Lernlabor Cybersicherheit

Prof. Dr. Daniel Loebenberger, OMNISECURE 2020, Berlin, 22. Januar 2020

Fraunhofer
AISEC

Lernlabor
Cybersicherheit

Überblick

Konzepte der IT-Sicherheit

IT-Sicherheit im Unternehmen

IT-Sicherheit im Entwicklungsprozess

Ansatz des Lernlabor Cybersicherheit

Zusammenfassung

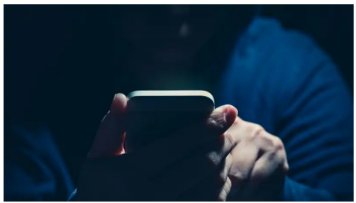
Motivation

Sicherheitsvorfälle auf heise.de, Januar 2020

US-gefördertes Handy kommt mit Malware aus China

Ein subventionierter Mobilfunkdienst für arme US-Amerikaner verkauft ein billiges Smartphone. Es enthält Malware ab Werk.

Lesezeit: 1 Min. In Pocket speichern 222



(Bild: Shutterstock.com / weedezign)

12.01.2020 11:52 Uhr | Security

Von Daniel AJ Sokolov

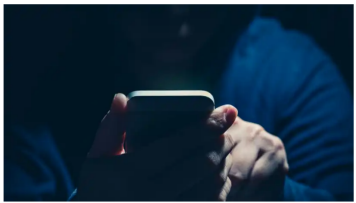
Motivation

Sicherheitsvorfälle auf heise.de, Januar 2020

US-gefördertes Handy kommt mit Malware aus China

Ein subventionierter Mobilfunkdienst für arme US-Amerikaner verkauft ein billiges Smartphone. Es enthält Malware ab Werk.

Lesezeit: 1 Min. In Pocket speichern 222



(Bild: Shutterstock.com / weedezign)

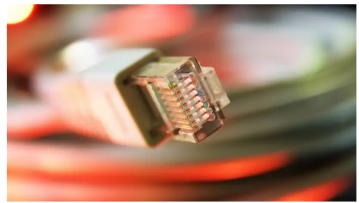
12.01.2020 11:52 Uhr | Security

Von Daniel AJ Sokolov

Cable-Haunt-Lücke soll Millionen Kabel-Modems weltweit gefährden

Sicherheitsforscher warnen vor einer Sicherheitslücke, die Schadcode auf Millionen Kabel-Modems durchlassen könnte.

Lesezeit: 1 Min. In Pocket speichern 246



(Bild: alexskopje/Shutterstock.com)

16.01.2020 15:42 Uhr | Security

Von Dennis Schirrmacher

Fraunhofer AISEC

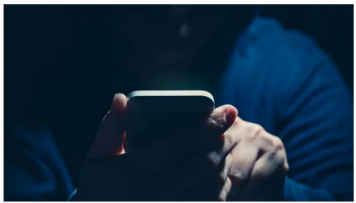
Motivation

Sicherheitsvorfälle auf heise.de, Januar 2020

US-gefördertes Handy kommt mit Malware aus China

Ein subventionierter Mobilfunkdienst für arme US-Amerikaner verkauft ein billiges Smartphone. Es enthält Malware ab Werk.

Lesezeit: 1 Min. In Pocket speichern 222



(Bild: Shutterstock.com / weedezign)

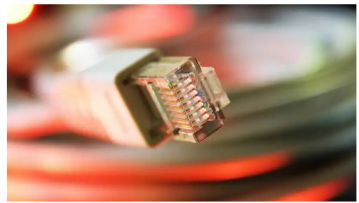
12.01.2020 11:52 Uhr | Security

Von Daniel AJ Sokolov

Cable-Haunt-Lücke soll Millionen Kabel-Modems weltweit gefährden

Sicherheitsforscher warnen vor einer Sicherheitslücke, die Schadcode auf Millionen Kabel-Modems durchlassen könnte.

Lesezeit: 1 Min. In Pocket speichern 246



(Bild: alexskopje/Shutterstock.com)

16.01.2020 15:42 Uhr | Security

Von Dennis Schirrmacher

Handel mit Zugangsdaten: FBI beschlagnahmt Website WeLeakInfo

Hacker hatten per Abo Zugriff auf angeblich 12 Milliarden Datensätze. Die Website WeLeakInfo verkaufte Zugangsdaten und wurde nun vom FBI beschlagnahmt.

Lesezeit: 1 Min. In Pocket speichern 13

(Bild: Illus_man/Shutterstock.com)

19.01.2020 12:48 Uhr

Von Bernd Mewes

Quelle: Heise Medien GmbH & Co. KG

Fraunhofer AISEC

Motivation

Warum sind so viele IT-Komponenten immer noch nicht sicher?

