Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für wissenschaftliche Weiterbildung (IWW)

European Cyber Security Month (ECSM) 2021

Innentäter: Bedrohungen durch Hacking Hardware

Tobias Scheible, M.Eng.

- 1999 GeoCities Website, 2000 eigene Domain, 2001 erste Projekte
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Netzsicherheit I Hochschulzertifikatsprogramm
    - Grundlagen der digitalen Forensik Master-Studiengang IT GRC Management
    - Digitale Forensik Bachelor-Studiengang IT Security
    - Internet Grundlagen Master-Studiengang Digitale Forensik
    - Cybersecurity Bachelor-Studiengang IT Security
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Master-Studiengang IT GRC
- Blog scheible.it | Zeitschriftenartikel | Vorträge und Workshops

Hochschule Albstadt-Sigmaringen

- 1971 Gründung der Fachhochschule Sigmaringen
- 1988/89 Campus Albstadt
- 2004 Fachhochschule wird in Hochschule umbenannt
- 2012 Weiterbildung (berufsbegleitende Angebote)
- 24 Bachelor- und Masterstudiengänge

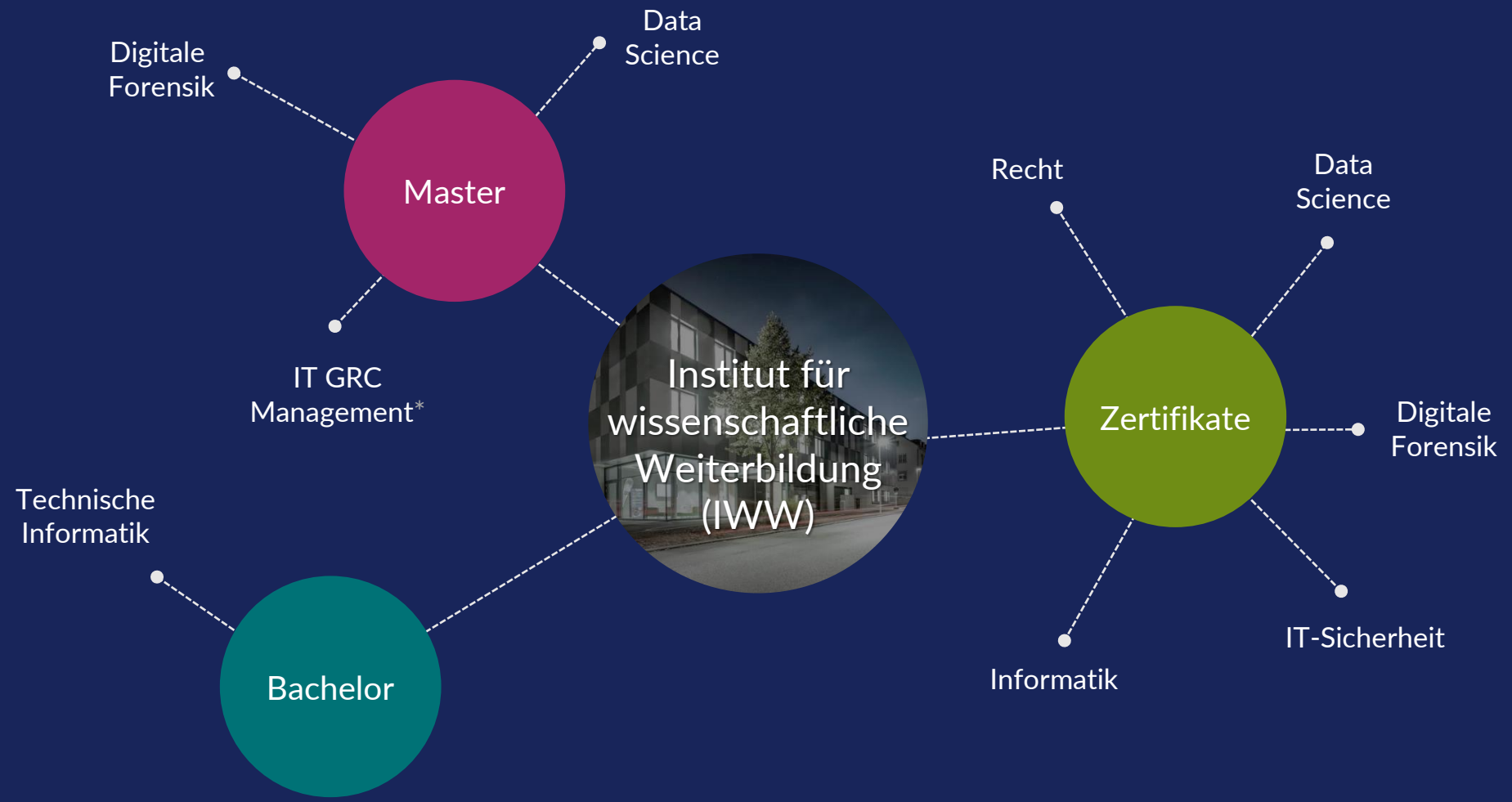
Fakultät Engineering

Fakultät Business Science and Management

Fakultät Life Sciences

Fakultät Informatik

Institut für wissenschaftliche Weiterbildung



Weitere Infos: https://hs-albsig.de/iww

* wird aktuell neu strukturiert

Innentäter: Bedrohungen durch Hacking Hardware

Agenda

- Hacking Hardware
- Spionage-Gadgets
- Key- & Screen-Logger
- BadUSB Tools & USB-Killer
- Kabelgebundene Netzwerke
- WLAN-Verbindungen
- Bluetooth-Kommunikation
- RFID-Zugangssysteme
- Funktechnik
- Zusammenfassung

Hinweis
Die komplette Präsentation wird im Anschluss per Mail und online bereitgestellt.

Hacking Hardware

Beschreibung

Hacking Hardware: Geräte, mit denen Rechnersysteme oder Kommunikations-verbindungen angegriffen werden können. Dabei handelt es sich um kompakte Geräte mit einem Mikrocontroller, die vorab programmierte Befehle ausführen. Zum Teil können sie über Funk-Chips ferngesteuert werden.

- Sie wurden für White Hat Hacker, Penetration-Tester, Security-Forscher und Sicherheitsbeauftragte entwickelt, um Schwachstellen aufzuspüren und anschließend schließen zu können.
- Allerdings werden sie auch immer wieder von kriminellen Angreifern eingesetzt.
  - Es handelt sich dabei um sehr gezielte Angriffe
  - Meist werden diese Geräte von Innentäter eingesetzt
  - Hacking Hardware ist i.d.R. einfach zu bedienen
