Proseminar

Entwicklung sicherer Software

Übung im Wintersemester 2008/2009

Martin Gruhn
http://www.inf.fu-berlin.de/inst/ag-se/

Agenda

Freie Universität Berlin

- **Einführung**
  - Inhalt & Ziele
- Tipps für Ausarbeitung
  - Wissenschaftliches Arbeiten
  - Struktur der Ausarbeitung
  - Arbeit mit Literatur (Recherche, Zitieren)
  - Hilfe zur Selbsthilfe
- Organisation
  - Genereller Ablauf
  - Gegenseitige Bewertung
  - Notenkriterien
- Themen
  - Vorstellung
  - Vergabe

Worum geht's?

- Werkzeuge und Praktiken für die Entwicklung sicherer Software
- Typische Angriffe und Verletzlichkeiten im Bereich Webanwendungen
- Themengebiete
  - Entwicklungsprozess für sichere Software
  - Wie misst man Sicherheit?
  - Praktiken und Werkzeuge bei Entwicklung und Tests
  - Angriff & Verteidigung
  - Am Rande: Usability, Open Source

Worum geht's **nicht**?

- Sicherheit ist mehr als Kryptographie und Zugriffsschutzmechanismen
- Wir betrachten keine: Algorithmen, Protokolle, ...
  - Da gibt es genügend Spezialisten für
- Sichere Software benötigt holistischen Ansatz
  - Software Engineering >> Programmiersprachen
  - Security Engineering >> Kryptographie

Ziele

- Üben, sich selbständig anhand wissenschaftlicher Quellen in ein Thema **einzuarbeiten** und es zu strukturieren.
- Erfahrung sammeln, ein kompliziertes Thema **als Vortrag aufzubereiten** und verständlich vorzutragen und zu vermitteln.
- Üben, technisches Material **schriftlich zusammenzufassen**, in eine vorgegebene Form zu strukturieren und es zu **kommentieren und bewerten**.
- Lernen, Arbeiten anderer Teilnehmender zu **begutachten** und hilfreiche Verbesserungsvorschläge zu formulieren.
- Proseminar vs. Seminar:
  - Weniger Inhalt, dafür mehr Wert auf Form
- Außergewöhnlich: Baut nicht direkt auf VL des ersten Studienjahres auf

Zielgruppe, Voraussetzungen

Freie Universität Berlin

- Voraussetzungen
  - Wissen eines 3. Semesters
  - OO Programmierung in Java
  - Vorlesung Anwendungssysteme
  - Selbstsändiges Arbeiten
    (auf dem Niveau eines 3. Semesters)
- Manche Themen setzen voraus
  - Erste Erfahrung mit Webanwendungen
    - Grob: Datenbanken/SQL, HTML, Javascript
    - Evtl. weitere Technologien (z.B. HTTP)
  - Vorlesungen SWT, Netzprogrammierung
  - Oder:
    - Selbstvertrauen in eigene Arbeit und keine Berührungsangst
    - Bereitschaft für etwas Mehrarbeit

Agenda

- Einführung
  - Inhalt & Ziele
- **Tipps für Ausarbeitung**
  - Wissenschaftliches Arbeiten
  - Struktur der Ausarbeitung
  - Arbeit mit Literatur (Recherche, Zitieren)
  - Hilfe zur Selbsthilfe
- Organisation
  - Genereller Ablauf
  - Gegenseitige Bewertung
  - Notenkriterien
- Themen
  - Vorstellung
  - Vergabe

Wissenschaftliche Literatur

Freie Universität Berlin

- Was ist *wissenschaftliche* Literatur?
  - Aufsätze zu wissenschafltichen Konferenzen (s.u.)
  - Aufsätze in wissenschaftlichen Zeitschriften (Journals)
  - Fachbücher
- Was ist *nicht* wissenschaftlich
  - wikipedia.org
  - c't, ix, heise.de, golem.de (online wie offline)
  - Blogbeiträge
- Nicht wissenschaftliche Quellen
  - Sind häufig nützlich, um Überblick zu bekommen (wikipedia)
  - Weisen manchmal in eine gute Richtung – manchmal nicht!
  - Sind häufig nicht zitierfähig, in gut begründeten Fällen schon
  - Gesunden Menschenverstand nutzen!