Überblick

Konzepte der IT-Sicherheit

IT-Sicherheit im Unternehmen

IT-Sicherheit im Entwicklungsprozess

Ansatz des Lernlabor Cybersicherheit

Zusammenfassung

Schutzziele der IT-Sicherheit

Vertraulichkeit	Daten dürfen lediglich von autorisierten Benutzern gelesen und geändert werden
Integrität	Daten dürfen nicht unbemerkt verändert werden
Authentizität	Die Herkunft der Daten darf nicht unbemerkt verändert werden

Schutzziele der IT-Sicherheit

Vertraulichkeit	Daten dürfen lediglich von autorisierten Benutzern gelesen und geändert werden
Integrität	Daten dürfen nicht unbemerkt verändert werden
Authentizität	Die Herkunft der Daten darf nicht unbemerkt verändert werden

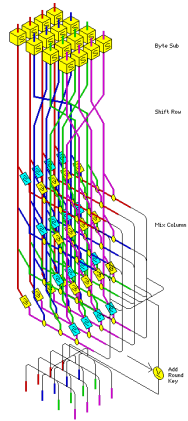
Zusätzliche Ziele: *Verfügbarkeit*, *Verbindlichkeit*, *Zurechenbarkeit* und *Anonymität*

Kryptographie

Eigenschaften moderner kryptographischer Verfahren

Gängige kryptographische Primitive wie AES...

- ...realisieren *Kerckhoffs' Prinzip*
  - offene Standards
  - nur der Schlüssel ist geheim

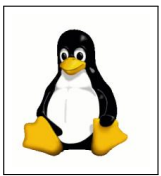


AES (Runde)

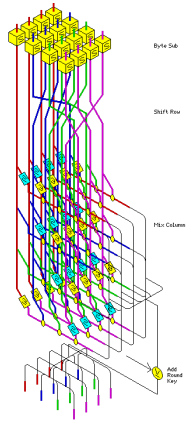
Eigenschaften moderner kryptographischer Verfahren

Gängige kryptographische Primitive wie AES...

- ...realisieren *Kerckhoffs' Prinzip*
  - offene Standards
  - nur der Schlüssel ist geheim
- ...haben *beweisbare Sicherheit*
  - wohldefinierte Konstruktion
  - festes Angreifermodell



Quelle: Tux, das Linux Maskottchen, Larry Ewing, 1996



AES (Runde)

Wie wird all das in der Praxis eingesetzt?

Überblick

Konzepte der IT-Sicherheit

IT-Sicherheit im Unternehmen

IT-Sicherheit im Entwicklungsprozess

Ansatz des Lernlabor Cybersicherheit

Zusammenfassung

Voranschreitende Digitalisierung

Digitale Geschäftsmodelle

- IT-Produkte und -Dienstleistungen (Apple Inc., Microsoft Corp., . . .)
- Versandhandel (Amazon.com, Inc., Zalando SE, . . .)
- Auktionshäuser (eBay Inc., . . .)
- Reisebuchungen (Expedia Group Inc., Flüge.de GmbH, . . .)
- Personentransport (Uber, Taxi.de, . . .)
- . . .

Voranschreitende Digitalisierung

Digitale Geschäftsprozesse

- Betriebssysteme (MacOS X, Windows, Linux, . . .)
- Buchhaltung, Lager- und Personalwesen (SAP, . . .)
- Kommunikation (E-Mail, Messenger, Blogs, . . .)
- Datenaustausch (Cloud-Speicher, Netzlaufwerke, . . .)
- . . .

Probleme bei der Benutzung

- Fehlendes Bewusstsein für IT-Sicherheit
- Schwache Passworte
- Umgehen von Sicherheismaßnahmen
- (Spear-)Phishing
- Malware/Ransomware
- Social Engineering
- . . .

Quelle: Unbekannt

Probleme bei der Administration

- Einsatz kryptographischer Verfahren
- Wahl der Schlüssellängen
- Upgrade von Systemen
- Patchen von Anwendungssoftware
- Gestaltung interner Netze (z.B. Netzübergänge)
- Konfiguration von Sicherheitskomponenten

Überblick

Konzepte der IT-Sicherheit

IT-Sicherheit im Unternehmen

IT-Sicherheit im Entwicklungsprozess

Ansatz des Lernlabor Cybersicherheit

Zusammenfassung

Anwendungsspezifische Anforderungen

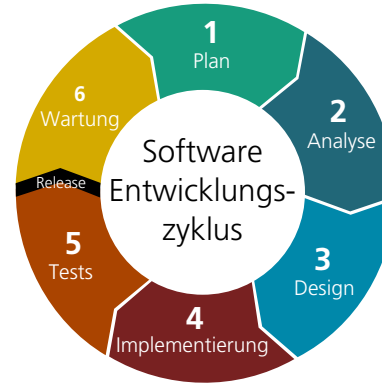
- Betriebssystem- und Kernel-Entwicklung
- Klassische Anwendungssoftware
- Mobile „Apps“
- Eingebettete Geräte
- Treiber- und Firmware-Entwicklung
- Hardware-Entwicklung