- Hacking Gadgets, Pentest Hardware/Tools, IT Security Hardware/Tools sind alternative Bezeichnungen

Typen von Hacking Hardware

Spionage

- Spionage Gadgets
- Keylogger
- Screenlogger

Angriffe gegen Rechnersysteme

- BadUSB
- USB-Killer

Netzwerke

- LAN
- WLAN
- Bluetooth

Funkverbindungen

- RFID
- Funkprotokolle

Innentäter

Innentäter sind durch ihre Zugangsmöglichkeiten und ihres Insiderwissens über innerbetriebliche Gegebenheiten in der Lage, mehr Schaden anzurichten als es externen Tätern möglich ist.

- Dazu gehören zum Beispiel frustrierte oder entlassene Mitarbeiter, die sich an ihrem (ehemaligen) Unternehmen rächen möchten.
- Zum Kreis der Innentäter werden auch temporäres Personal wie Praktikant*innen, die gezielt eingeschleust wurden, oder externe Dienstleister wie zum Beispiel das Reinigungspersonal, das sich frei im Unternehmen bewegen kann, gezählt.

Zu den einfachsten Formen gehören die Weitergabe von Insiderinformationen an Dritte über die Weitergabe von Zugangsdaten oder physischen Schlüsseln bis hin zu eignen Aktionen zur Sabotage oder Erpressung.

Durch den weniger eingeschränkten Zugang, das Wissen über interne Abläufe und dem Faktor Zeit, ist diese Angreifergruppe sehr gefährlich. Gleichzeitig können Schutz-maßnahmen von Innentätern über einen längeren Zeitraum hinweg beobachtet und analysiert werden.

Angriffsszenario

Kamera / Mikrofon

Keylogger / BadUSB

Opfer

WLAN / LAN

ehemaliges oder frustriertes Personal

Personal von Drittfirmen

Praktikant* innen

Angreifer
Innentäter

falsche Kunden

Bezugsquellen

- IT Security Hardware muss nicht über zwielichtige Kanäle oder gar über das Darknet beschafft werden, sondern kann teilweise z.B. über die Onlineshops von Amazon und eBay einfach bestellt werden.
- Neben großen Shoppingplattformen gibt es mehrere Onlineshops, die sich auf den Vertrieb dieser Art von Hardware spezialisiert haben.
- In Deutschland werden diese Geräte auch häufig über Online-Shops angeboten, die im Bereich der Detektivausrüstung aktiv sind.
- Einige Geräte sind in Deutschland nicht erlaubt, können jedoch sehr einfach im Ausland bestellt werden – teilweise auch in EU-Nachbarstaaten.

Spionage-Gadgets

Spionage-Gadgets

Spionage-Gadgets interagieren nicht mit einem Rechnersystem, sondern werden eingesetzt, um heimlich z.B. sicherheitskritische Informationen zu entwenden. Sie werden zum Beispiel in einer Vorstufe eines Angriffs eingesetzt, um Zugangsdaten auszuspähen.

