Themen zur Computersicherheit

Einleitung

PD Dr. Reinhard Bündgen
buendgen@de.ibm.com

Attacken in den Nachrichten

- 11/2014: Sony Pictures Entertainment
- 02/2015: NSA/GCHQ hacked SIM manufacturer Gemalto
- 04/2015: AT&T to pay $25M
- 05/2015: Chinese breach: data of 4M fed workers
- 08/2015: Carphone Warehouse: 2,4M Kundendaten
- 08/2015: VW Hack: Wegfahrsperre
- 09/2015: Ashley Medison Seitensprungportal
- 03/2016: PKWs über Funk hackbar
- 03/2016: Digitaler Bankraub in Bangladesh
- 04/2016: Türkisches Wählerverzeichnis: 49M Wähler
- 06/2016: LinkedIn Hack 113M Passwort Hashes
- 09/2016: 800K klartext Passwörter bei Brazzers veröffentlicht
- 10/2016: Passwörter vom Dropbox Hack veröffentlicht
- 10/2016: DDoS auf Amazon, Twitter, Netfix, PayPal, Spotify ...

Attacken/Sicherheitslöcher mit Namen

- BEAST: SSL/CBC
- POODLE: SSL/Padding
- FREAK: SSL/short RSA keys
- RAWHAMMER: high frequency writes
- **Heart Bleed**: openSSL buffer overflow
- Logjam: small DH key, parameter reuse
- Shellshock: bash injection (string variables)
- Sweet32: birthday attack on 64 bit block ciphers
- Dirty Cow: Linux privilege escalation

Wie wichtig ist IT Sicherheit?

- im Durchschnitt kostet ein Einbruch in ein IT System $11M
- im Durchschnitt bleibt ein Einbruch 8 Monate lang unentdeckt
- die NSA kann die Telekommunikation einzelner Länder vollständig aufzeichnen
- in den USA wurden 2013 3000 Firmen über Hackerangriffe aufgeklärt

Abzusichernde IT Systeme

- online Geldtransaktionen
  - online banking
  - Internethandel
  - digitales Geld
- sensible Systeme (Privatsphäre)
  - online Steuererklärung
  - Gesundheitswesen
- demokratische Einrichtungen
  - Wählerregister
  - Wahlautomaten
- Dokumente, Kommunikation die Betriebsgeheimnisse enthalten
  - Bilanzen
  - Strategien
  - Entwürfe/Erfindungen
- Steuerungen von Industrieanlagen
  - stuxnet
- Energieversorgung
  - Smart-Meter
- Verkehr
  - elektrische Schlösser
  - Diebstahlsicherung
  - Verkehrsleitsysteme
  - vernetzte Autos
- IoT
  - ...
- ...

Sicherheit: Die Haustüre

- kontrolliert Zugang zum Haus
  - sichert Privatsphäre
  - sichert Eigentum
  - Was ist erlaubt? Wo ist die Grenze?
- Schutzarten
  - Regelungen (Versicherungen)
  - gesetzlicher Schutz
  - physischer Schutz
    - keine absolute Sicherheit
    - abhängig vom Werkzeug und Zeit
- Sicherheitsfragen
  - Ist die Türe der einzige Zugang zum Haus?
  - Mit welcher Disziplin wird abgeschlossen?
  - Liegt der Schlüssel unter der Fußmatte
  - soziale Bedrohungen / Erpressungen

Bedrohungen

- Gefährdungsfaktoren
  - höhere Gewalt
  - Fahrlässigkeit
  - technisches Versgagen
  - Vorsatz
  - organisatorische Mängel

