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?

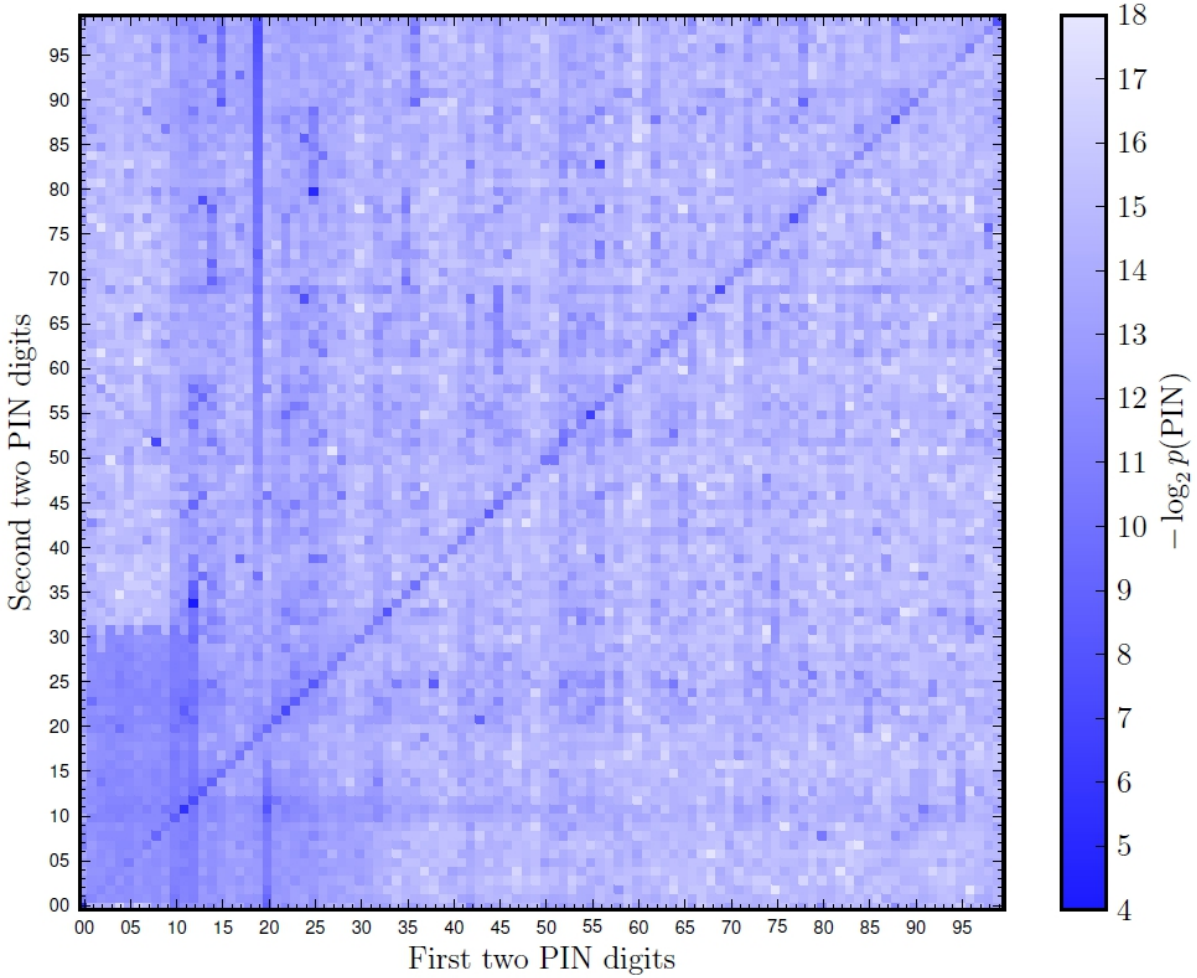
- Today: a password is a series of characters that authenticates a user
  - Vs. graphical passwords, etc.
  - Vs. unlock patterns
  - Vs. PINS (are they different?)

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!