Konferenzen und Verbände

Freie Universität Berlin

- Wissenschaftliche Konferenzen
  - z.B. “International Conference on Web Security”
  - Aufsätze (Paper) unterliegen Peer Review Verfahren
  - Paper werden in sog. “Proceedings” veröffentlicht
  - Gesponsort von Dachorganisationen (z.B. IEEE, ACM)
- Dachorganisationen in der Informatik
  - Gesellschaft für Informatik e.V. (GI)
  - Association for Computing Machinery (ACM)
  - IEEE Computer Society
- Peer Review Verfahren:
  - Call for Paper bis zu bestimmtem Datum (Paper Deadline)
  - Gutachten von Wissenschaftlern aus Programmkomitee
    - Accept/Reject und Verbesserungsvorschläge
  - Einreichen der camera-ready version

Vorgehen 1

- Thema auswählen
- Literatur (Fachbücher, Aufsätze) suchen
  - FB-Bibliothek oder Fernleihe (TU UB ist gut ausgestattet)
  - Wissenschaftliche Aufsätze findet man über
    - ACM The Guide (nicht nur ACM)
    - IEEE digital library
    - SpringerLink, Google Scholar, Citeseer
- Recherche
  - Zuerst: Zentrale Aufsätze (Überblicksartikel), nicht zu speziell, dann
  - Referenzierte Aufsätze (Schneeballprinzip)
- Literatur sichten
  - Heißt auch: Unpassende und/oder unverständliche Literatur verwerfen

Vorgehen 2

- Lese- und Arbeitstechniken
  - Lesen: Abstract + Summary + Querlesen
  - Literatur ablegen, keine Blattsammlungen
  - Exzerpieren kann nützlich sein
  - Literaturverwaltungssoftware empfehlenswert
- Schwerpunkt setzen
  - Hilfreiche Fragen an die eigene Arbeit:
    Worum geht es (in drei Sätzen)?
  - Warum ist das wichtig?
  - Welches sind die zentralen Erkenntnisse?

Ausarbeitung: Inhalt und Struktur

Freie Universität Berlin

- Titel
  - Erst Arbeitstitel, am Ende etwas Prägnantes/Bezeichnendes
- Zusammenfassung
  - Worum gehts, was sind die Kernaussagen (Ergebnisse vorwegnehmen)
  - Am Ende schreiben
- Einführung
  - Motivation
  - Einordnung und Abgrenzung
  - Gliederung/Inhaltsangabe
- Hauptteil
  - Literatur zusammenfassen gegenüberstellen und beurteilen
  - Achten auf Gedankenfluss, Nachvollziehbarkeit!
- Schluss
  - Zusammenfassung, Ausblick
  - Keine neuen Erkenntnisse!
- Literaturverzeichnis

Umfang: ca. 5 Seiten
(Anzahl Worte kommt noch)

Zitieren 1

- Bsp.: “Glisson, McDonald und Welland stellen in ihrem Aufsatz über Sicherheit bei Webanwendungen [GDW06] eine Studie vor, die...”.
- Direktes Zitieren in Informatik eher unüblich
- Literaturverzeichnis:

  [GDW06] Glisson, W. B.; McDonald, A. & Welland, R., *Web Engineering Security: A practitioner's perspective*. Proceedings of the 6th International Conference on Web Engineering (ICWE '06), 2006, 257-264.

