

TeleTrust-interner Workshop

Berlin, 26. - 27.06.2024

"Kryptoagilität"

Dr. Tobias Fehenberger, Adva Network Security, Leiter der
TeleTrust-AG "Kryptoagilität"

Kryptoagilität

Langfristige Sicherheit von IT-Systemen

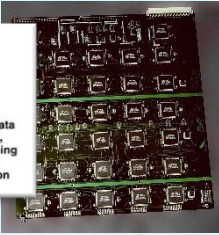


Angriffe auf Kryptografie

Brute-force

1998: Deep Crack
breaks DES

National Institute of Standards and
Technology
[Docket No. 040602169-5002-02]
Announcing Approval of the
Withdrawal of Federal Information
Processing Standard (FIPS) 46-3, Data
Encryption Standard (DES); FIPS 74,
Guidelines for Implementing and Using
the NBS Data Encryption Standard;
and FIPS 81, DES Modes of Operation



Mathematische Angriffe

An efficient key recovery attack on SIDH

Wouter Castryck^{1,2} and Thomas Decru¹

¹ imec-COSIC, KU Leuven, Belgium

² Vakgroep Wiskunde: Algebra en Meetkunde, Universiteit Gent, Belgium

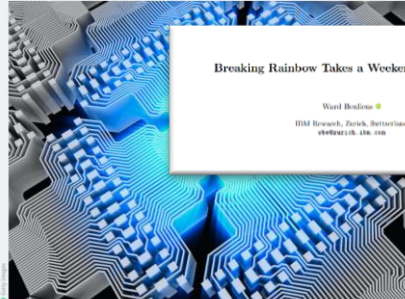
ars TECHNICA

CONTENDER BEING A CONTENDER

Post-quantum encryption contender is taken
out by single-core PC and 1 hour

Leave it to mathematicians to muck up what looked like an impressive new algorithm.

DAN GOODEN - 10/2/2022, 2:31 PM



Breaking Rainbow Takes a Weekend on a Laptop

Ward Beulens
IBM Research, Zurich, Switzerland
beulens@zurich.ibm.com

2022

Source: arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/

Implementierung 2017

The Return of Coppersmith's Attack:
Practical Factorization of Widely Used RSA Moduli*

Matus Nemecek
Masaryk University,
Czech Republic
nemecek@math.muni.cz

Marek Sys[†]
Masaryk University
sys@fi.muni.cz

Petr Svenda
Masaryk University
svenda@fi.muni.cz

Dusan Klinec
EnigmaBridge, Masaryk University
dusan@enigma-bridge.com

Vashek Matyas
Masaryk University
matyas@fi.muni.cz

2017



2016

CacheBleed: A Timing Attack on OpenSSL Constant
Time RSA

Konfiguration / Patching 2024

Important Security
Update - Stay
Protected Against
VPN Information
Disclosure (CVE-2024-
24919)



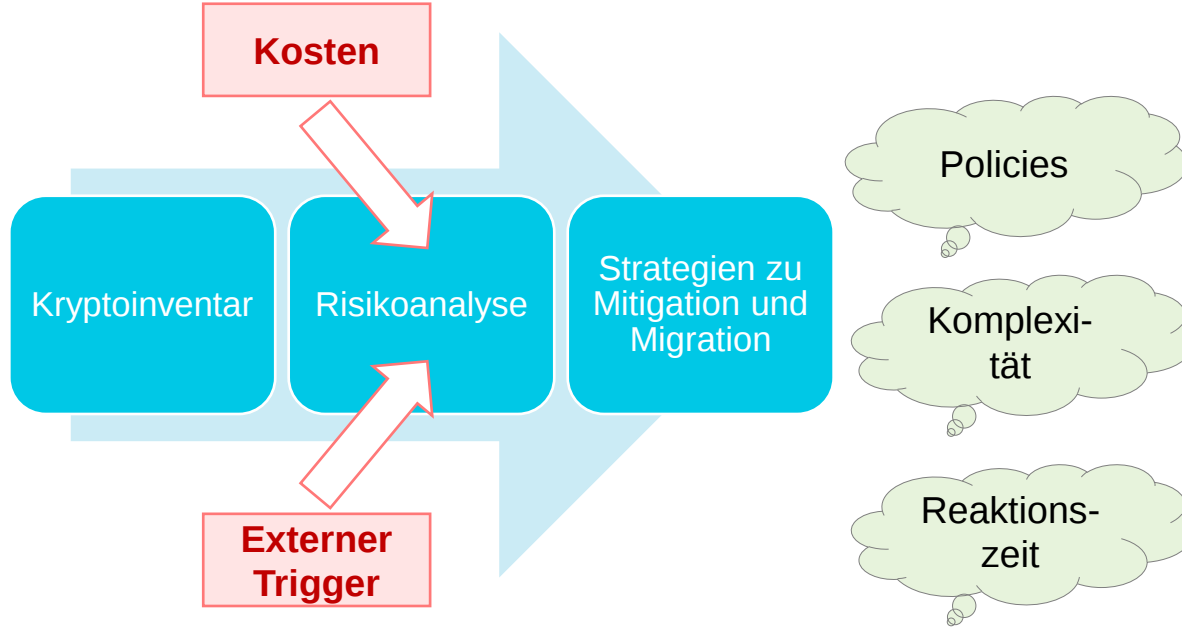
Kryptografie ist allgegenwärtig – und wird ständig gebrochen