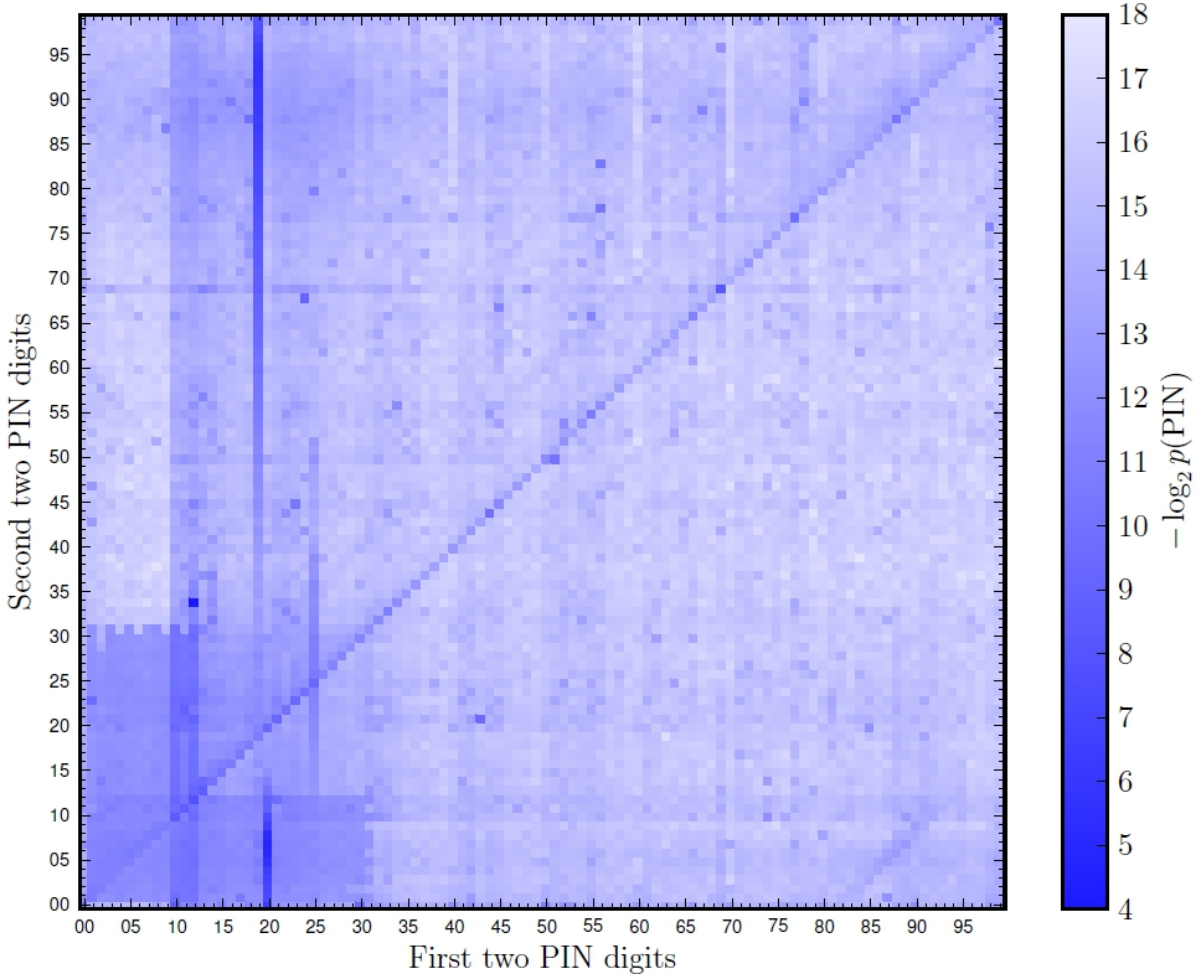
Passwords are useless.
Discuss.

