Developers are not the Enemy!

Karoline Busse

Usable Security and Privacy Lab, Universität Bonn

@kb_usec

Outline

- Chapter 1: Usable Security
  - From end-users to developers

- Chapter 2: Developers are not the Enemy
  - Password Security

- Chapter 3: The way forward
  - Studies, Usability & AI

Chapter 1

Usable Security & Privacy

Usable Security?

Usability + Security

Origins of Usable Security & Privacy

- Usable Security is to Security as Behavioural Economics is to Economics
  - User studies to asses problems / understand human factor
  - User studies to evaluate solutions

- The goal is to make security more user friendly
  - Enabling instead of restricting

- Founded in the late 90’s
  - “Users are not the Enemy” Adams and Sasse’99

Passwords

Password Advice

- Passwords are still a mainstay of modern security
  - and a very common cause of security problems
- Common password advice
  - make it long and random
  - use special characters
  - don’t write it down
  - change it often
  - don’t re-use across services

good technical advice

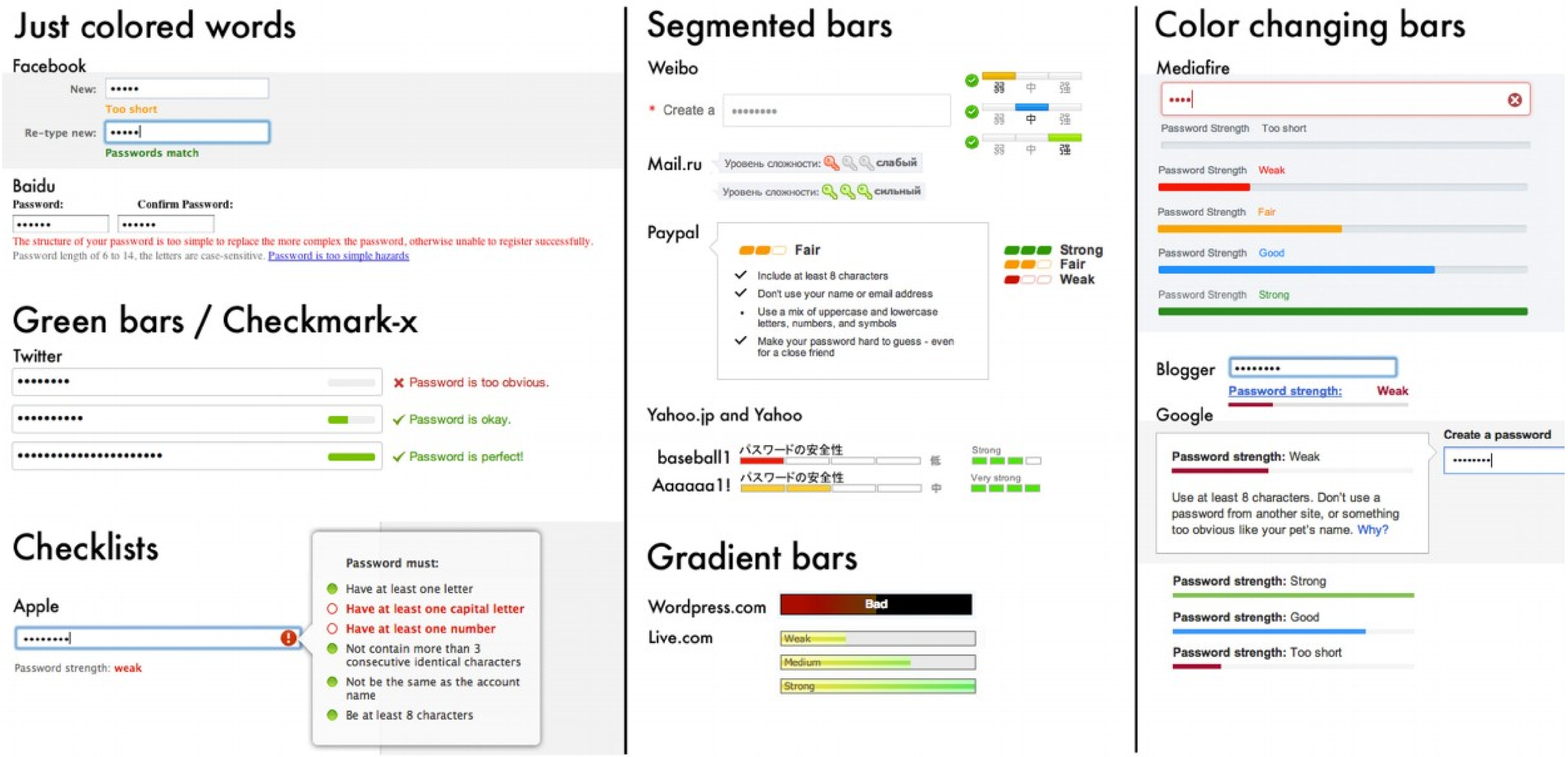
bad usability advice

- Password problems lead to
  - lost productivity
  - recovery cost
  - frustrated users who try and circumvent system

