Warum IT-Sicherheit heute so wichtig ist?

Prof. Dr.-Ing. Juraj Somorovsky
Arbeitsgruppe Systemsicherheit
Universität Paderborn

Wer sind wir?

- Arbeitsgruppe Systemsicherheit
- Themen:
  - Websicherheit
  - Angriffe auf Krypto (DROWN, ROBOT, Efail, Raccoon)
  - Angriffe auf Netzwerke und IoT-Systeme (z.B. Drucker)
  - Angewandte Kryptographie

Überblick

- Sicherheitslücken in der Praxis
- Capture the Flag (CTF) Challenges
- IT-Sicherheit in Paderborn
- Was macht mein Hund in der Vorlesung?

Tessa

Zoom Bug Allowed Snoopers Crack Private Meeting Passwords in Minutes

July 30, 2020 Ravie Lakshmanan

BIG BLUE BUTTON

Das große blaue Sicherheitsrisiko

Kritische Sicherheitslücken, die Golem.de dem Entwickler der Videochat-Software Big Blue Button meldete, sind erst nach Monaten geschlossen worden.

Eine Recherche von Hanno Böck

21. Oktober 2020, 9:00 Uhr

(Bild: włodi, Wikimedia Commons (Modifikation: Hanno Böck)/CC-

Die Software Big Blue Button ist sehr beliebt - aber leider handeln die Entwickler beim Umgang mit Sicherheitslücken nicht sehr professionell.