People are predictable (iPhone PINs)



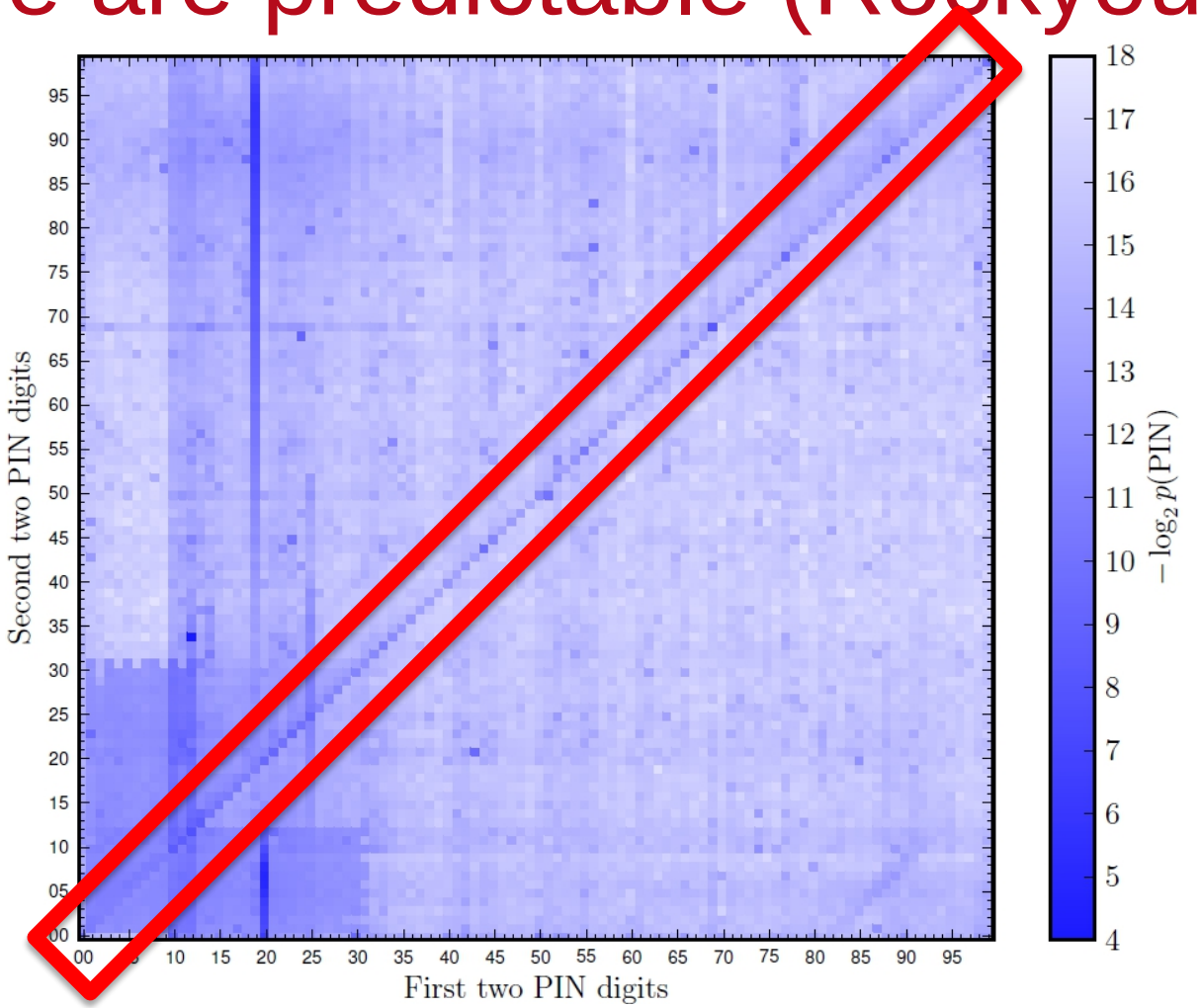
Joseph Bonneau, Sören Preibusch and Ross Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. FC '12

People are predictable (Rockyou)



