genua

Cyber Defense: Auf verlorenem Posten?

Dirk Loss, genua gmbh

Magenta Security 2016
Frankfurt, 2016-11-30

Bank Trojaner

Drive-by Exploits

Malware

APT

DDoS

Social Engineering

Car Hacking

Cyber-Spionage

IT-Sicherheitsprobleme überall

Botnets

Spam

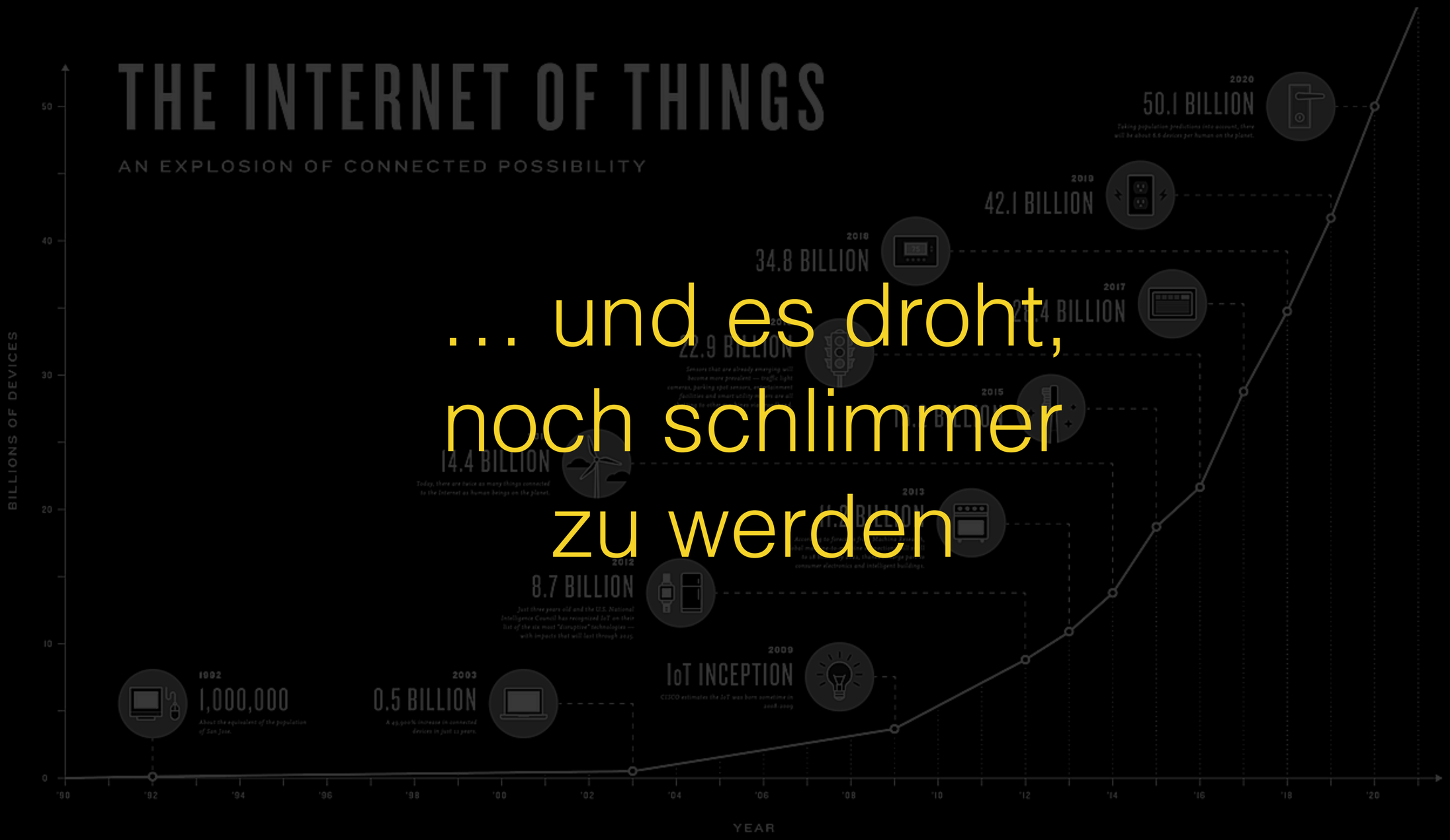
ICS Insecurity

Exploit Kits

Crypto-Ransomware

Cyber Crime

Identitätsdiebstahl



… und es droht,
noch schlimmer
zu werden


Cyber-Depression?

