

„Meine Daten verschenke ich nicht“ Live Hacking

Wie sicher sind Daten auf meinem Computer und Smartphone?



Wer bin ich?

Thomas Trimborn

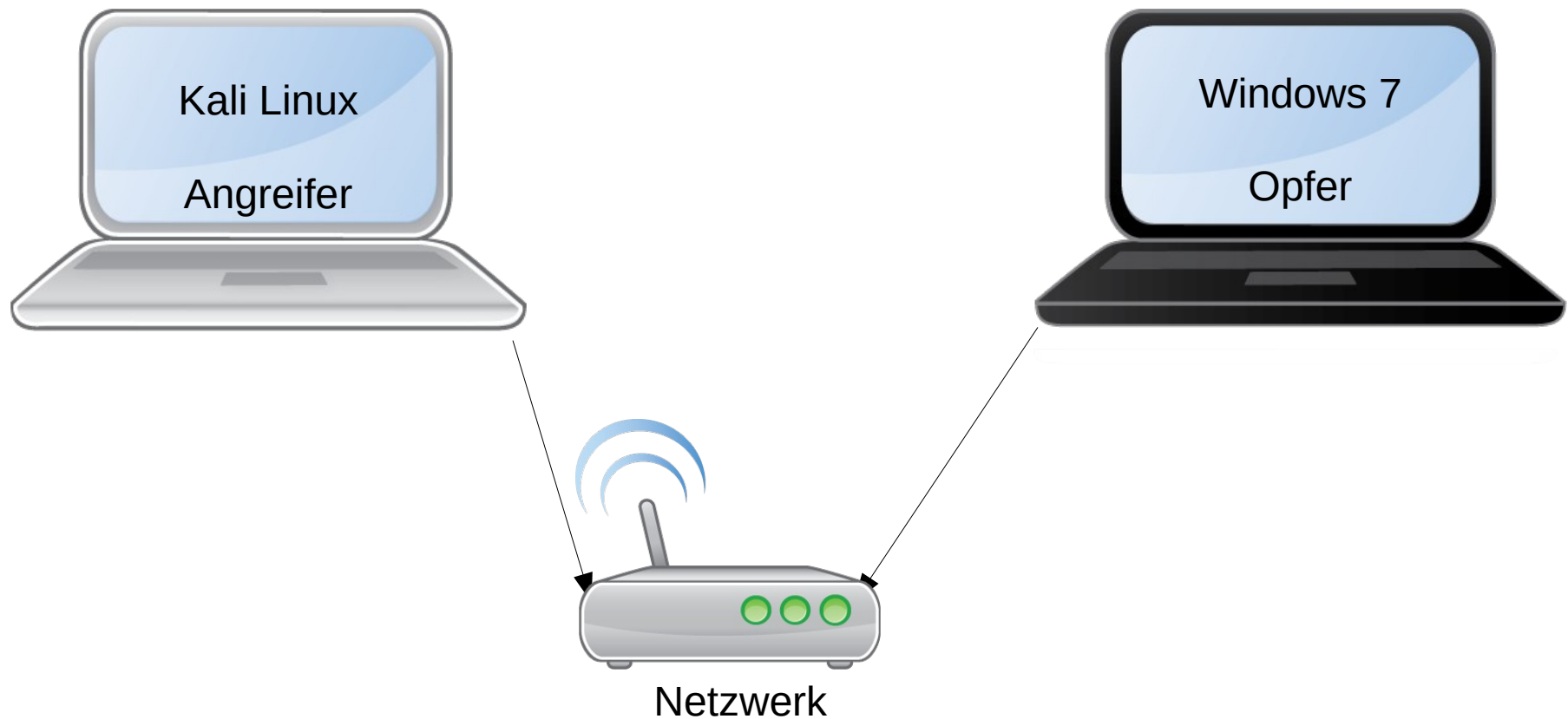
– Mitarbeiter Fraunhofer FKIE

- Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie
- Arbeitsgruppe Cyber Security
- Prof. Dr. Michael Meier

Live Hacking



Das Szenario



Live Hacking

Der Angreifer

- Kali Linux
 - Betriebssystem designed, um Schwachstellen in Computersystemen zu entdecken.
Notwendige Software ist vorinstalliert.
- Aktuelle Version
- Alle Updates installiert
- Umfangreich ausgestattet

Live Hacking

Das Ziel

- Windows 7
 - Original von Microsoft zum Testen angebotene Version
- Keine Veränderungen
- Software:
 - Adobe Flash Player 18 installiert
- Betriebssystem nicht manipuliert
- Alle aktuellen Updates installiert