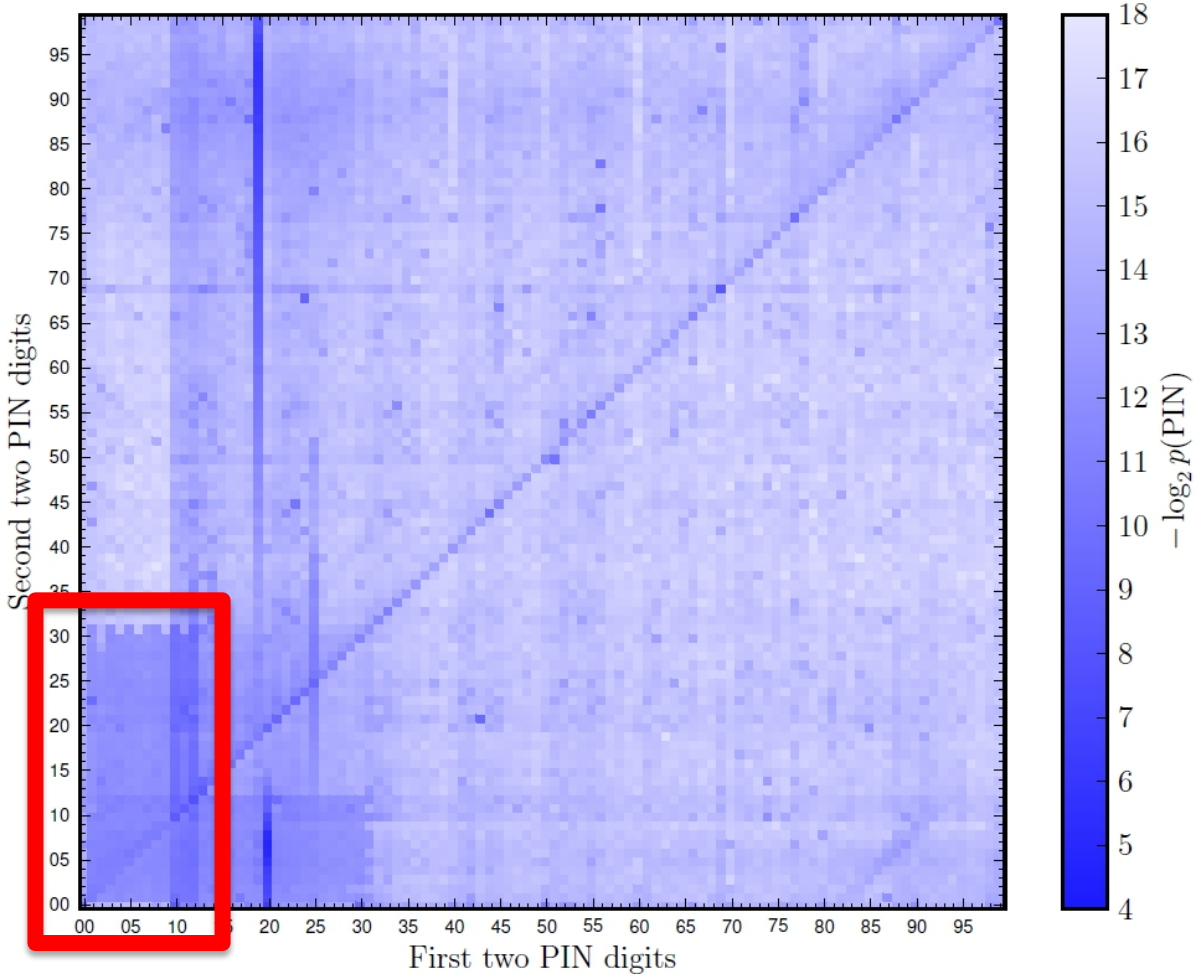
Joseph Bonneau, Sören Preibusch and Ross Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. FC '12

People are predictable (Rockyou)