OWASP Top 10

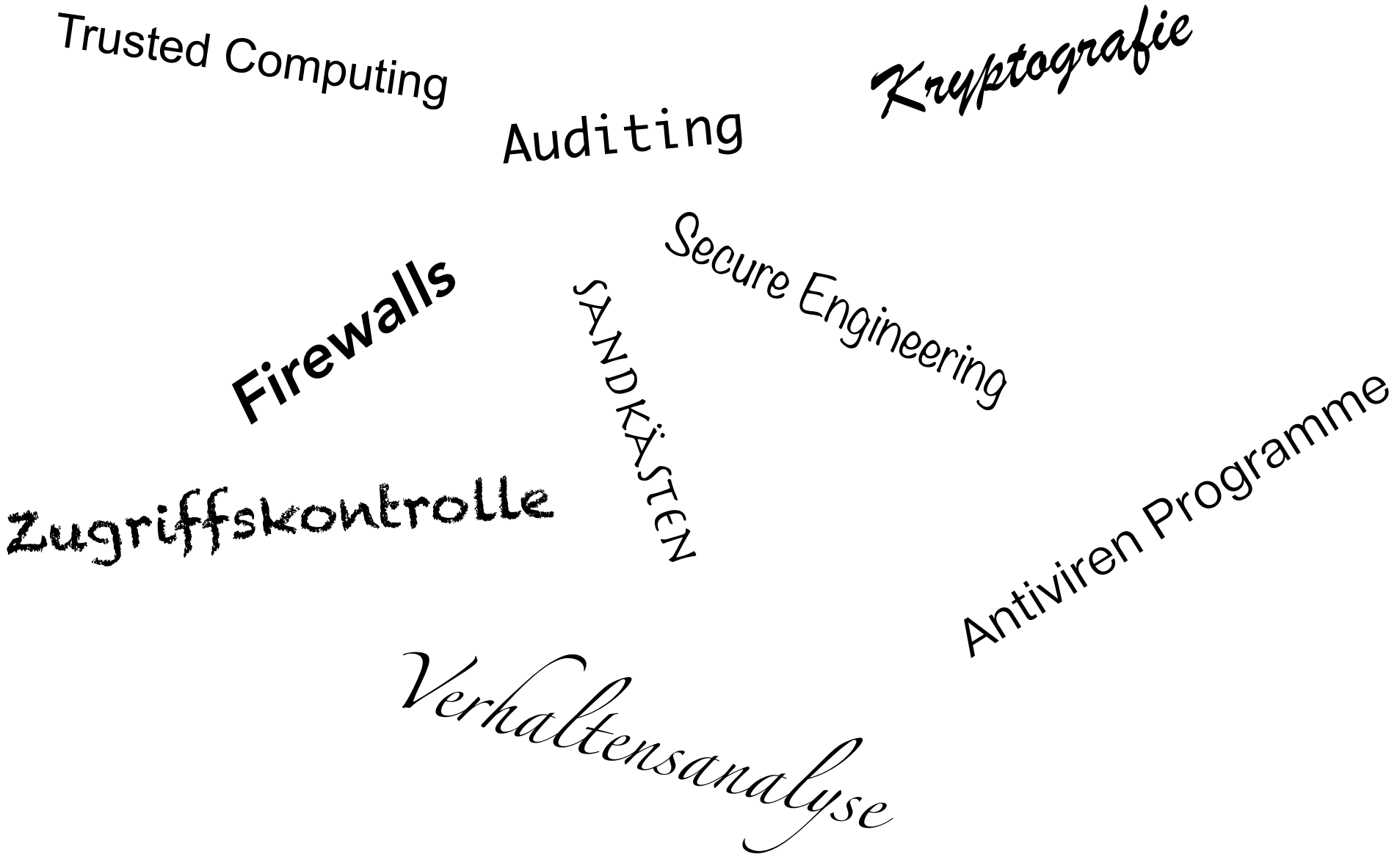
Open Web Application Security Project (OWASP)

- https://www.owasp.org/index.php/Main_Page
- sammelt die wichtigsten Bedrohungen für Web Applikationen

Top 10 für 2013

1) injection
2) broken authentication and session management
3) cross-site scripting (XSS)
4) insecure direct object references
5) security misconfigurations
6) sensitive data exposure
7) missing function level access control
8) cross site request forgery (CSRF)
9) using unknown vulnerable components
10) unvalidated redirects and forwards

Sicherheitstechnologien



Schutzziele

- Authentizität
  - Subjekt ist was/wer es vorgibt zu sein
- Datenintegrität
  - zu schützende Objekte werden nicht unerlaubt geändert
- Vertraulichkeit
  - Information ist nur Befugten zugänglich
- Verfügbarkeit
  - Daten oder Dienst sind immer Verfügbar
- Verbindlichkeit
  - ein Subjekt kann für eine Tat verantwortlich gemacht werden
- Anonymität
  - ein Dienst kann anonym genutzt werden
- Vertrauen
  - ein Dienst verhält sich wie erwartet