Hoffnung?

Erfolgsbeispiele?

Was tun?

„Angreifer sind prinzipiell im Vorteil!“

Militärhistorie

Carl von Clausewitz

- Erhalten ist leichter als gewinnen
- Verteidiger kennt das Gelände
- Moralischer Vorteil und Unterstützung durch Bevölkerung

(„Vom Kriege“, 1832)

Vom Kriege.

Hinterlaſſenes Werk
des
Generals Carl von Clauſewitz.

Fünfte durchgeſehene Auflage.

Mit einer Einführung vom Chef des Generalſtabes der Armee
Generaloberſt Grafen von Schlieffen, Excellenz.

„Verteidiger kennt das Gelände“

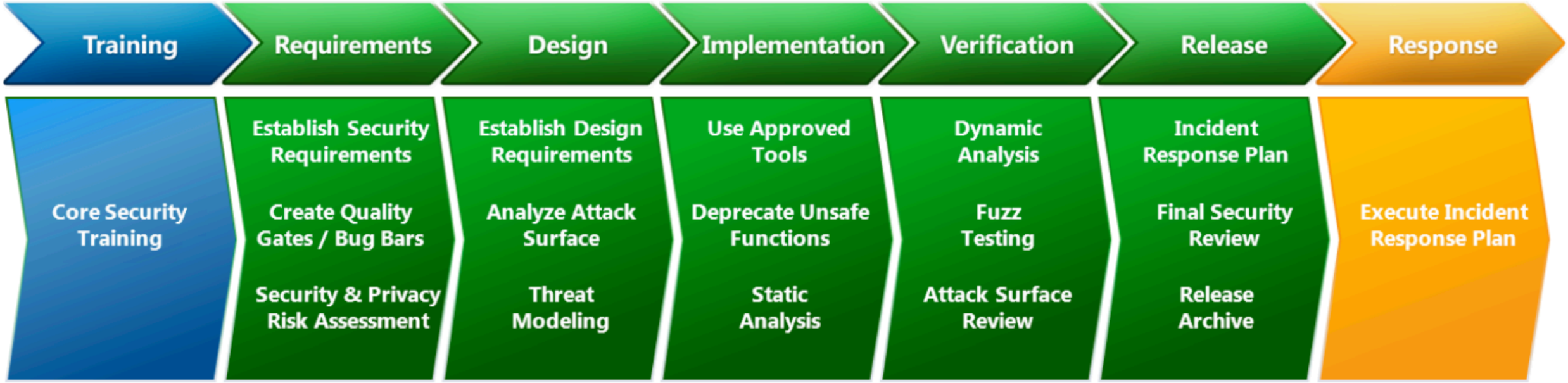
„Our key to success is knowing that network better than the people who set it up.“

Rob Joyce, NSA TAO

„Software hat Sicherheitslücken!“

Microsoft

Security Development Lifecycle (SDL)



iOS Security

Steigende Preise für Exploits

Product / Exploit Type	New Price	Previous Price
Apple iOS 10 (Remote Jailbreak)	**$1,500,000**	$500,000
Android 7 (Remote Jailbreak)	**$200,000**	$100,000
Flash (RCE) + Sandbox Escape	**$100,000**	$80,000
MS Edge + IE (RCE) + Sandbox Escape	**$80,000**	$50,000

(Zerodium)

halvarflake
@halvarflake

Following

Days required to find and exploit a big in a nontrivial unknown codebase seems to double every 24 months for me. Moore's law???

