Computersystemsicherheit

Prof. Marc Fischlin, Wintersemester 18/19

08
Zusammenfassung

Rückblick: „Erwartete“ Themen

Zertifikate +Signaturen
✓ 03

vernetzte Systeme
✓ 05

Bedrohungsanalyse
Angriffszenarien Schutzziele
Schutzmechanismen
(✓ 01-07)

DDoS
✓ 05

Spectre
✓ 06

Bluetooth

Kryptographie
✓ 02+03

Datenschutz

Passwörter
✓ 04

Sicherheitslücken
(✓ 01-07)

Betriebssystemsicherheitsschichten/
Containersysteme
(✓ 06)

SQL-Injection
✓ 07

Buffer Overflows
✓ 06

Exploits
(✓ 01-07)

Mindesanforderung/
Rechtslage

„Konvention“

Authentifizierung
✓ 04

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Übersicht

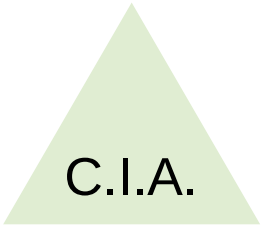
TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

01 Einleitung

„Komplexität ist der (erste) Feind der Sicherheit.“

„Sicherheit selbst ist komplex.“

Confidentiality



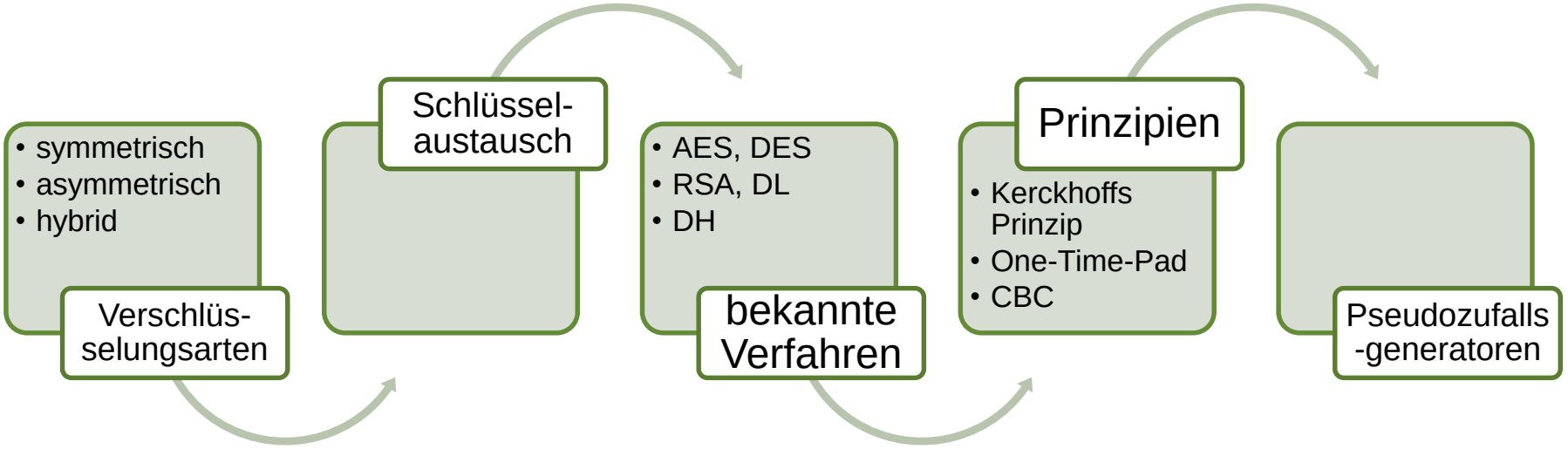
Integrity

Availability

Threats
Vulnerabilities
Consequences
Exploit
Countermeasures

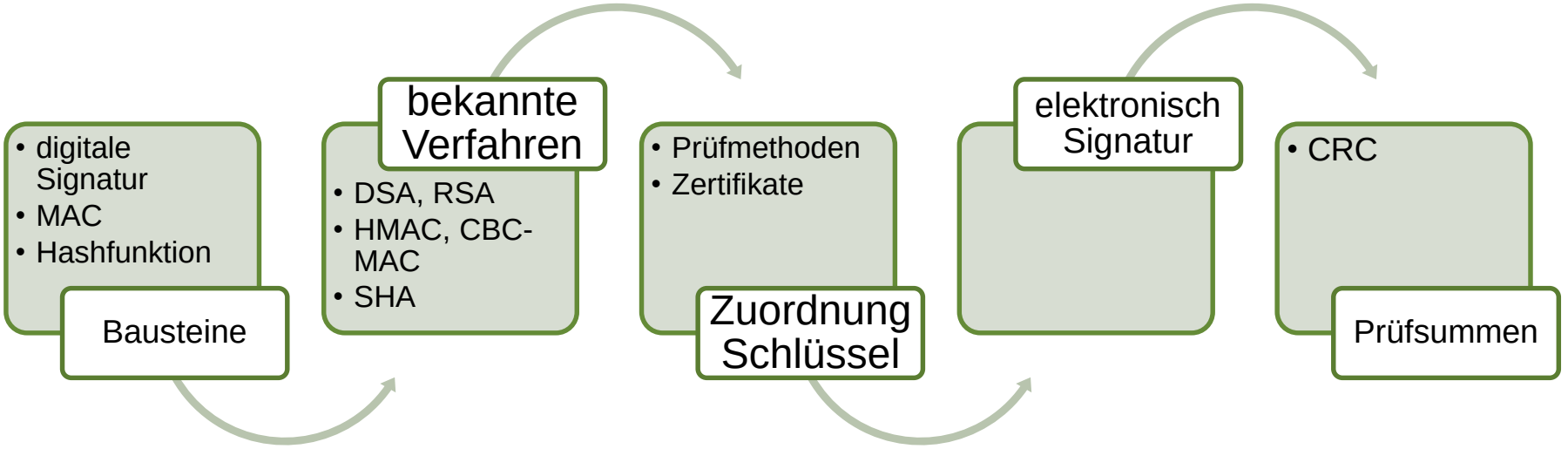
TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

01 Einleitung



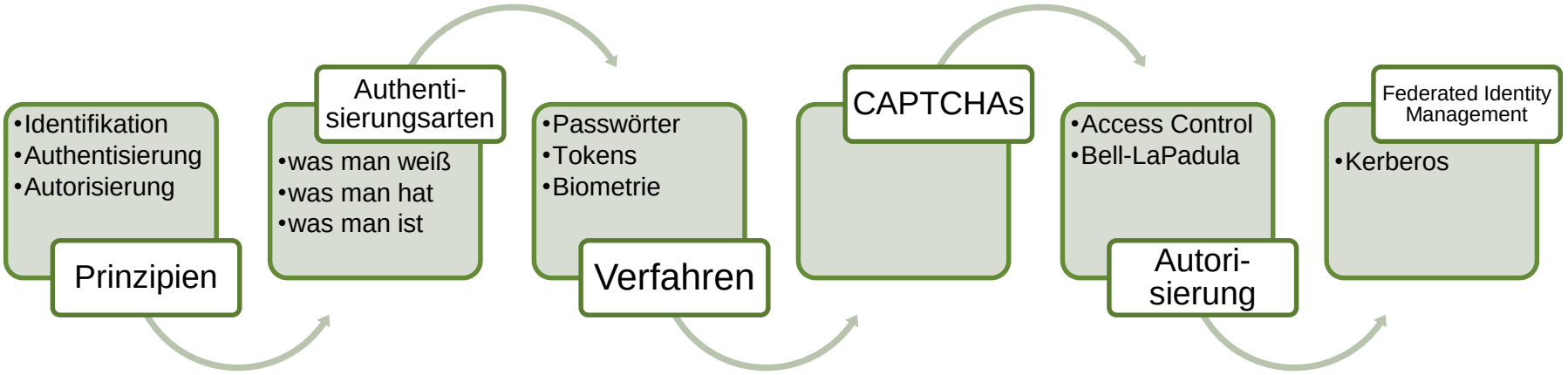
TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