- Angreifer können ein Opfer gezielt ausspionieren
- Es gibt eine große Bandbreite von verschiedenen Tools
- Tools werden unbemerkt platziert und später wieder abgeholt
- Es können Video- und Audioaufzeichnungen angefertigt werden

Mini-Aufnahmegerät

GSM-Aufnahmegerät

Spionagekamera

WLAN-Minikamera

GPS-Tracker

Key- & Screen-Logger

Key- & Screen-Logger

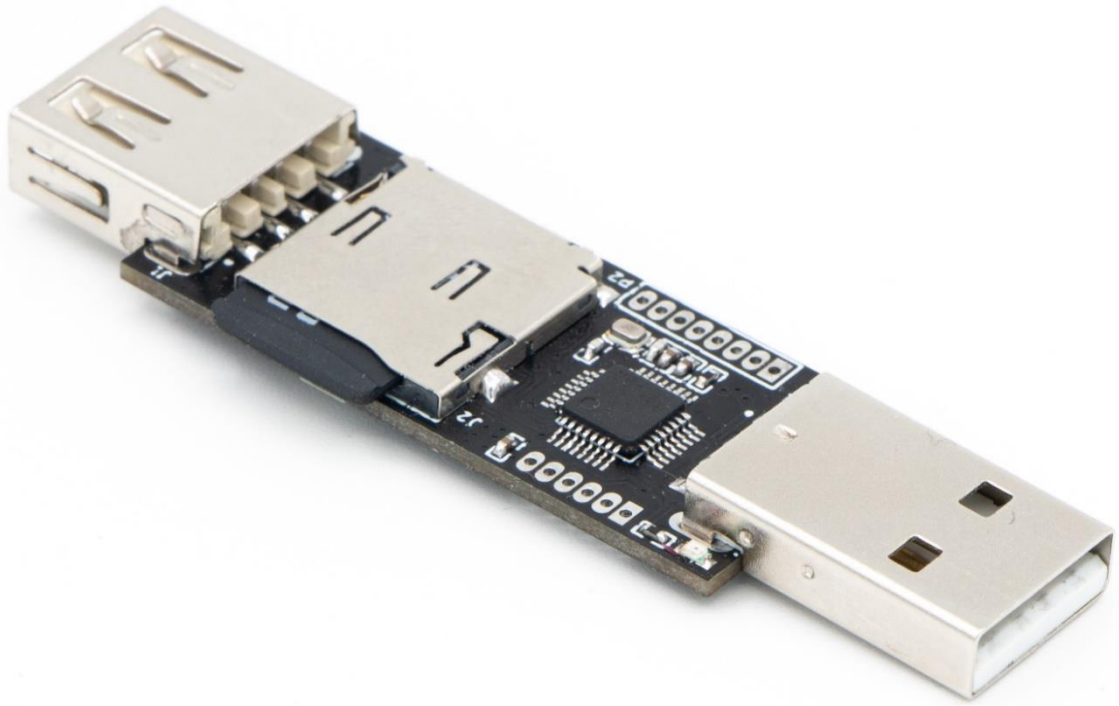
Ein Keylogger wird von Angreifern verwendet, um jeden Tastendruck, der auf einer externen Tastatur eines Computers eingegeben wird, aufzuzeichnen. Screenlogger zeichnen heimlich Monitorsignale auf.

- Keylogger zeichnen die Tastatureingaben direkt nach dem Start auf
- Bei Varianten mit WLAN - Verbindung kann der Angreifer diese aus der Entfernung abfragen
- Intelligente Keylogger können auf Eingaben mit Änderungen reagieren
- Screenlogger werden zwischen Rechner und Bildschirm angeschlossen
- Es gibt sie für verschiedene Schnittstellen (VGA, DVI, DisplayPort, HDMI)
- Sie zeichnen den Bildschirminhalt als Screenshots oder Video auf

USB-Keylogger

WLAN-Keylogger

EvilCrow Keylogger



Key Croc Keylogger

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für wissenschaftliche Weiterbildung (IWW)

VideoGhost

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für wissenschaftliche Weiterbildung (IWW)

