites. How does that work?
- ❑ Cross Site Scripting
  - What can happen if you inject Java Script into a web site via an badly implemented interface?
- ❑ Attacking Online Games
  - Online gaming is an important industry. Attackers try to disrupt services and/or cheat. How does that work?

Exploits and Malware

- ❑ Buffer Overflows
  - What happens if you write more data into a buffer as it can hold? What if your data contains executable code, …?
- ❑ Return Oriented Programming
  - Instead of injecting code from outside, hackers can modify the instruction flow of an application. How does that work?
- ❑ Malware: Of Trojans, Bot Nets and Viruses
  - Learn about different kinds of malware.
- ❑ Host Integrity Protection
  - Applications exist that help an administrator defending her network. Learn how they work and about their limitations.

Questions?

Are there any questions left?