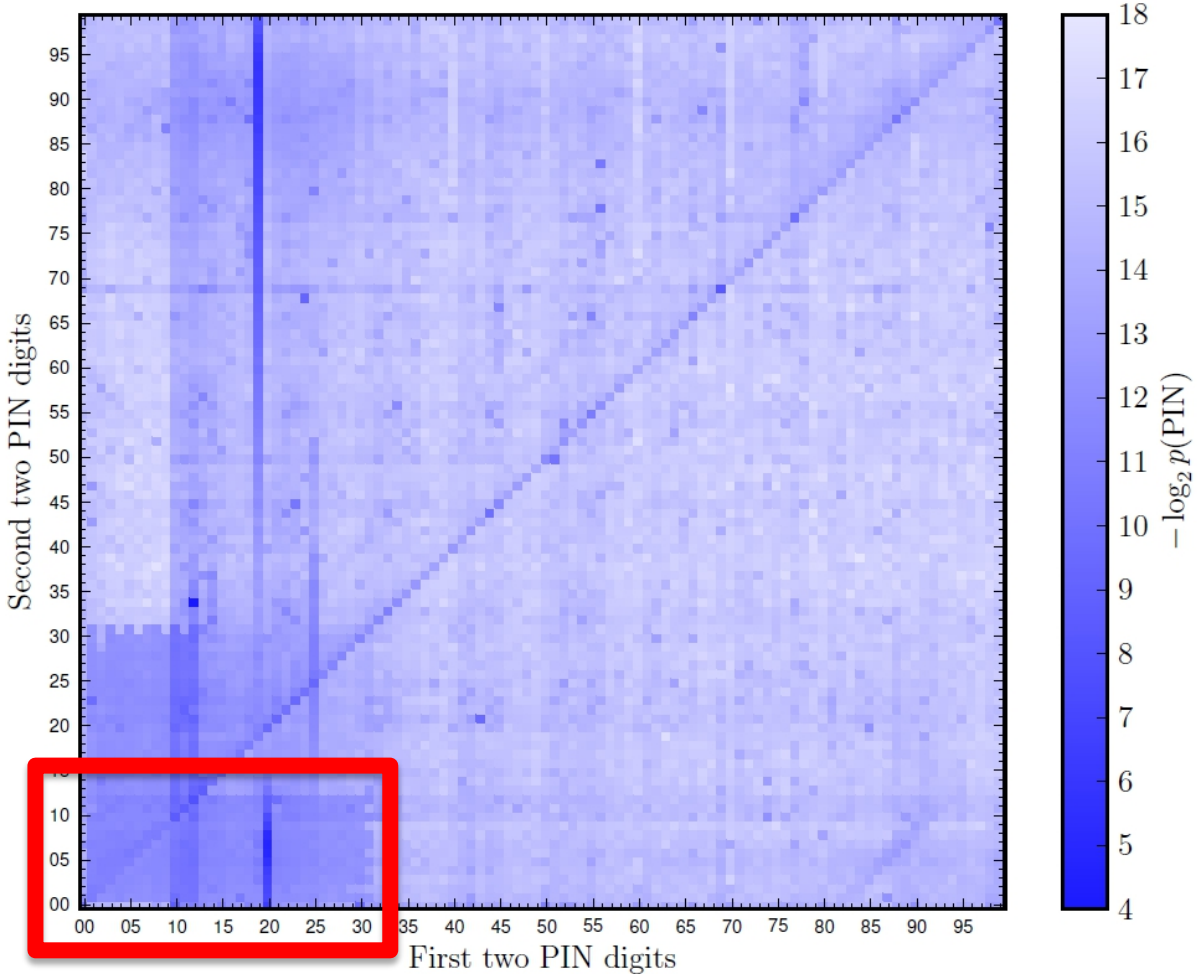
Joseph Bonneau, Sören Preibusch and Ross Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. FC '12

People are predictable (Rockyou)