Top 10 Passwords 2018

Rank	Password	Change from 2017
1	123456	Unchanged
2	password	Unchanged
3	123456789	Up 3
4	12345678	Down 1
5	12345	Unchanged
6	111111	New
7	1234567	Up 1
8	sunshine	New
9	qwerty	Down 5
10	iloveyou	Unchanged

Password Meters



Just colored words

Facebook

New: •••••
Too short
Re-type new: •••••
Passwords match

Baidu

Password: •••••• Confirm Password: ••••••
The structure of your password is too simple to replace the more complex the password, otherwise unable to register successfully.
Password length of 6 to 14, the letters are case-sensitive. Password is too simple hazards

Green bars / Checkmark-x

Twitter

•••••••• ✗ Password is too obvious.
•••••••••• ✓ Password is okay.
•••••••••••••••••••••• ✓ Password is perfect!

Checklists

Apple

••••••••
Password strength: weak

Password must:
- ● Have at least one letter
- ○ Have at least one capital letter
- ○ Have at least one number
- ● Not contain more than 3 consecutive identical characters
- ● Not be the same as the account name
- ● Be at least 8 characters

Segmented bars

Weibo

* Create a ••••••••

弱 中 强
弱 中 强
弱 中 强

Mail.ru

Уровень сложности: слабый
Уровень сложности: сильный

Paypal

Fair
- ✓ Include at least 8 characters
- ✓ Don't use your name or email address
- • Use a mix of uppercase and lowercase letters, numbers, and symbols
- ✓ Make your password hard to guess - even for a close friend

Strong
Fair
Weak

Yahoo.jp and Yahoo

baseball1 パスワードの安全性 低 Strong
Aaaaaa1! パスワードの安全性 中 Very strong

Gradient bars

Wordpress.com Bad

Live.com Weak
Medium
Strong

Color changing bars

Mediafire

••••
Password Strength Too short
Password Strength Weak
Password Strength Fair
Password Strength Good
Password Strength Strong

Blogger

••••••••
Password strength: Weak

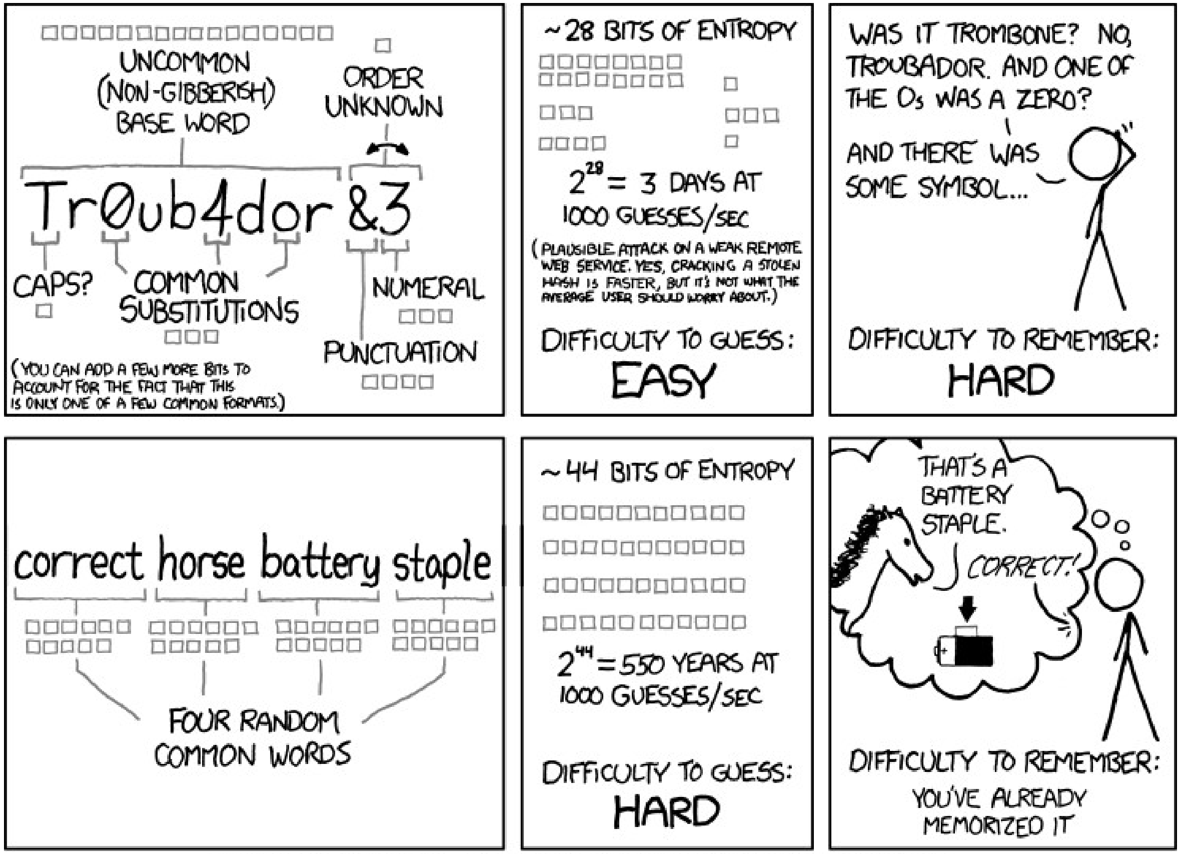
Google

Create a password
••••••••
Password strength: Weak
Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?