RETWEETS 7 LIKES 17

1:08 PM - 20 Sep 2016

halvarflake
@halvarflake

Following

Time-to-exploit went from a day 15yrs ago to a week or so 10yrs ago to months now.

Global Commission
on Internet Governance

ourinternet.org

PAPER SERIES: NO. 16 — JULY 2015

Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime

Eric Jardine

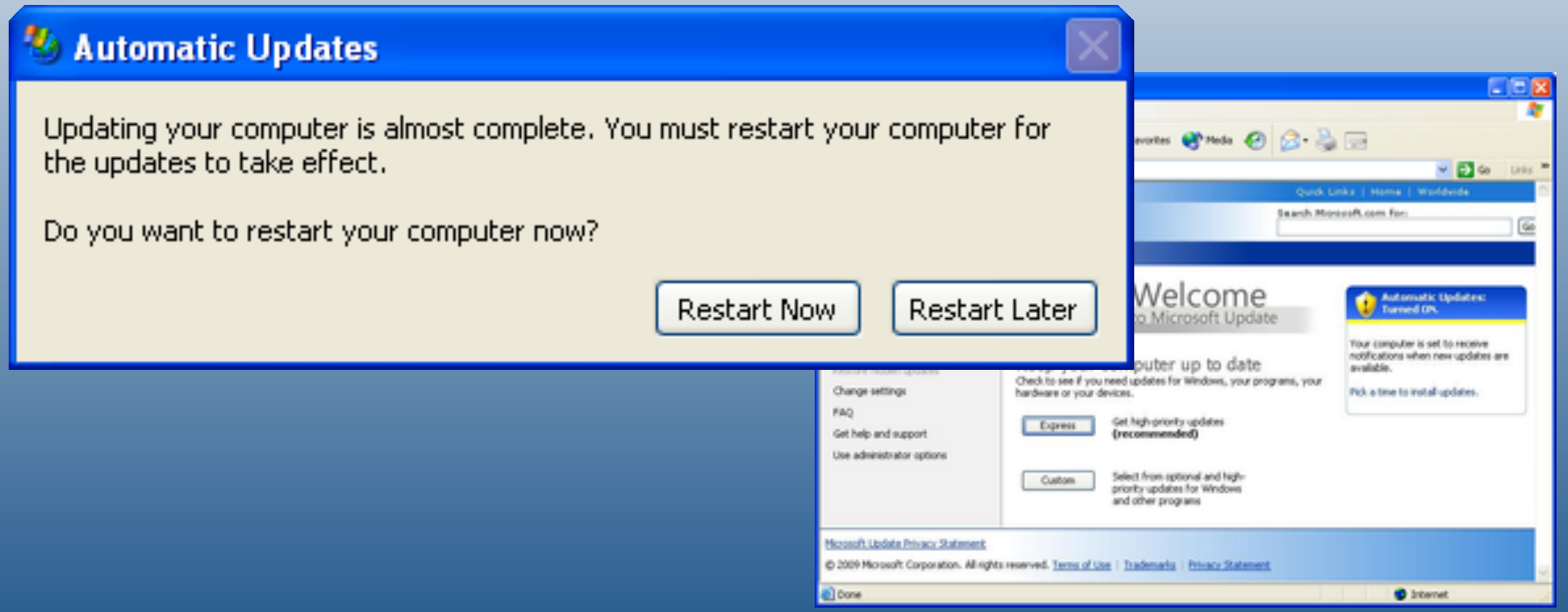
… cybercrime statistics need to be expressed as a **proportion** of the growing size of the Internet …

… the absolute numbers say things are getting worse, while the normalized numbers show that the **situation is improving**

„Legacy Systeme
lassen sich nicht absichern!“

Spitzentechnik von heute ist die Altlast von morgen…

Updates

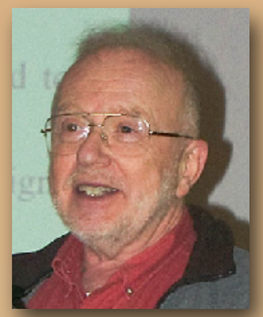

Automatic Updates
Updating your computer is almost complete. You must restart your computer for the updates to take effect.
Do you want to restart your computer now?
Restart Now
Restart Later
Welcome
Microsoft Update
Automatic Updates: Turned Off
Your computer is set to receive notifications when new updates are available.
Pick a time to install updates.
Change settings
FAQ
Get help and support
Use administrator options
Express
Get high-priority updates (recommended)
Custom
Select from optional and high-priority updates for Windows and other programs
Microsoft Update Privacy Statement
© 2009 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement
Done
Internet

