09- Passwords

Lorrie Cranor and Blase Ur

February 11, 2014

05-436 / 05-836 / 08-534 / 08-734 Usable Privacy and Security Carnegie Mellon University CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy



What is a password?

- Today: a password is a series of characters that authenticates a user
 - Vs. graphical passwords, etc.
 - Vs. unlock patterns
 - Vs. PINS (are they different?)

How passwords should be stored

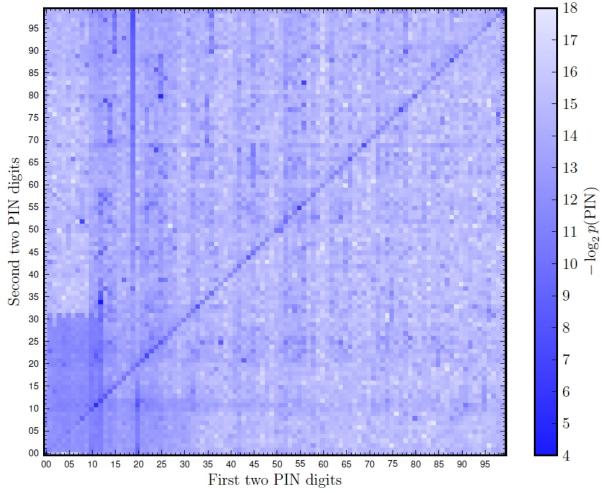
- Password: monkeyprincess
- Hashed (using md5 in this example) 4f83051773ad6eaa0afd1f01fe326c07

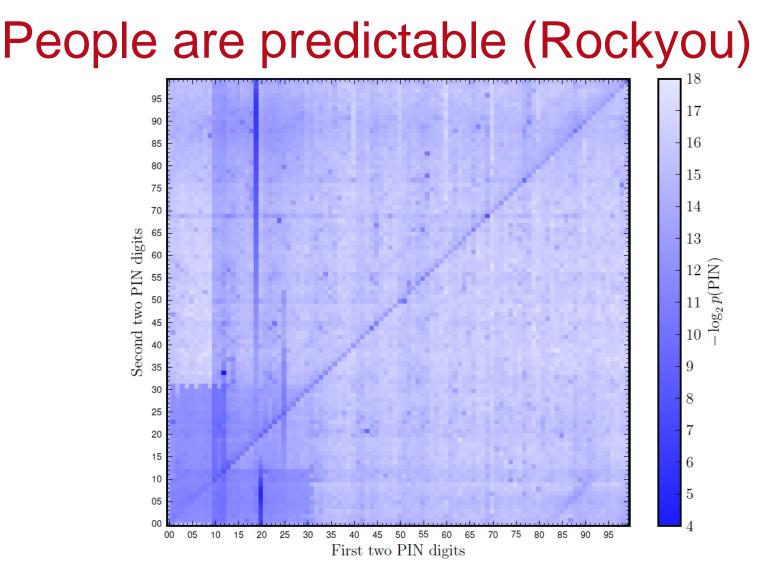
- Problem: rainbow tables can be used

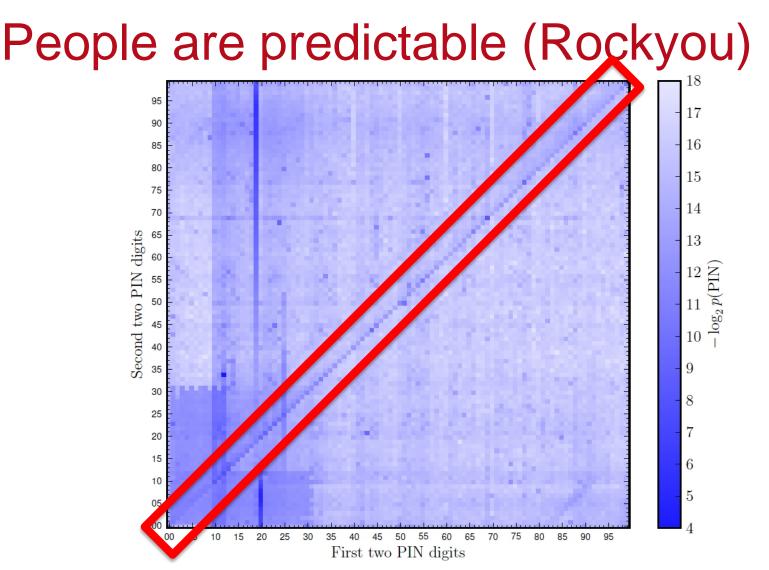
- Better: salted and hashed passwords
 - Generate random string (salt) for each person
 - hash(password|salt) or equivalent
 - Use a slow hash (PBKDF or bcrypt), not md5!

