



Keynote: Ihr Passwort, bitte!

Abendseminar «Innovative Alternativen zum Passwort»
26.10.2010, Hotel Novotel, Zürich

Dr. Thomas Dübendorfer

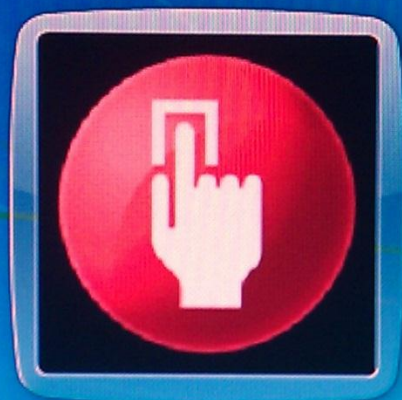
Präsident, Information Security Society Switzerland (ISSS)



thomas

Locked





Please scan your finger.

Computer is locked
Press ESC for the Welcome screen

Other Credentials

Passwörter im Web-Alltag

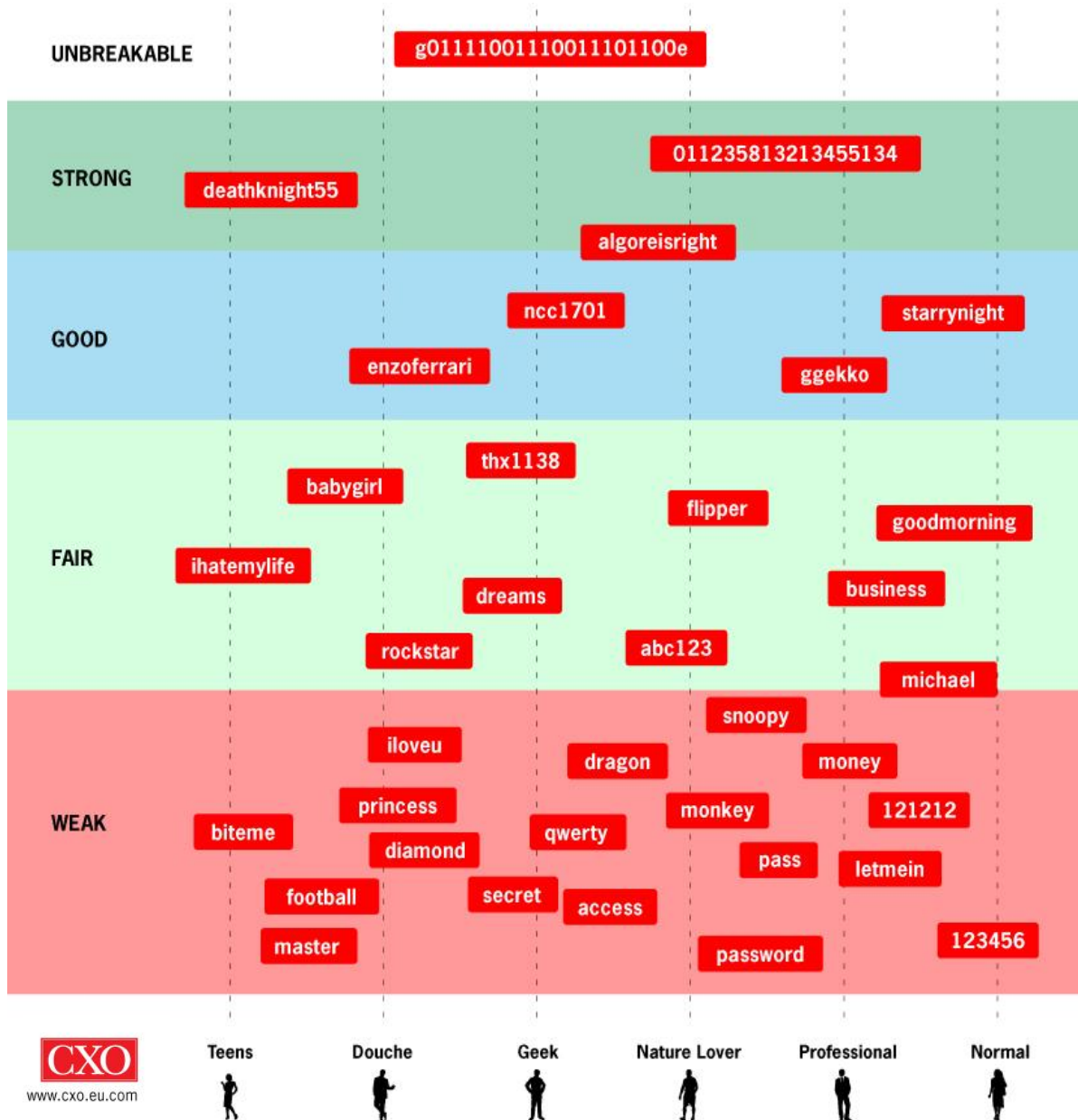
Ein Internetbenutzer

- tippt ca. 8 mal pro Tag ein Passwort ein
- hat ca. 25 Web-Accounts
- merkt sich ca. 6.5 verschiedene Passwörter
- **verwendet ein Passwort für ca. 3.9 Websites**