Separation

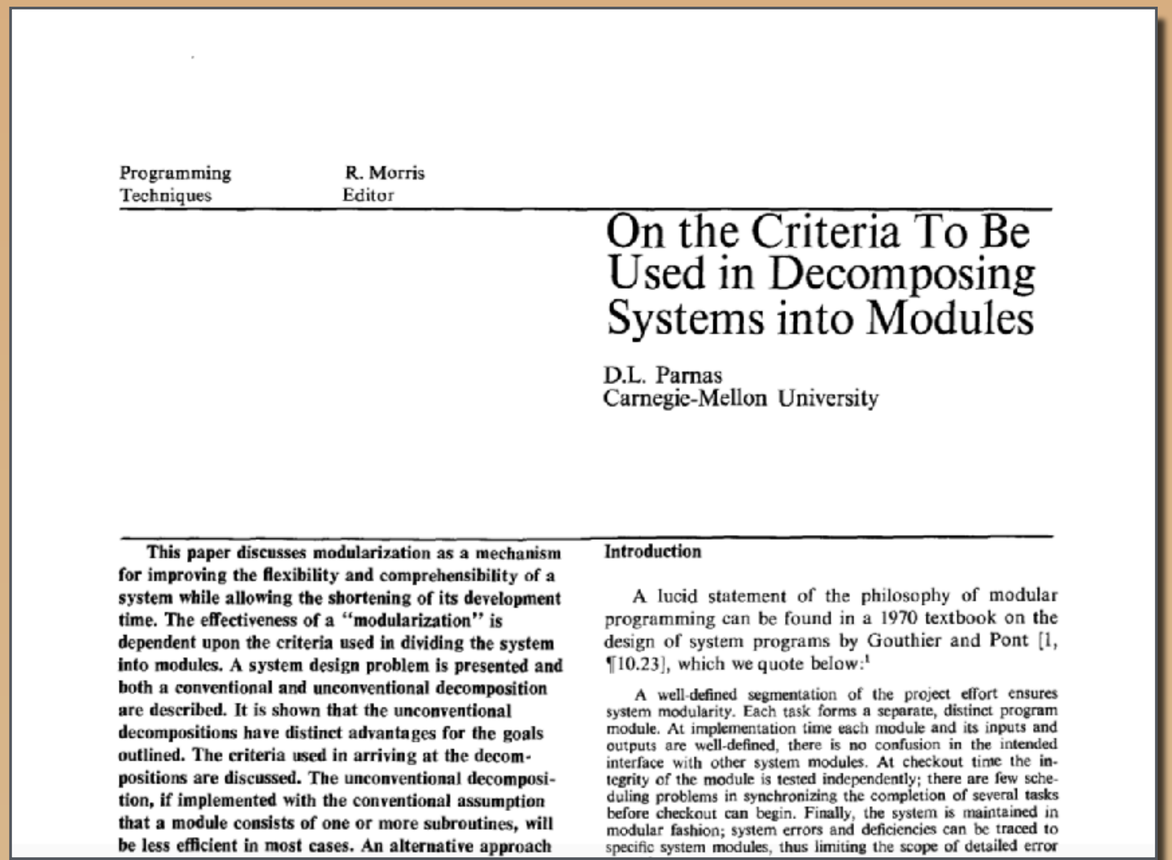
„Die Komplexität ist kaum beherrschbar!“

Komplexität reduzieren

Was sich schnell ändert,
trennen von dem,
was sich langsam ändert



Information Hiding (Parnas, 1972)



