## CSE 484 / CSE M 584: Computer Security and Privacy

# Authentication (Continued)

Autumn 2018

Tadayoshi (Yoshi) Kohno
yoshi@cs.Washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Ada Lerner, John Manferdelli, John Mitchell, Franziska Roesner, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

# Admin

- HW2: Due Nov 7, 4:30pm

- Looking ahead, rough plan:
- Lab 2 out Nov 5, due Nov 20, 4:30pm
  - Quiz section this week extended office hours
- HW 3 out ~Nov 19, due ~Nov 30
- Lab 3 out ~Nov 26, due Dec 7 (Quiz Section on Nov 29)

- No class Nov 21; video review assignment instead

# Admin

- Final Project Proposals: Nov 16 – group member names and brief description
- Final Project Checkpoint: Nov 30 – preliminary outline and references
- Final Project Presentation: Dec 10 – 12-15-minute video – **must** be on time
- Explore something of interest to you, that could hopefully benefit you or your career in some way – technical topics, current events, etc

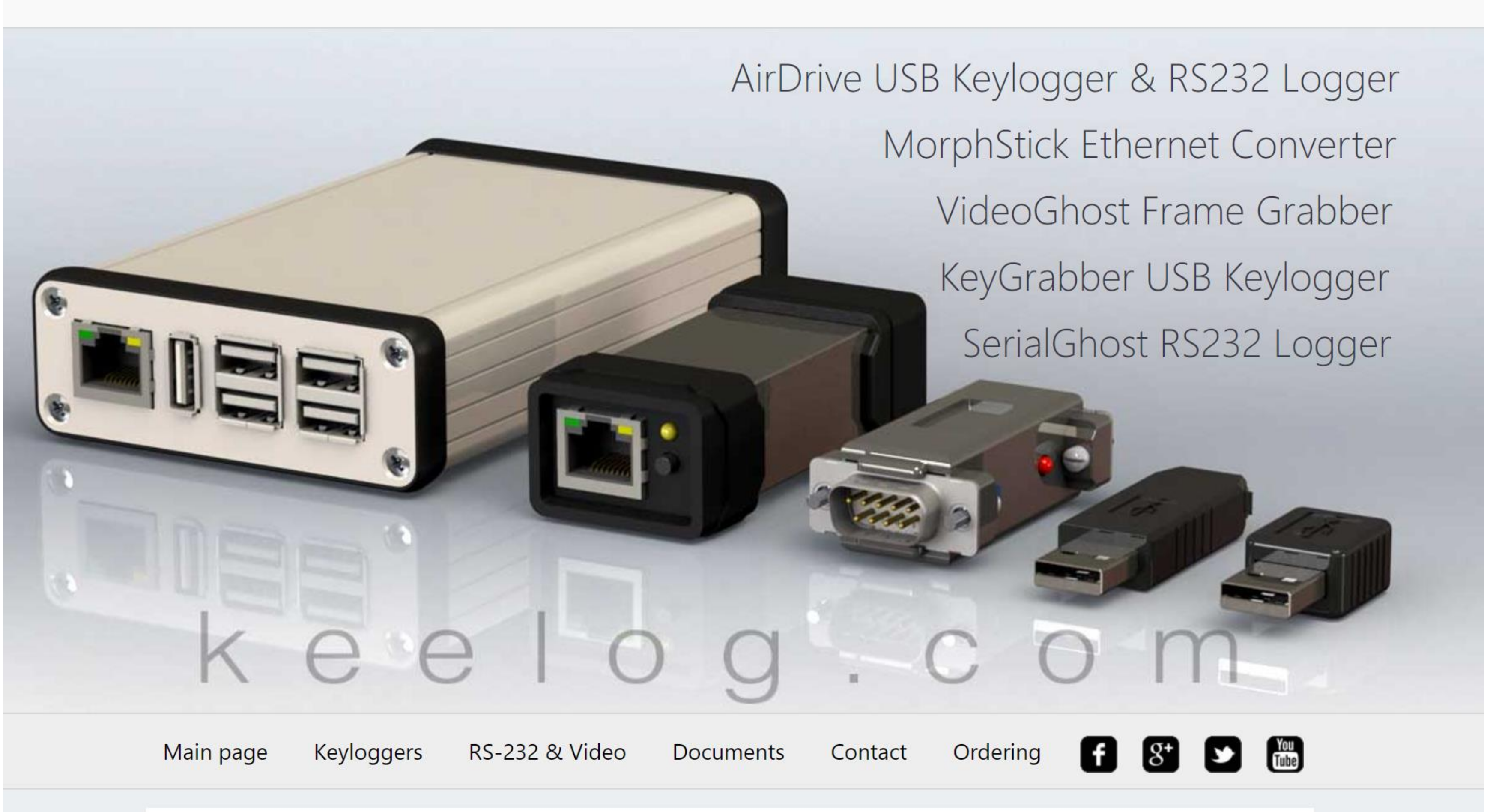
# Review: Many Ways to Prove Who You Are

- What you know
  - Passwords
  - Answers to questions that only you know
- Where you are
  - IP address, geolocation
- What you are
  - Biometrics
- What you have
  - Secure tokens, mobile devices

# Review: Other Password Security Issues

- Keystroke loggers
  - Hardware
  - Software (spyware)
- Shoulder surfing
- Same password at multiple sites
- Broken implementations
  - TENEX timing attack

# Review: Examples from One Company



AirDrive USB Keylogger & RS232 Logger

MorphStick Ethernet Converter

VideoGhost Frame Grabber

KeyGrabber USB Keylogger

SerialGhost RS232 Logger

# Review: Even More Issues

- Usability
  - Hard-to-remember passwords?
  - Carry a physical object all the time?
- Denial of service
  - Attacker tries to authenticate as you, account locked after three failures
- Social engineering