Screen Grab

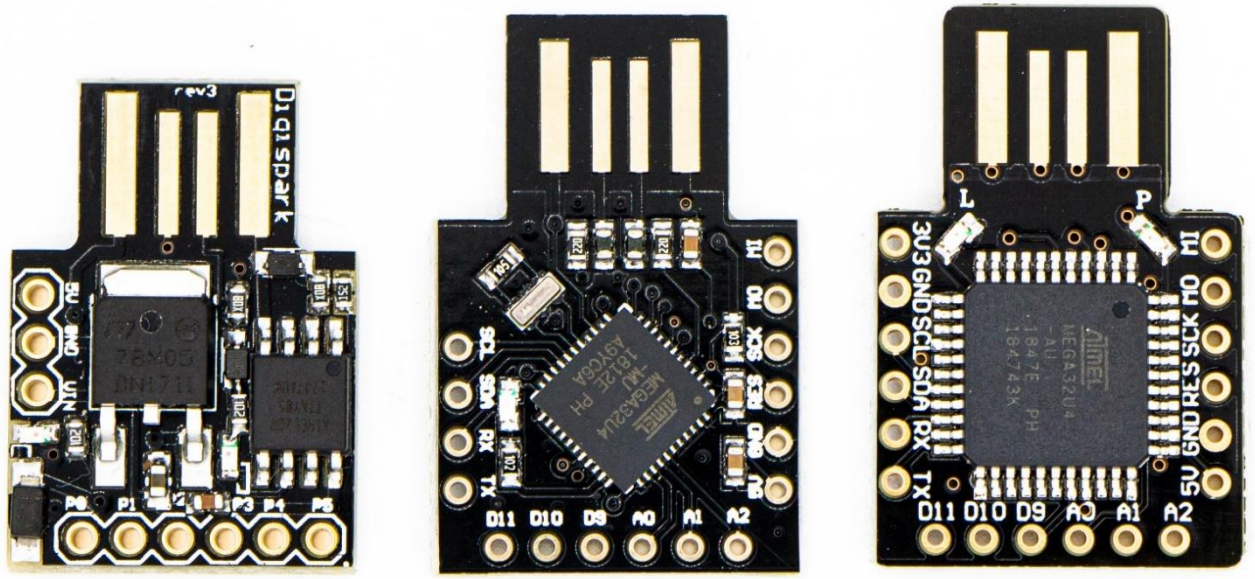
BadUSB Tools & USB-Killer

BadUSB Tools & USB-Killer

Bad USB-Geräte führen mit einer virtuellen Tastatur schadhafte Befehle auf einem Rechner aus. Dabei kann es sich um USB-Geräte mit veränderter Firmware oder um spezialisierte Mikrocontroller handeln. Durch die weite Verbreitung der USB-Schnittstelle und die Tarnung als „harmloses“ Gerät kann großer Schaden angerichtet werden.

- Viele BadUSB Tools sehen wie gewöhnliche USB-Sticks aus
- Sie können als ein beliebiges USB-Gerät fungieren
- Die Microcontroller werden in gewöhnliche USB-Geräte integriert
- USB-Killer zerstören Rechner durch einem Stromschlag