Password strength: Strong
Password strength: Good
Password strength: Too short

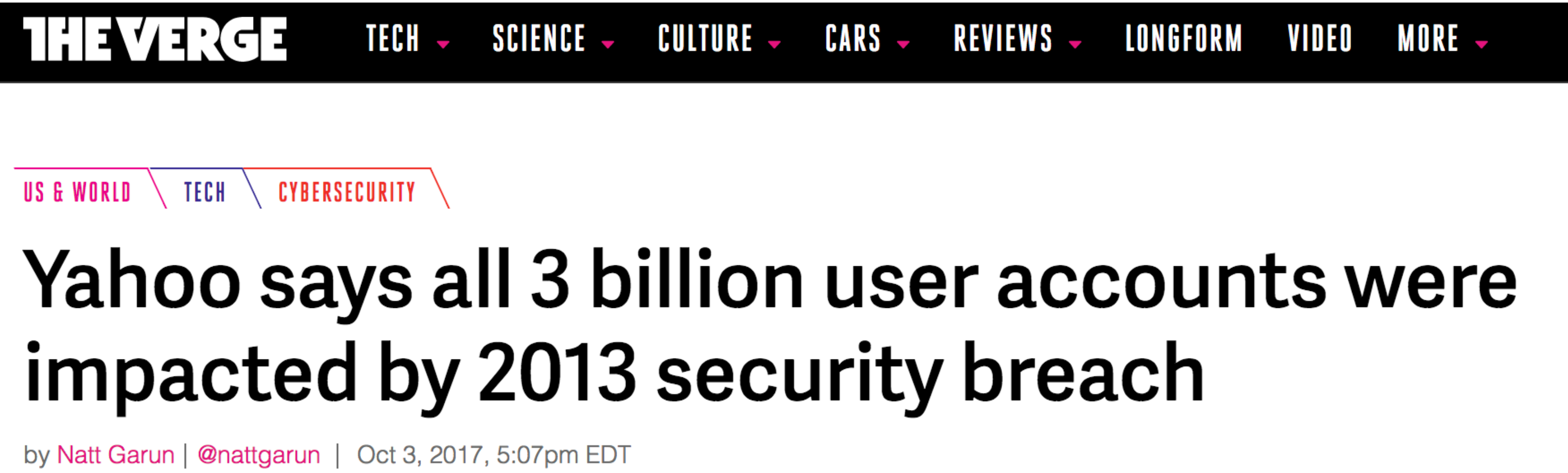
Ur et al. How Does Your Password Measure Up?
The Effect of Strength Meters on Password Creation, USENIX Security'12

Passphrases


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

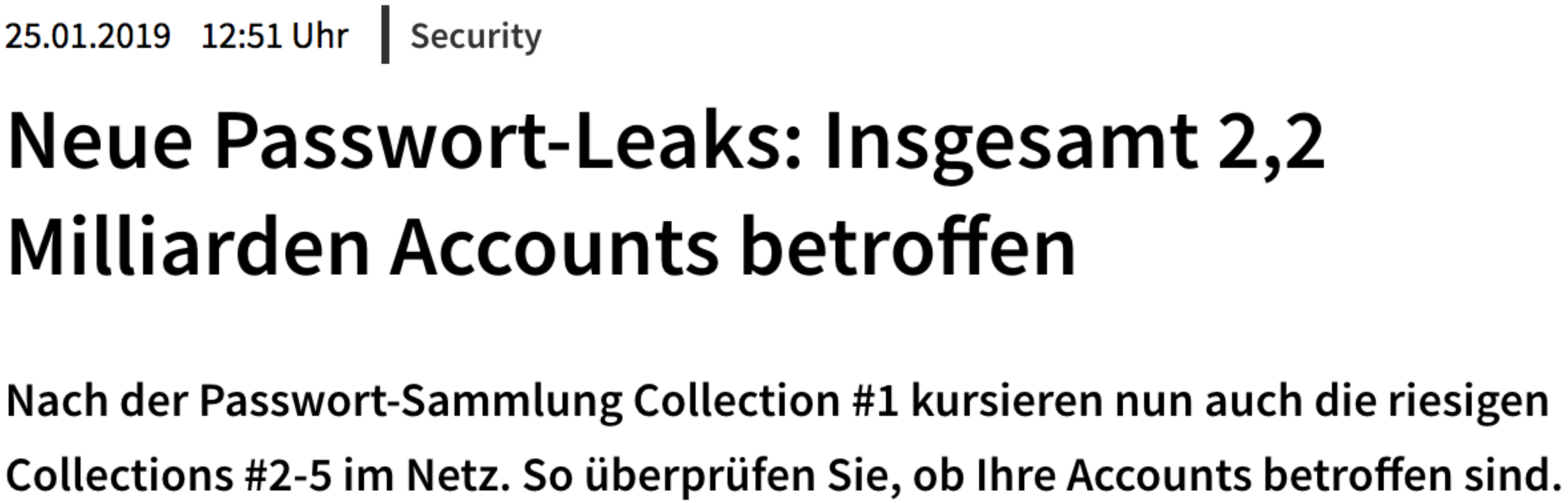
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Shay et al. Correct horse battery staple: Exploring the usability of system-assigned passphrases, SOUPS‘12