# Default Passwords

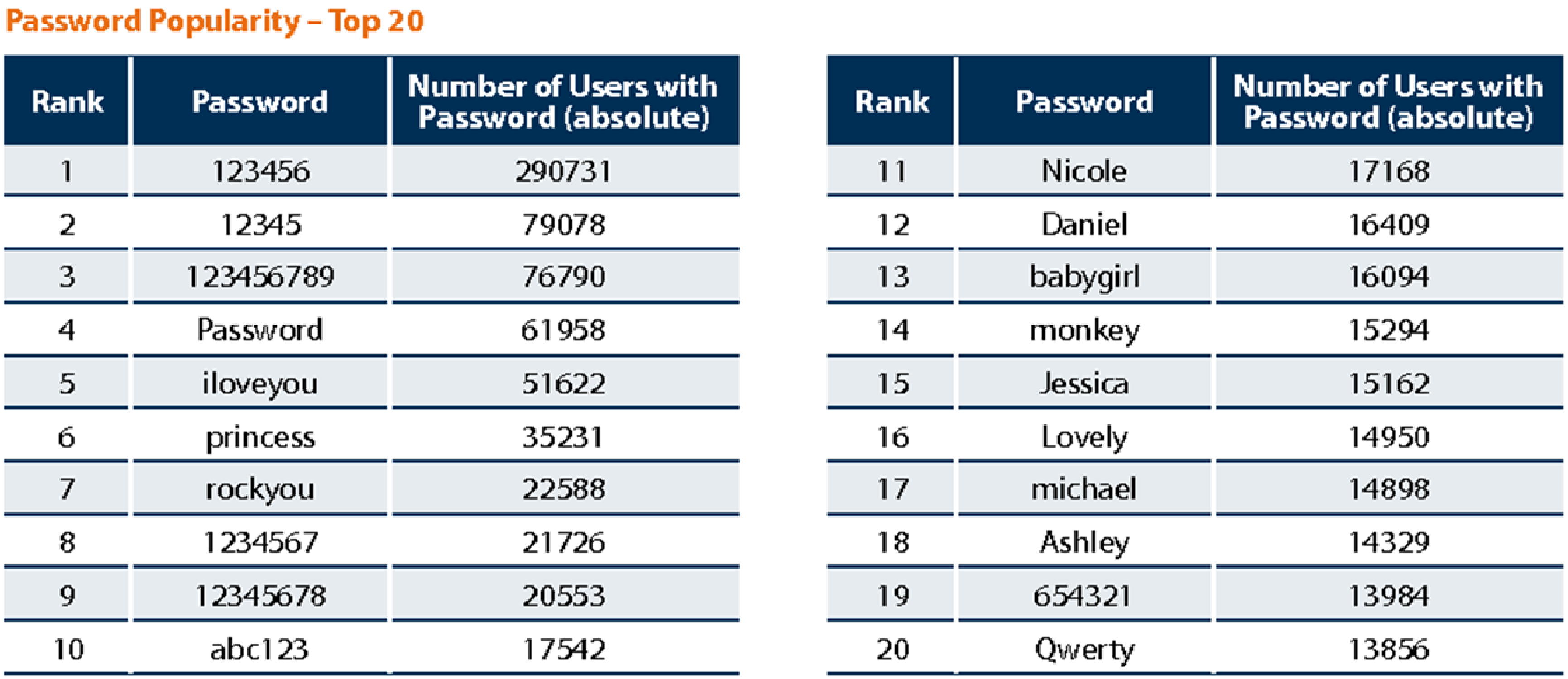
- Examples from Mitnick's "Art of Intrusion"
  - U.S. District Courthouse server: "public" / "public"
  - NY Times employee database: pwd = last 4 SSN digits
- Mirai IoT botnet
  - Weak and default passwords on routers and other devices

# Weak Passwords

- RockYou hack
  - "Social gaming" company
  - Database with 32 million user passwords from partner social networks
  - Passwords stored in the clear
  - December 2009: entire database hacked using an SQL injection attack and posted on the Internet
  - One of many such examples!

# Weak Passwords

- RockYou hack



Password Popularity – Top 20

| Rank | Password | Number of Users with Password (absolute) |
|---|---|---|
| 1 | 123456 | 290731 |
| 2 | 12345 | 79078 |
| 3 | 123456789 | 76790 |
| 4 | Password | 61958 |
| 5 | iloveyou | 51622 |
| 6 | princess | 35231 |
| 7 | rockyou | 22588 |
| 8 | 1234567 | 21726 |
| 9 | 12345678 | 20553 |
| 10 | abc123 | 17542 |

| Rank | Password | Number of Users with Password (absolute) |
|---|---|---|
| 11 | Nicole | 17168 |
| 12 | Daniel | 16409 |
| 13 | babygirl | 16094 |
| 14 | monkey | 15294 |
| 15 | Jessica | 15162 |
| 16 | Lovely | 14950 |
| 17 | michael | 14898 |
| 18 | Ashley | 14329 |
| 19 | 654321 | 13984 |
| 20 | Qwerty | 13856 |

[Inglesant and Sasse, "The True Cost of Unusable Password Policies"]

# Password Policies

- Old recommendation:
  - 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords…

# Password Usability

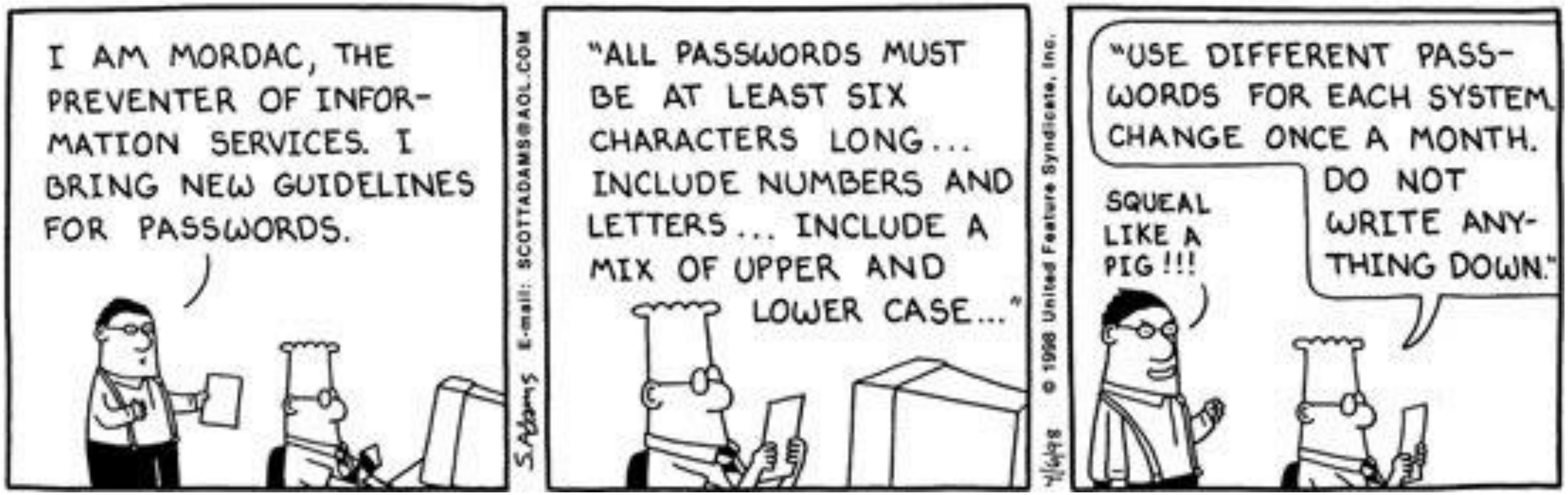

I AM MORDAC, THE PREVENTER OF INFORMATION SERVICES. I BRING NEW GUIDELINES FOR PASSWORDS.
"ALL PASSWORDS MUST BE AT LEAST SIX CHARACTERS LONG... INCLUDE NUMBERS AND LETTERS... INCLUDE A MIX OF UPPER AND LOWER CASE..."
"USE DIFFERENT PASSWORDS FOR EACH SYSTEM. CHANGE ONCE A MONTH. DO NOT WRITE ANYTHING DOWN."
SQUEAL LIKE A PIG!!!
S.Adams
E-mail: SCOTTADAMS@AOL.COM
© 1998 United Feature Syndicate, Inc.