03 Digitale Signaturen



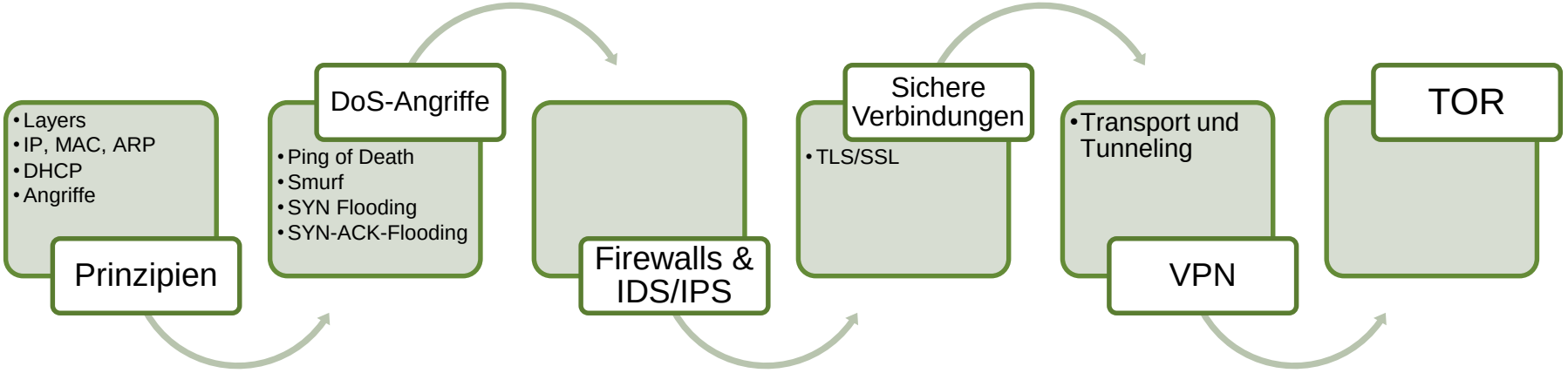
TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

04 Authentisierung und Autorisierung



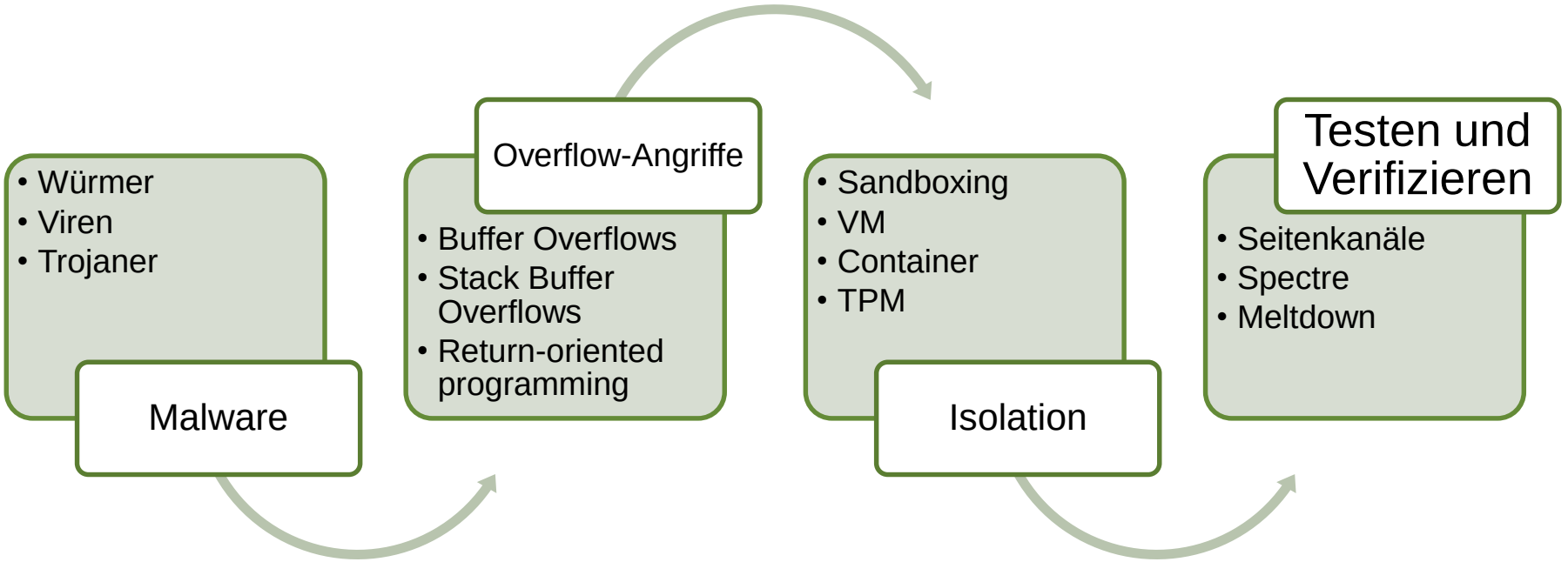
TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