Programming Techniques — R. Morris Editor

On the Criteria To Be Used in Decomposing Systems into Modules

D.L. Parnas
Carnegie-Mellon University

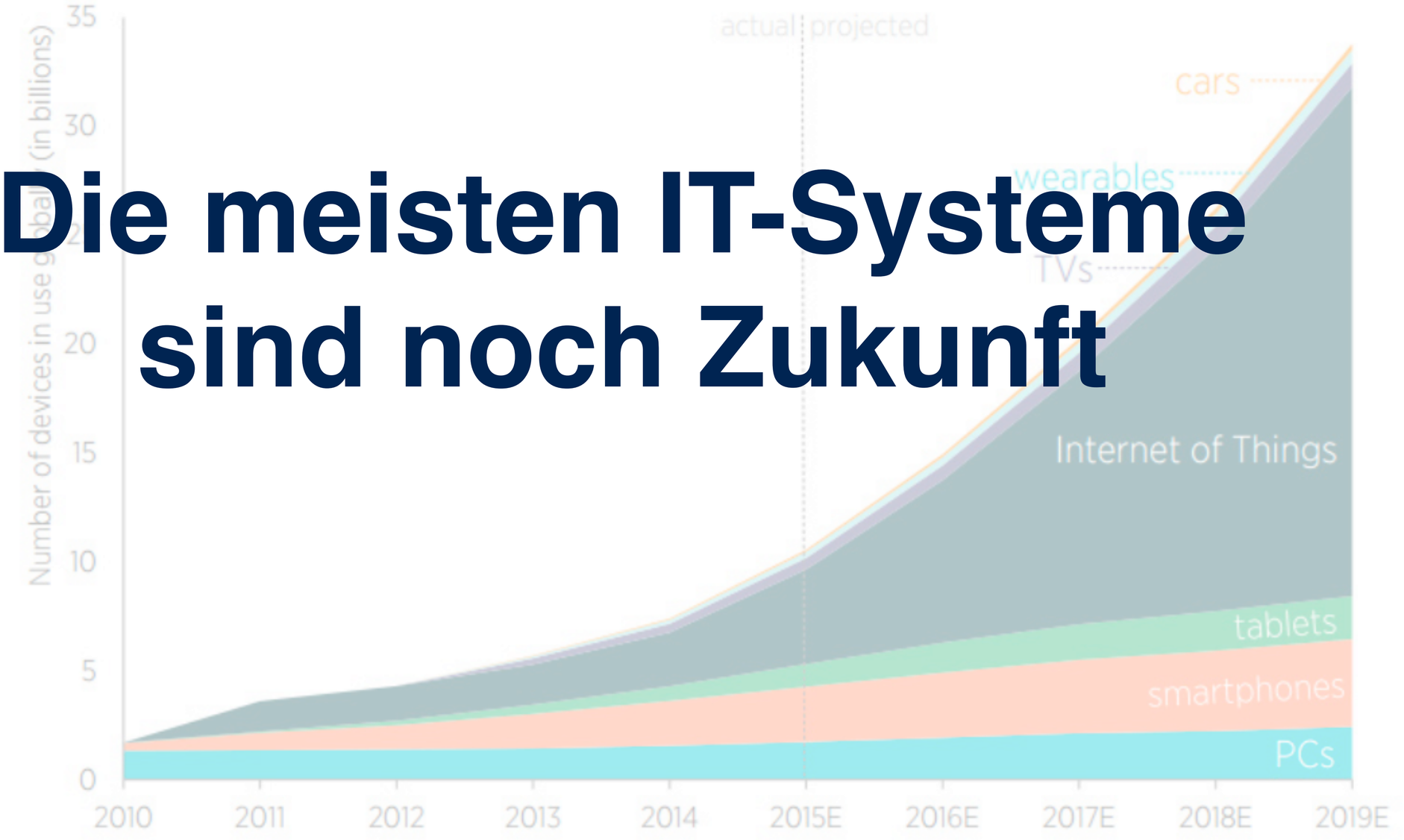
This paper discusses modularization as a mechanism for improving the flexibility and comprehensibility of a system while allowing the shortening of its development time. The effectiveness of a "modularization" is dependent upon the criteria used in dividing the system into modules. A system design problem is presented and both a conventional and unconventional decomposition are described. It is shown that the unconventional decompositions have distinct advantages for the goals outlined. The criteria used in arriving at the decompositions are discussed. The unconventional decomposition, if implemented with the conventional assumption that a module consists of one or more subroutines, will be less efficient in most cases. An alternative approach

