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

Attacken 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)

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
- Sensitive Systeme (Privatsphäre)
  - online Steuererklärung
  - Gesundheitswesen
- Dokumente, Kommunikation die Betriebsgeheimnisse enthalten
  - Bilanzen
  - Strategien
  - Entwürfe/Erfindungen
- Steuerungen von Industrieanlagen
  - stuxnet
- Energieversorgung
  - Smart-Meter
- Verkehr
  - elektrische Diebstahlsicherung
  - Verkehrsleitsysteme
  - vernetzte Autos

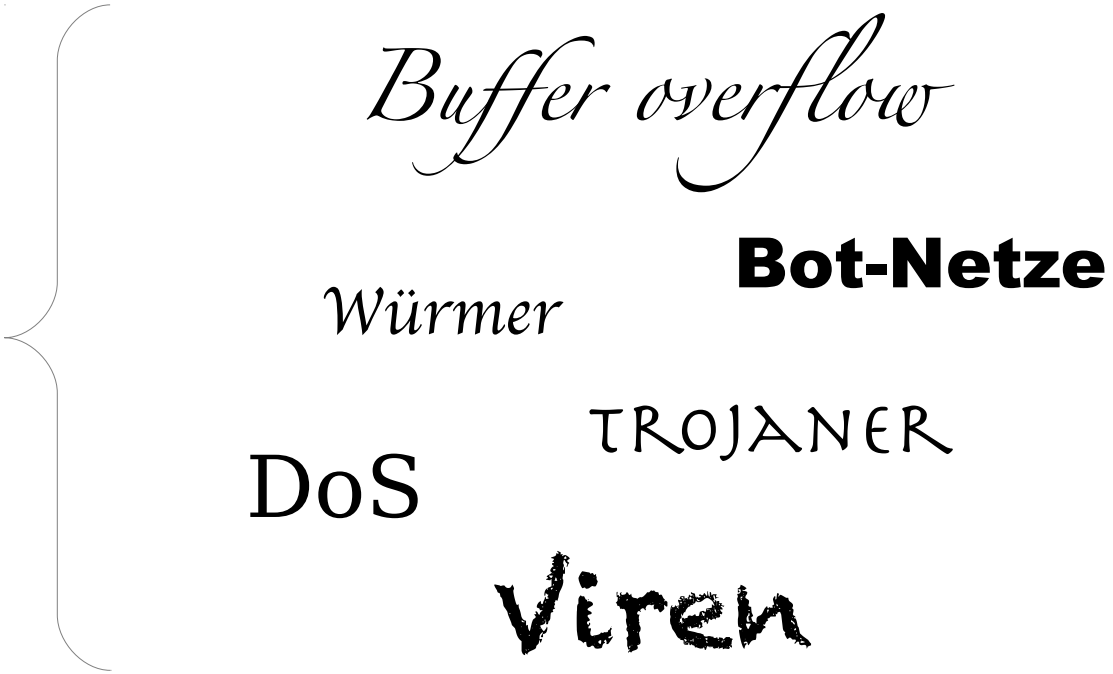
...

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 2013

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

Trusted Computing

Auditing

Kryptografie

Firewalls

SANDKÄSTEN

Secure Engineering

Zugriffskontrolle

Antiviren Programme

Verhaltensanalyse

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

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

Literatur

- 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

Inhalt der Vorlesung

1. Einleitung
2. Authentisierung
3. Autorisierung
4. Verschlüsselung
5. MACs & Signaturen
6. Schlüsselverwaltung
7. HSMs
8. PKCS #11
9. SSL/TLS

Optional

- TPM
- Zufall
- JCA/JCE
- ePersonalausweis

Organisatorisches

- 23.10. fällt aus
- Prüfungstermin: 19.2.2016