Sirrix AG
security technologies

ROHDE&SCHWARZ

Paradigmenwechsel im Mobile Security

Ammar Alkassar

ECO Internet Security Evening
9. Juli 2015 | München

SecurITy made in Germany

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Deutschland Land der Ideen
Ausgewählter Ort 2012

Software-Cluster

TeleTrusT
Pioneers in IT security.

eurobits
Europäisches Kompetenzzentrum für IT-Sicherheit • Bochum

TRUSTED COMPUTING GROUP™

BITKOM

bitmi
Bundesverband IT-Mittelstand e.V.

SecurITy made in Germany

Ursprünge in der Spitzenforschung

- Gegründet 2005 als Spin-Off der Universität des Saarlandes und des Deutschen Forschungszentrums für Künstliche Intelligenz
- Heute High-Tech Produkthaus für Behörden und Unternehmen
- Internationaler Technologieführer im Bereich „Trusted Infrastructures“

Kernziele

- Standardsysteme und -prozesse nachweisbar vertrauenswürdig machen

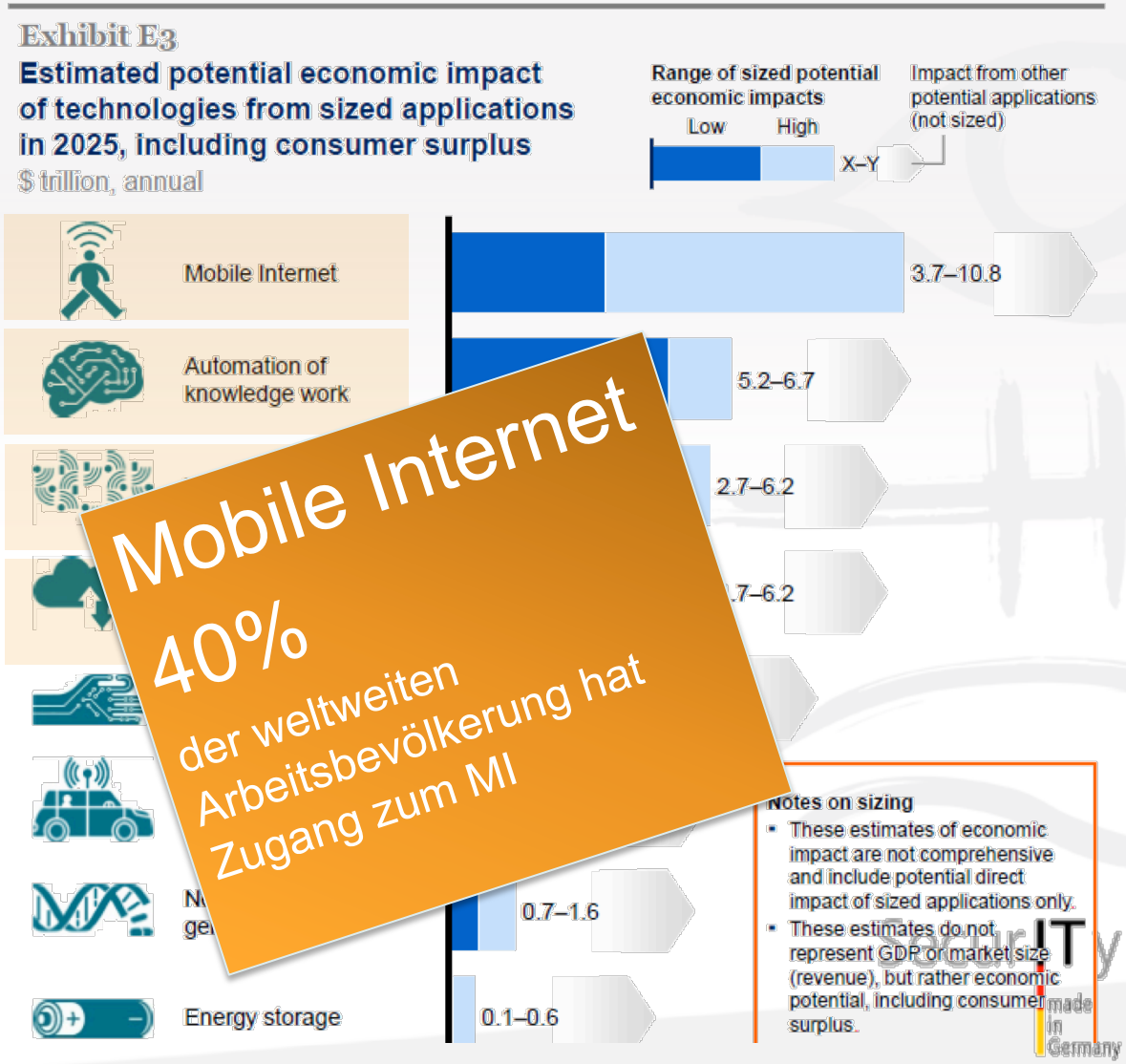
2012, 2014
Großer Preis des MITTELSTANDES
Oskar-Patzelt-Stiftung

