
SBA
Research

EHR: System Architecture and Systems Security – An Analysis of Interdependencies

SBA Research &
Vienna University of Technology

Edgar R. Weippl

SBA Research

Typical Security Errors in Large-Scale Systems

SBA Research &
Vienna University of Technology
Edgar R. Weippl

SBA Research

Basic Architectures

http://datacenterpost.com/wp-content/uploads/2014/11/mainframe-apps.jpg

http://www.futuretimeline.net/subject/images/computer-storage-timeline.jpg

SBA Research

Basic Architectures

http://www.datacenterknowledge.com/wp-content/uploads/2013/07/cloud-vm-movement.jpg

http://conversation.which.co.uk/wp-content/uploads/2011/03/peer-to-peer_shutterstock_56319415.jpg

SBA Research

Architectures

	Centralized	Distributed
Historic		
Hype		

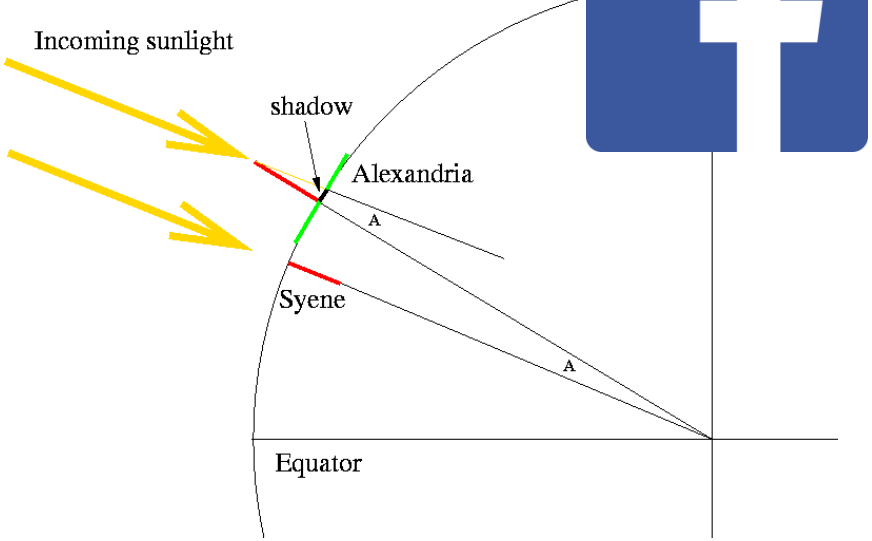
SBA Research

Architectures

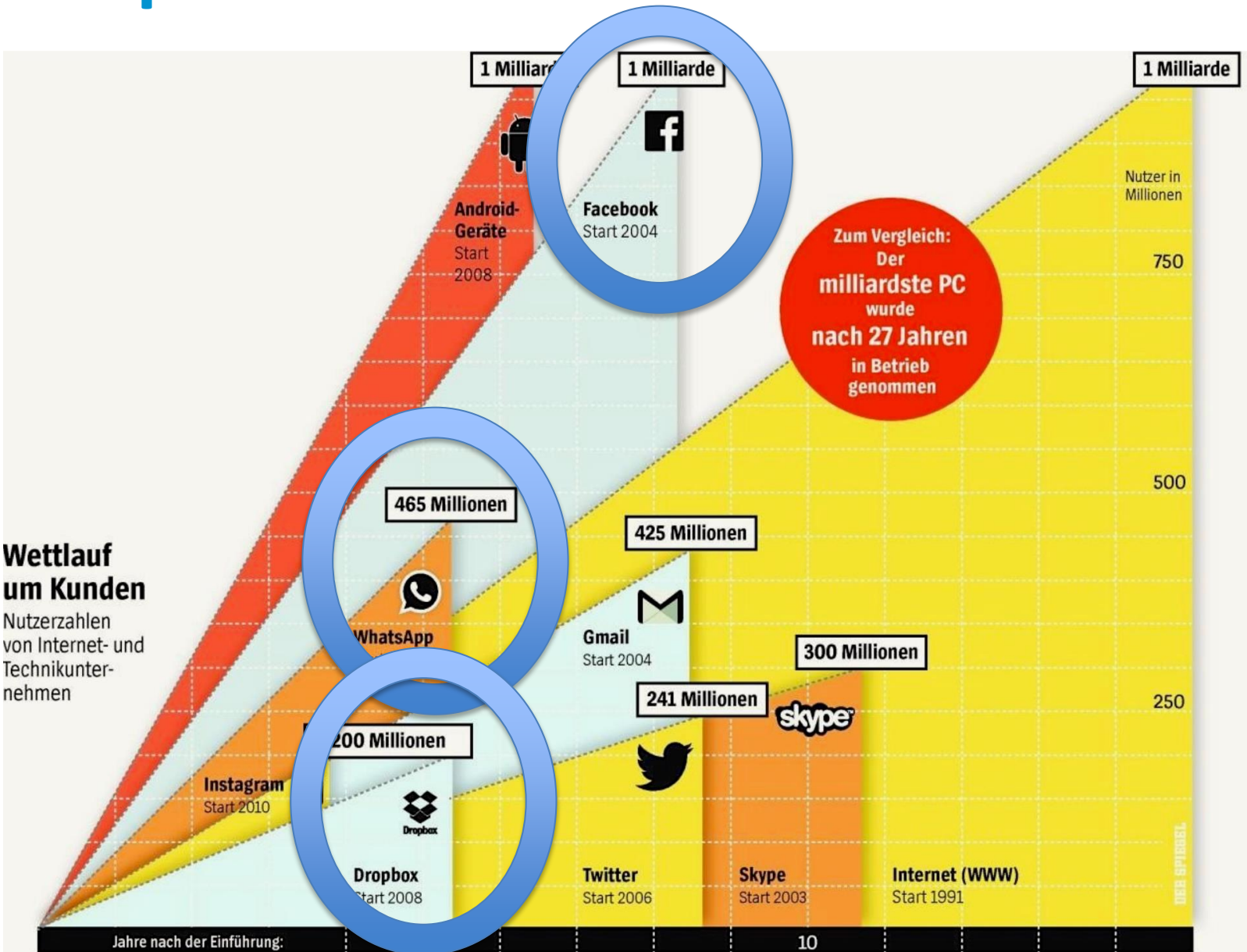
	Centralized	Distributed
Historic	**Mainframe** • Admins understand systems and can observe everything • Server-based security	**Client-Server** • Admins understand systems and can observe servers and communication • Decentral / private data
Hype	**Cloud Computing** • Internals hidden / protected • Arms race in analysis	**P2P / Grassroots Infrastructure** • Trust in majority • Sybil attack

