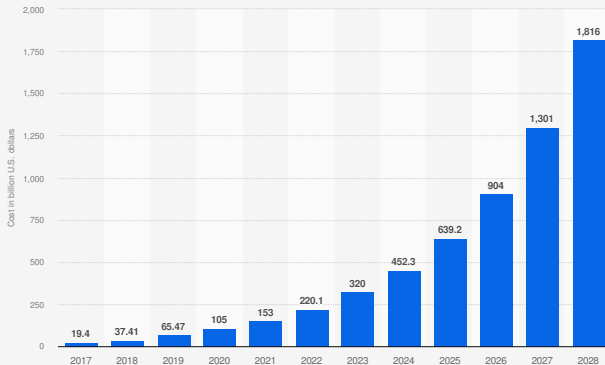


Wie wichtig ist Cybersecurity?

Estimated annual cost of cybercrime in the United States from 2017 to 2028 (in billion U.S. dollars)



Sources

Statista; Statista Technology Market Insights
© Statista 2025

Additional Information:

United States; Statista Technology Market Insights; 2017 to 2025

”[...] there is a significant mismatch in supply and demand of skilled professionals.”

Leslie F. Sikos, Paul Haskell-Dowland - Cybersecurity Teaching in Higher Education

RaspberryPi CyberSec Lab: Development of a Penetration Testing Platform

Bachelorarbeitsvortrag

betreut von

14.05.2025



- 1 Projektübersicht
- 2 Einführung Cybersecurity
- 3 Einführung Wi-Fi
- 4 Pentesting Demonstration
- 5 Zusammenfassung und Ausblick

- 1 Projektübersicht
- 2 Einführung Cybersecurity
- 3 Einführung Wi-Fi
- 4 Pentesting Demonstration
- 5 Zusammenfassung und Ausblick

Projektziele und Funktionen

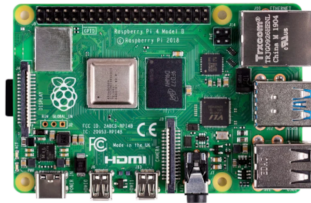
Ziele

- Unterstützung der Cybersicherheits-Ausbildung
- Praktische Pentesting-Übungen
- Einsatz von portabler Hardware (Raspberry Pi)
- Demonstration von Cyberangriffen

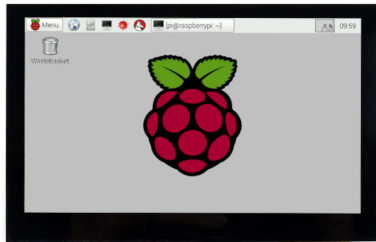
Funktionen

- Flexibles, modulares System
- Einfache Handhabung
- Drahtlose Protokolle (WLAN)
- Webanwendungen (OWASP Juice Shop)