2012-2014
Deloitte. 2012
Technology Fast 50
Deutschland

2013, 2014
INNOVATIONSPREIS-IT
INNOVATIONSPREIS-IT
SIEGER 2013
initiative mittelstand
IT-SECURITY

McKinsey 2013:

12 Economically Disruptive Technologies



Mobile Internet

40%

der weltweiten Arbeitsbevölkerung hat Zugang zum MI

Attack Vectors of Malware

- 3rd Party Apps
- Browser
- Multimedia/PDF
- Communication services
- Remote access
- Operating system
- Baseband CPU
- User

Vulnerabilities of Smartphones (1/2)

Smartphones get lost or are stolen

- *Risk: Disclosure of stored information (mails, contacts, documents, …)*

Passphrases are not secure and will be broken

- *Risk: Disclosure of stored data, unauthorized access to enterprise resources (Intranet, Mails, …)*

Eavesdropping of the communication

- *Risk: Disclosure of transmitted information (passphrases, PINs, credentials, …), eavesdropped telephone calls*

Information collecting (Datensauger) Apps

- *Risk: Disclosure of confidential information (contacts, calendar, location,, …)*

Vulnerabilities of Smartphones (2/2)

Exploits of Vulnerabilities of Apps

- Direct access to app data
- Indirect access to data of other apps

➲ *Risk: Disclosure of confidential information*

Exploits of Vulnerabilities of Android

- Access to cryptographic keys
- Bypassing of isolation and encryption mechanisms

➲ *Risk: Disclosure of confidential information, unauthorized access to enterprise resources (intranet, mail, …)*

SecurITy made in Germany

Expolits

Falsche SSL-Implementierung ermöglicht Angriff auf mobile Geräte

Sicherheitslücke in Android-Apps

10.12.13 | Redakteur: Peter Schmitz

XING 0 Empfehlen 0 Twittern 0 +1 0

PDF | Weiterempfehlen | Merken | Drucken

Durch eine Sicherheitslücke in einigen Android-Apps können Angreifer Zugangsdaten stehen. Am größten ist das Risiko bei Banking-Apps und Anwendungen die Single-Sign-On z.B. zu den Google- oder Microsoft-Diensten nutzen. (Bild: Fraunhofer SIT)

Viele beliebte Android-Apps haben einen schwerwiegenden Sicherheitsfehler, darunter auch Apps von Banken, Verlagen und anderen großen Organisationen. Angreifer können so im schlimmsten Fall Zugangsdaten zum Bankkonto oder zu den Cloud- und Mail-Diensten von Microsoft und Google erbeuten.

Mitarbeiter des Testlabors am Fraunhofer-Institut für Sichere Informationstechnologie in Darmstadt haben festgestellt, dass viele beliebte Apps der Android-Plattform einen schwerwiegenden Sicherheitsfehler bei der Implementierung von SSL aufweisen.

PCWorld

WHAT'S HOT | REVIEWS | HOW-TO | BUSIN

Security · Games · Productivity · Music & au

20

41 Tweet

ANTIVIRUS SOFTWARE

Over half of Andr
have unpatched
vulnerabilities, re

By Lucian Constantin, IDG-News-Service:Romania-

Over half of Android devices are vulnerable to kno
malicious applications to gain complete access to
stored on it, according to a report from mobile sec

This conclusion is based on scans performed dur
a free Android vulnerability assessment tool devel
devices for known privilege escalation vulnerabilities that

was some

Box on this page and saw just how much is going on...
PayPal CISO refutes compromise

So, No News is Good News, Right?