  - Ob Punkt oder Komma zwischen den Feldern ist egal, hauptsache einheitlich!
- Bei Aufsätzen aus Proceedings taucht im Literaturverzeichnis die Printversion auf (nicht die URL zum PDF)
- Literaturverwaltungssoftware empfehlenswert

Zitieren 2

Freie Universität Berlin

- Zitieren von Internetquellen
  - Wie bei Aufsätzen, das heißt:
    - Autor(en), Jahr der Veröffentlichung, URL und Datum des Abrufs angeben (“Zugriff: 28.10.2008”)
  - Wenn das nicht da steht: Sehr schlechte Quelle!
  - Quelle als PDF lokal speichern
- Bildzitate (Faustregeln)
  - Ja: Wenn das Bild selbst diskutiert wird.
  - Schwierig: Als bloße Illustrierung des eigenen Textes.
  - Besser: Selbst nachzeichnen (Inkscape, OpenOffice Draw)

Vorgaben und Ratbeger

Freie Universität Berlin

- Ratgeber: Schreiben & Zitieren
  - Weitere Ratgeber werden von der Homepage verlinkt (kommt noch)
- Format und Schreibwerkzeuge
  - Latex ist schon schön (siehe Inf Brückenkurs!)
  - Meinetwegen aber auch Word oder OpenOffice
  - Author Kit: Vorlagen verlinkt von Homepage (kommt noch)
- Empfehlung:
  - LyX (WYSIWYW) + JabRef (Einarbeitungsaufwand lohnt sich!)

Vortrag

Freie Universität Berlin

- Der Vortrag
  - Sollte ca. 30 Minuten dauern
- Nach dem Vortrag
  - Klärung von Sachfragen
  - Inhaltliche Diskussion: VortragendeR gibt Startpunkt für Diskussion
- Nach der Diskussion
  - Feedback zum Vortrag selbst
  - Feedbackzettel von allen

Agenda

Freie Universität Berlin

- Einführung
  - Inhalt & Ziele
- Tipps für Ausarbeitung
  - Wissenschaftliches Arbeiten
  - Struktur der Ausarbeitung
  - Arbeit mit Literatur (Recherche, Zitieren)
  - Hilfe zur Selbsthilfe
- **Organisation**
  - Genereller Ablauf
  - Gegenseitige Bewertung
  - Notenkriterien
- Themen
  - Vorstellung
  - Vergabe

Organisation: Peer Review

Freie Universität Berlin

- JedeR wird von zwei Schrift- und zwei Vortrags-GutachterInnen begutachtet
  - Und begutachtet selbst zwei Ausarbeitungen und zwei Vorträge
- **Am 23.02.2009**
  - Ausarbeitung und Folien an Schriftgutachter (und CC an mgruhn@...)
- **Am 27.02.2009**
  - Gutachten per Email an AusarbeiterIn (und CC an mgruhn@...)
- Zuordnung gebe ich rechtzeitig auf Webseite bekannt

Organisation: Zwischentreffen

Freie Universität Berlin

- Gesammelte Sprechstunde
  - 4-5 Leute gleichzeitig (Themenbezogen) für ca. 1h
- Bis dahin
  - Ergebnisse der Literaturrecherche
  - Schwerpunkt (Inhalt in 3 Sätzen)
  - Vorläufige Gliederung
  - JedeR macht Handout für die anderen
- 3 Termine
  - **Dienstag, 13.01.2009 (16-17 und 17-18h)**
  - **Donnerstag, 15.01.2009 (16-17 und 17-18h)**
  - **Dienstag, 20.01.2009 (16-17 und 17-18h)**
- Außerdem: Zeitplan für Blocktermin
  - Anforderung: ca. 5h täglich (entspricht 2 SWS)
  - 6 Vorträge pro Tag (à 1h) -> nur bis Donnerstag