Yahoo says all 3 billion user accounts were impacted by 2013 security breach

by Natt Garun | @nattgarun | Oct 3, 2017, 5:07pm EDT

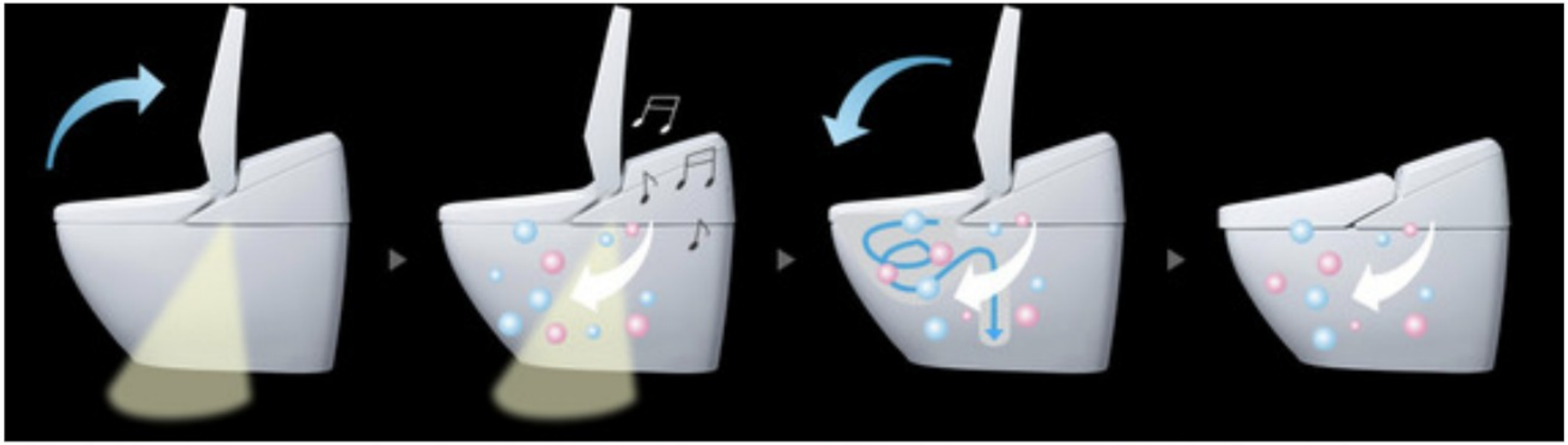

25.01.2019 12:51 Uhr | Security

Neue Passwort-Leaks: Insgesamt 2,2 Milliarden Accounts betroffen

Nach der Passwort-Sammlung Collection #1 kursieren nun auch die riesigen Collections #2-5 im Netz. So überprüfen Sie, ob Ihre Accounts betroffen sind.

Internet of (broken) Things

- Internet of broken Things
  - Satis IoT bidet by LAXIL
  - Connects to your smartphone
  - Hardcoded Bluetooth password 0000



This bidet plays music, deodorizes, relaxes, and IT CAN BE HACKED. (LAXIL)

