RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

the adventures of

alice & bob

Password Secrets Revealed!

All you want to know but are afraid to ask...

Microsoft® Most Valuable Professional MVP

Speaker：Paula Januszkiewicz

Job Title：IT Security Auditor, CEO

Company Name：CQURE

Microsoft | Security Trusted Advisor

STEP SPRINGBOARD SERIES TECHNICAL EXPERT PANEL

CQURE Security WorldWide

Agenda

What are passwords for… nothing!

Things you should remember

Bad and even worse password usage scenarios!

What to expect?

- Life without passwords…
- Passwords in the Web
- Protected Storage
- Passwords in the Operating System
- Wireless (In) Security
- Rainbow tables
- Cracking toolkit
- Summary

… would be beautiful, but it is not

- Strong passwords or / and user awareness

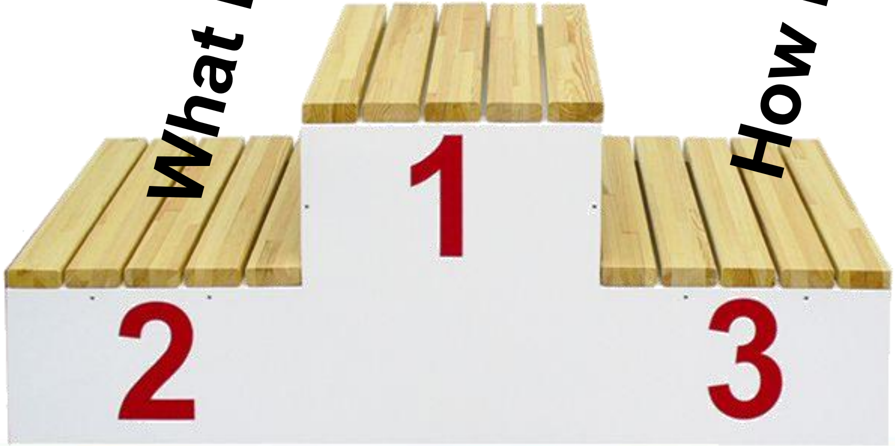
Complexity Characters	Letters (Lower)	Letters (Upper & Lower)	Letters (All) & Digits	Letters & Digits & Special
6	308,915,776	19,770,609,664	56,800,235,584	304,006,671,424
8	208,827,064,576	53,459,728,531,456	218,340,105,584,896	2,044,140,858,654,976
10	141,167,095,653,376	144,555,105,949,057,024	839,299,365,868,340,224	13,744,803,133,596,058,624
12	95,428,956,661,682,176	390,877,006,486,250,192,896	3,226,266,762,397,899,821,056	92,420,056,270,299,898,187,776

Time to crack passwords

Complexity Characters	Letters (Lower)	Letters (Upper & Lower)	Letters (All) & Digits	Letters & Digits & Special
6	154,4 seconds	164,7 hours		
8	29 hours	…	…	…
10	816 days	…	…	…
12	51152123 years	…	…	87918622783,7 years

Avg. password cracking: 2 millions per second

3 cryptography basics



What is the alghoritm?

Where is the key?

How long is the key?

What to expect?

- Life without passwords…
- Passwords in the Web
- Protected Storage
- Passwords in the Operating System
- Wireless (In) Security
- Rainbow tables
- Cracking toolkit
- Summary

Passwords in the Web: Inside the SSL Tunnel

DEMO

What to expect?

- Life without passwords…
- Passwords in the Web
- Protected Storage
- Passwords in the Operating System
- Wireless (In) Security
- Rainbow tables
- Cracking toolkit
- Summary

Protected Storage Internals

- Now: Read-Only
- DPAPI
  - Data Blob + Entropy
  - Master Key
  - User Password

What to expect?

- Life without passwords…
- Passwords in the Web
- Protected Storage
- Passwords in the Operating System
- Wireless (In) Security
- Rainbow tables
- Cracking toolkit
- Summary

Crack Basics: Windows

- Locally: Security Accounts Manager
- Domain: NTDS.dit
- Direct reading? Why not?
  - SAMInside, Cain, ERD Commander, pwdump + L0phtCrack, john the ripper
- PSTORE

SAM (Tools), DefineDosDevice, System Privileges, SAPD, Notification Package, GINA.DLL, Computer Password

DEMO

What to expect?

- Life without passwords…
- Passwords in the Web
- Protected Storage
- Passwords in the Operating System
- Wireless (In) Security
- Rainbow tables
- Cracking toolkit
- Summary

Tools for Recognition

- AIRODUMP-NG
- NetStumbler
- ViStumbler
- More
- … and more

Wireless (In) Security: Recognition & Attack

DEMO

What to expect?

- Life without passwords…
- Passwords in the Web
- Protected Storage
- Passwords in the Operating System
- Wireless (In) Security
- Rainbow tables
- Cracking toolkit
- Summary

Rainbow Tables

- OphCrack
- RainbowCrack

- Available in free editions!

What to expect?

- Life without passwords…
- Passwords in the Web
- Protected Storage
- Passwords in the Operating System
- Wireless (In) Security
- Rainbow tables
- Cracking toolkit
- Summary

Password Cracking Tools

- Linux
  - John the Ripper (http://www.openwall.com/john/)
- Windows
  - John the Ripper
  - SamInside / Passwords Pro (http://www.insidepro.com)
  - Cain (http://www.oxid.it/cain.html)
  - LC5 / pwdump
  - Top 10 Tools: http://sectools.org/crackers.html

What to expect?

- Life without passwords…
- Passwords in the Web
- Protected Storage
- Passwords in the Operating System
- Wireless (In) Security
- Rainbow tables
- Cracking toolkit
- Summary

Summary

- Have your own dictionary file
- Use well-designed password policies
- Train users – show them what may happen if their password is revealed
- Test your users’ passwords

Q&A

Resources

- Good Rainbow Tables:
  - http://www.insidepro.com/tables.php
  - http://www.freerainbowtables.com/en/tables/ntlm/
  - https://www.objectif-securite.ch/en/
- Wireless Hacking:
  - http://wpa-crack.com
  - http://wpa.darkircop.org