Security Engineering ist schwer

Software Engineering

- positive Ziele (Funktion, Performanz, Nutzerfreundlichkeit, …)
- bekannte Schnittstellen
- Modularität
- SW Erweiterung → modulweise Kompatibilität

Security Engineering

- negative Ziele (was nicht passieren darf)
- potenziell unbekannte Angriffsflächen
- das schwächste Glied des Systems bestimmt seine Sicherheit → E2E Sicherheit
- SW Erweiterung → neue E2E Sicherheitsanalyse

2011 CWE/SANS Top 25 Most Dangerous Software Errors

http://cwe.mitre.org/top25/

Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3]	79.0	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75.0	CWE-798	Use of Hard-coded Credentials
[8]	75.0	CWE-311	Missing Encryption of Sensitive Data
[9]	74.0	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)
[13]	69.3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[14]	68.5	CWE-494	Download of Code Without Integrity Check
[15]	67.8	CWE-863	Incorrect Authorization
[16]	66.0	CWE-829	Inclusion of Functionality from Untrusted Control Sphere
[17]	65.5	CWE-732	Incorrect Permission Assignment for Critical Resource
[18]	64.6	CWE-676	Use of Potentially Dangerous Function
[19]	64.1	CWE-327	Use of a Broken or Risky Cryptographic Algorithm
[20]	62.4	CWE-131	Incorrect Calculation of Buffer Size
[21]	61.5	CWE-307	Improper Restriction of Excessive Authentication Attempts
[22]	61.1	CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
[23]	61.0	CWE-134	Uncontrolled Format String
[24]	60.3	CWE-190	Integer Overflow or Wraparound
[25]	59.9	CWE-759	Use of a One-Way Hash without a Salt

insecure interaction between components

risky resource management

Porous Defenses

Prinzipen für Security Engineering

- KISS: „keep it small and simple“
- erlaube viele Reviews
- keine „security by obscurity“
  - obskure Systeme
    - können unbekannte Sicherheitslöcher enthalten
    - können unerkannt manipuliert sein
  - *Kerckhoffs Prinzip*: Die Sicherheit eines kryptographischen Verfahrens darf nicht von der Geheimhaltung des Verfahrens abhängen
- Ferguson et al: professional paranoia

Beheben von Sicherheitslücken

Regelmäßige Wartung von

- Firmware,
- Betriebsysteme
- Programmen

Sicherheitskorrekturen anwenden

- SW hat ein Verfallsdatum

Unbekannte Sicherheitslücken: „zero days“

- CVEs
  - Common Vulnerabilities and Exposures
- CVSS
  - Common Vulnerability Scoring System
    - Base Score:
      - exploitability metrics
      - authorization scope
      - impact metrics
    - Temporal Score
    - Environmental Score

Hausaufgaben

- Lesen Sie die OWASP Top 10 Vulnerabilities nach
- Lesen Sie die Beschreibungen von mindestens 5 der Top 25 CWE durch
- Schauen Sie sich das Beispiel für CWE-78 „OS command injection“ an

Inhalt der Vorlesung

1. Einleitung
2. Authentisierung
3. Autorisierung
   - theoretische Modelle
   - HW Konzepte
   - Unix Konzepte
4. Verschlüsselung
5. MACs & Signaturen
6. Schlüsselverwaltung
7. HSMs
8. PKCS #11
9. SSL/TLS
10. Sicherheit in der Cloud
11. Bitcoins

Optional

- PCI-DSS
- ePersonalausweis

Literatur (Auswahl)

- C. Eckert: IT-Sicherheit, Oldenburgverlag
- N. Ferguson, B. Schneier, T. Kohno: Cryptography Engineering, Wiley 2010
- R. Anderson: Security Engineering, Wiley
- A. Beutelsbacher, H. Neumann, T. Schwarzpaul: Kryptographie in Theorie und Praxis, Teubner+Vieweg, 2010
- Neuigkeiten
  - Linux Weekly New (lnw.net): security column
  - Heisse news
  - Schneiers news letter

Organisatorisches

- Prüfungstermin: 17.2.2016