Image from http://www.interactivetools.com/staff/dave/damons_office/

[Inglesant and Sasse, “The True Cost of Unusable Password Policies”]

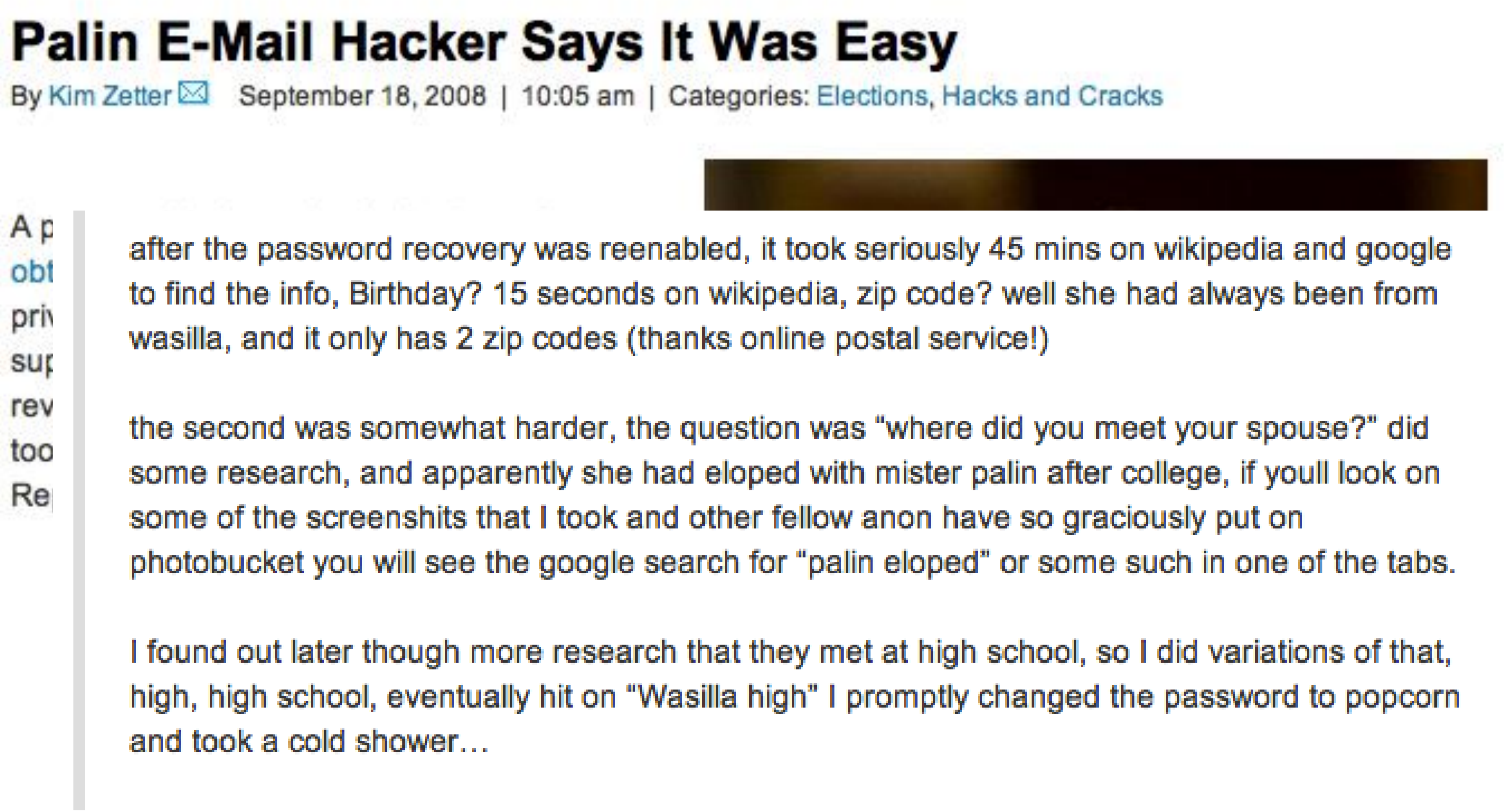
# Password Policies

- Old recommendation:
  - 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords…
- But … results in frustrated users and less security
  - Burdens of devising, learning, forgetting passwords
  - Users construct passwords insecurely, write them down
    - Can’t use their favorite password construction techniques (small changes to old passwords, etc.)
  - Heavy password re-use across systems
  - (Password managers can help)

# More Password / Authentication Issues

- Credential Stuffing (using stolen credentials on other sites)
- Website permits brute force / automated guesses
- Not supporting multi-factor authentication (future slides)
- Weak password recovery mechanisms (next slides)
- Application timeouts too long

# Recovering Passwords



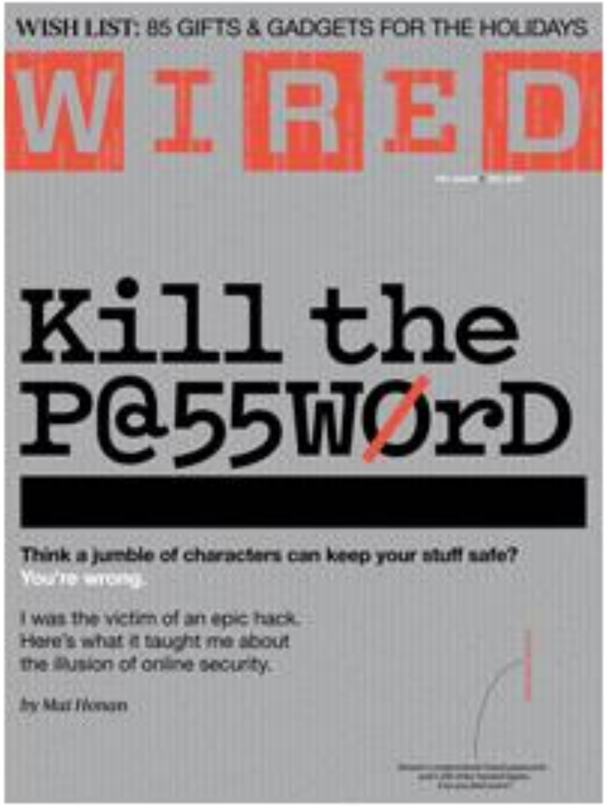
## Palin E-Mail Hacker Says It Was Easy

By Kim Zetter ✉ September 18, 2008 | 10:05 am | Categories: Elections, Hacks and Cracks

A p
obt
pri
sup
rev
too
Re

> after the password recovery was reenabled, it took seriously 45 mins on wikipedia and google to find the info, Birthday? 15 seconds on wikipedia, zip code? well she had always been from wasilla, and it only has 2 zip codes (thanks online postal service!)
>
> the second was somewhat harder, the question was "where did you meet your spouse?" did some research, and apparently she had eloped with mister palin after college, if youll look on some of the screenshits that I took and other fellow anon have so graciously put on photobucket you will see the google search for "palin eloped" or some such in one of the tabs.
>
> I found out later though more research that they met at high school, so I did variations of that, high, high school, eventually hit on "Wasilla high" I promptly changed the password to popcorn and took a cold shower…

# Wired Cover Story (Dec 2012)



WISH LIST: 85 GIFTS & GADGETS FOR THE HOLIDAYS

WIRED

Kill the P@55WØrD

Think a jumble of characters can keep your stuff safe? You're wrong.

I was the victim of an epic hack. Here's what it taught me about the illusion of online security.