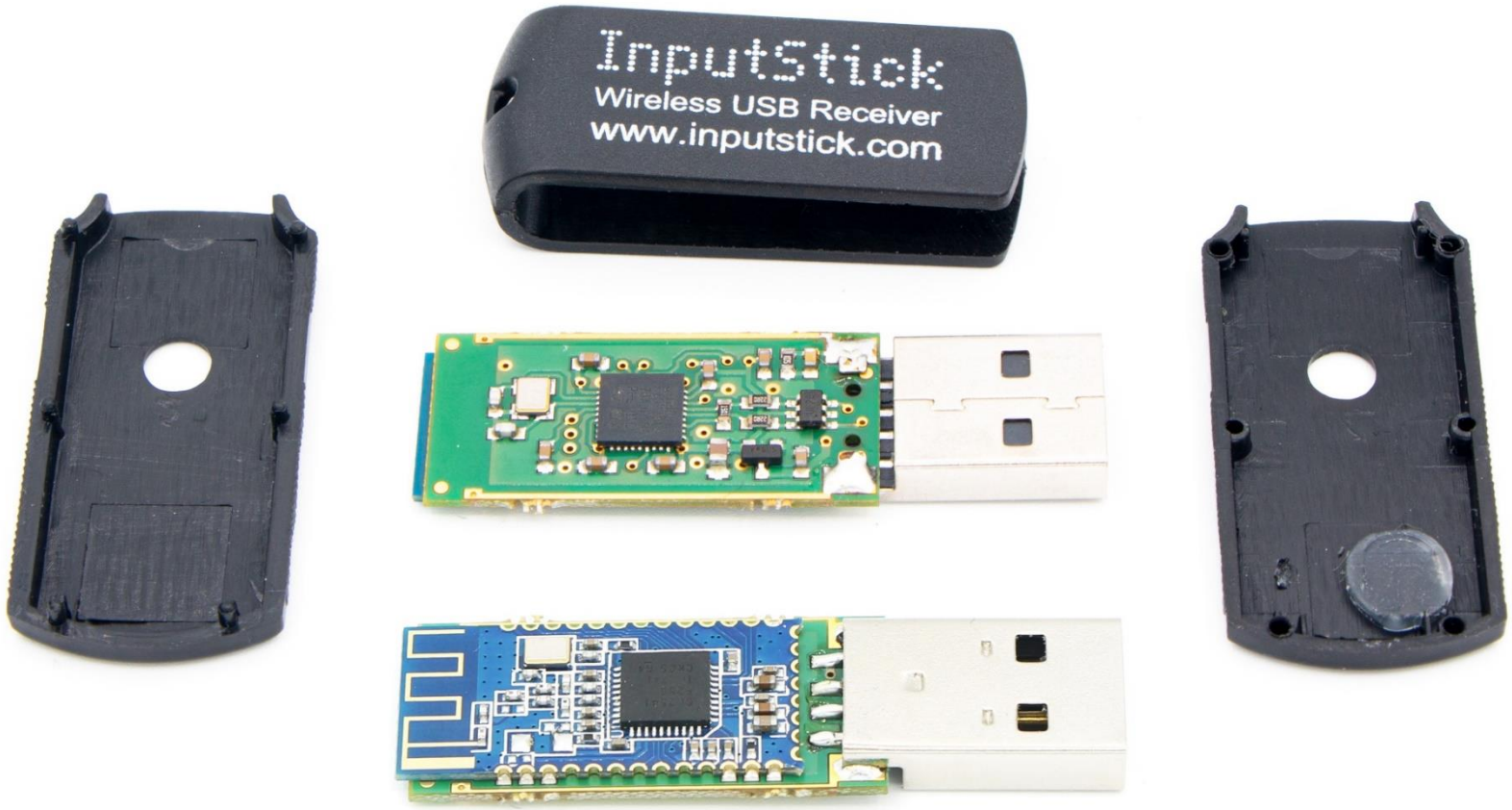
DigiSpark



Rubber Ducky

MalDuino Elite

InputStick



USBNinja

USBKill

Kabelgebundene Netzwerke

Kabelgebundene Netzwerke

LAN-Netzwerke sind das Bindeglied unserer modernen IT-Infrastruktur. Dadurch, dass sie überall verbaut sind, können sie teilweise auch von Angreifern vor Ort angezapft werden. Mit entsprechender Hardware kann der Traffic ausgeleitet und analysiert werden.

- Ausleiten von Netzwerk-Verbindungen
- Aufzeichnen von Netzwerk-Übertragungen
- Manipulation von unverschlüsselten Netzwerkverkehr