Online Shopping für Piraten

Source: Pirates of the Caribbean

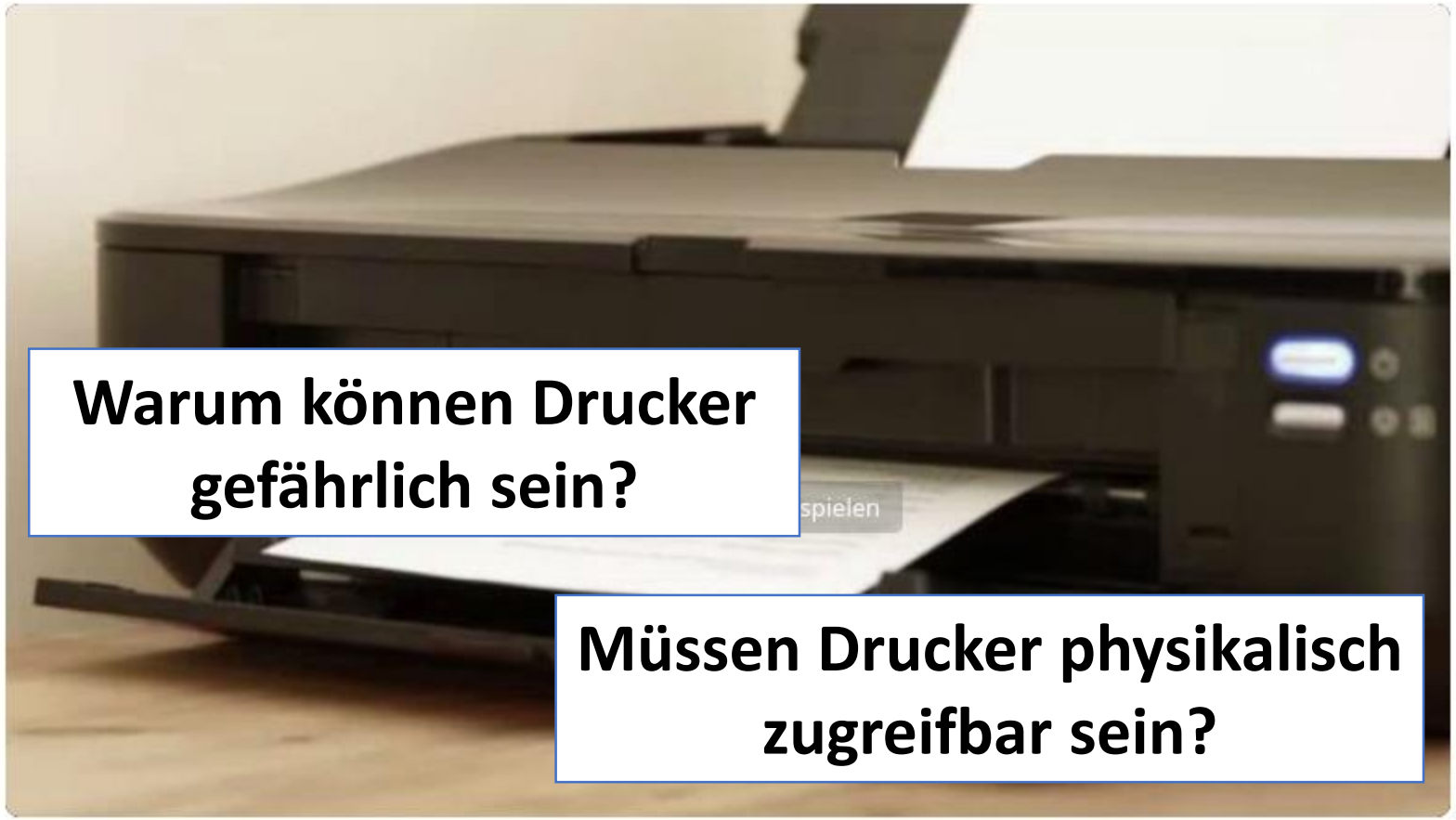
Online Shopping für Piraten

Source: Pirates of the Caribbean

CHIP Corona care TEST & KAUFBERATUNG NEWS DOWNLOADS MEHR CHIP 365

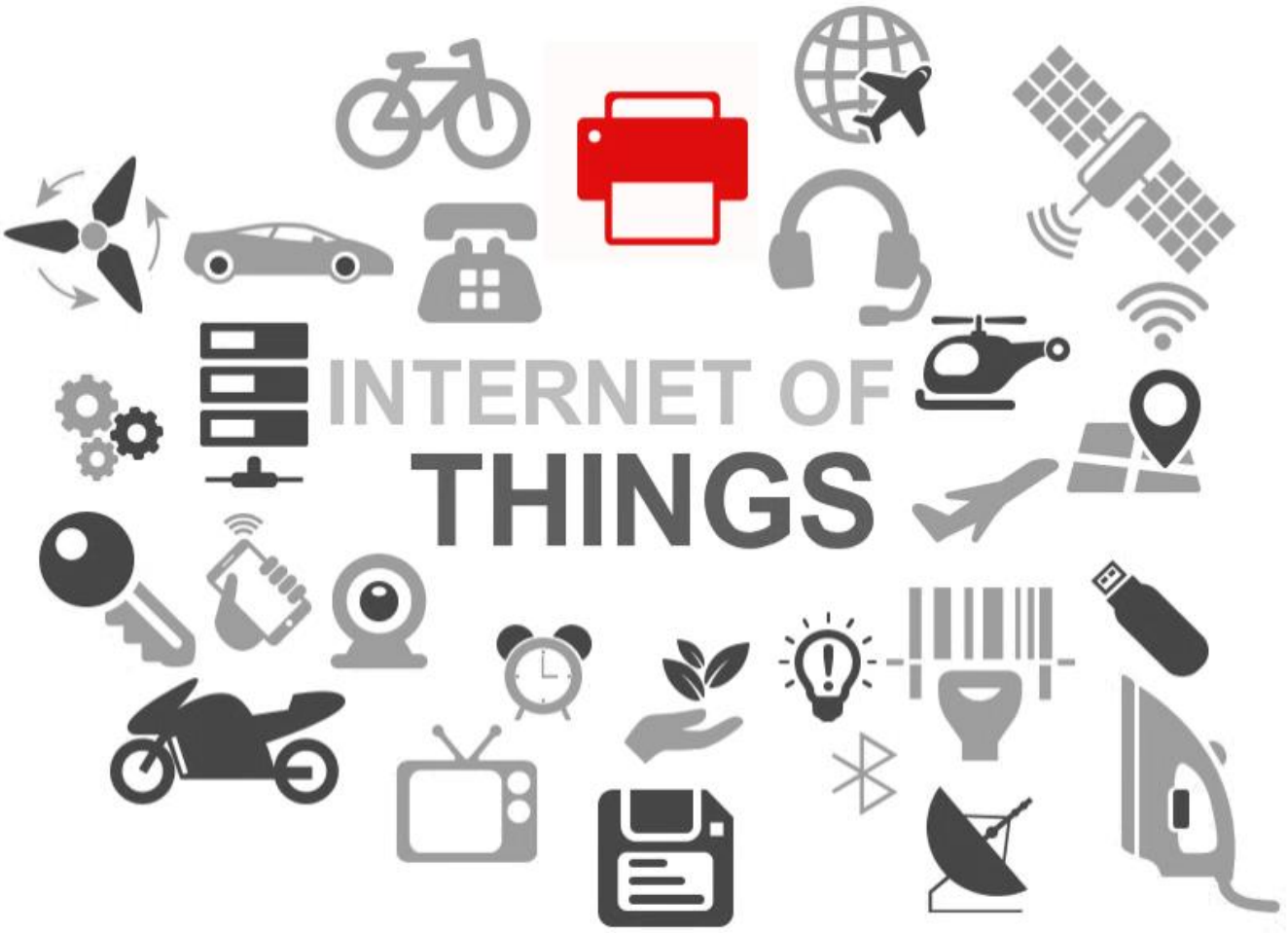
Stellen Sie sofort das Drucken ein! Schock-Nachricht von deutschen Forschern