*by Mat Honan*

**Also in this issue**

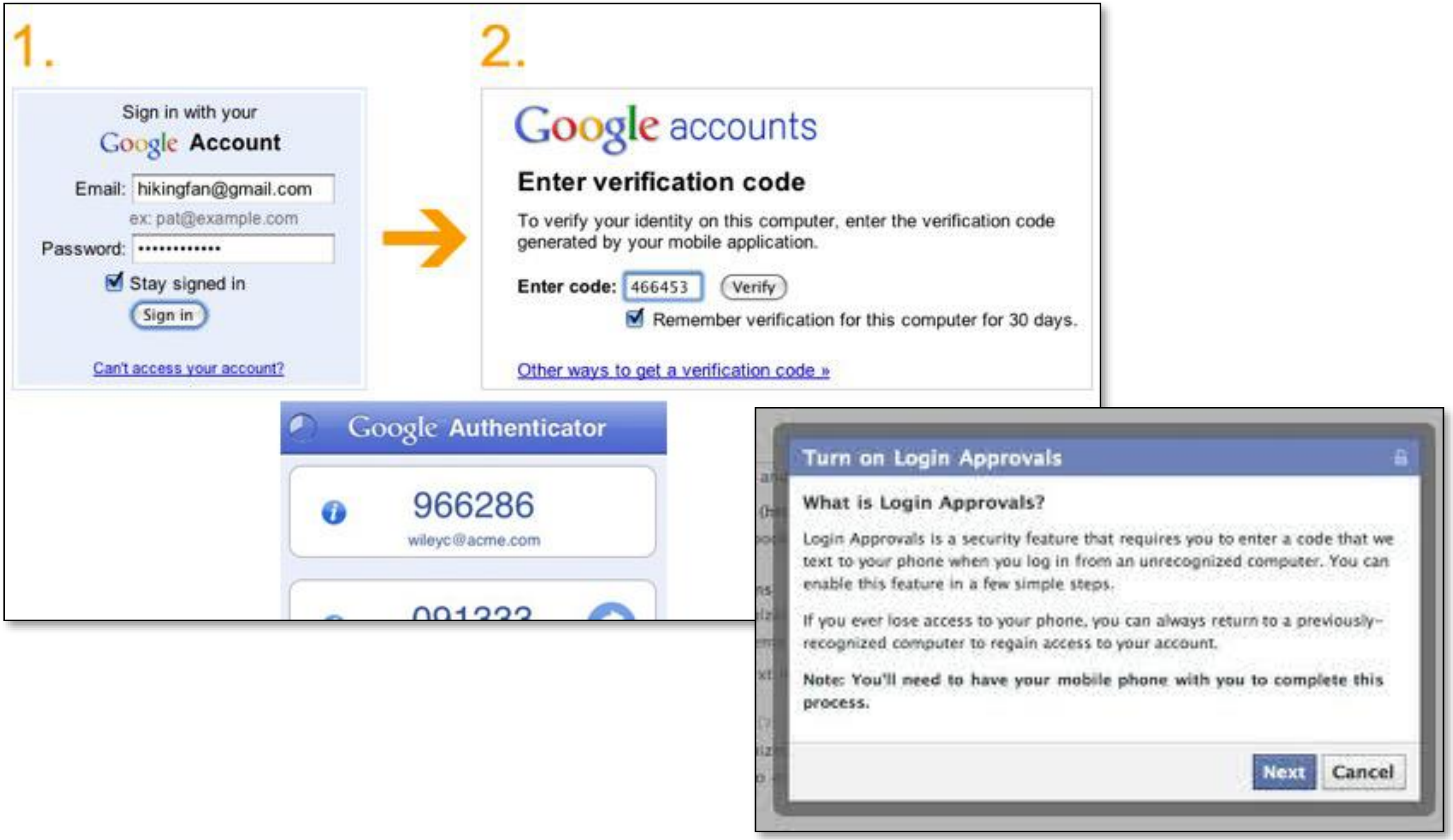
Kill the Password: Why a String of Characters Can't Protect Us Anymore

*"This summer, hackers destroyed my entire digital life in the span of an hour. My Apple, Twitter, and Gmail passwords were all robust—seven, 10, and 19 characters, respectively, all alphanumeric, some with symbols thrown in as well—but the three accounts were linked, so once the hackers had conned their way into one, they had them all. They really just wanted my Twitter handle: @mat."*

# Improving(?) Passwords

- Add biometrics
  - For example, keystroke dynamics or voiceprint
- Graphical passwords
  - Goal: easier to remember?  no need to write down?
- Password managers
  - Examples: LastPass, built into browsers
  - Can have security vulnerabilities…
- Two-factor authentication
  - Leverage phone (or other device) for authentication

# Multi-Factor Authentication



1.

Sign in with your Google Account

Email: hikingfan@gmail.com

ex: pat@example.com

Password: •••••••••••••

☑ Stay signed in

Can't access your account?

2.

Google accounts

**Enter verification code**

To verify your identity on this computer, enter the verification code generated by your mobile application.

**Enter code:** 466453

☑ Remember verification for this computer for 30 days.

Other ways to get a verification code »

Google Authenticator

966286

wileyc@acme.com

Turn on Login Approvals

**What is Login Approvals?**

Login Approvals is a security feature that requires you to enter a code that we text to your phone when you log in from an unrecognized computer. You can enable this feature in a few simple steps.

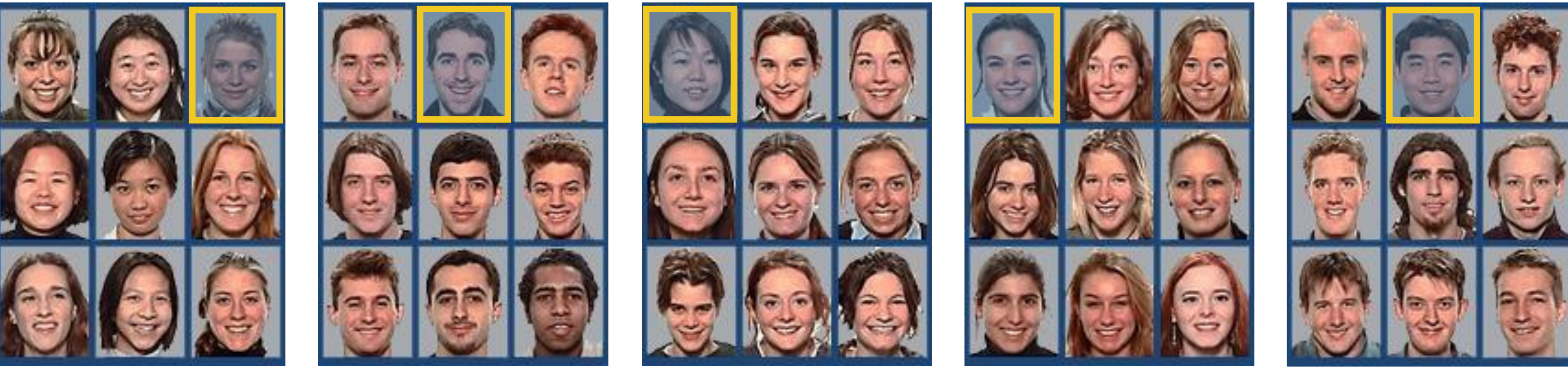
If you ever lose access to your phone, you can always return to a previously-recognized computer to regain access to your account.