Source: The Atlantic

Frontiers of Usable Security

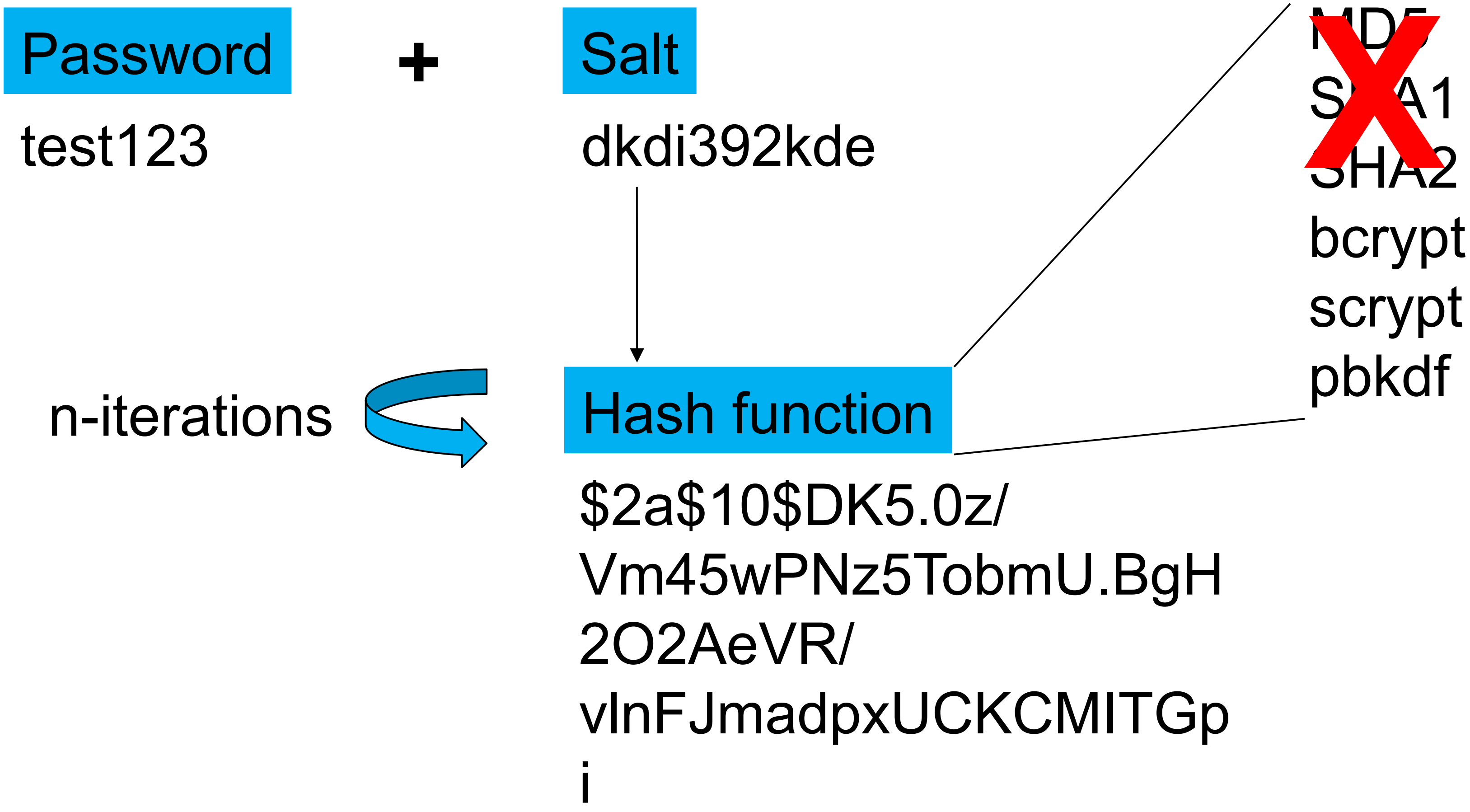
- End-users are only a small part of the password ecosystem
- Administrators are responsible for (terrible) password policies
- Developers are responsible for storing passwords (insecurely)
- Alternative authentication systems might make things better – they might also make them worse...

Chapter 2

Developers are not the enemy!

Smith & Green IEEE S&P Magazin'16

How to store a password



Password

test123

+

Salt

dkdi392kde

n-iterations

Hash function

~~MD5~~

~~SHA1~~

~~SHA2~~

bcrypt

scrypt

pbkdf

$2a$10$DK5.0z/Vm45wPNz5TobmU.BgH2O2AeVR/vlnFJmadpxUCKCMITGpi

Trust me! I know what I‘m doing!

Study Design

- **Laboratory Study**
  - one working day (8 hours)

- **Participants**
  - 40 Computer Science students from the University of Bonn

- **Role-playing scenario**
  - Social networking platform: code for user registration and user authentication

- **Meta-Study: Priming / Task Description**
  - Password Security vs. API Usability

- **Primary Study :Framework**
  - Plain Java vs Spring

Security Score 0-7

- The end-user password is **salted** *(+1)* and **hashed** *(+1)*.
- The **derived length of the hash** is **at least 160 bits** long *(+1)*.
- The **iteration count** for key stretching is
  - at least 1 000 *(+0.5)* or 10 000 *(+1)* for **PBKDF2** and
  - at least 2^{10} = 1 024 for **bcrypt** *(+1)*.
- A **memory-hard hashing function** is used *(+1)*.
- The **salt** value is generated **randomly** *(+1)*.
- The **salt** is **at least 32 bits** in length *(+1)*.

How many of the 20 non-primed participants stored the user passwords with any security?

o

How many of the 20 primed participants stored the user passwords with any security?

12/20

Comparing JSF to Spring

Looking only at those who implemented some security:

- Java Score
  - Min 2, Median 5.5, Mean 4.3, and Max 6.
- Spring Score
  - Min 6, Median 6, Mean 6, and Max 6.