12.02.2017, 15:06 | VON NIELS HELD



Wie finde ich Drucker?

Jenseits der Drucker…Angriffe auf IoT



https://github.com/nebgnahz/awesome-iot-hacks

Schlechte Passwörter

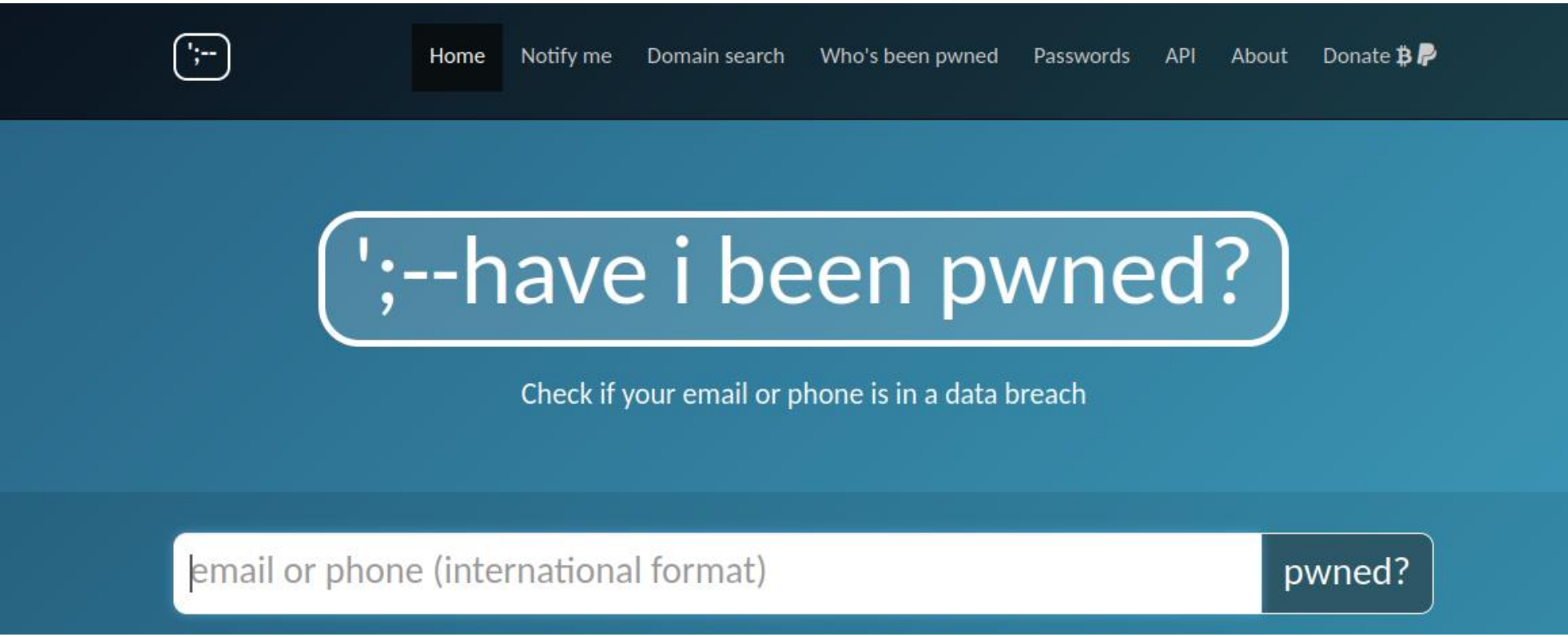
Das Hasso-Plattner-Institut (HPI) weist seit vielen Jahren auf die Notwendigkeit sicherer Passwörter hin. Der Blick auf die Top Twenty der in Deutschland meistgenutzten Passwörter 2020 zeigt jedoch, dass schwache und unsichere Zahlenreihen weiterhin Spitzenplätze belegen.