**Note: You'll need to have your mobile phone with you to complete this process.**

# FIDO + Hardware Two Factors

# Graphical Passwords

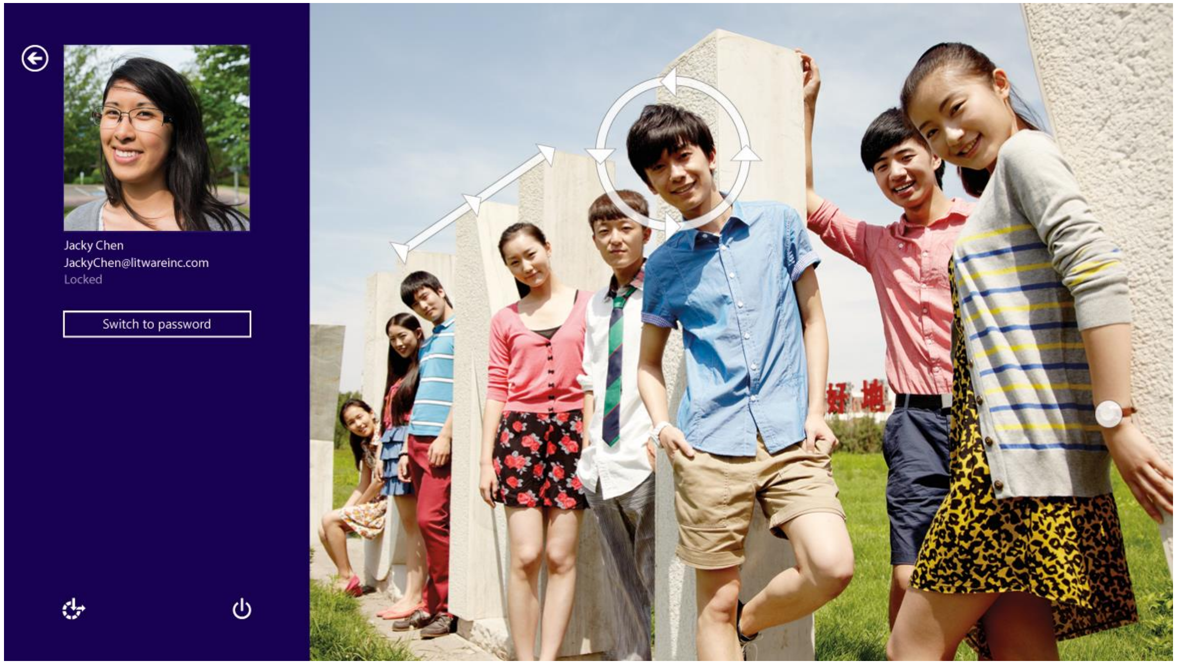
- Many variants… one example: Passfaces
  - Assumption: easy to recall faces



  - Problem: to make passwords easy to remember, users choose predictable faces

# Graphical Passwords

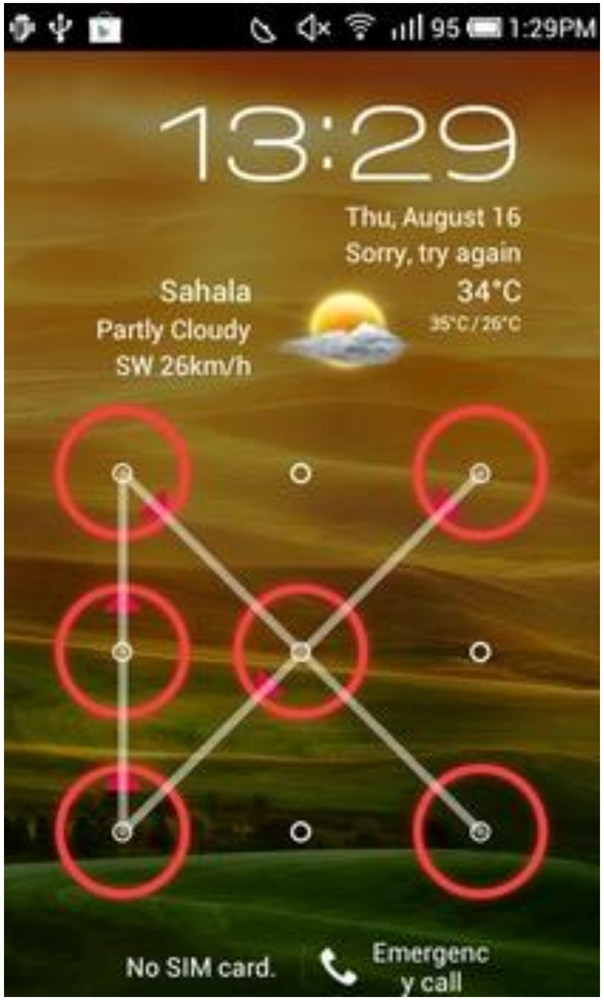
- Another variant: draw on the image (Windows 8)



Jacky Chen
JackyChen@litwareinc.com
Locked

- Problem: users choose predictable points/lines

# Unlock Patterns



- Problems:
  - Predictable patterns (sound familiar by now??)
  - Smear patterns
  - Side channels: apps can use accelerometer and gyroscope to extract pattern!

# What About Biometrics?

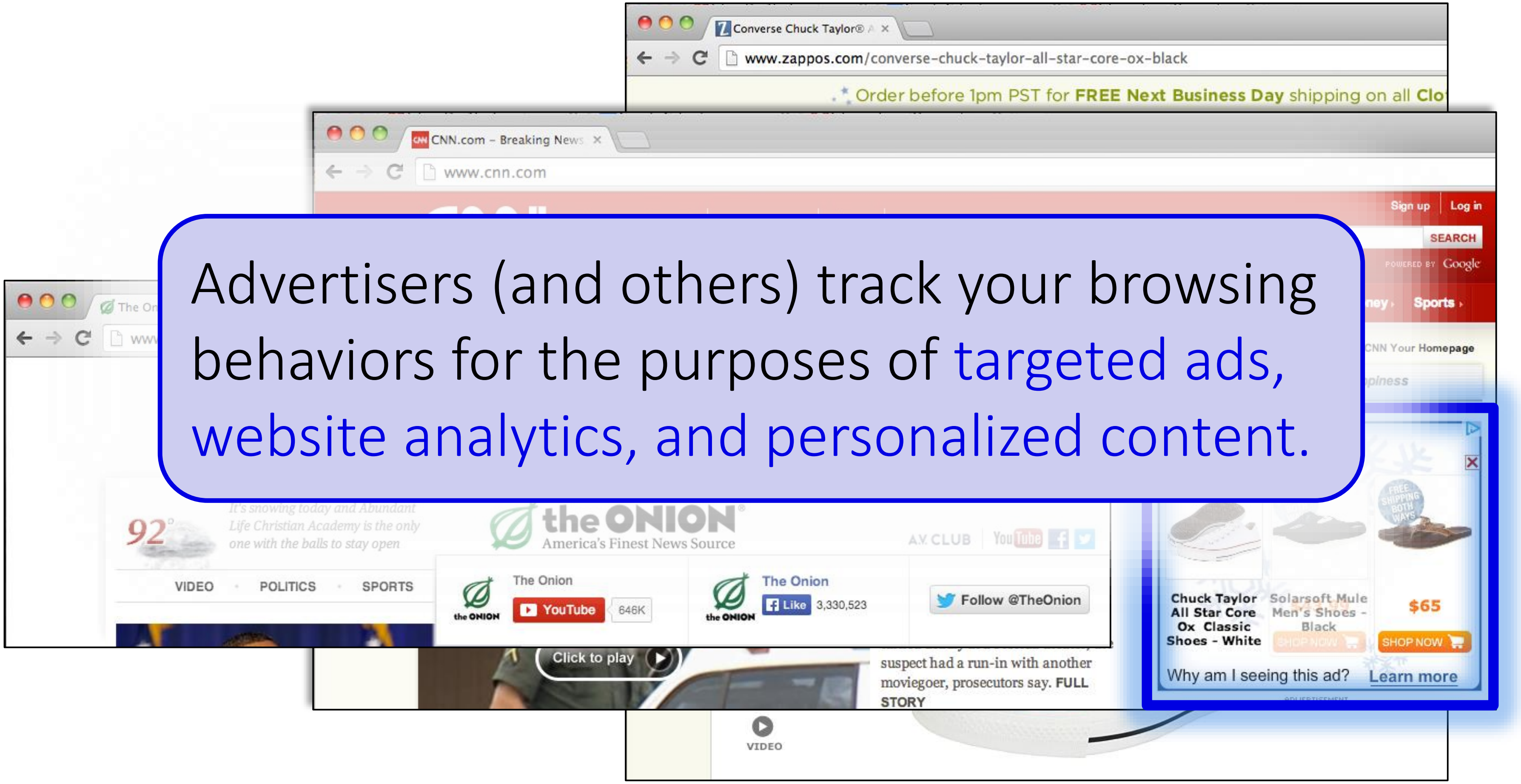
- Authentication: **What you are**
- Unique identifying characteristics to authenticate user or create credentials
  - Biological and physiological: Fingerprints, iris scan
  - Behaviors characteristics - how perform actions: Handwriting, typing, gait
- Advantages:
  - Nothing to remember
  - Passive
  - Can’t share (generally)
  - With perfect accuracy, could be fairly unique