- Mann-Whitney U = 15, *p* = 0.051, *cor*-*p* = 0.20
  - Bonferroni-Holm correction with family = 6

It’s time to talk about ditching statistical significance,
Nature Editorial 567, 283 (2019)
Moving to a World Beyond “p < 0.05”
Wasserstein et al. American Statistical Association (2019)

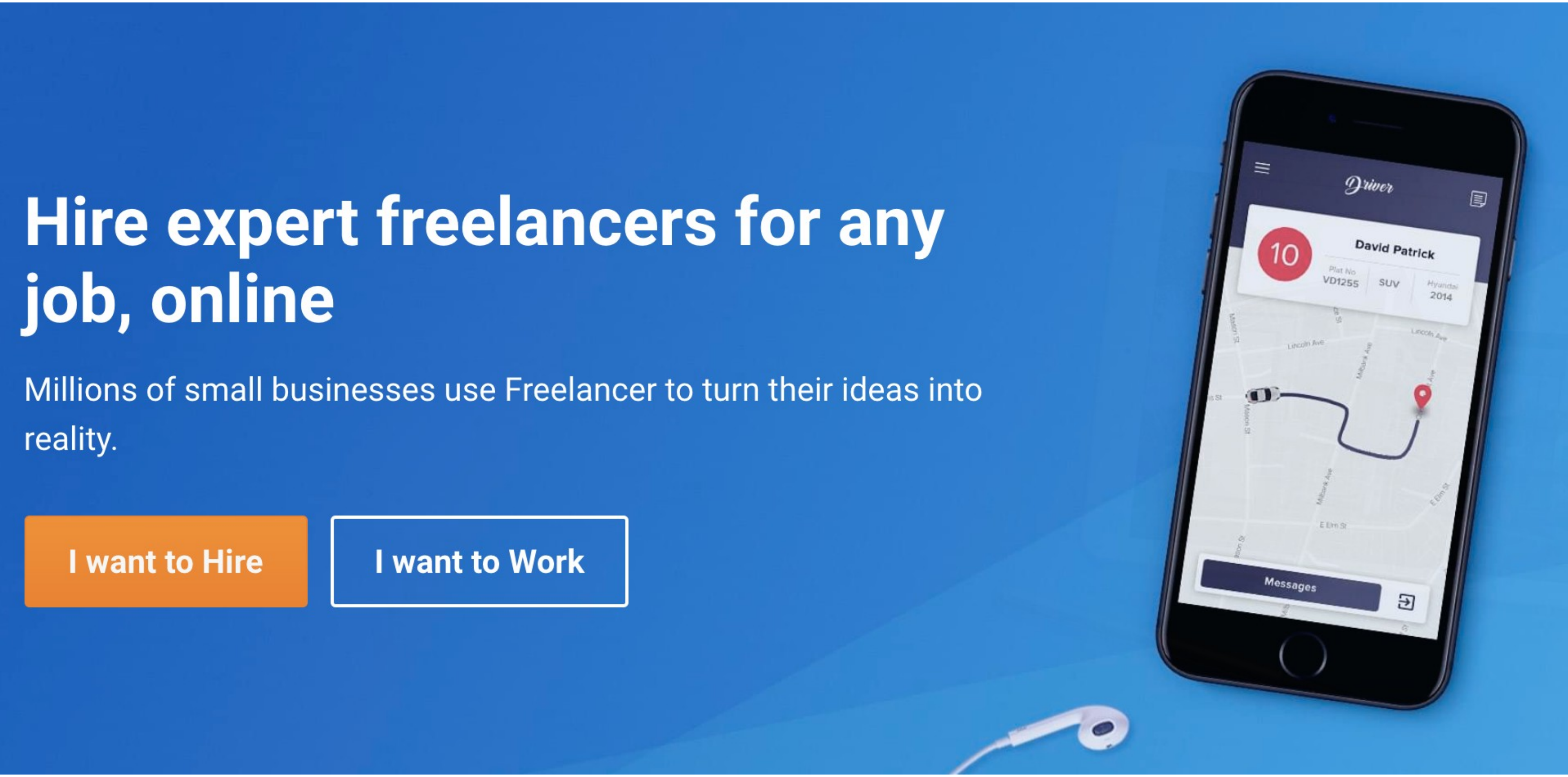
Study bias?

“

It depends on the company.

If it had been a security company I would have thought of something because they would have minded.