Throwing Star LAN Tap Pro

Packet Squirrel

Plunder Bug

WLAN-Verbindungen

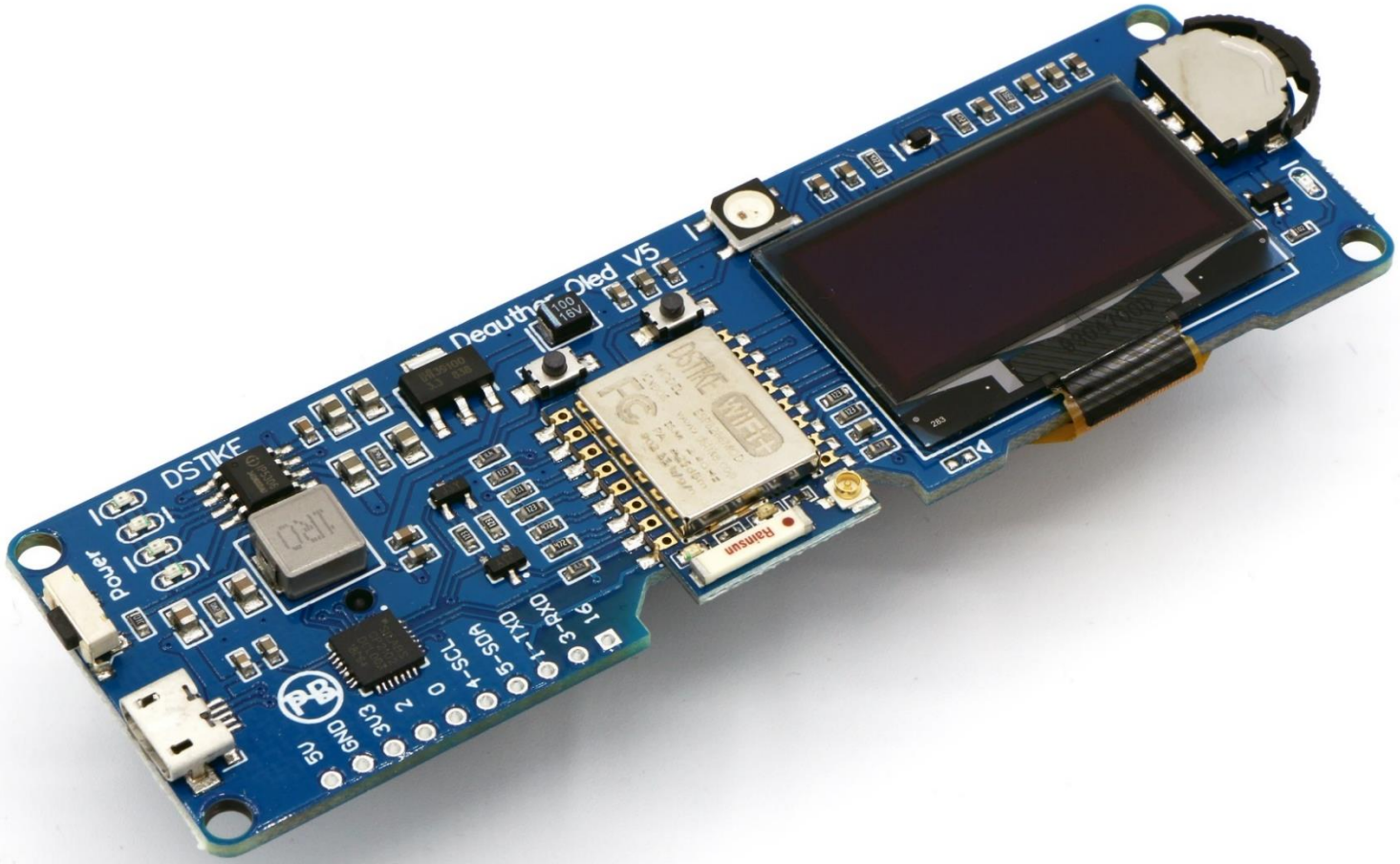
WLAN-Verbindungen

WLAN gehört mittlerweile zum Standard und wird für viele Bereiche der IT verwendet. Diese wichtige Infrastruktur kann mit einem Deauther-Angriff gezielt unterbrochen werden oder es werden bösartige Zugangspunkte simuliert.

- Nachahmen von vorhandenen Netzen - Evil-Twin-Accesspoint
- Unterbrechung von vorhandenen WLAN-Verbindungen

WiFi Pineapple NANO

Deauther



Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für wissenschaftliche Weiterbildung (IWW)

Bluetooth-Kommunikation

Bluetooth-Kommunikation

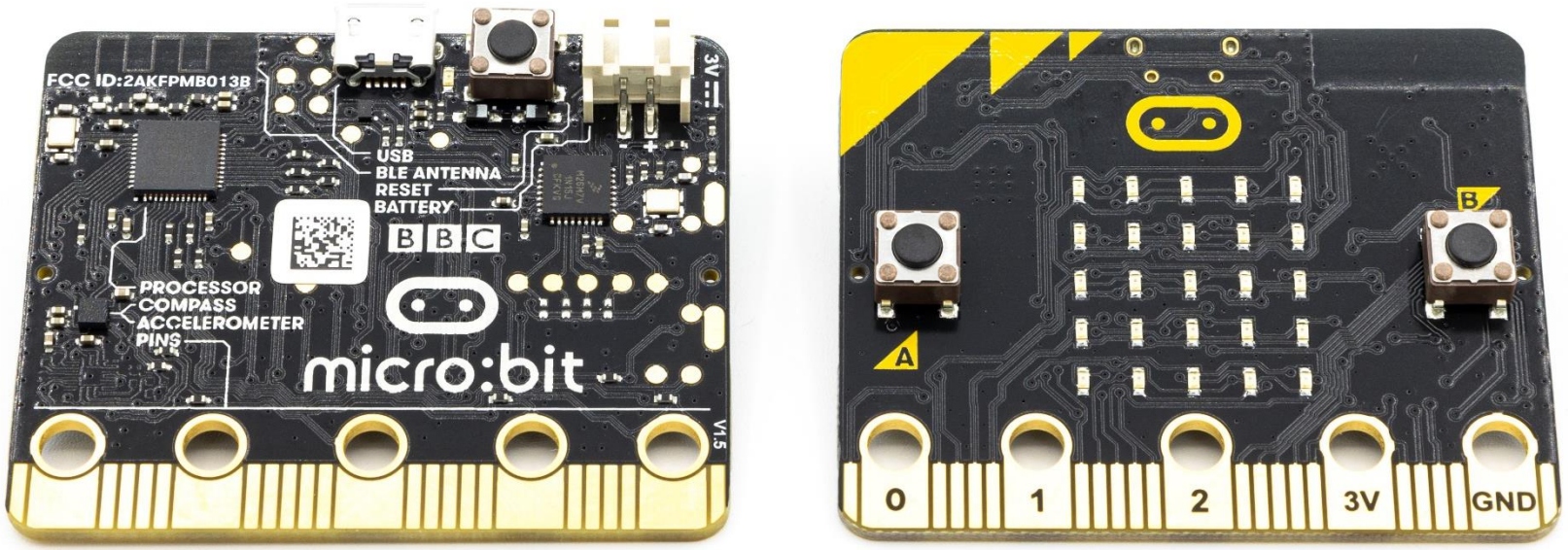
Bluetooth hat sich zum dominierenden Standard für Funkverbindungen im Nahbereich entwickelt. Das Sicherheitskonzept ist sehr umfangreich, trotzdem werden immer mehr Angriffsvektoren bekannt. Gerade Geräte, die Bluetooth Low Energy verwenden, können mit der passenden Hardware angegriffen bzw. belauscht werden.