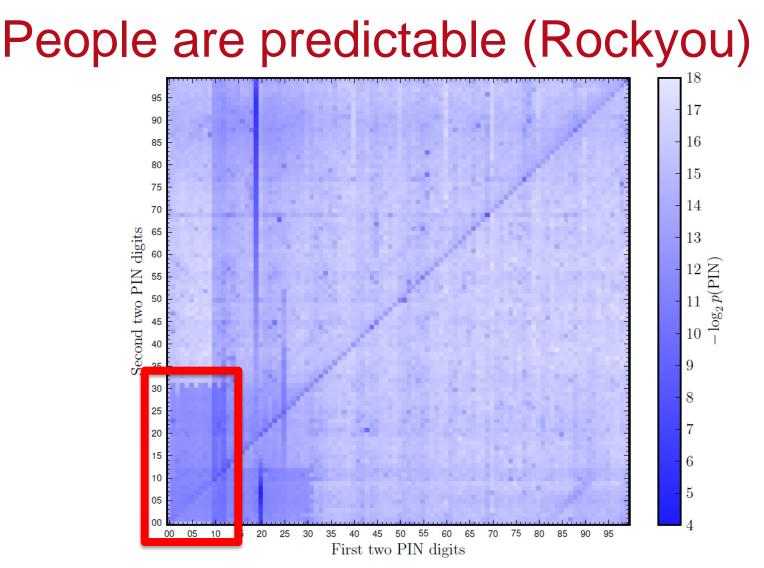
Passwords are useless. Discuss.