05 Netzwerksicherheit

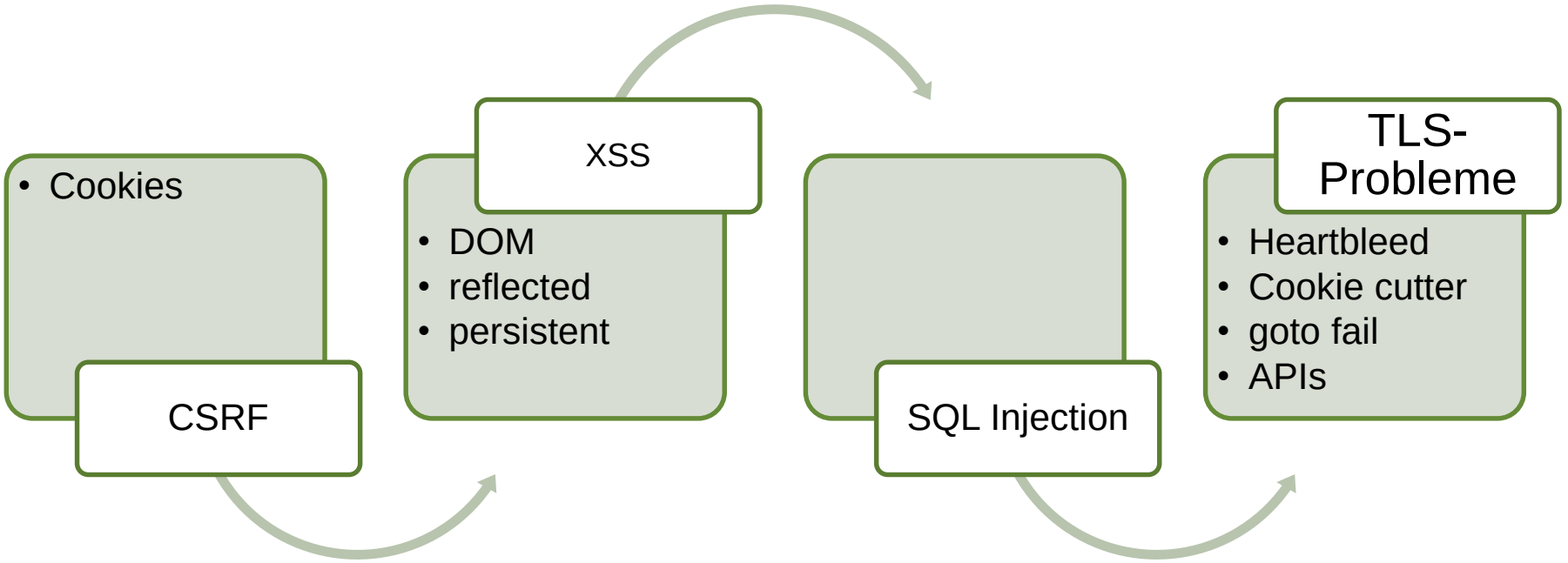


TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

06 Betriebssystem-Sicherheit



07 Web-Sicherheit



Weitere Themen

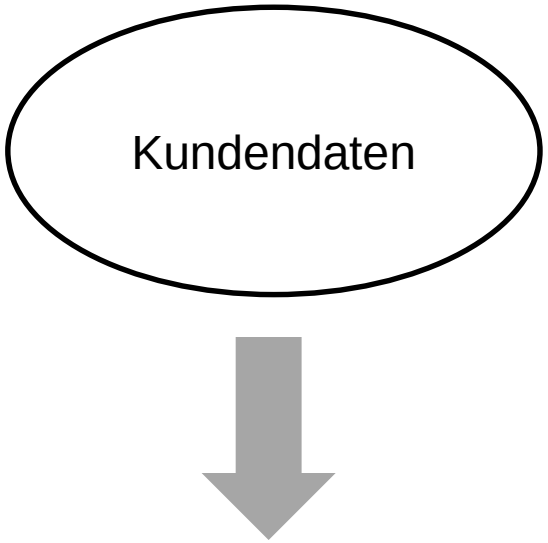
TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Abdeckung weiterer Themenbereiche

	02 Verschlüs-selung	03 Signaturen	04 Auth+Aut	05 Netzwerke	06 Betriebs-systeme	07 Web
Privacy & Anonymität		Abstreit-barkeit		TOR		
Usability			Passwörter Phishing		Malware Buffer Overflows	TLS-API
Availability		Prüfsummen	CAPTCHAs	(D)DoS		

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Weiterführendes Beispiel für Privacy: Datenanalysen



extrahiere Information
wie durchschnittliche Ausgaben,
ohne Privacy des jeweiligen
Kunden zu verletzen

COMPUTERWOCHE VON IDG

IBM EXPERTS UPDATE YOUR BUSINESS

Was ist Differential Privacy?