Top 20 deutscher Passwörter:

1	123456	11	qwertz
2	123456789	12	michael
3	passwort	13	killer
4	hallo123	14	michelle
5	12345678	15	hallo
6	ichliebedich	16	sonnenschein
7	1234567	17	alexander
8	1234567890	18	Passwort
9	lol123	19	abc123
10	12345	20	daniel

https://hpi.de/news/jahrgaenge/2020/die-beliebtesten-deutschen-passwoerter-2020-platz-6-diesmal-ichliebedich.html

Wurden meine Passwörter geleaked?



https://haveibeenpwned.com

Welche Rolle spielen Sicherheitsexperten?

- White hats

Die "guten": Möchten Schwachstellen finden und sie beheben.

- Black hats

Die "bösen": Möchten Schwachstellen für illegale Zwecke ausnutzen.

Source: Star Wars :)

ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

iOS
Android
Any OS

Up to $2,500,000										1.001 Android FCP Zero Click (Android)
Up to $2,000,000										1.002 iOS FCP Zero Click (iOS)
Up to $1,500,000									2.001 WhatsApp RCE+LPE Zero Click (iOS/Android)	2.002 iMessage RCE+LPE Zero Click (iOS)
Up to $1,000,000									2.003 WhatsApp RCE+LPE (iOS/Android)	2.004 SMS/MMS RCE+LPE (iOS/Android)
Up to $500,000	3.001 Persistence (iOS)	2.005 WeChat RCE+LPE (iOS/Android)	2.006 iMessage RCE+LPE (iOS)	2.007 FB Messenger RCE+LPE (iOS/Android)	2.008 Signal RCE+LPE (iOS/Android)	2.009 Telegram RCE+LPE (iOS/Android)	2.010 Email App RCE+LPE (iOS/Android)	4.001 Chrome RCE+LPE (Android)	4.002 Safari RCE+LPE (iOS)	
Up to $200,000	5.001 Baseband RCE+LPE (iOS/Android)		6.001 LPE to Kernel/Root (iOS/Android)	2.011 Media Files RCE+LPE (iOS/Android)	2.012 Documents RCE+LPE (iOS/Android)	4.003 SBX for Chrome (Android)	4.004 Chrome RCE w/o SBX (Android)	4.005 SBX for Safari (iOS)	4.006 Safari RCE w/o SBX (iOS)	
Up to $100,000	7.001 Code Signing Bypass (iOS/Android)	5.002 WiFi RCE (iOS/Android)	5.003 RCE via MitM (iOS/Android)	6.002 LPE to System (Android)	8.001 Information Disclosure (iOS/Android)	8.002 [k]ASLR Bypass (iOS/Android)	9.001 PIN Bypass (Android)	9.002 Passcode Bypass (iOS)	9.003 Touch ID Bypass (iOS)	

Hackertechniken ethisch testen

- Zerodium: ethisch korrekt ist es nicht!