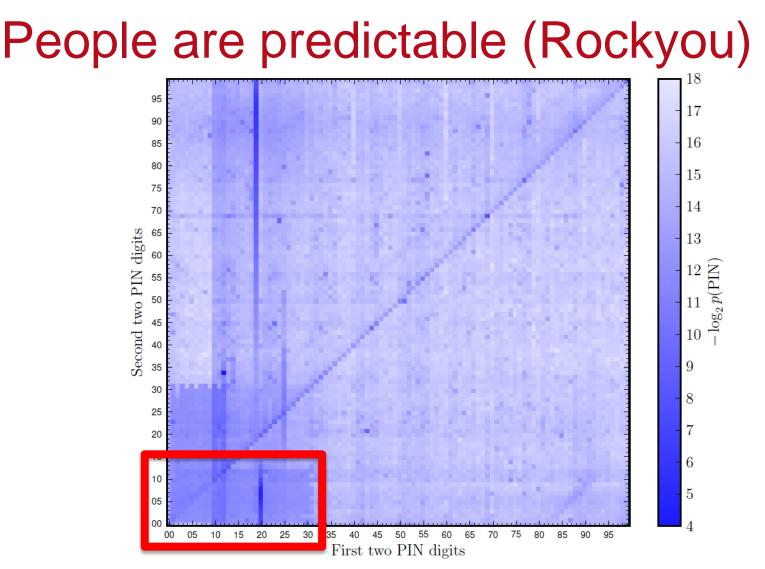


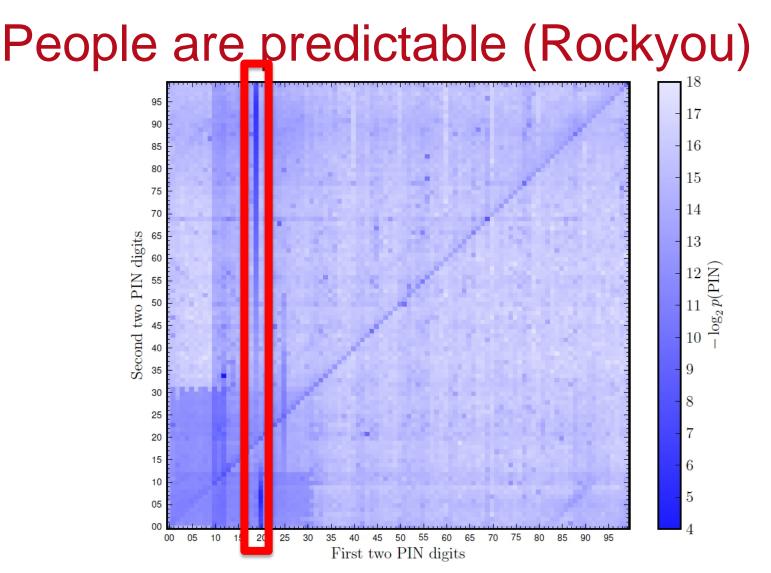












Advances in password cracking

- Online attack: submit guesses to a server
 - Targeted attacks (knowledge about the person) are more effective
- Offline attack: get a list of hashes (and salts) from a site's password database
 - Shorter passwords, unsalted passwords, fast hash functions → can be brute forced!
 - Make a guess, hash the guess, and check to see if it matches the hash

Attackers can guess quickly

- oclHashcat on Ubuntu 13.04 64 bit, Catalyst 13.11b, 1x AMD hd7970
 - 8,089,000,000 guesses/second for MD5
 - 2,510,000,000 guesses/second for SHA1
 - 142,000,000 guesses/second for SHA3
 - 131,000 guesses/second for WPA/WPA2

Ways of guessing passwords

- Wordlists and mangling rules
 - John the Ripper
 - Hashcat (oclHashcat uses GPUs)
- Markov chains
- Probabilistic context-free grammar

• These all rely on training data

Leaks

 RockYou, a maker of social games (Gourmet Ranch, Zoo World) had 32 million passwords stolen in 2009

– Plaintext passwords!

- Smaller breaches happen all the time
 - Sometimes plaintext
 - Sometimes hashed (and sometimes salted)
 - Sometimes encrypted



Leaks

• Adobe (2013) - Encrypted

- ECB mode

HACKERS RECENTLY LEAKED 153 MILLION ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS. ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL: USER PASSWORD HINT 4e18acc1ab27b2d6 WEATHER VANE SWORD He18acc1ab2762d6 Hellacciab270206 aDa2876cblealfca NAME1 Shahb6299e06eb6d DUH Shabb6299e06eb6d aDa2876cblcalfca 86066299e066666 85e9da81a8a78adc 57 4e18acc1ab2762d6 FAVORITE OF 12 APOSTLES 1ab29ac86da6e5ca 7a2d6a0a2876eb1e WITH YOUR OWN HAND YOU HAVE DONE ALL THIS a1F96266299e7a26 eadec1e6a6797397 SEXY EARLOBES a1f96266299e7626 617a60277727ad85 BEST TOS EPISODE 3973867ad6068at7 617a60277727ad85 SUGARLAND 106290e86da6e5ca NAME + JERSEY # 877ab7889d3862b1 ALPHA 877ab78893386261 877ab7889d3862b1 877ab78898386261 OBVIOUS 877ab78893386261 MICHAEL JACKSON 3807c9279cadeb44 9dcald79d4dec6d5 38a7c9279cadeb44 9dcald79d4dec6d5 HE DID THE MASH, HE DID THE PURLOINED 38a7c9279cadeb44 SUSTISTISTIC GOODITS FOUL ATER-3 POKEMON THE GREATEST CROSSWORD PUZZLE http://xkcd.com/1286/ IN THE HISTORY OF THE WORLD

Leaks

 Common passwords in Adobe breach include 123456, 123456789, password, adobe123, 12345678, qwerty, photoshop, abc123, adobe1, macromedia, azerty, iloveyou, aaaaaa, 666666, letmein, monkey, princess, dragon, adobeadobe, chocolate,...

Passwords are useful. Discuss.