Apple und die Sache mit den Daten

29.07.2016 Von Axel Oppermann (Experte) IDG EXPERTEN NETZWERK

Apple hat angekündigt Differential Privacy für die Analyse der Kundendaten zu nutzen. Fährt Apple mit dieser Strategie besser als Google, Microsoft, Facebook & Co.?

www.computerwoche.de, 29.Juli 2016

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity

Differential Privacy

Beispiel:
bestimme durchschnittliche Größe

Name	Größe
Alice	185 cm
Bob	169 cm
Carrol	176 cm
…	…

Datenbank DB
Datenbank DB* = entferne einen Eintrag

Prinzip der Differential Privacy:

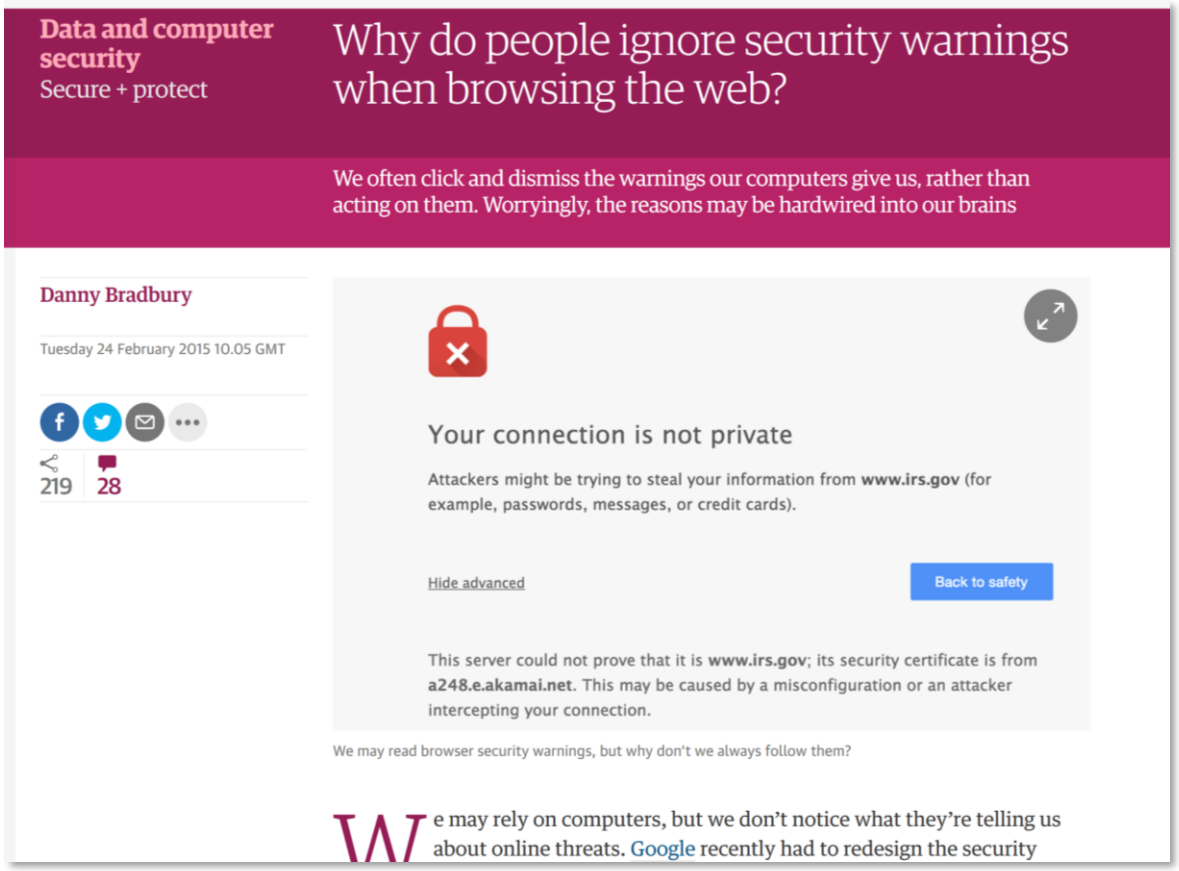
Verrausche Antwort,
so dass individueller Eintrag quasi keinen Einfluss mehr hat

Datenbank-Algorithmus Algo is differentially private,
wenn für alle DB*=DB \ {Element} gilt:

$$\Pr[\text{Algo}(DB) \text{ liefert Antwort } a] \approx \Pr[\text{Algo}(DB^*) \text{ liefert Antwort } a]$$

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Weiterführendes Beispiel für Usability



Data and computer security
Secure + protect

Why do people ignore security warnings when browsing the web?