SBA Research

Observation & Empirical Research

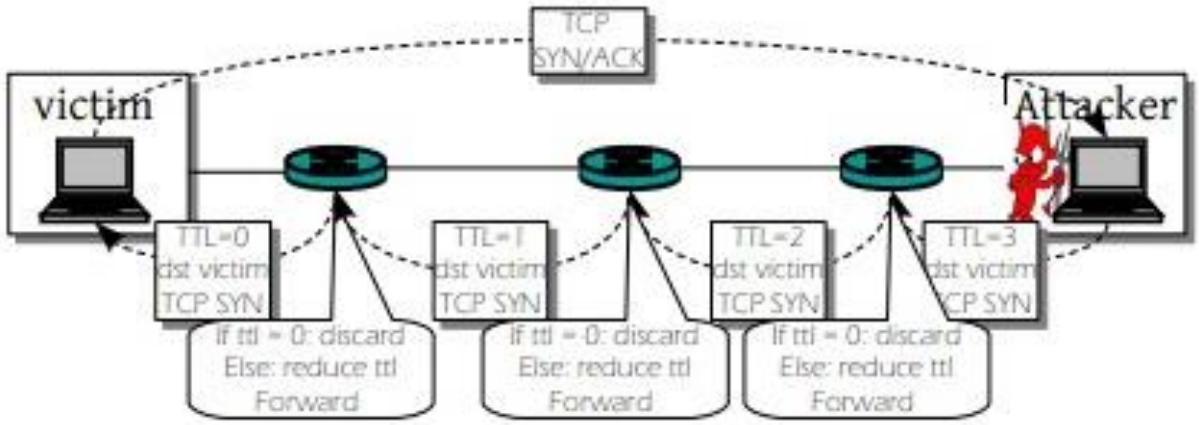


Impact


1 Milliarde
1 Milliarde
1 Milliarde
Nutzer in Millionen
750
500
250
Android-Geräte Start 2008
Facebook Start 2004
Zum Vergleich: Der milliardste PC wurde nach 27 Jahren in Betrieb genommen
465 Millionen
425 Millionen
300 Millionen
241 Millionen
200 Millionen
Wettlauf um Kunden
Nutzerzahlen von Internet- und Technikunternehmen
WhatsApp
Gmail Start 2004
Instagram Start 2010
Dropbox
Dropbox Start 2008
Twitter Start 2006
Skype Start 2003
Internet (WWW) Start 1991
Jahre nach der Einführung:
10
DER SPIEGEL

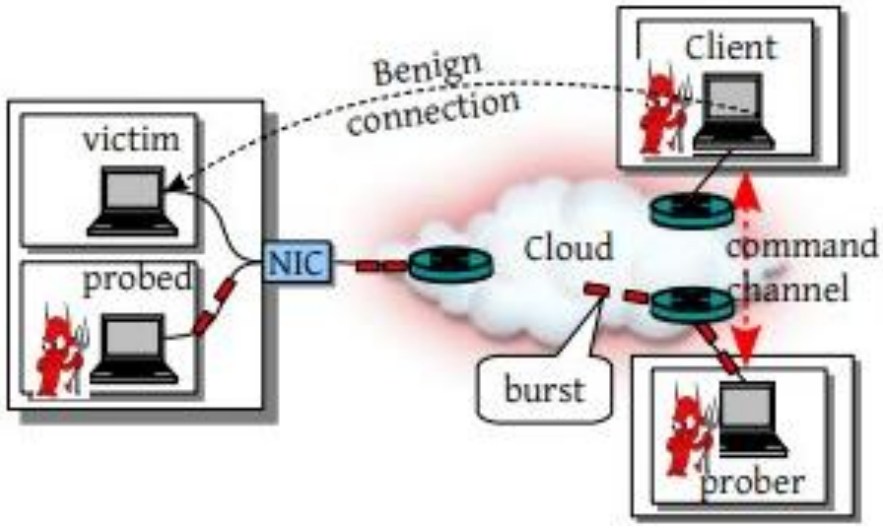
Hop-count measuring

- Cloud platforms block ICMP errors, control messages
- Our idea: Scan with incrementing TTL
  - Use timing side-channel to count hosts



Co-residence Testing

- Place prober on same host as victim
  - Check if TTL scan to victim is 0
  - Check patterns to prober via interrupt-based side-channel
- If both pass – attacker is co-resident with victim