Hardware



RaspberryPI SBC



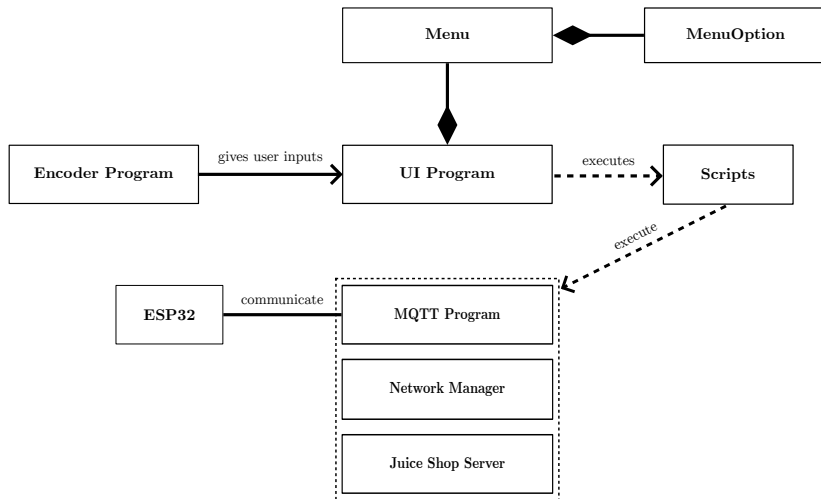
Waveshare 4.3 inch LCD Display

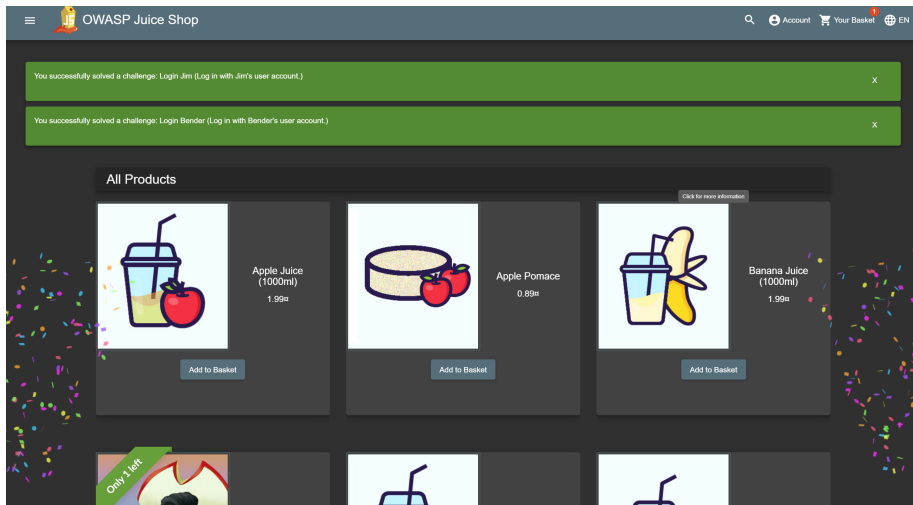


Fenvi Network Card

Rotary
EncoderESP32
MCU

Software





Quelle: <https://github.com/OWASP/www-project-juice-shop/blob/master/tab-overview.md>

- 1 Projektübersicht
- 2 Einführung Cybersecurity**
- 3 Einführung Wi-Fi
- 4 Pentesting Demonstration
- 5 Zusammenfassung und Ausblick

Bedrohungen

Motiv

- finanziell
- politisch
- sozial
- militärisch

Bedrohungen

Motiv

- finanziell
- politisch
- sozial
- militärisch

Absicht

- Erpressung
- Spionage
- Diebstahl
- Betrug
- Sabotage
- Korruption

Bedrohungen

Motiv

- finanziell
- politisch
- sozial
- militärisch

Absicht

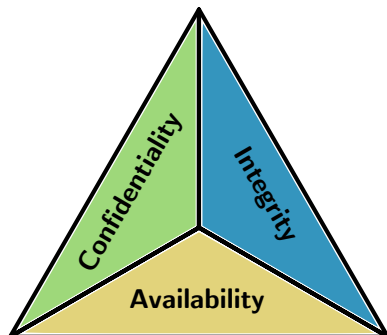
- Erpressung
- Spionage
- Diebstahl
- Betrug
- Sabotage
- Korruption

Angriffsvektor

- Malware
- Social Engineering
- Denial of Service (DoS)
- Cracking
- Spoofing
- Man-in-the-Middle (MitM)

Ziele von Cybersecurity - CIA Acronym

Vertraulichkeit
Information ist nur für
berechtigte Personen
lesbar



Integrität
Information ist
unverfälscht

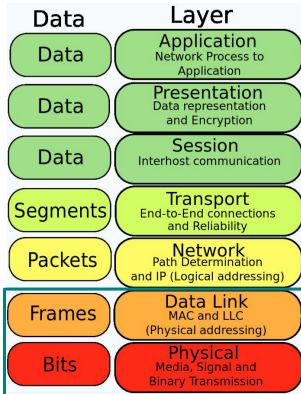
Verfügbarkeit
Daten und Services sind mit
benötigter Leistung zum
benötigten Zeitpunkt verfügbar

Schutzstrategien

- Security Awareness
- Sicherheitsarchitektur
- Verschlüsselung
- Authentifizierung
- Pentesting

- 1 Projektübersicht
- 2 Einführung Cybersecurity
- 3 Einführung Wi-Fi**
- 4 Pentesting Demonstration
- 5 Zusammenfassung und Ausblick

Architektur



MAC Layer:

Netztopologie, Adressierung, Verbindungsaufbau, Zugriffssteuerung

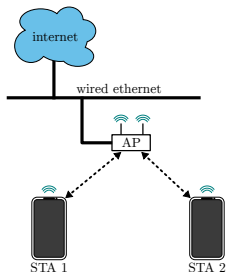
PHY Layer:

Funkübertragung, Datenkonvertierung

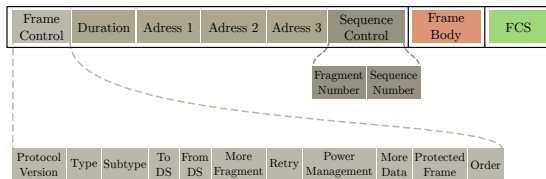
Quelle: <https://www.vroque.co/post/osi-model-7-layers-of-osi-model-and-how-it-works-lmn-vroque-co>