Share 127

Email

le history

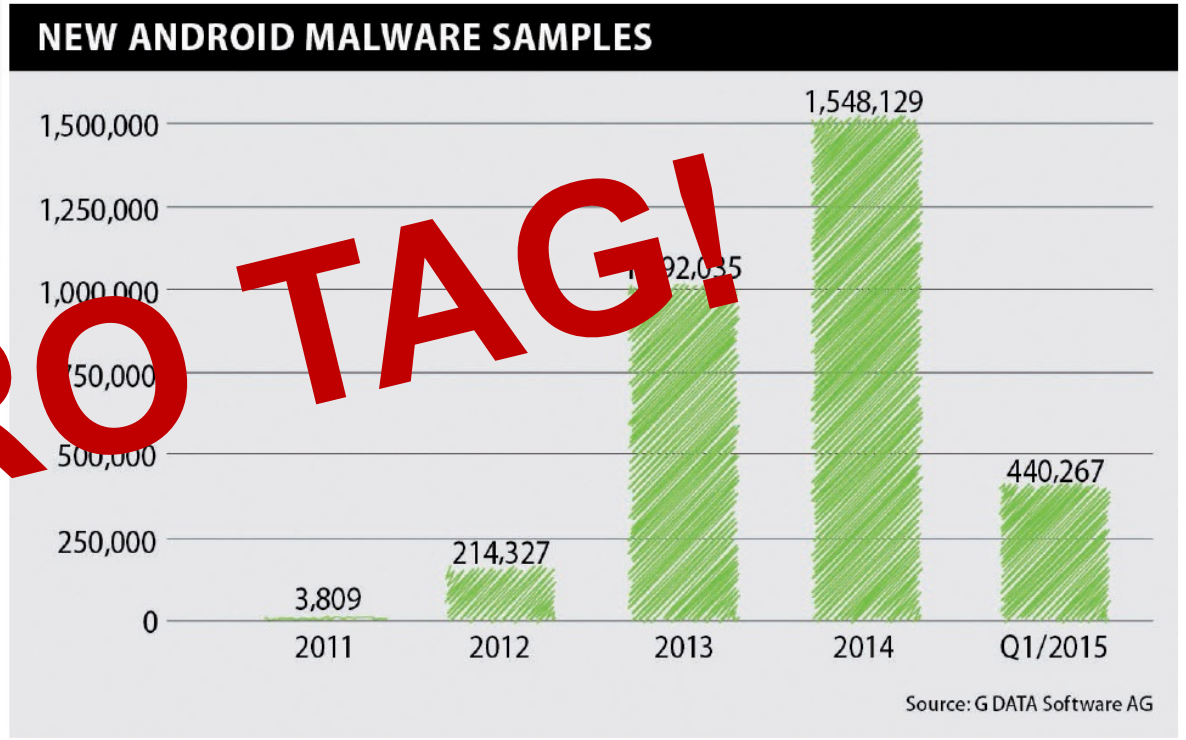
hnology
nsung · HTC ·
ware · Data and
nputer security ·
king · Android ·
artphones · Mobile
nes

e news

Related

Create

Ganz praktische Herausforderungen…



PRO TAG!

Neue Anwendungsfelder
Beispiel „Albert“ Payment Terminal

- Commonwealth Bank of Australia
- Expected market share in Australia:
  70% until end of 2016
- Android-Device und
  Android-Apps

VISA

MasterCard

Maestro

SecurITy made in Germany

Paradigmenwechsel zu pro-aktiven Systemen

Reaktive Ansätze:

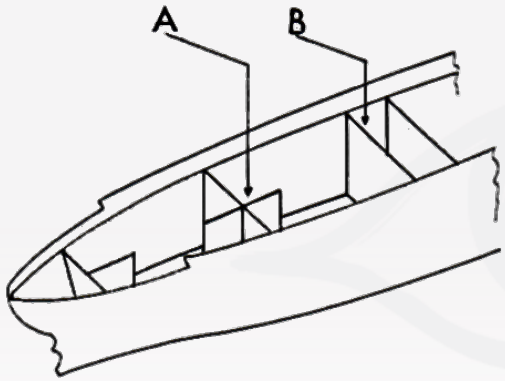
- „Airbag-Methode“:
  Wenn‘s passiert soll es weniger „weh tun“

Proaktive IT-Sicherheit:

- „ESP-Strategie“: Verhindern, dass man überhaupt ins Schleudern kommt

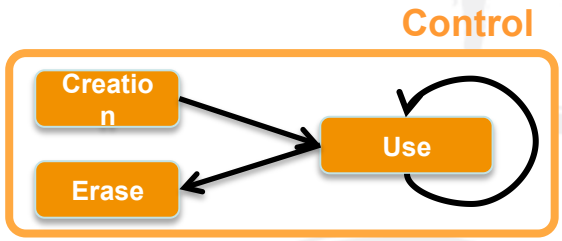
SecurITy made in Germany

Pro-aktive Konzepte



Separation, Integritätsprüfung

- Separierung kritischer Bereiche
  in von einander isolierte Komponenten
- Reduzierung der sicherheitsrelevanten Komponenten (TCB)
- Integritätsschutz der Komponenten
- Datenaustausch nur über klar definierte Schnittstellen
- TECHNOLOGIEN: Virtualisierung, Sicherheitskerne



Informationsflusskontrolle statt Zugriffskontrolle

- Kontrolle der Daten über gesamten Lebenszyklus
- Verarbeitung nur durch integritätsgeschützte Komponenten
- TECHNOLOGIEN: Trusted Computing, Remote-Attestation

SecurITy made in Germany

Example: BizzTrust

Secure Mobile Computing

- Enables strict separation between business and personal apps and data
- Prevents from malware infection and APT attacks
- Even in the presence of exploits in android framework or in any app.
- Provides information-flow control and includes strong encryption for stored data and communication data.

Technology

- Uses TURAYA™ Type-Enforcement Security Kernel
- Fully manageable with TOM

SecurITy made in Germany

THANK YOU!

Sirrix AG
Im Stadtwald, Geb. D3 2
66123 Saarbrücken
GERMANY

Tel **+49** (0)681/95986-0
Fax **+49** (0)681/95986-500

Email info@sirrix.com
Web www.sirrix.com