Branchenspezifische Anforderungen

- Branchenspezifische Standards
- Eingliederung in existierendes „Ökosystem“
- Unterschiedlicher Schutzbedarf
- Interoperabilität (ggf. branchenübergreifend)

Entwicklungszyklus

- Software durchläuft verschiedene Phasen
- In jeder Phase ist Sicherheit relevant
- Fehlendes Bewusstsein für IT-Sicherheit in jeder Phase impliziert Probleme
- Damit öffnen sich Schwachstellen
- Und: Sicherheit ist oft kein verkaufbares Feature
- Daher wird oft einfach an Sicherheit gespart!



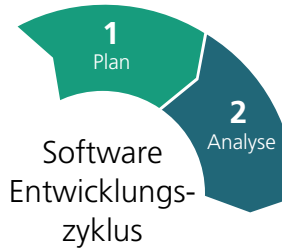
Planungsprinzipien

- Grundprinzipien wie z.B. Saltzer und Schroeder
- Anforderungsanalyse
- Erkennen von Angriffsflächen
- Einsatz guter Kryptographie
- Einsatz sinnvoller Sicherheitsprotokolle
- Optimal: Erstellung eines Sicherheitsmodells

Software Entwicklungs-zyklus

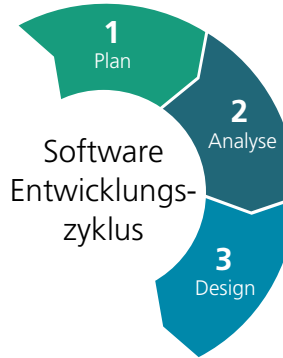
Anpassung der Prinzipien auf das konkrete Problem

- Konkreter Einsatz kryptographischer Verfahren
- Schlüssellängen, Re-Keying Dauer, . . .
- Auswahl kryptographischer Bibliotheken
- ggf. Analyse der Sicherheitsanforderungen
- Prototypische Umsetzung



Umsetzung der Prinzipien

- Festlegung von Subsystemen und Modulen
- Spezifikation von Schnittstellen
- API Spezifikationen
- Hinterfragen von Angriffsflächen
- Abdeckung von gestellten Sicherheitszielen
- ggf. Analyse des Resultats im Hinblick auf das Sicherheitsmodell
- So erreicht man *Security by Design*



Sicheres Implementieren

- Strukturierung des Entwicklungsprozesses
- Vermeiden typischer Implementierungsfehler
- Änderungsmanagement für Quellcode
- Code Review durch vier/sechs Augen Prinzip
- Automatisiertes Build-System
- ggf. weitere organisatorische Maßnahmen

Entwicklungs- und Penetrationstests

- (Live-)Tests während der Entwicklung
- Entwurf vollständiger Testpläne
- Tests von Randfällen
- Testen von Schutzkonzepten
- Wichtig: Unabhängige Tests
- Sichtung und Bewertung bekannter Schwachstellen
- Auffinden neuer Schwachstellen

Fehlermeldung und -behebung

- Strukturiertes Vorgehen bei der Meldung von Fehlern
- ggf. Bug-Bounty Programm ausschreiben
- Bewertung von Schwachstellen
- Erstellung von Patches
- Bereitstellung neuer Versionen
- Wichtig: Authentizität des Patches!

Überblick

Konzepte der IT-Sicherheit

IT-Sicherheit im Unternehmen

IT-Sicherheit im Entwicklungsprozess

Ansatz des Lernlabor Cybersicherheit

Zusammenfassung

Separater Foliensatz!

Überblick

Konzepte der IT-Sicherheit

IT-Sicherheit im Unternehmen

IT-Sicherheit im Entwicklungsprozess

Ansatz des Lernlabor Cybersicherheit

Zusammenfassung

Zusammenfassung

- Angriffsflächen lauern überall
- Betroffen sind nicht nur Entwickler
- Im Entwicklungsprozess ist IT-Sicherheit in allen Phasen relevant
- Auch gibt es branchenspezifische Angriffsflächen
- Ansatz: Wissen schützt!
- Umfangreiches Schulungsangebot im Lernlabor Cybersicherheit

Kontaktinformation

Prof. Dr. Daniel Loebenberger

Fraunhofer Institut für
Angewandte und Integrierte Sicherheit AISEC
Standort Weiden

Adresse: Hermann-Brenner-Platz 1
92637 Weiden i.d.Opf.
Internet: http://www.aisec.fraunhofer.de

E-Mail: daniel.loebenberger@aisec.fraunhofer.de