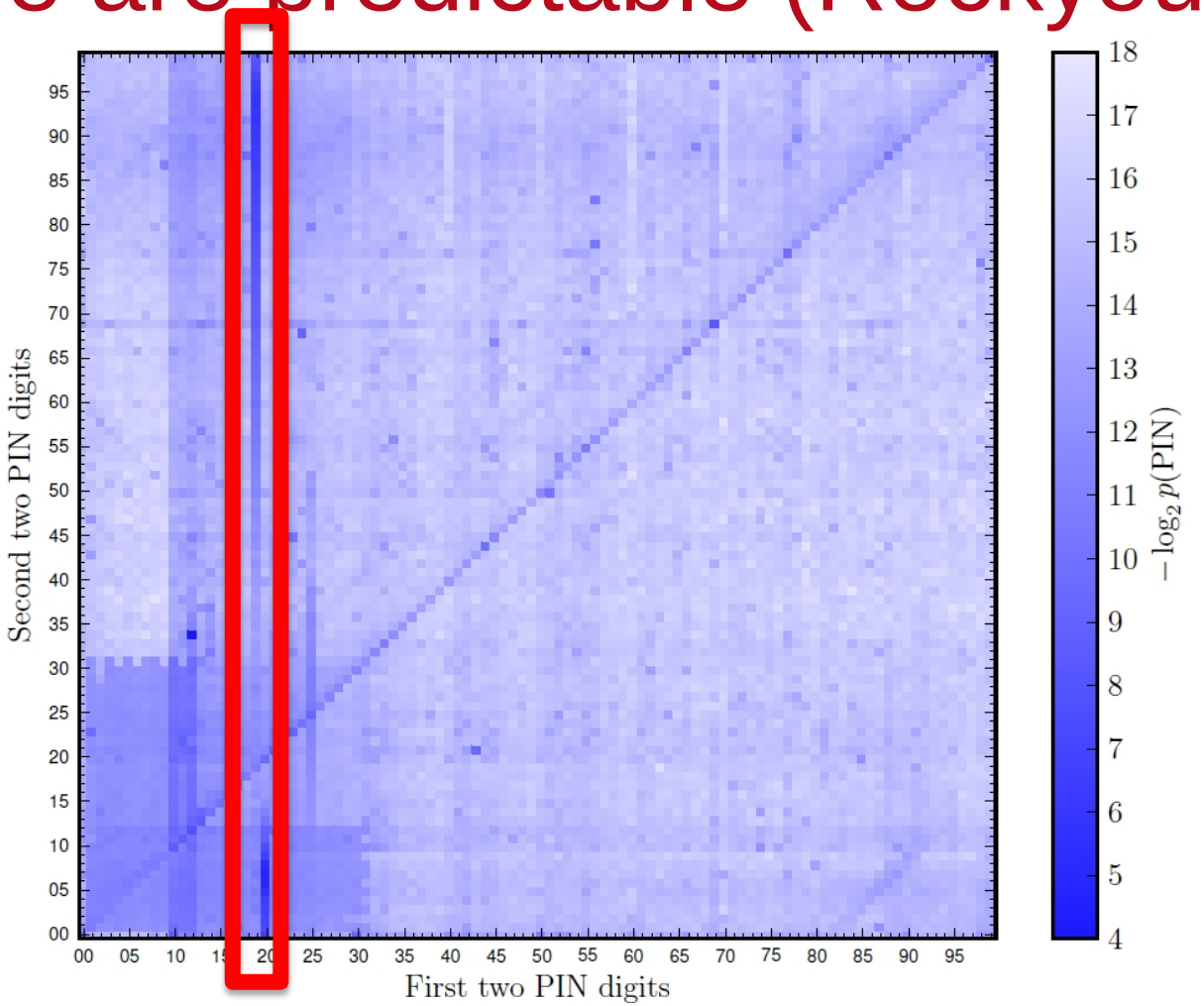
Joseph Bonneau, Sören Preibusch and Ross Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. FC '12

People are predictable (Rockyou)



Joseph Bonneau, Sören Preibusch and Ross Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. FC '12

People are predictable (Rockyou)



Joseph Bonneau, Sören Preibusch and Ross Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. FC '12