Referenz:

"A Large Scale Study of Web Passwords Habits", Dinei Florêncio, Cormac Herley, WWW '07





Password-Stärke

gemäss Gmail
 Passwortstärken-
 anzeige

Fallstudie: Passwörter auf RockYou.com

rockyou

The image shows a screenshot of the RockYou.com password creation interface. The form includes fields for 'New RockYou Password' (masked with dots), 'Retype Password', a checkbox for 'I agree to the Terms of Service', and a light blue box containing 'Year of Birth', 'Sex', 'Country' (set to 'None'), and 'Zip/Postal' fields. 'Submit' and 'Back' buttons are at the bottom. A red callout box with a white border contains the text: 'Create a Password Almost done! Password must be 5 to 15 characters long. No special characters (#, %, !, etc...).' A red arrow points from this box to the word 'bad' written in a red, outlined font below it.

Referenz: TechCrunch.com

<http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/>

Fallstudie: Passwörter auf RockYou.com

- Passwort per Klartext im Bestätigungsemail


Your Login Info for RockYou Inbox | X

☆ **RockYou** to nik [show details](#) 8:56 PM (0 minutes ago)

We have received your request for password recovery.
This login will allow you to log back into www.RockYou.com to access your slideshows.
login: nik@techcrunch.com
password: notmypassword

Use RockYou! to create cool slideshows that you can use anywhere.
Come back soon!

RockYou! Team
<http://www.rockyou.com/>



worse

Referenz: TechCrunch.com

<http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/>

Fallstudie: Passwörter auf RockYou.com

- RockYou speichert Passwörter anderer sozialer Netzwerke (im Klartext!)

The screenshot shows a sidebar on the left with social media icons for Email, Myspace, HI5, Friendster, Facebook, Tagged, and Orkut. The Orkut option is highlighted in orange. The main content area features a red-bordered box titled "Automatically post to your profile! (Free!)". Inside this box, there is a form labeled "Post to Orkut:" with two input fields: "Orkut email:" and "Orkut passw ord:". Below the fields is a "Post" button. A smaller red-bordered box below the main form contains the text "Login info will never be saved". Below the red-bordered box, there is a section titled "Copy this Code (just click on the textbox below and press Ctrl+C)" with a yellow background containing the following code: `<embed src="http://apps.rockyou.com/rockyou.swf?instanceid=155530233&ver=102906" quality="high" salign="lt" width="426" height="319" wmode="transparent" name="rockyou" />`. Below the code is a blue link: "Click here if you can't see the code."

Referenz: TechCrunch.com

<http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/>

Fallstudie: Passwörter auf RockYou.com

- Ein schwarzer Tag im Dezember 2009:
SQL Injection Hack auf RockYou.com
- **32 Millionen Accounts** mit Klartextpasswörtern von RockYou.com geklaut (inkl. gespeicherte Drittaccounts von MySpace, Orkut etc.).

Referenz: TechCrunch.com

<http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/>

qwerty

abc123

princess

12345

123456

Analyse der 32 Millionen Passwörter

- «123456» (1%) am häufigsten
- «12345» am zweithäufigsten
- «princess», «abc123» und «qwerty» in Top 20
- **20%** (=6.4 Millionen) der Passwörter waren aus einer Menge von nur 5000 leicht erratbaren Passwörtern
- Nur ca. **0,2%** (!) waren **verhältnismässig sicher** (Buchstaben in Gross-/Kleinschreibung, Zahlen und Sonderzeichen)

Referenz:

Amichai Shulman, CTO, Imperva, 2009

http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

Vorteile von Passwörtern

- Einfach zu verstehen
- Einfach zu erinnern (falls selbstgewählt)
- Nur System und Benutzer kennen das Passwort
- Einfach zu ändern
- Verschiedene Passwörter für verschiedene Systeme möglich
- Einfache Weitergabe möglich
- Kostengünstig

Probleme mit Passwörtern

- Geheimhaltung der Passwörter schwierig
 - Problem 1: Braucht sicheren Kanal für Übermittlung
 - Problem 2: Bei jedem Login Preisgabe an Service
 - Problem 3: Phishing, Keyloggers, Post-it Notizen, ...
- Sichere Passwörter sind lang und komplex
 - Problem: schwierig zu merken, daher werden oft kurze, einfache Passwörter gewählt, was unsicher ist
- Zu viele Accounts verlangen Passwörter
 - Problem: Mehrfachverwendung von Passwörtern
- Einfache Weitergabe von Passwörtern möglich

Zukunft der Authentifizierungssysteme

- Authentifizierungssysteme sollten
 - **einfach** sein für den Benutzer, aber
 - **kompliziert** für den Angreifer und
 - **günstig** in der Anschaffung und im Betrieb
- Vermehrte Authentifizierung durch Dritte bei Webapplikationen dank Standardprotokollen (z.B. OpenID/OAuth, SAML)
 - Passwörter nicht mehr im Klartext an Webapplikation
 - weniger Passwörter nötig
- **Fazit:**
Innovative Alternativen zum Passwort sind nötig

Danke für Ihre Aufmerksamkeit!