# Issues with Biometrics

- Private, but not secret
  - Maybe encoded on the back of an ID card?
  - Maybe encoded on your glass, door handle, ...
  - Sharing between multiple systems?
- Revocation is difficult (impossible?)
  - Sorry, your iris has been compromised, please create a new one...
- Physically identifying
  - Soda machine to cross-reference fingerprint with DMV?
- Birthday paradox
  - With false accept rate of 1 in a million, probability of false match is above 50% with only 1609 samples

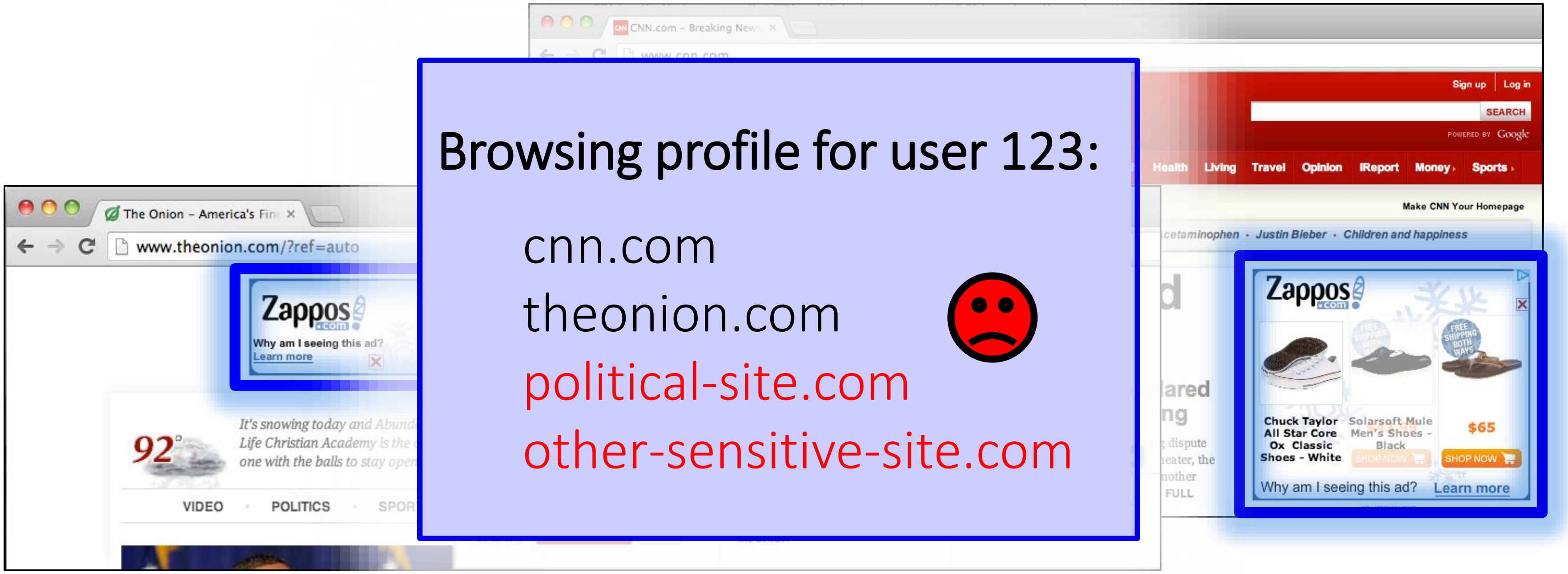
# Web Tracking

# Ads That Follow You


Converse Chuck Taylor®
www.zappos.com/converse-chuck-taylor-all-star-core-ox-black
Order before 1pm PST for FREE Next Business Day shipping on all Clo
CNN.com – Breaking News
www.cnn.com
Sign up
Log in
SEARCH
POWERED BY Google
Sports
CNN Your Homepage
The On
www
92°
It's snowing today and Abundant Life Christian Academy is the only one with the balls to stay open
the ONION
America's Finest News Source
A.V. CLUB
VIDEO
POLITICS
SPORTS
The Onion
YouTube
646K
The Onion
Like
3,330,523
Follow @TheOnion
Click to play
suspect had a run-in with another moviegoer, prosecutors say. FULL STORY
VIDEO
FREE SHIPPING BOTH WAYS
Chuck Taylor All Star Core Ox Classic Shoes - White
Solarsoft Mule Men's Shoes - Black
$65
SHOP NOW
Why am I seeing this ad?
Learn more

Advertisers (and others) track your browsing behaviors for the purposes of targeted ads, website analytics, and personalized content.