Daten

Absender

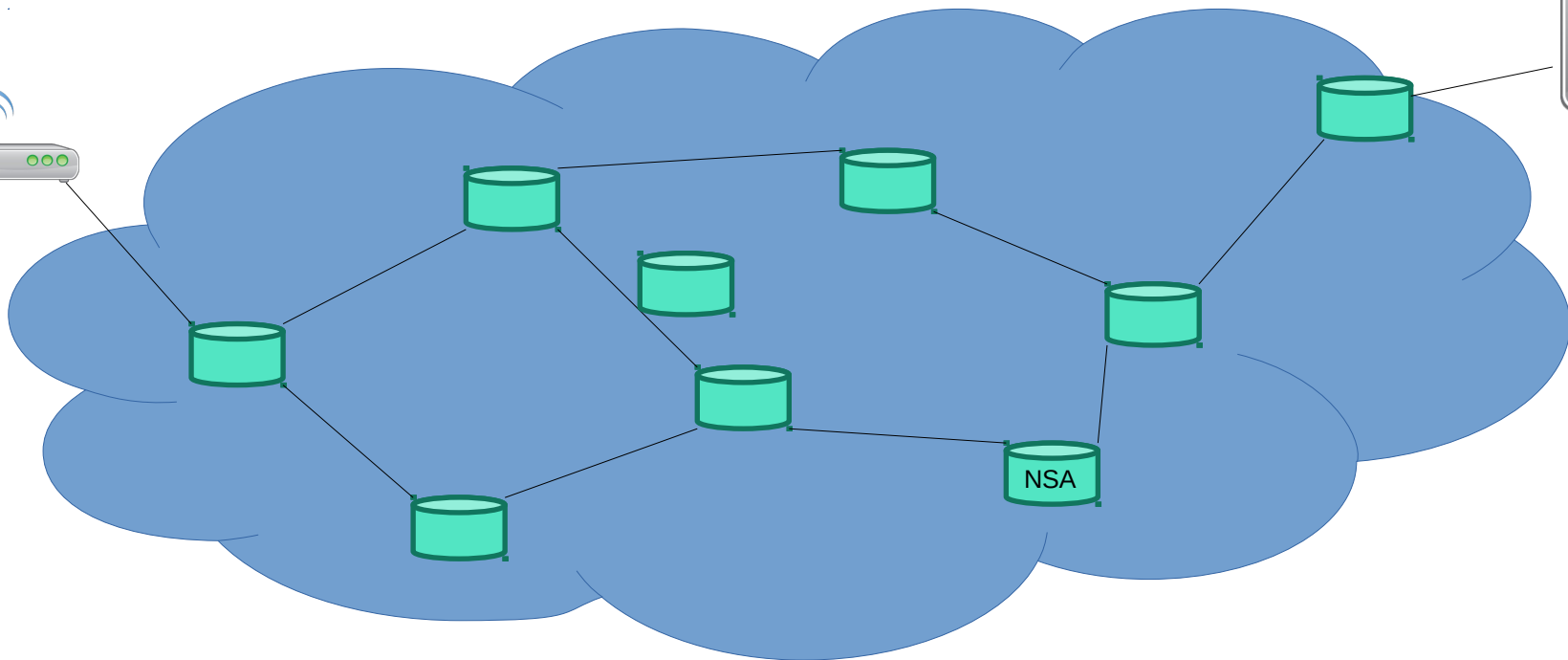
Text

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

0,70€

Adresse

Das Internet



Was für Daten können wir verlieren?

- Dokumente
 - Hausarbeiten, Präsentationen, Notizen
- Bilder und Videos
 - Urlaub, Partys, Erlebnisse, ...
- Kontodaten
 - Online-Banking
 - Social Media: Facebook, Instagram, ...
 - Spieleplattformen: Steam, Origin, Blizzard, PSN, Xbox Live
- Persönliches Profil
 - Interessen
 - Beziehungen
 - Standortdaten
 - Surfverhalten
 -

Was für Daten können wir verlieren?

- Dokumente
 - Hausarbeiten, Präsentationen, Notizen
 - Noten, Bewertungen, ...
- Bilder und Videos
 - Urlaub, Partys, Erlebnisse, ...
- Kontodaten
 - Online-Banking
 - Social Media: Facebook, Instagram, ...
 - Spieleplattformen: Steam, Origin, Blizzard, PSN, Xbox Live
- Persönliches Profil
 - Interessen
 - Beziehungen
 - Standortdaten
 - Surfverhalten
 -



Geteilter Rechner?

Wo können wir Daten verlieren?