We often click and dismiss the warnings our computers give us, rather than acting on them. Worryingly, the reasons may be hardwired into our brains

Danny Bradbury

Tuesday 24 February 2015 10.05 GMT

219 28

Your connection is not private

Attackers might be trying to steal your information from **www.irs.gov** (for example, passwords, messages, or credit cards).

Hide advanced

Back to safety

This server could not prove that it is **www.irs.gov**; its security certificate is from **a248.e.akamai.net**. This may be caused by a misconfiguration or an attacker intercepting your connection.

We may read browser security warnings, but why don't we always follow them?

We may rely on computers, but we don't notice what they're telling us about online threats. Google recently had to redesign the security

`www.theguardian.com`, 25.Februar 2015

Warum reagieren Anwender falsch auf Warnungen?

Warum entwickeln Programmierer unsichere Lösungen?

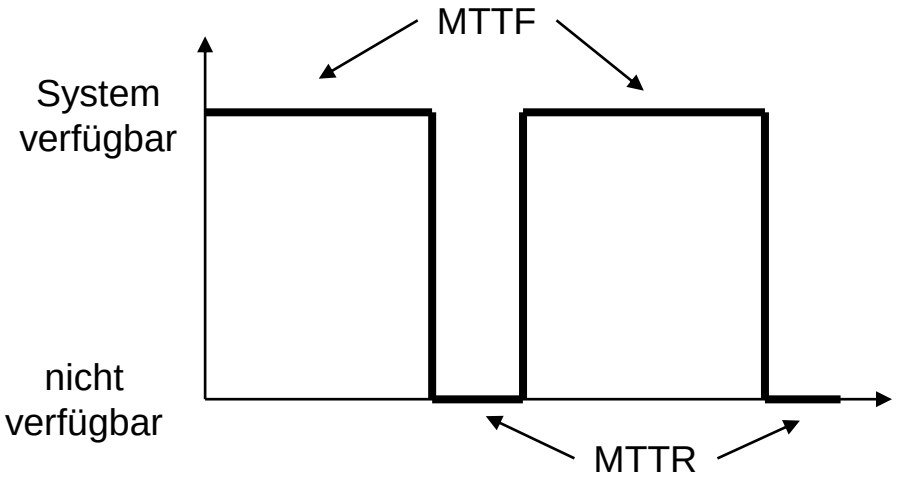
…

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Weiterführendes Beispiel für Availability

Availability

Verfügbarkeit des Systems
(in Prozent der Laufzeit)



MTTF = Mean Time To Failure
MTTR = Mean Time To Recovery
Availability = MTTF / (MTTF + MTTR)

Reliability

Zuverlässigkeit des Systems
(Wahrscheinlichkeit, dass
das System funktioniert)

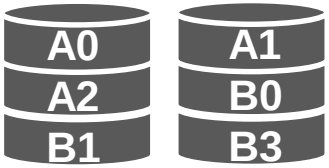
Beispiel: Redundanz
(siehe nächste Folie)

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Reliability

Beispiel: Redundant Arrays of Independent Disks (RAID)

RAID 0 (Stripping)



„Reißverschluss“

halbiert Geschwindkeit (parallel)

RAID 1

„Duplizieren“

verdoppelt Speicherbedarf

RAID 5

„Verteilen und Paritätsbits“

leicht erhöhter Speicherbedarf, verbessert Geschwindigkeit

	RAID 0	RAID 1	RAID 5
Ausfallwskeit	$1-(1-p)^2$	p^2	$1-[4p(1-p)^3+(1-p)^4]$
Beispiel p=1%	1,99%	0,01%	0,059%

p = (unabhängige) Ausfallwahrscheinlichkeit einer Platte

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Ende der Vorlesung

TECHNISCHE UNIVERSITÄT DARMSTADT
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de