Organisation Themenvergabe

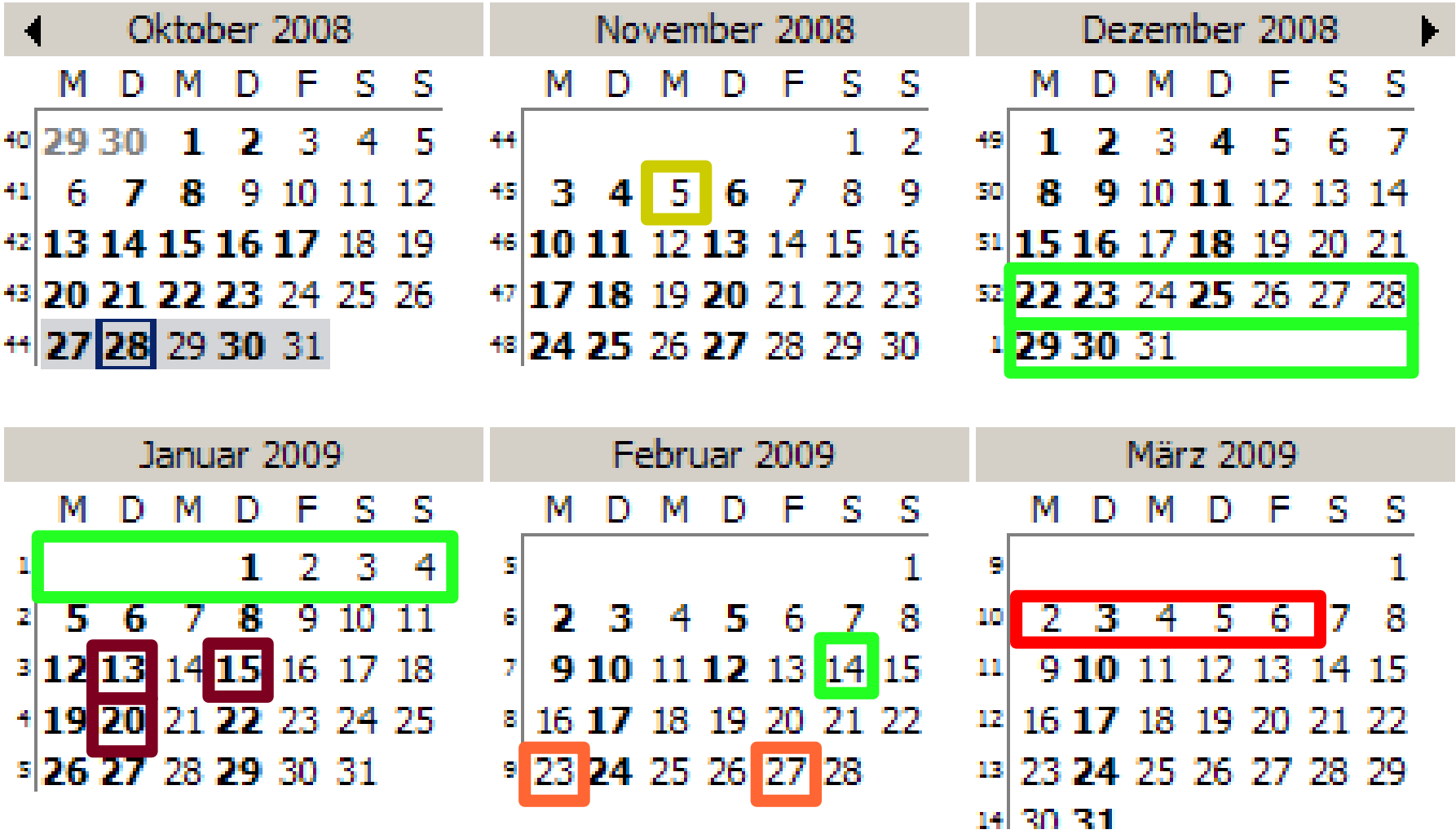
Freie Universität Berlin

- **Bis 05.11.2008**
  - JedeR schickt mir per Email 3 Themenwünsche in priorisierter Reihenfolge
    - Adresse: mgruhn@inf...
    - Folgenden Betreff verwenden!

      [PSS08]<Thema_prio1><Thema_prio2><Thema_prio3>

      z.B.: [PSS08] AV4, PP3, EZ2
      (ggf. Sicherheitshalber nochmal mit vollen Titeln in Email)
  - Gern auch eigene Themenvorschläge, idealerweise mit Literaturangabe(n)
- **Bis 12.11.2008**
  - Bekanntgabe der Themenverteilung auf LV-Homepage