# Third-Party Web Tracking

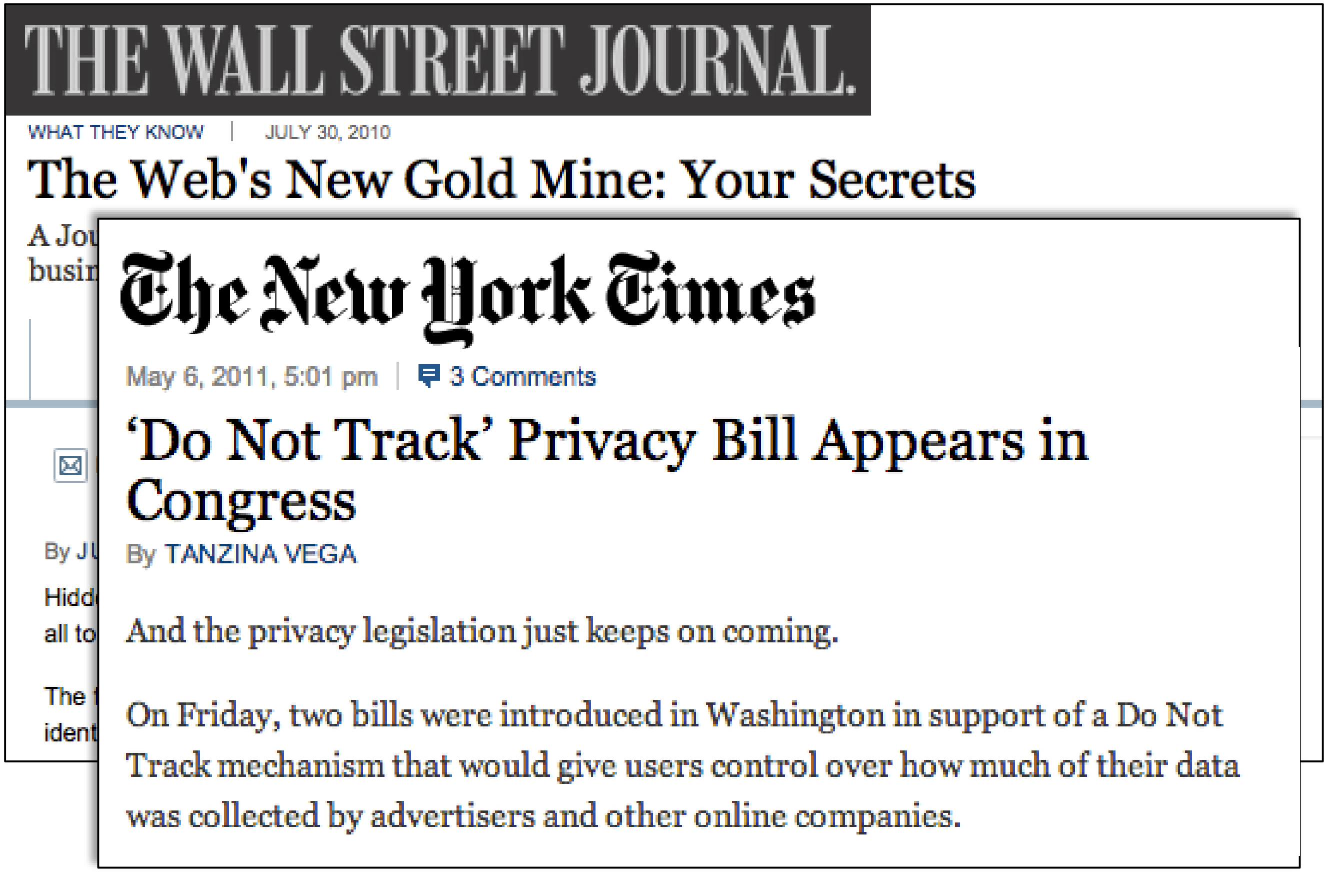

CNN.com – Breaking News
www.cnn.com
Sign up
Log in
SEARCH
POWERED BY Google
Health
Living
Travel
Opinion
iReport
Money
Sports
Make CNN Your Homepage
Acetaminophen · Justin Bieber · Children and happiness
Zappos.com
Chuck Taylor All Star Core Ox Classic Shoes - White
Solarsoft Mule Men's Shoes - Black
$65
FREE SHIPPING BOTH WAYS
SHOP NOW
Why am I seeing this ad?
Learn more
The Onion – America's Fin
www.theonion.com/?ref=auto
Zappos.com
Why am I seeing this ad?
Learn more
92°
It's snowing today and Abund
Life Christian Academy is the
one with the balls to stay open
VIDEO
POLITICS
SPOR

Browsing profile for user 123:

cnn.com
theonion.com ☹
political-site.com
other-sensitive-site.com

These ads allow **criteo.com** to link your visits between sites, even if you never click on the ads.

# Concerns About Privacy (2010 – 2011)



THE WALL STREET JOURNAL.

WHAT THEY KNOW | JULY 30, 2010

The Web's New Gold Mine: Your Secrets

A Jou
busin

By JU

Hidd
all to

The f
ident

The New York Times

May 6, 2011, 5:01 pm | 3 Comments

'Do Not Track' Privacy Bill Appears in Congress

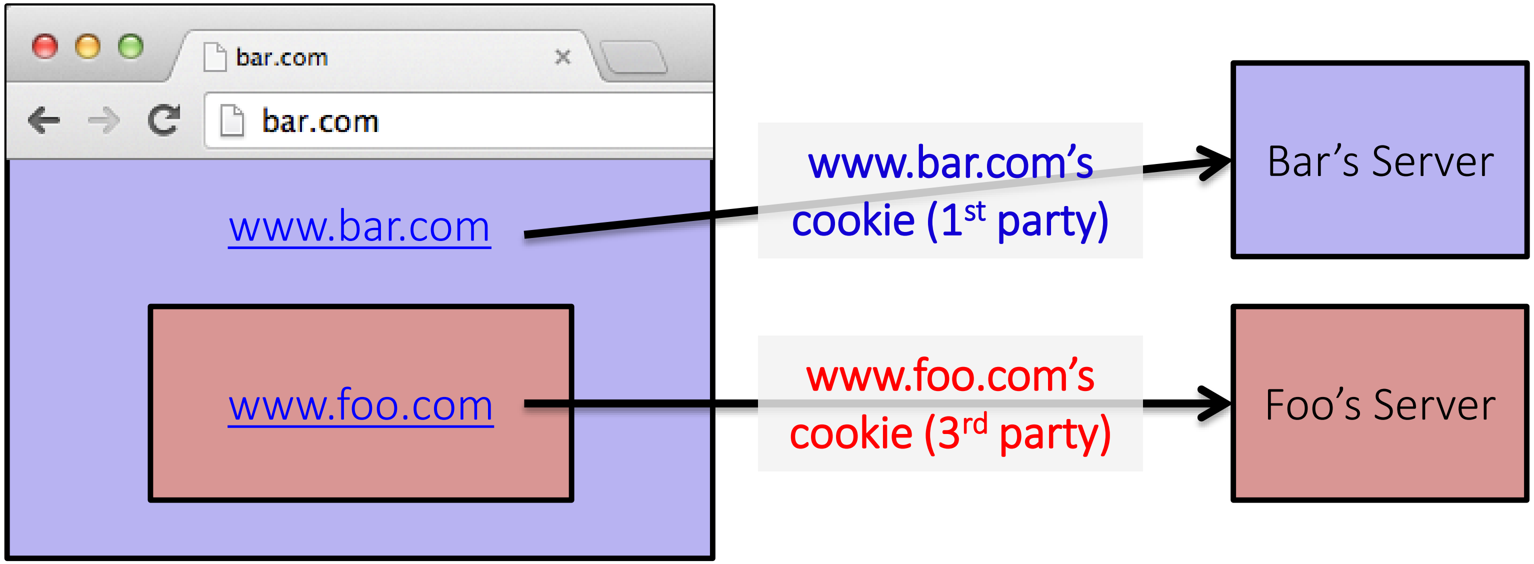
By TANZINA VEGA

And the privacy legislation just keeps on coming.