- Tracking von Bluetooth Geräten
- Manipulation von Bluetooth LE Verbindungen

Bluefruit LE-Sniffer

Ubertooth One

BtleJack + BBC micro:bit



RFID-Zugangssysteme

RFID Technologie

RFID-Tags werden in immer mehr Bereichen eingesetzt – von automatisierten Kassen über Türschließanlagen bis hin zur Logistikabfertigung. Einfache Tags ohne Sicherung können sehr einfach angegriffen werden.

- Einfaches Kopieren von unsicheren RFID-Tags
- Duplikate von gesicherten RFID-Chips
- Knacken unsicherer Standards

RFID Cloner

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Institut für wissenschaftliche Weiterbildung (IWW)

Keysy

Proxmark

NFCKill

Funktechnik

Funkverbindungen

Immer mehr Verbindungen werden per Funk realisiert. Per Software Defined Radio (SDR) lassen sich Funksignale in verschiedenen Frequenzbändern aufzeichnen, analysieren und erneut senden. Dadurch können Funkverbindungen angegriffen werden, ohne dass das verwendete Protokoll bekannt sein muss.

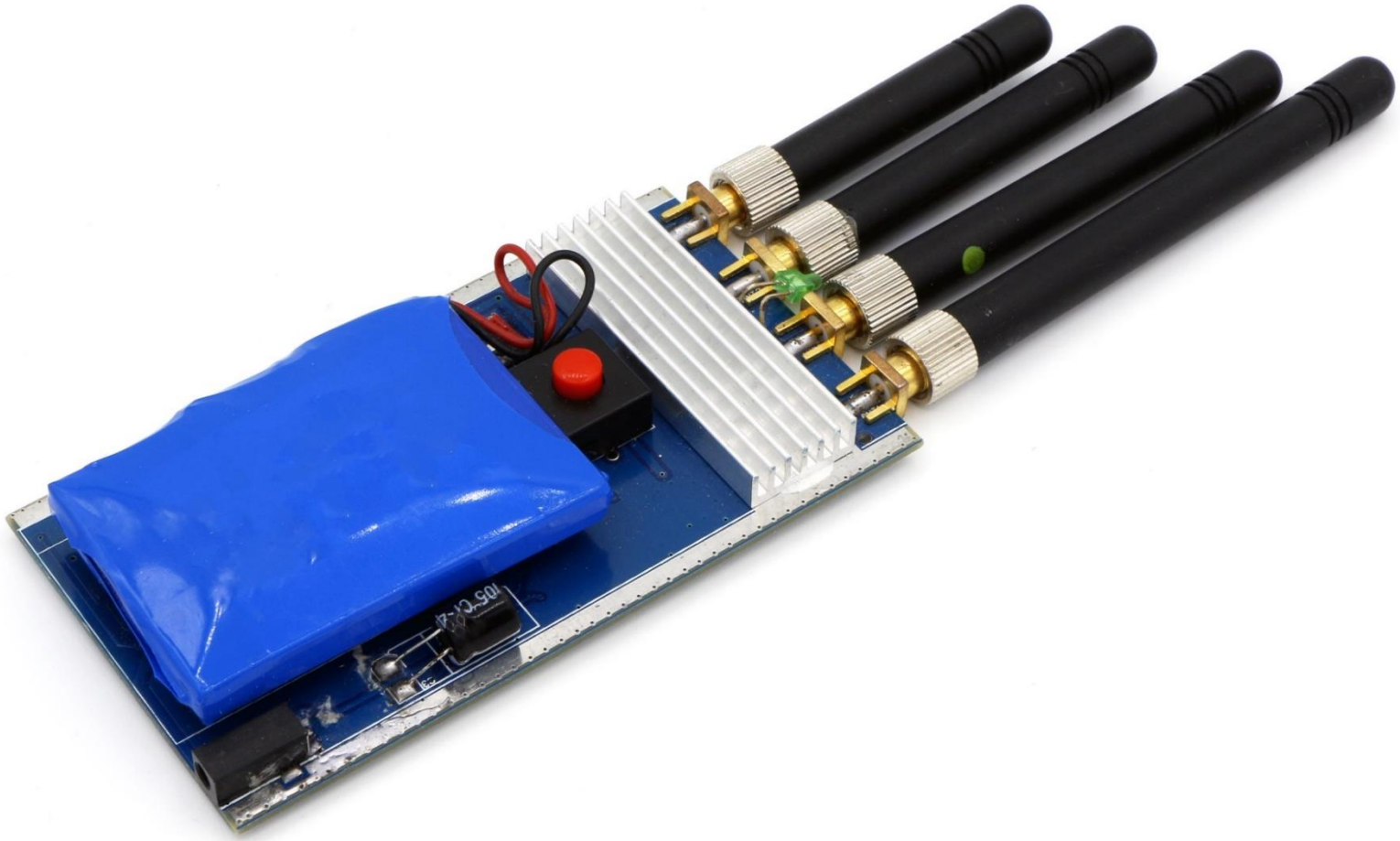
- Einfaches „Kopieren“ / Clonen von ungesicherten Funkübertragungen
- Analyse und Aufspüren von Funkverbindungen
- Angriff durch Wiederholung eines Signals - Replay-Angriff