Zeitplan


Oktober 2008
M D M D F S S
40 29 30 1 2 3 4 5
41 6 7 8 9 10 11 12
42 13 14 15 16 17 18 19
43 20 21 22 23 24 25 26
44 27 28 29 30 31
November 2008
M D M D F S S
44 1 2
45 3 4 5 6 7 8 9
46 10 11 12 13 14 15 16
47 17 18 19 20 21 22 23
48 24 25 26 27 28 29 30
Dezember 2008
M D M D F S S
49 1 2 3 4 5 6 7
50 8 9 10 11 12 13 14
51 15 16 17 18 19 20 21
52 22 23 24 25 26 27 28
1 29 30 31
Januar 2009
M D M D F S S
1 1 2 3 4
2 5 6 7 8 9 10 11
3 12 13 14 15 16 17 18
4 19 20 21 22 23 24 25
5 26 27 28 29 30 31
Februar 2009
M D M D F S S
5 1
6 2 3 4 5 6 7 8
7 9 10 11 12 13 14 15
8 16 17 18 19 20 21 22
9 23 24 25 26 27 28
März 2009
M D M D F S S
9 1
10 2 3 4 5 6 7 8
11 9 10 11 12 13 14 15
12 16 17 18 19 20 21 22
13 23 24 25 26 27 28 29
14 30 31

Schriftbegutachtung

Freie Universität Berlin

- Leitfragen
  - Was ist gut gelungen? Was fehlt offensichtlich oder ist inkonsistent oder sachlich falsch? Was ist schwer verständlich?
  - Bei Folien: Ist der Detailgrad (z.B. Folienanzahl) geeignet für die vorgesehene Vortragsdauer?
- Kritik
  - Wird ausschließlich an den Dokumenten geübt, niemals an der Person, die sie geschrieben hat.
  - Kritik darf nicht pauschal sein, sondern muss sich deutlich auf bestimmte Aspekte oder Stellen beziehen
  - Idealerweise ist Kritik konstruktiv, macht also einen konkreten Verbesserungsvorschlag.
- Die Erfahrung sagt, dass die Studierenden oft sehr "nett" zueinander sind. Damit ist aber niemandem geholfen.

Vortragsbegutachtung

Freie Universität Berlin

- Aufbau des Vortrags, u.a.:
  - Gibt es eine Inhaltsübersicht und Zusammenfassung?
- Inhalt des Vortrags, u.a.:
  - Sind die Erklärungen und Gedankenketten logisch, verständlich, vollständig, einsichtig, schlüssig?
- Sprachgebrauch, Vortragsstil, u.a.:
  - Wird für das selbe Konzept durchgängig das selbe Wort verwendet? Ist der Satzbau hinreichend einfach?
- Foliensatz, u.a.:
  - Sind die Folien gut lesbar? Sind (wo sinnvoll) Abbildungen enthalten?
- Insgesamt, u.a.:
  - Hat man in diesem Vortrag etwas gelernt? Hat er Spaß gemacht? War er überzeugend?

Scheinkriterien, Notenmaßstab

Freie Universität Berlin

- Voraussetzung
  - Anwesenheit (max. 1 Fehltag während Block)
- Note (in dieser Reihenfolge)
  - Ausarbeitung
  - Vortrag
  - Einhaltung von Terminen (für Gutachten)
  - Mitarbeit im Seminar
  - Studentische Beurteilung

Bei Problemen

1. Problem identifizieren.
2. In Ratgebern nachlesen.
3. Im Wiki der Lehrveranstaltung nachlesen.
4. Mailingliste der Lehrveranstaltung (siehe Homepage)
5. Betreuer ansprechen (Email, Sprechstunde)

Themen

- A: Sicherheit allgemein
- PP: Prozessmodell und Praktiken
- AV: Angriff und Verteidigung
- PW: Praktiken und Werkzeuge
- EZ: Evaluieren und Zertifizieren
- SOS: Sicherheit und Open Source
- S: Sonstiges

Sicherheit allgemein (A)

Freie Universität Berlin

A1) Was ist (IT-) Sicherheit

- Überblick über Sicherheit: Begriffe
- Akteure im Bereich Sicherheit
  - BSI, Certs, CVD/NVD
- Vorgegebene Literatur:
  - Security in the real world; Security Assurance

Prozessmodelle und Praktiken (PP)