Introduction

A lucid statement of the philosophy of modular programming can be found in a 1970 textbook on the design of system programs by Gouthier and Pont [1, ¶10.23], which we quote below:[1]

A well-defined segmentation of the project effort ensures system modularity. Each task forms a separate, distinct program module. At implementation time each module and its inputs and outputs are well-defined, there is no confusion in the intended interface with other system modules. At checkout time the integrity of the module is tested independently; there are few scheduling problems in synchronizing the completion of several tasks before checkout can begin. Finally, the system is maintained in modular fashion; system errors and deficiencies can be traced to specific system modules, thus limiting the scope of detailed error

Die meisten IT-Systeme sind noch Zukunft



Source: John Greenough, "The Internet of Everything 2015," *Business Insider Intelligence*. Produced by Adam Thierer and Andrea Castillo, Mercatus Center at George Mason University, 2015.

"Angriffe sind automatisierbar!"

Diversität

- ***Monokulturen vermeiden***
- **RANDomisierung**
- Changing Targets

Skalierbarkeit

GUTSCHEINE | NEWSLETTER | PREISVERGLEICH | ABC & SHOP | VIP-CLUB | FORUM LOGIN

Computer Bild 20 Jahre Computer

START TECHNIK DOWNLOADS SPIELE AKTIONEN VIDEOS

Suchbegriff oder Webcode eingeben SUCHEN

Home › Technik › Mobil › App-Check › News

SPECIAL Special: Sicherheits-Center – Sicher Chatten, Telefonieren & Co.

WhatsApp macht dicht: Sichere Ende-zu-Ende-Verschlüsselung aktiviert

06.04.2016, 15:07 Uhr **Der beliebte Messenger WhatsApp setzt ab sofort auf eine umfassende Ende-zu-Ende-Verschlüsselung auf allen Geräten. Ein deutliches Zeichen nach dem Streit zwischen Apple und dem FBI.**

von Markus Schmidt

Twittern Empfehlen 925

Themenübersic

Win-10-Spionage-Stopper: 2017er-Version gratis

Gegen Locky & Co.: Die besten Schutz-Tools für lau

Microsoft-Patchday: 67 Lücken geschlossen

THE VERGE TECH SCIENCE CULTURE CARS REVIEWS LONGFORM MOR

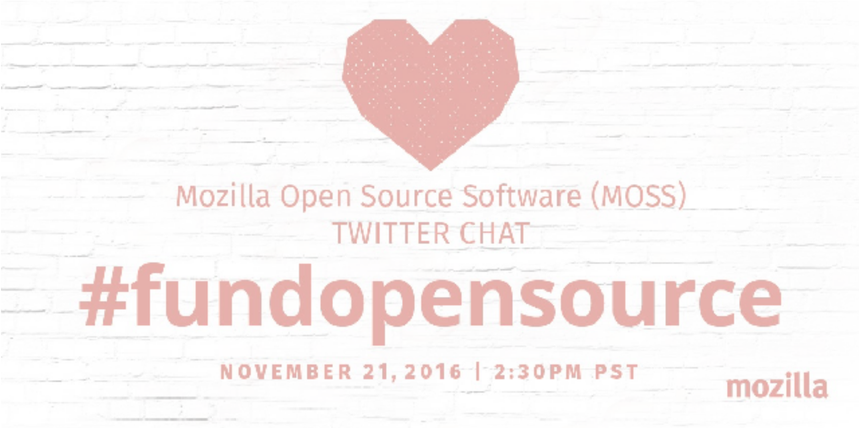
GOOGLE TECH

Chrome is stepping up its war on the unencrypted web

by Russell Brandom | @russellbrandom | Sep 8, 2016, 11:15am EDT

Open Source fördern

- Lizenz ermöglicht hohe Verbreitung
- Investitionen in Sicherheit nutzen Vielen
- Offener Quellcode ermöglicht Audits
- Basis-Infrastruktur für alle