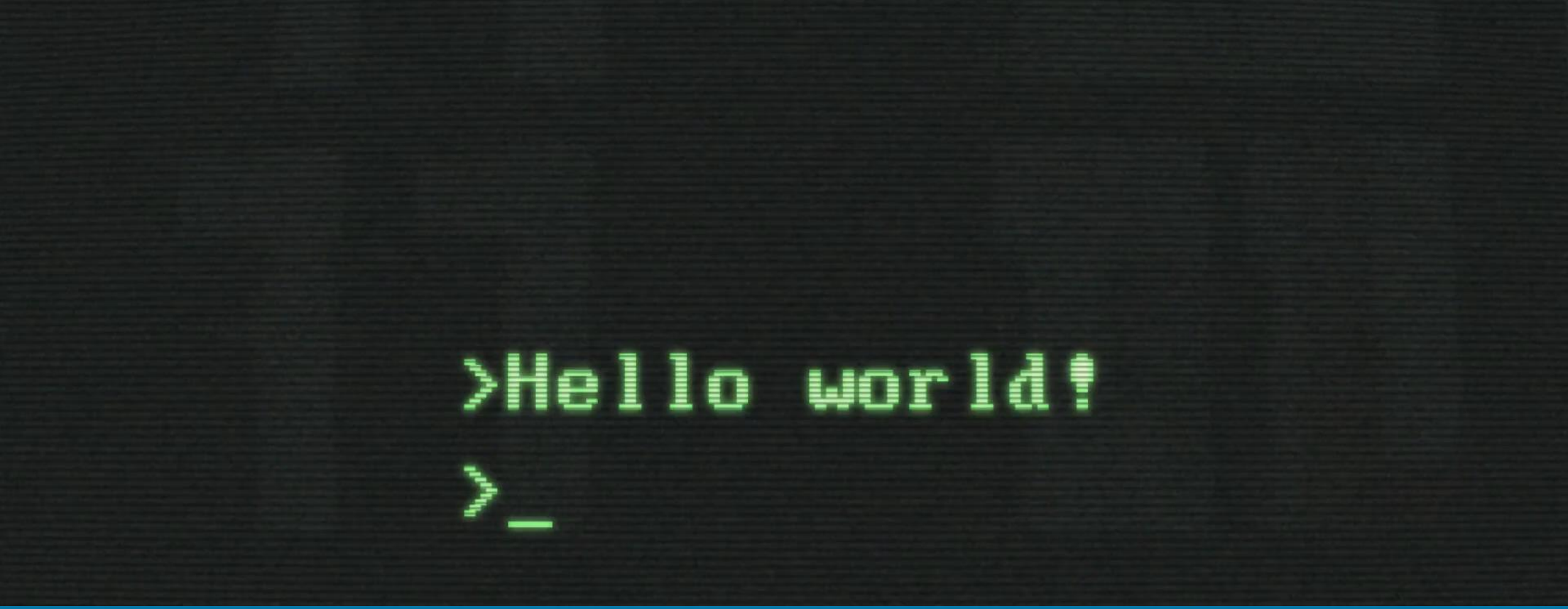
Cloner

NooElec NESDR SMArt

HackRF One

Störsender





Zusammenfassung

Gegenmaßnahmen

- Hacking Hardware Geräte und ihre Funktionsweise kennen
- Allgemein
  - Zugangsbeschränkung, damit nur autorisierte Personen Zutritt haben
  - Übersichtliche und aufgeräumte Arbeitsplätze (Kabelmanagement)
  - (Awareness) Schulung von Mitarbeitenden, um Hacking Hardware zu erkennen
- Detektion
  - Kameradetektor, um Geräte mit einem Bildsensor aufzuspüren
  - Wanzenfinder, um Geräte mit einer Funkverbindung aufzuspüren
- Rechnersysteme
  - Sicherung von Rechnersystemen durch bauliche Maßnahmen
  - Erkennen und melden von Unterbrechungen, wenn die Verbindung zu einzelnen Geräten vorübergehend verloren gegangen ist

Vielen Dank !
Fragen?

Vielen Dank für Ihre Teilnahme

Berufsbegleitende/Nebenberufliche Weiterbildung

- Berufsbegleitende Online-Fernstudienangebote
- Fernstudium neben Beruf und Familie
- Online-Vorlesungen und Präsenzwochenenden
- Umfassende Betreuung durch E-Tutoren
- Zukunftssichere wissenschaftliche Methodenkompetenz
- Intensiver & praxisorientierter Kompetenzaufbau
- Renommierte Dozenten aus dem Fachgebiet
- Hochqualifizierte wissenschaftliche Mitarbeiter
- Namhafte Kooperationspartner aus der Industrie

Weitere Infos:
https://hs-albsig.de/iww

* wird aktuell neu strukturiert