SBA Research

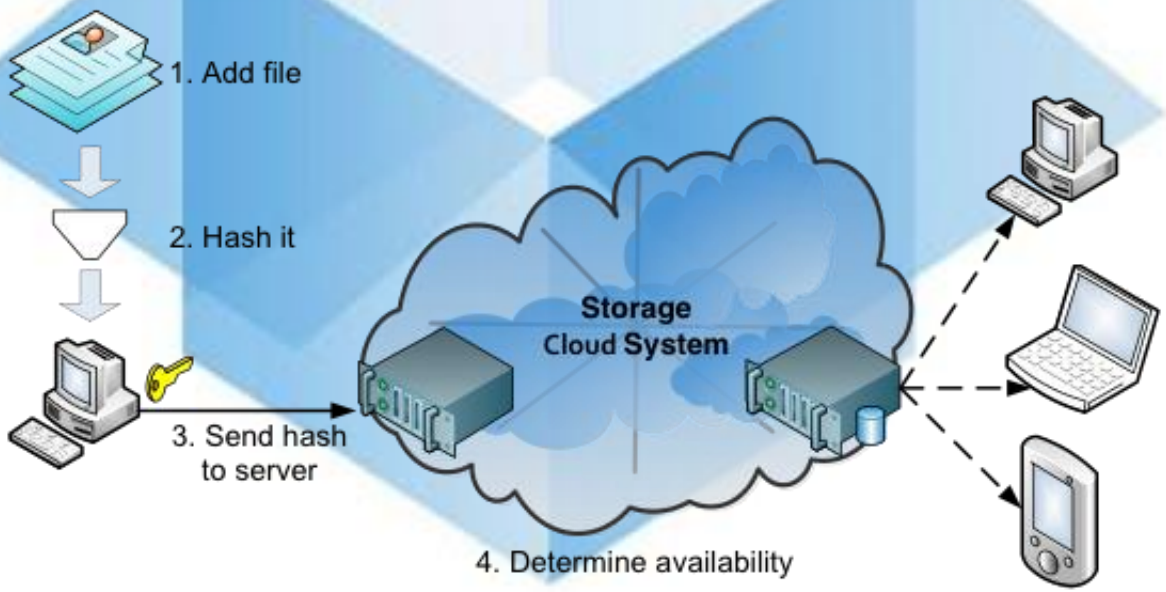
Data Deduplication

At the server

- Same file only stored once
- Save storage space at server

At the client

- Calculate hash or other digest
- Reduce communication



SBA Research

Authentication

SBA Research

Re-Evaluation 2014

Application	Account Hijacking	Unrequested SMS	Enumeration	Other Vulnerabilities
eBuddy XMS	yes (no)	yes	yes	no
EasyTalk	yes* (yes)	yes	yes	no
Forfone	yes (no)	yes	yes	no (yes)
HeyTell	yes	no	limited	no
Tango	yes	yes	yes	no (yes)
Viber	no	yes	yes	no
WhatsApp	no (yes)	yes	yes	no (yes)
WowTalk	yes	yes	yes	no (yes)
fring	no	yes	yes	no
GupShup	no	yes	yes	no
hike	no	yes	yes	no
JaxtrSMS	no*	yes	no	no
KakaoTalk	no	yes	yes	no
Line	no	yes	limited	no
Samsung ChatOn	no	yes	yes	yes
textPlus	no	yes	yes	no
WeChat	no*	yes	limited	no

SBA Research

Empirical Research

Dropbox

Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, and Edgar R. Weippl. **Dark clouds on the horizon**: Using cloud storage as attack vector and online slack space. USENIX Security, 8/2011.

WhatsApp

Sebastian Schrittwieser, Peter Fruehwirt, Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Markus Huber, and Edgar R. Weippl**. Guess who is texting you?** evaluating the security of smartphone messaging applications. In Network and Distributed System Security Symposium (NDSS 2012), Feb 2012.

Facebook

Markus Huber, Sebastian Schrittwieser, Martin Mulazzani, and Edgar Weippl**. Appinspect: Large-scale evaluation of social networking apps**. In ACM Conference on Online Social Networks (COSN), 2013.

Amazon

Amir Herzberg and Haya Shulman and Johanna Ullrich and Edgar R. Weippl, **Cloudoscopy: Services Discovery and Topology Mapping**, in Proceedings of the ACM Cloud Computing Security Workshop (CCSW) at ACM CCS 2013, 2013.

Tor

Philipp Winter and Richard Koewer and Martin Mulazzani and Markus Huber and Sebastian Schrittwieser and Stefan Lindskog and Edgar R. Weippl, **Spoiled Onions: Exposing Malicious Tor Exit Relays,** in Proceedings of the 14th Privacy Enhancing Technologies Symposium, 2014

GSM

Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar R. Weippl, **IMSI-Catch Me If You Can: IMSI-Catcher-Catchers** in Proceedings of ACSAC, 2014

SBA Research

Take Aways

- Implement or improve monitoring
  - Typical rates of queries
  - Amount of storage allocated
  - Reuse statistics for data duplications
  - …
- Analyze attack surface
- Active probing
  - Bad node behavior
  - …

SBA Research

Architectures

	Centralized	Distributed
Historic	**Mainframe** • Admins understand systems and can observe everything • Server-based security	**Client-Server** • Admins understand systems and can observe servers and communication • Decentral / private data
Hype	**Cloud Computing** • Internals hidden / protected • Arms race in analysis	**P2P / Grassroots Infrastructure** • Trust in majority • Sybil attack

SBA Research

eweippl@sba-research.org