„Immer wieder werden
neue Angriffstechniken erfunden!“

IDS

Antivirus

Public Key Cryptography

Firewalls

CERTs

Auch in der Defensive sind Quantensprünge möglich

Homomorphe Verschlüsselung

Formale Methoden

Blockchain

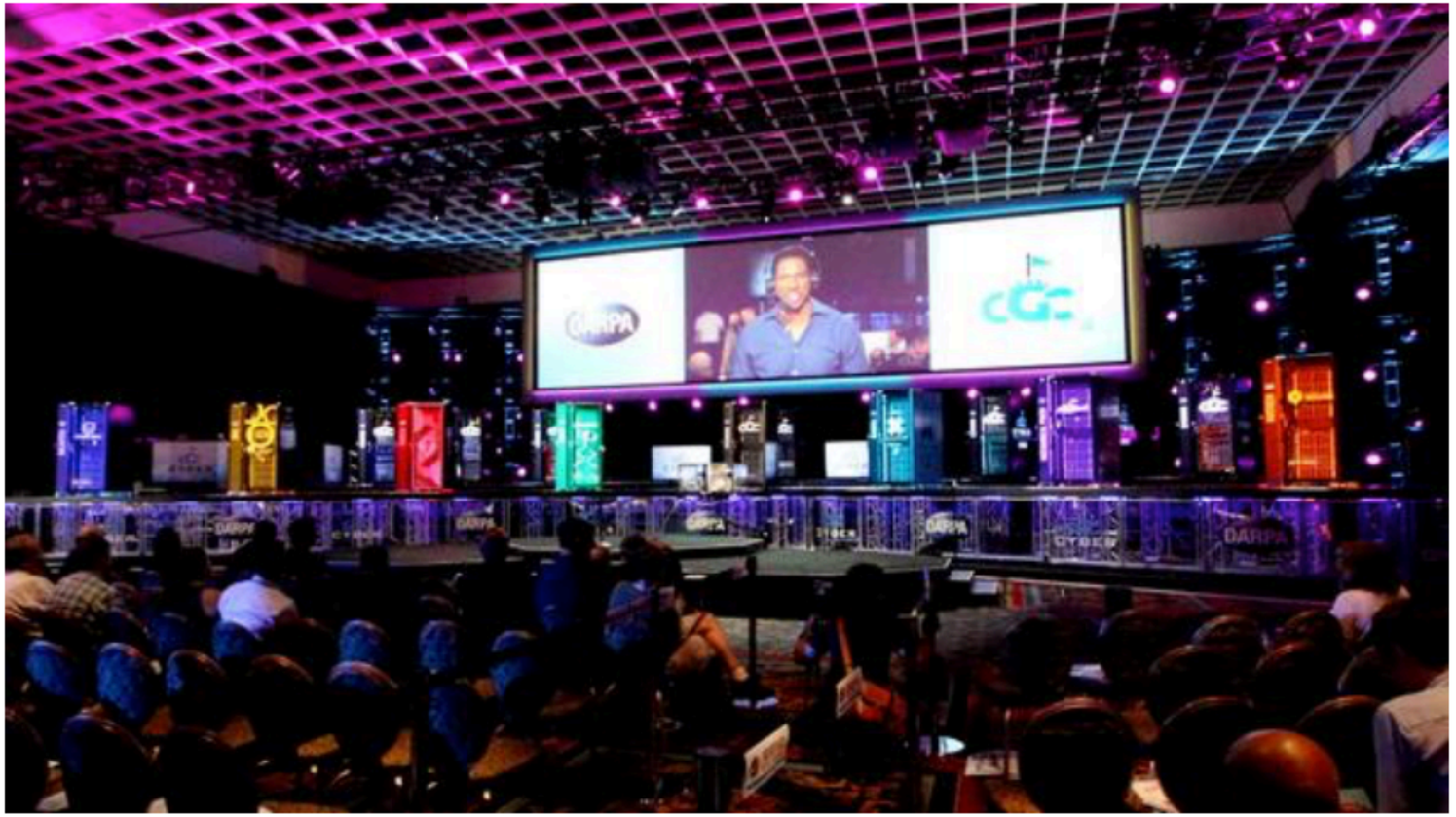
Machine Learning

Private Information Retrieval

Cyber Grand Challenge: Unsichere Computer heilten sich selbst

05.08.2016 09:54 Uhr – Daniel AJ Sokolov

vorlesen



Am Vorabend der Def Con richtete die DARPA das Finale der Cyber Grand Challenge aus. (Bild: Adrian Dabrowski)

Die Cyber Grand Challenge der DARPA zeigte, dass sich Umwälzungen in der IT-Security anbahnen. 7 vernetzte, autonom agierende Systeme hackten einander und schrieben Hunderte Programme neu, um Sicherheitslücken zu schließen. Ganz ohne menschliches Zutun.

(www.heise.de)

Was tun?

Defensive stärken!

„National leaders, cybersecurity innovators, and thought leaders need to set ourselves the strategic goal of a defensible cyberspace, where the defense not the attackers, have the advantage.“