On Friday, two bills were introduced in Washington in support of a Do Not Track mechanism that would give users control over how much of their data was collected by advertisers and other online companies.

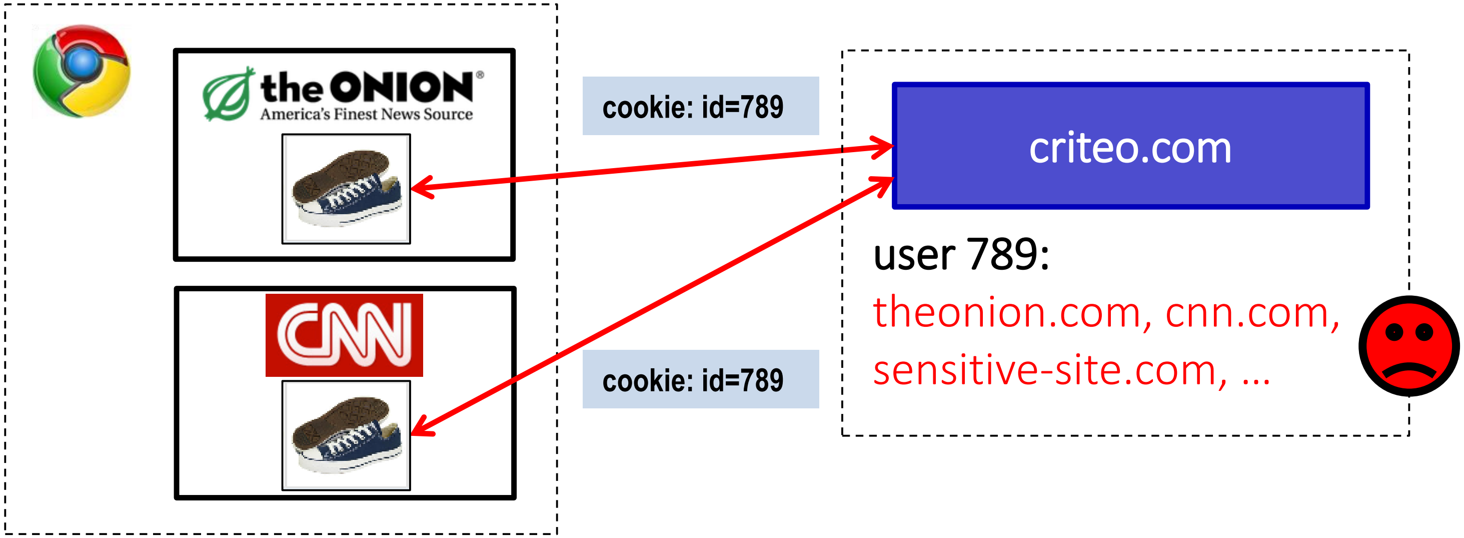
# First and Third Parties

- First-party cookie: belongs to top-level domain.
- Third-party cookie: belongs to domain of embedded content (such as image, iframe).


bar.com
bar.com
www.bar.com
www.foo.com
www.bar.com's cookie (1st party)
www.foo.com's cookie (3rd party)
Bar's Server
Foo's Server

# Anonymous Tracking

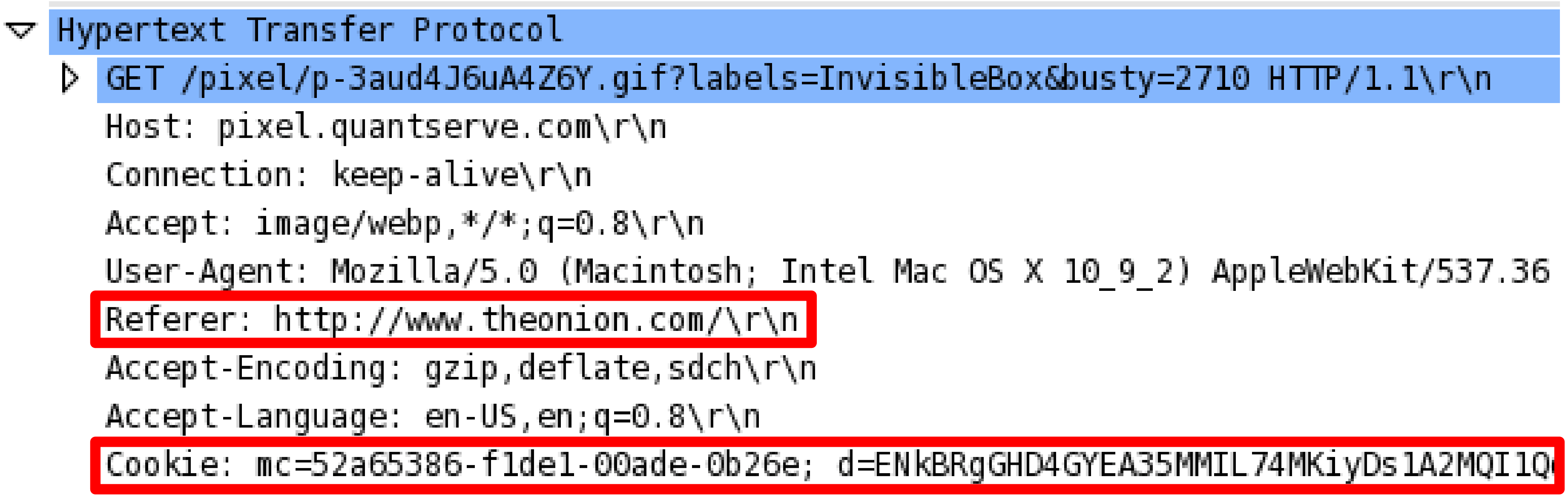
Trackers included in other sites use third-party cookies containing unique identifiers to create browsing profiles.



user 789:
theonion.com, cnn.com,
sensitive-site.com, ...

# Basic Tracking Mechanisms

- Tracking requires:
  (1) re-identifying a user.
  (2) communicating id + visited site back to tracker.



```
Hypertext Transfer Protocol
  GET /pixel/p-3aud4J6uA4Z6Y.gif?labels=InvisibleBox&busty=2710 HTTP/1.1\r\n
  Host: pixel.quantserve.com\r\n
  Connection: keep-alive\r\n
  Accept: image/webp,*/*;q=0.8\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36
  Referer: http://www.theonion.com/\r\n
  Accept-Encoding: gzip,deflate,sdch\r\n
  Accept-Language: en-US,en;q=0.8\r\n
  Cookie: mc=52a65386-f1de1-00ade-0b26e; d=ENkBRgGHD4GYEA35MMIL74MKiyDs1A2MQI1Q
```

# Tracking Technologies

- HTTP Cookies
- HTTP Auth
- HTTP Etags
- Content cache
- IE userData
- HTML5 protocol and content handlers
- HTML5 storage

- Flash cookies
- Silverlight storage
- TLS session ID & resume
- Browsing history
- window.name
- HTTP STS
- DNS cache

- "Zombie" cookies that respawn (http://samy.pl/evercookie)

# Fingerprinting Web Browsers

- User agent
- HTTP ACCEPT headers
- Browser plug-ins
- MIME support
- Clock skew

- Installed fonts
- Cookies enabled?
- Browser add-ons
- Screen resolution
- HTML5 canvas (differences in graphics SW/HW!)