- Zu Hause
 - Computer / Tablet / Smartphone
 - Smart TV / Kühlschrank / Home
 - Sicherheitstechnik
- Unterwegs
 - Smartphone
- Außerhalb unserer Reichweite
 - Auf Servern hinterlegte Daten

Verbreitung von Schadsoftware

- Versteckt in „kostenloser“ Software
 - Illegale Quellen von Filmen, Musik, Software, Apps sind bekannt als Verbreiter von Malware
- Per Nachricht
 - E-Mail, Whats-App, Telegram, Facebook, ...
 - Als Link
 - Als Anhang (Bild, Video, ausführbare Datei, Musik, ...)
- Manipulierte Websites
 - Es reicht ein manipulierter Teil
 - Eingebettetes Video, Werbebanner, ...
 - Links in Sozialen Medien
 - Je mehr Besucher, desto mehr mögliche Opfer!

Wie schwer ist es, Daten zu bekommen?

- Verlorene Datensätze:

- MySpace: 359 Mio.
- Dropbox: 68 Mio.
- Tumblr: 65 Mio.
- Yahoo:



Wie schwer ist es, Daten zu bekommen?

- Verlorene Datensätze:
 - MySpace: 359 Mio.
 - Dropbox: 68 Mio.
 - Tumblr: 65 Mio.
 - Yahoo:
 - Ende 2014: 500 Mio.



Wie schwer ist es, Daten zu bekommen?

- Was glaubt ihr?
- Verlorene Datensätze:
 - MySpace: 359 Mio.
 - Dropbox: 68 Mio.
 - Tumblr: 65 Mio.
 - Yahoo:
 - Ende 2014: 500 Mio.
 - Ende 2016: 1 Mrd.



Wie schwer ist es, Daten zu bekommen?

- Was glaubt ihr?
- Verlorene Datensätze:
 - MySpace: 359 Mio.
 - Dropbox: 68 Mio.
 - Tumblr: 65 Mio.
 - Yahoo:
 - Ende 2014: 500 Mio.
 - Ende 2016: 1 Mrd.
- Ransomware
 - Locky: 5000 Infektionen pro Stunde
nur in Deutschland
=> Fast 4 Mio. pro Monat



So schlimm wird es schon nicht sein ...

- Stagefright 4.0
- Aktuell auf fast allen Android Geräten
- Seit April 2015 immer mehr Lücken in gleicher Bibliothek

- 2,32 Mrd Smartphone User
- 86,1% Android
- 40,7% nicht angreifbar
- => 1,18Mrd Smartphones angreifbar

Quellen:

<https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>

<https://www.googlewatchblog.de/2017/05/gartner-android-ios-quartal2017/>

<https://developer.android.com/about/dashboards/index.html>

So schlimm wird es schon nicht sein ...

- Beliebte Serie an Routern
 - Netgear RXXXX
 - Hier zur Demonstration: R6400
 - 12.12.2016
 - Alle Funktionen und Einstellungen über manipulierte Website änderbar
 - Updates innerhalb weniger Wochen
 - Wer hat diese schon installiert?

Zugriff auf WhatsApp?



• Quelle: Whatsapp.com

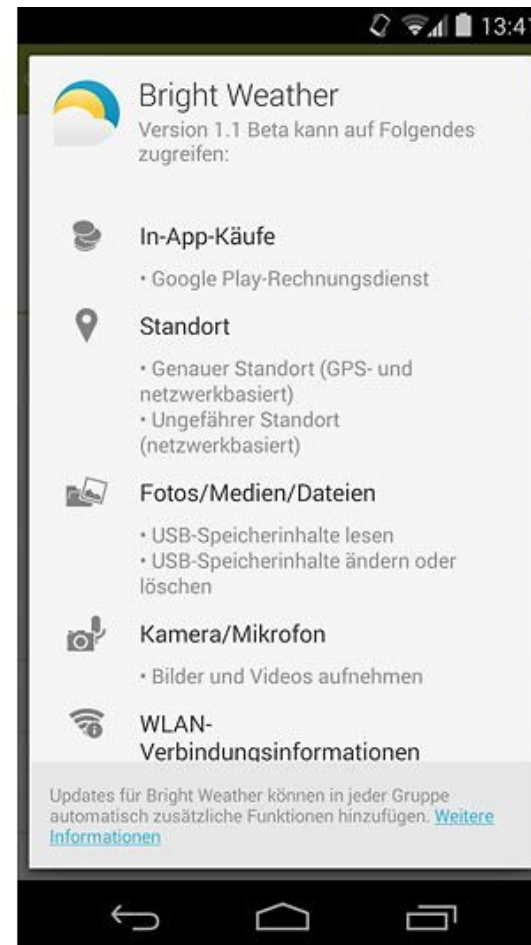
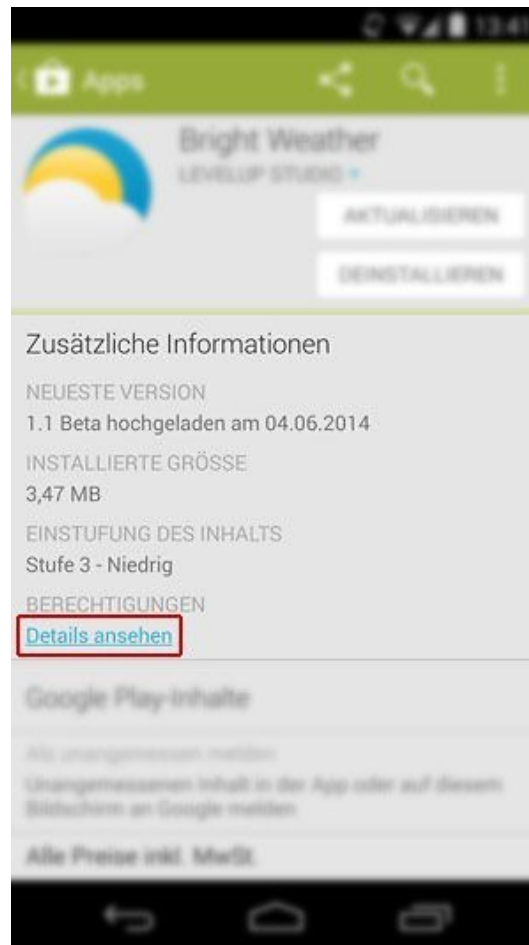
- Jetzt sicher dank Verschlüsselung?