Hire some real developers (like Boeing)



Hire expert freelancers for any job, online

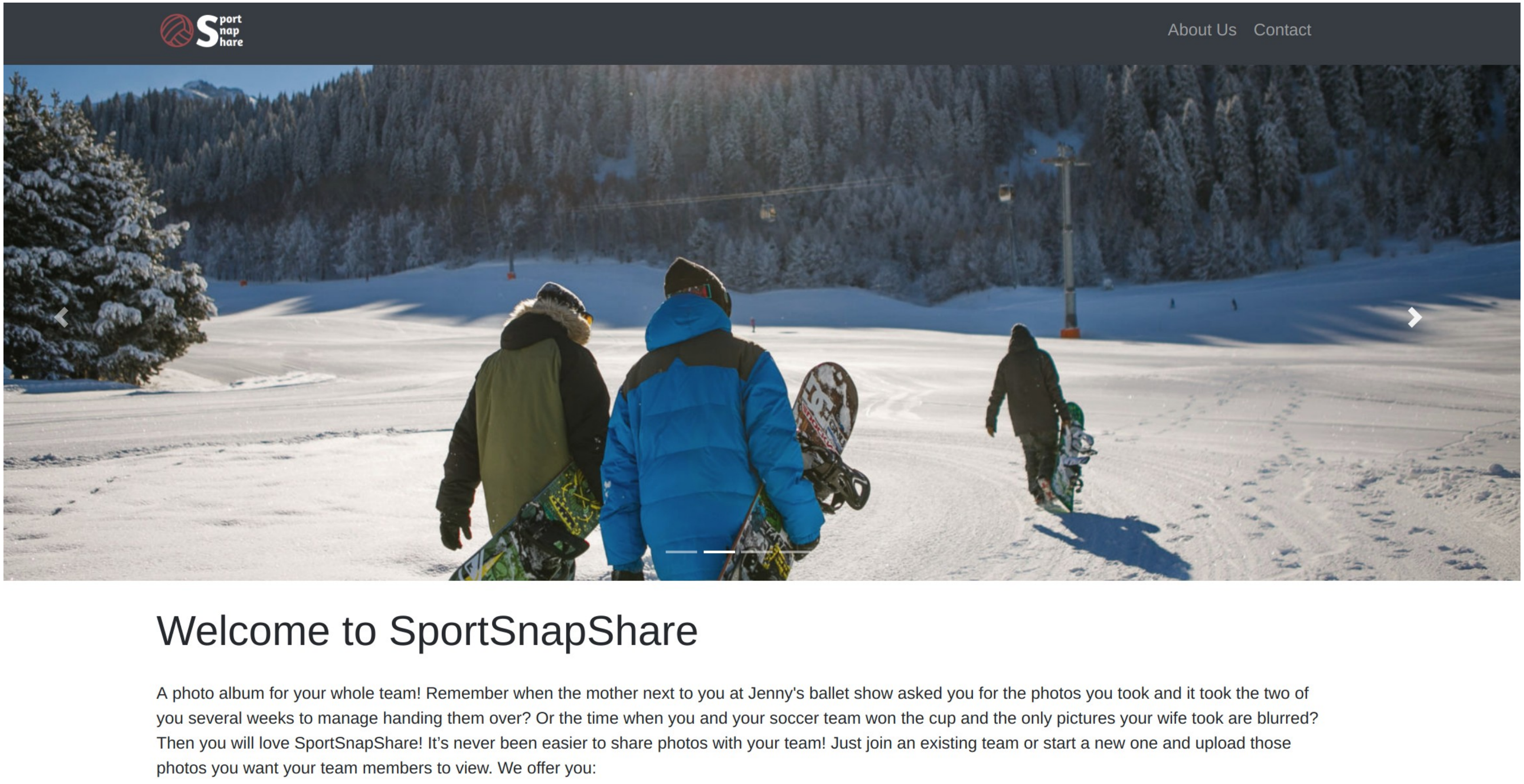
Millions of small businesses use Freelancer to turn their ideas into reality.

I want to Hire

I want to Work

freelancer.com

Fake Start-up



Welcome to SportSnapShare

A photo album for your whole team! Remember when the mother next to you at Jenny's ballet show asked you for the photos you took and it took the two of you several weeks to manage handing them over? Or the time when you and your soccer team won the cup and the only pictures your wife took are blurred? Then you will love SportSnapShare! It’s never been easier to share photos with your team! Just join an existing team or start a new one and upload those photos you want your team members to view. We offer you:

Participants

- **42 freelancers**
  - 29 freelancing main profession

- **30 years old (sd = 7.6), 39 male**

- **14 India, 8 China**
  - 4 Pakistan, 3 USA, 3 Egypt, others (≤2)

- **Programming: 8 years (sd = 3.6)**
  - Java: 6.4 years (sd = 2.6)

How many of the 21 non-primed participants stored the user passwords with any security?

(Reminder: students 0 / 20)

4/21

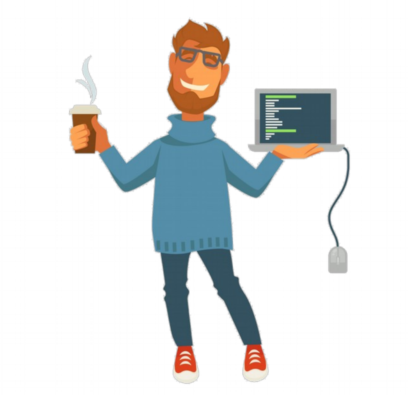
How many of the 21 primed participants stored the user passwords with any security?