Definition Kryptoagilität

Kryptoagilität beschreibt einen unternehmensweiten Prozess bei Herstellern und Anwendern von IT-Systemen, bei dem als Reaktion auf externe Einflüsse sicherheitsrelevante Bestandteile eines IT-Systems ausgetauscht werden, ohne dass Kernfunktionalitäten beeinträchtigt werden.

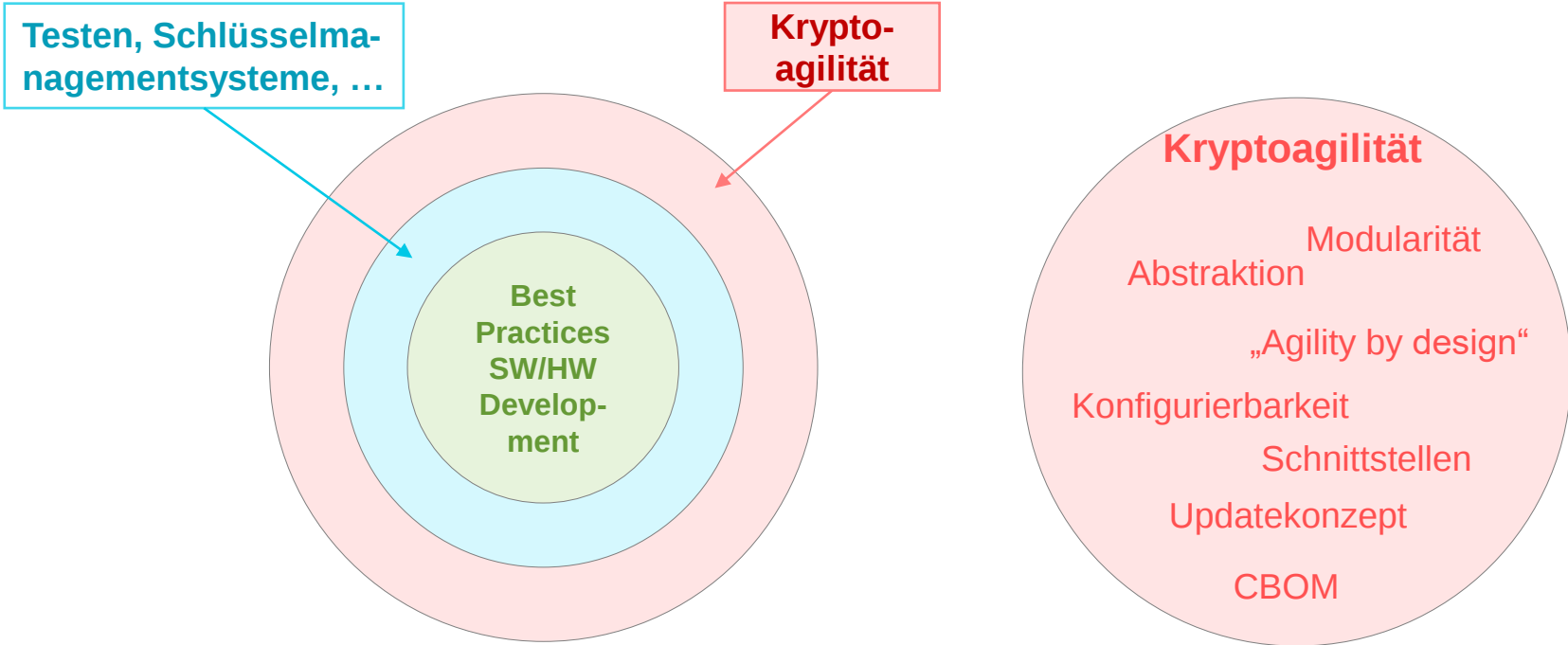
Viel mehr als ein Software-Update!

Vorbereitende Maßnahmen



Prozessdenken ist entscheidend für Kryptoagilität

Technische Umsetzung [Hersteller]



Komplexe Design- und Entwicklungsvorgaben für Hersteller

**Danke an die
AG Kryptoagilität**

tobias.fehenberger@advasecurity.com