Evaluating authentication schemes

- Usability = effortless to remember, nothing to carry, easy to learn, infrequent errors, etc.
- Deployability = accessible, server compatible, cheap, non-proprietary, etc.
- Security = resists physical observation, resistant to throttled/unthrottled guessing, unlinkable, resistant to internal observation

Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. Oakland '12

~ .				Usability					Deployability					Security								
(Incumbent)	Web passwords		[13]		٠		• •	0	•	• •	• •	•	•		0					٠	• •	
Password managers	Firefox	IV-A			• •	0	• •	۲		• •	•		• •	0	0				۲	٠	• •	•
	LastPass		[42]	O	• •	0	••	۲	0	•	•		•	0	0	Ö	o	C		•	-	•
Proxy	URRSA	IV-B	[5]	۲			• =	0			• •	•			0		(D	۲			•
	Impostor		[23]		•		• =		•	•	•	0			0		¢	D	۲	•		•
Federated	OpenID	IV-C	[27]	O I	•	Ö	•	ĕ	•	• •		٠	•	0	0	Ö	Ö			•	•	
	Microsoft Passport		[43]	O	•	o	••	۲	•	•		٠	•	Ø	0	Ö	Ö			•		
	Facebook Connect		[44]	Ø	• •	ø	• •	۲	•	• •		٠	•	Ø	0	Ö	Ö	Ľ.		•		
	BrowserID		[45]	0	•	ø	• •	۲	•	• •		0	0	0	0	Ö	o			•	•	
	OTP over email		[46]	0	•		•	۲	•	• •		٠		0	0	Ö	O			•		
Graphical	PCCP	IV-D	[7]		•		• 0	0	•			٠			۲	Ö				٠	• •	•
	PassGo		[47]		•		• 0	0	•			٠	0		۲					٠	• •	• •
Cognitive	GrIDsure (original)	IV-E	[30]		•		• 0	0	•			٠			ĕ					٠	• •	•
	Weinshall		[48]	1	٠							٠		0	۲			Ľ.		٠	• •	•
	Hopper Blum		[49]		•					• •		٠		Ø	۲			Ľ.		٠	• •	•
	Word Association		[50]		٠		••	ο	0	• •		٠								٠	• •	•
Paper tokens	OTPW	IV-F	[33]				• =		•			٠	•		۲	۲	•		۲	٠	• •	•
	S/KEY		[32]	۲			• =	0	•			٠	• •		۲	۲			0		• •	•
	PIN+TAN		[51]	1			• =	0	0	1	0	٠	• •		۲	ĕ				0	• •	• •
Visual crypto	PassWindow		[52]	۲					=		0	٠	•	0	۲	ě,	ē (D) Ö		• •	• •
Hardware tokens	RSA SecurID	IV-G	[34]				• 0	0				٠	•		۲	ĕ				•		• •
	YubiKey		[53]				• •	0		•		٠	•	i.	۲	۲			۲	•	•	•
	IronKey		[54]	O		Ø	0 0	ο		•	•	•	•		0		¢	D	۲	٠	• •	•
	CAP reader		[55]				• •	0				٠	•		۲	ĕ				٠	• •	•
	Pico		[8]			۲	0	0	=						۲	ĕ				0	• •	• •
Phone-based	Phoolproof	IV-H	[36]		0		• 0	0		0	0 0				۲	ĕ	ē (D) 🎽	٠	• •	
	Cronto		[56]	1	0		• •	0			0	٠	•	i.	۲	۲	• (D	۲	٠	• •	•
	MP-Auth		[6]	1	0		• 0		0	0 0	o				0				۲	٠	• •	•
	OTP over SMS				• •		• =	0	0	0		٠	• •		۲	۲	• (D		0		• •
	Google 2-Step		[57]	1	0		• •	0	0	0		٠	•	Ø	0	۲	ĕ			٠	• •	•
Biometric	Fingerprint	IV-I	[38]		•	O	• 0		_	0			0			ĕ					• •	
	Iris		[39]	Ŭ.	•	Ø	• •			0			٥	i.		۲					• 3	0
	Voice		[40]		•	Ö	• •			0	o	0	0			Ø					• •	
Recovery	Personal knowledge		[58]		•		• •	0	•	• •		٠	•							•	• •	•
	Preference-based		[59]	o	٠		• •	۲	0	• •		٠			0				۲	٠	• •	• •
	Social re-auth.		[60]		٠		•	۲		• •		٠	0	0		۲	• (D		•	•	0

•= offers the benefit; •= almost offers the benefit; no circle = does not offer the benefit.

|||= better than passwords; == worse than passwords; no background pattern = no change.

Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. Oakland '1²⁰

The anatomy of a password study (demo)