Freie Universität Berlin

PP1) Microsofts Security Development Lifecycle (SDL)

- Vorstellung des Entwicklungsprozesses und Ergebnisse der Anwendung
- Vergleich mit CLASP

PP2) Comprehensive, Lightweight Application Security Process

- Vorstellung des CLASP des OWASP
- Struktur, Inhalt und Funktion
- Vergleich mit SDL

PP3) Entwicklungsprozess für sichere Software in der Praxis

- Studien über den tatsächlich durchgeführten Sicherheitsprozess
- Startpunkt für Literatur vorgegeben

PP4) Spezielle Praktiken des Security Engineering

- Allgemeine Prinzipien des Security Engineering
- Praktiken und Werkzeuge zur Risikomodellierung, Angriffsmodellierung

Angriff und Verteidigung (AV)

Freie Universität Berlin

AV1) Schwachstellendatenbanken und -taxonomien
- Vorstellung der Taxonomien: Inhalt und Zweck
- CVE, CWE und CAPEC von Mitre

AV2) Hacker-Kultur
- Konferenzen und wichtige Akteure im Bereich IT-Sicherheit
- Welche Rolle haben “Hacker” im Bereich Sicherheit

AV3) Spezielle Schwachstellen: SQL Injection
- Schwachstelle, Voraussetzungen
- Angriffsmöglichkeiten
- Gegenmaßnahmen

AV4) Spezielle Schwachstellen: Cross-Site-Scripting

AV5) Spezielle Schwachstellen: Eine weitere aus OWASP Top 10

Praktiken und Werkzeuge (PW)

Freie Universität Berlin

PW1) Statische Werkzeuge für Sicherheitstests

- z.B. Code-Analyse
- Vorstellung und Vergleich verschiedener Werkzeuge
- Einordnung in den Entwicklungsprozess

PW2) Dynamische Werkzeuge für Sicherheitstests und Laufzeitüberwachung

- z.B. Intrusion Detection System (IDS)
- s.o.

PW3) Praktiken für Web Application Security / Bau sicherer LAMP Anwendungen

- Praktisches Thema für Fortgeschrittene
- Ähnlich den obigen Themen (Praktiken, Werkzeuge, Entwicklungsprozess), aber angewandt und übergreifend
- LAMP: Linux, Apache, MySQL, PHP (Perl, Python)

Evaluieren und Zertifizieren (EZ)

Freie Universität Berlin

EZ1) Systems Security Engineering Capability Maturity Model

- Prozessreifemodell zum Evaluieren des Entwicklungsprozesses sicherer Software
- Inhalt, (Un-) Sinn und Zweck

EZ2) Common Criteria

- Rahmenwerk zum Evaluieren von Produkten bzgl. Sicherheit
- Geschichte, Inhalt, (Un-) Sinn und Zweck

EZ3) Security Metrics

- Wie misst man Sicherheit?
- Vorstellung verschiedener Metriken
- Kritik

Sicherheit und Open Source (SOS)

Freie Universität Berlin

SOS1) Sicherheit in OSS: Chancen und Risiken

- Was spricht für und gegen Open Source Software mit Bezug zu Sicherheit
- Zusammenstellung von Argumenten bekannter Forscher und Sicherheitsexperten

SOS2) Studien über Sicherheit und Open Source

- In Abstimmung mit Security Metrics
- Vorstellung und Kritik verschiedener Studien zu Open Source vs. Closed Source Sicherheit
- Beantwortung der Frage “Was ist sicherer?” möglich?

Sonstiges (S)

Freie Universität Berlin

S1) Usability: Nutzbarkeit und IT-Sicherheit

- Vorgegebenes Paper: Why Johnny can't encrypt?
- Schwierigkeiten bei der Anwendung von Sicherheitsmaßnahmen

S2) Wahlmaschinen

- Problematik, Anforderungen
- Vorgegebenes Paper: How To Cheat at the Lottery?

Nicht vergessen

Freie Universität Berlin

- Bei Mailingliste angemeldet?
- Thema notiert?
- Termine vermerkt (insb. Sprechstunden!)?

Danke!