- Bug bounties sammeln:
  - https://www.hackerone.com/
  - https://bugcrowd.com/
- Capture the Flag (CTF)
  - Inspiriert durch CTF Wettbewerbe
  - Ziel: Flaggen mit Hackertechniken zu kriegen

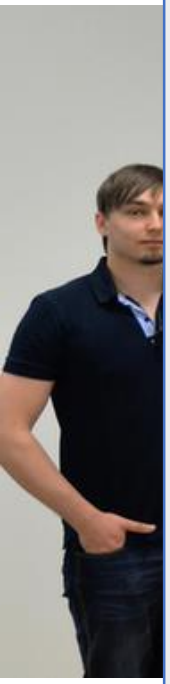
/upb/hack

https://upbhack.de/

Universität Paderborn

19.06.2018 | Pressemitteilung

Informatik-Studierende der Universität Paderborn landen bei internationalem Hackerwettbewerb in Stockholm auf Platz drei



Angekommen in der Weltspitze der studentischen Hacker: Informatik-Studierende der Universität Paderborn haben im Finale des internationalen Hackerwettbewerbs „Midnight Sun CTF“, das am 16. und 17. Juni in Stockholm stattfand, den dritten Platz belegt. Das 35-köpfige Team „/upb/hack“ konnte sich im vorherigen Wettbewerbsverlauf gegen 260 andere Mannschaften von Unis aus der ganzen Welt durchsetzen.

Das Finale von „Midnight Sun CTF“ fand an der Königlich Technischen Hochschule (KTH) in Stockholm statt und dauerte 24 Stunden. 14 Teams, u. a. aus Polen, Frankreich und Schweden, hatten es ins Finale geschafft, davon sieben studentische. Insgesamt 24 Aufgaben mussten gelöst werden. Das Paderborner Team bewältigte zwölf erfolgreich. Zu den Hauptaufgaben gehörte es, IT-Sicherheitslücken, die Cyber-Angriffe ermöglichen, schnell und effizient ausfindig zu machen. Sind die Lücken erst einmal erkannt, lassen sich IT-Systeme künftig besser gegen Cyberangriffe schützen.

Unter der Leitung von Bachelor-Student Heinrich Orlov überraschte „/upb/hack“ bereits Mitte April im Halbfinale des Wettbewerbs mit Platz acht und qualifizierte sich als bestes deutsches Team fürs Finale.

CTFs

- Gleich geht’s los, vorher noch ein paar Basics…

- Wer von euch kennt HTML?
- Wer von euch kennt CSS?
- Wer von euch kennt JavaScript?

HyperText Markup Language (HTML)

- Markup zum Erstellen von Webseiten
- Struktur:
  - Head: Titel, Metadaten, Skripte ...
  - Body: die Webseite

```
<html>
  <head>
…
  </head>
  <body>
…
   </body>
</hmtl>
```

HTML: Beispiel

```
<html>
<head>
  <title>IT-Sicherheit</title>
</head>
<body>
  <h1>IT-Sicherheit ist cool</h1>
  <form action="#">
    <input type="text" value="Ich stimme zu">
    <input type="submit" value="absenden">
  </form>
  <!-- Niemand sieht Kommentare -->
</body>
</html>
```

HTML: Beispiel

```
<html>
<head>
  <title>IT-Sicherheit</title>
</head>
<body>
  <h1>IT-Sicherheit ist cool</h1>
  <form action="#">
    <input type="text" value="Ich stimme zu">
    <input type="submit" value="absenden">
  </form>
  <!-- Niemand sieht Kommentare -->
</body>
</html>
```

HTML: Beispiel

```
<html>
<head>
  <title>IT-Sicherheit</title>
</head>
<body>
  <h1>IT-Sicherheit ist cool</h1>
  <form action="#">
    <input type="text" value="Ich stimme zu">
    <input type="submit" value="absenden">
  </form>
  <!-- Niemand sieht Kommentare -->
</body>
</html>
```

CTF - Demo

Interessiert in CTFs?

- https://portswigger.net/web-security
- https://www.hackthebox.eu/
- https://owasp.org/www-project-webgoat/

- CTFs als Teil von unseren Vorlesungen:
  - IT-Sicherheit
- Andere Bachelorveranstaltungen:
  - Secure Software Engineering
  - Einführung in die Kryptographie
  - Practical Usable Security and Privacy

Master-Veranstaltungen (Focus Area Security)

- Advanced Distributed Algorithms and Data Structures
- Designing code analyses for large-scale software systems
- Foundations of Cryptography
- Introduction to Quantum Computation
- Quantum Complexity Theory
- Machine Learning for Biometrics
- Human Factors in Security and Privacy
- Privacy and Technology
- Usable Security and Privacy
- Real World Crypto Engineering
- Web Security

Jetzt wird richtig gespielt