Jason Healey, „Defense at Hyperscale“

Defensive stärken!

- Starke Defensive reduziert Risiko für Konflikte:

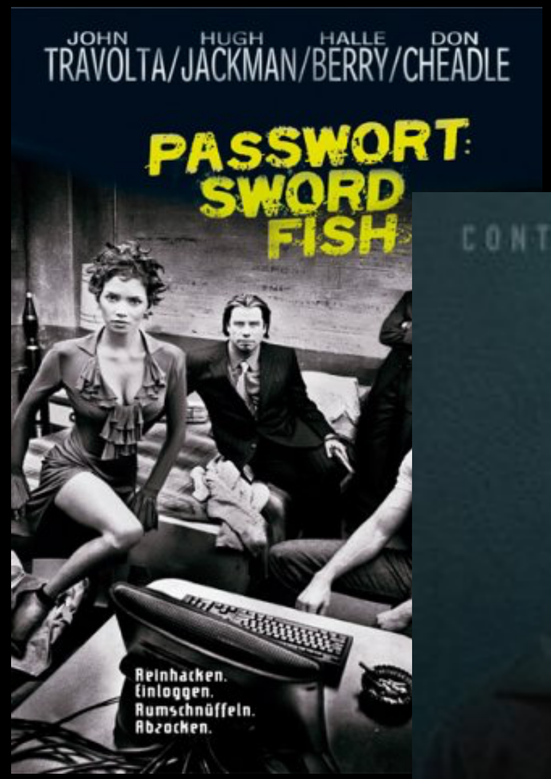
  Defensive des Gegners stärken nützt auch mir

- Starke Offensive führt zu Spirale der Aufrüstung:

  Abschreckung aufbauen, als Erster angreifen

(Dale Peterson: „Defense Will Win“, S4xEurope 2016)

Hacking ist nicht mehr cool



Zusammenarbeit intensivieren

Die Sicherheit meines Systems
hängt von der Sicherheit
deines Systems ab

„Moralischer Vorteil und Unterstützung durch die Bevölkerung“

Cyber Defense: Auf verlorenem Posten?

Nein,

- Verteidiger müssen nicht immer im Nachteil sein
- Wir haben Fortschritte gemacht, es gibt Erfolgsbeispiele
- Also: Nicht den Mut verlieren!
- Gemeinsam die Cyber Defensive stärken
  - Komplexitätsreduktion, Zusammenarbeit, Skalierbarkeit
  - Angreifer sind uncool

genua

Cyber Defense:
Auf verlorenem Posten?

Dirk Loss, genua gmbh, Kirchheim bei München

dirk_loss@genua.de
089 - 99 1950-0