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

http://hashcat.net/oclhashcat/

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

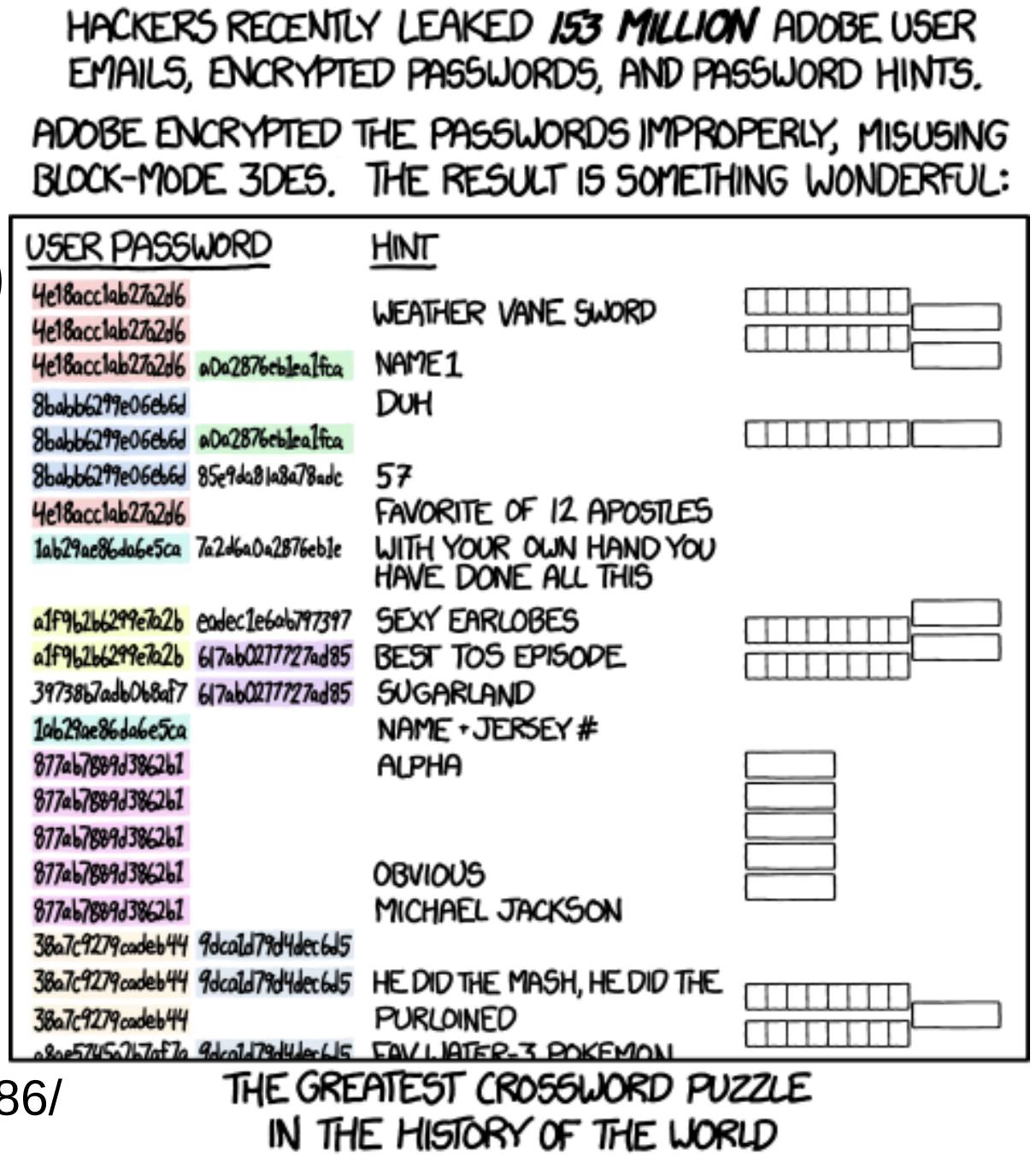
Leaks

- 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


123456789
password
iloveyou
12345
princess
rockyou
12345678
1234567
abc123
nicole
monkey
qwerty
babygirl
daniel
michael
michelle
jessica
ashley
lovely
tigger
sunshine
anthony
butterfly
chocolate
jordan
secret
password1
654321
1234567890
iloveu
friends
fuckyou
tinkerbell
loveme
soccer
joshua
jonathan
tweety
computer
superman
eminem
andrea
purple
hannah
brandon
family
robert
spongebob
amanda
elizabeth
yellow
flower
angel
hello
justin
andrew
football
bubbles
jennifer
teamo
chelsea
dragon
softball
barbie
lovers
matthew
carlos
angels
basketball
samantha
jasmine
pretty
princesa
shadow
whatever
mylove
richard
tequiero
beauty
louise
987654321
123123
forever
william
thomas
hottie
naruto
alexis
stephanie
taylor
danielle
poohbear
alexandra
sweety
joseph
charlie
iloveme
summer
melissa
cookie
666666
0