Architektur

Basic Service Set (BSS) Topologie



MAC Frame



Header: Adressierung, Management Funktionen

Body: Datenträger

FCS: Integritätskontrolle

Sicherheit

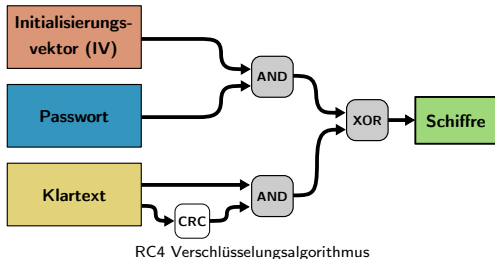
Durch die Funkübertragung werden Verschlüsselung, Authentifizierung und Integritätskontrolle benötigt um CIA zu gewährleisten.

Sicherheit

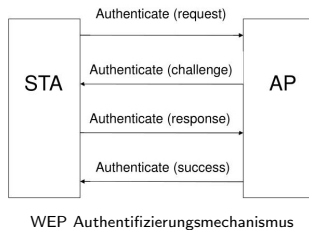
Durch die Funkübertragung werden Verschlüsselung, Authentifizierung und Integritätskontrolle benötigt um CIA zu gewährleisten.

Wired Equivalent Privacy (WEP) verwendet folgende Mechanismen:

Verschlüsselung



Authentifizierung

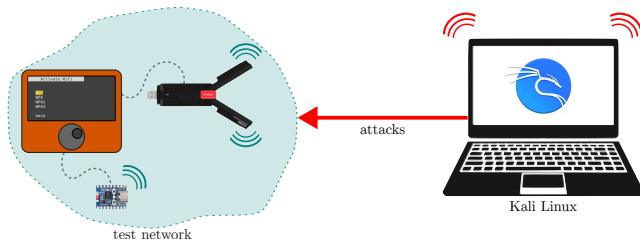


Schwachstellen von WEP

- Schwache Verschlüsselung mit RC4-Streamcipher
- Initialisierungsvektoren (IVs) nur 24 Bit lang
- Verwendung des selben Key für Verschlüsselung und Authentifizierung
- Schwache Integritätskontrolle mit CRC32

- 1 Projektübersicht
- 2 Einführung Cybersecurity
- 3 Einführung Wi-Fi
- 4 Pentesting Demonstration**
- 5 Zusammenfassung und Ausblick

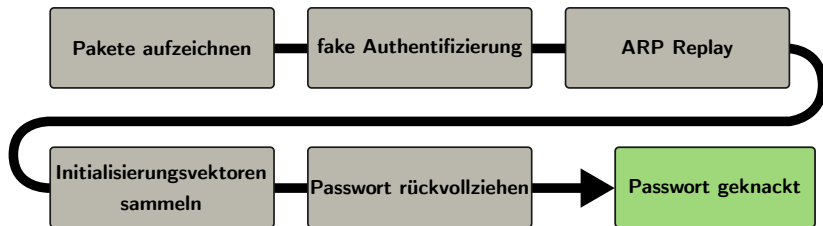
Übersicht



Zusammenfassung

- nötig für ARP Replay
- möglich durch CRC32

- Injektion von ARP Paketen
- Erzeugen von IVs



- hohe Wahrscheinlichkeit der Wiederholung
- möglich bei Wiederholung der IVs

- 1 Projektübersicht
- 2 Einführung Cybersecurity
- 3 Einführung Wi-Fi
- 4 Pentesting Demonstration
- 5 Zusammenfassung und Ausblick

Anwendungsmöglichkeiten

Cybersecurity	Awareness	Web Entwicklung
Wi-Fi Pentesting Übung	Demonstration von Wi-Fi Angriffen	Awareness für übliche Fehler in Webanwendungen schaffen
Web Pentesting Übung		
Implementation sicherer Systeme	Simulation von echten Szenarien	Software Testing
Incident Response		

aktuell möglich
zukünftige Erweiterungen

Ausblick

Überarbeitung

- Fehlerbehandlung implementieren
- Software Standard einhalten
- Zuverlässigkeit verbessern

Ausblick

Überarbeitung

- Fehlerbehandlung implementieren
- Software Standard einhalten
- Zuverlässigkeit verbessern

Erweiterungen

- Batteriebetrieb
- Bluetooth
- NFC
- SSL/TLS Umgebungen
- Sicherheitssysteme, wie IDS
- Incident Response Umgebungen

Kontakt

J
s

Weitere Informationen

<https://github.com/Der-Erzfeind/Raspi-CyberSec-Lab-Project.git>