(Reminder: students 12 / 20)

13/21

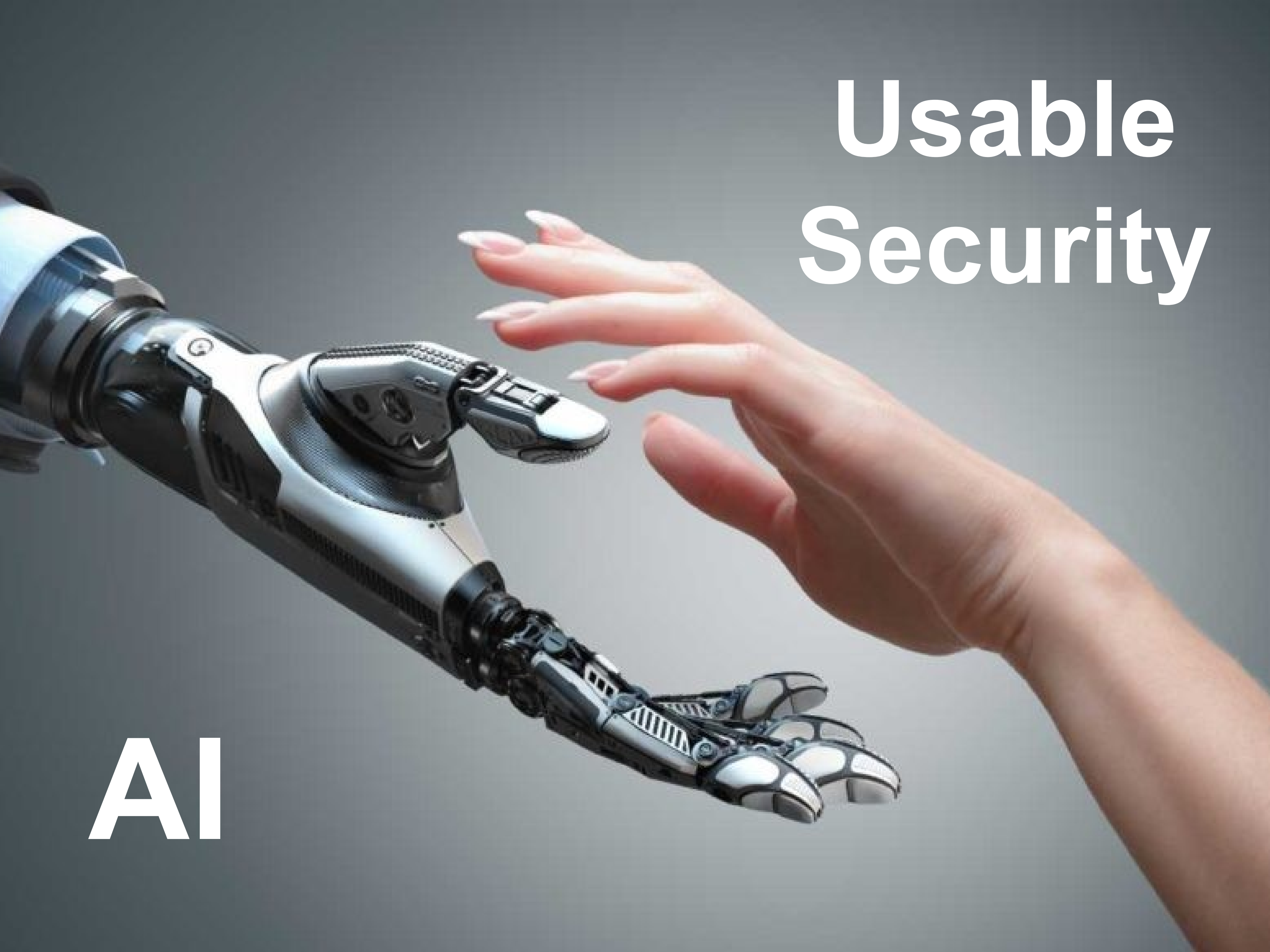
Security score comparison

100 €



200 €

Mean	Students	Freelance 100€	Freelance 200€
all	2.15	1.89	2.4
did something	4.3	2.1	2.9



Usable Security

AI

Bugs that shook the world

Scope of the problem

A single line of code can compromise the entire system

- *systemd* is a system and service manager for Linux
  - 1.2 million lines of code
- Debian SID
  - 1.5 billion lines of code

What can we do about it?

- Education?
  - Does not scale
  - Does not age well
  - Teach the impossible?
  - Method of last resort
- We need to understand the problem
  - Large scale analysis
  - Empirical studies
- Smarter & Human Centric Development & Testing
  - AI/usability assisted software development
  - AI/usability assisted usable Software Testing

Questions?

Contact:

Karoline Busse
Usable Security and Privacy Lab
University of Bonn
busse@cs.uni-bonn.de
@kb_usec