Leaks

- Adobe (2013)
  - Encrypted
  - ECB mode



http://xkcd.com/1286/

Leaks

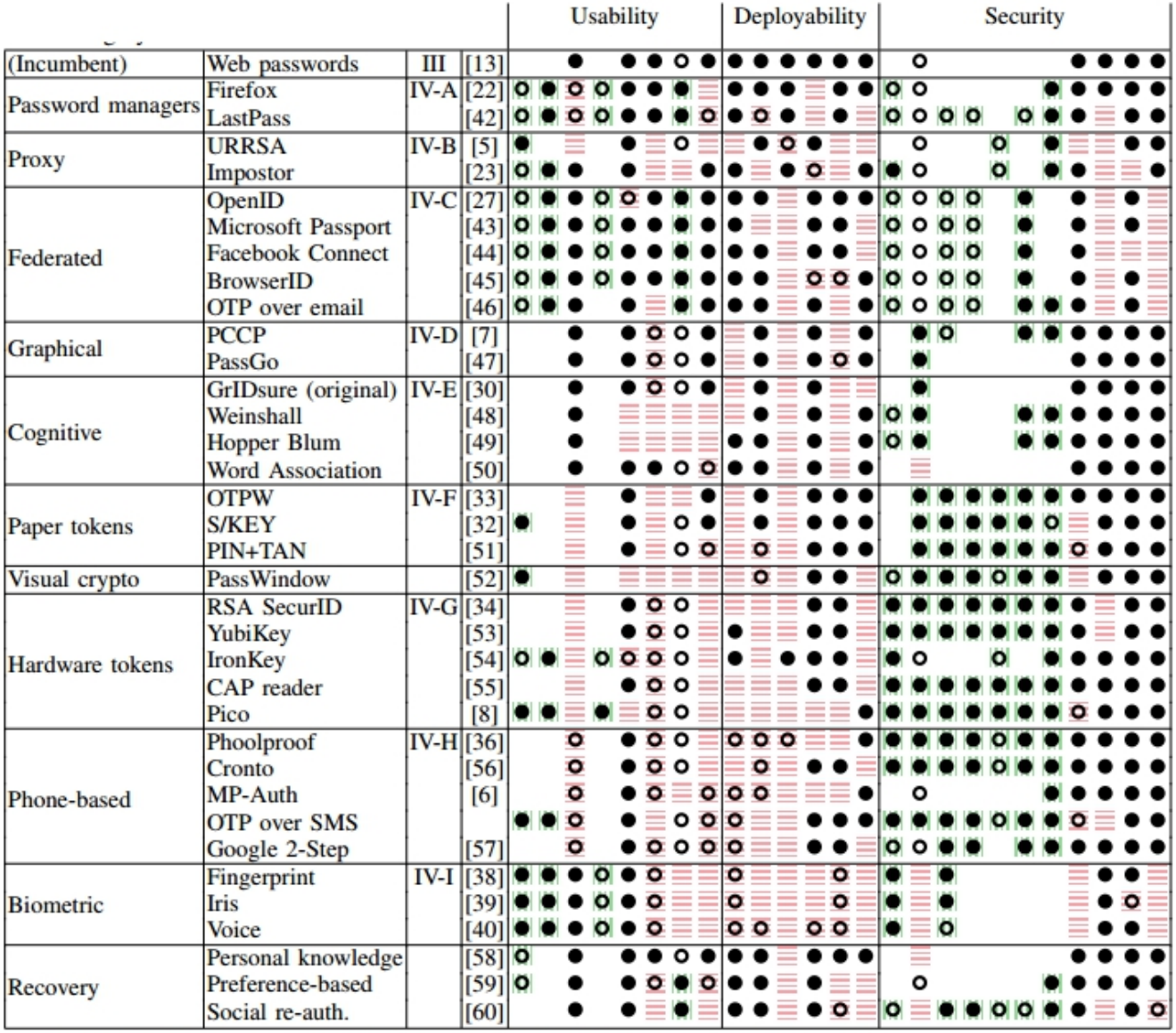
- Common passwords in Adobe breach include 123456, 123456789, password, adobe123, 12345678, qwerty, photoshop, abc123, adobe1, macromedia, azerty, iloveyou, aaaaaa, 666666, letmein, monkey, princess, dragon, adobeadobe, chocolate,...

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



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

The anatomy of a password study (demo)