WhatsApp

- Wer hat kontrolliert, ob wirklich verschlüsselt wird?
- Kann das jemand mitleesen?
- Was sollte man bei WhatsApp tun und was besser nicht?

App Berechtigungen

- Braucht eine App wirklich alles, was sie will?



Quelle: Androidpit.de

Zurück zu WhatsApp

- WhatsApp braucht:
 - Kontaktdaten lesen
 - Daten über Fremde
 - Kontaktdaten ändern
 - Standort
 - SMS empfangen und senden
 - Speicherinhalte lesen / verändern / löschen
 - Bilder und Videos aufnehmen
 - Audio aufnehmen
 - Daten aus dem Internet abrufen
 - Beim Start ausführen
 - Systemeinstellungen verändern
 - Audioeinstellungen verändern
 - uvm.
- Quelle: play.google.com

Zurück zu WhatsApp

- WhatsApp braucht:
 - Kontaktdaten lesen
 - Daten über Fremde
 - Kontaktdaten ändern
 - Standort
 - SMS empfangen und senden
 - Speicherinhalte lesen / verändern / löschen
 - Bilder und Videos aufnehmen
 - Audio aufnehmen
 - Daten aus dem Internet abrufen
 - Beim Start ausführen
 - Systemeinstellungen verändern
 - Audioeinstellungen verändern
 - uvm. Quelle: play.google.com
- Vertrauen wir dem Hersteller?
- Wer ist der Hersteller von WhatsApp?
- Woher installieren wir eine App?

Aus dem App-Store



colourblock

Retgumhoap Kanumep Puzzle

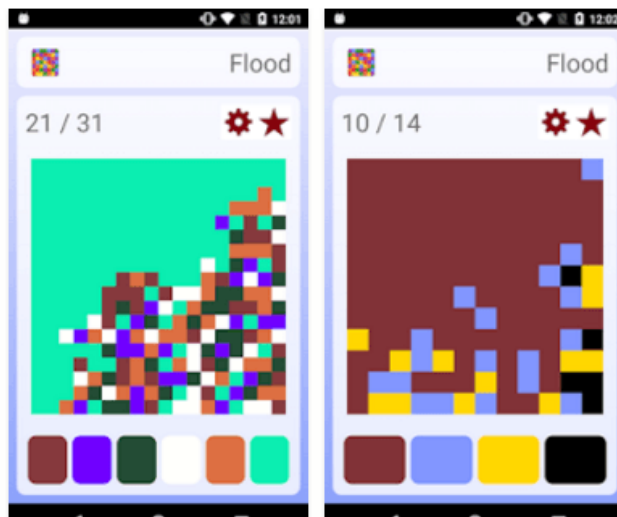
Everyone

Contains ads

This app is compatible with all of your devices.

★★★★★ 75

Installed



colourblock is a Simplest, Challenging, addictive puzzle game.

Bild: Kaspersky

Fragen?

Werbung

- Vorträge zu:
 - Gefahren im Internet
 - Live Hacking
 - Computer sicherer machen

Werbung

- Workshops
 - Hacking
 - Computer sicher machen
 - Richtiger (Wissenschaftlicher) Umgang mit Google (und anderen Suchmaschinen)

Werbung

- Projekte
 - IT Sicherheit
 - Roboterbau + Programmierung
 - Was sind Algorithmen?
 - Ein Einstieg in die Programmierung
 - ...

Kontakt

- Thomas Trimborn
- trimborn@cs.uni-bonn.de
- 0160-94714324
- Kölner Straße 50
53913 Swisttal