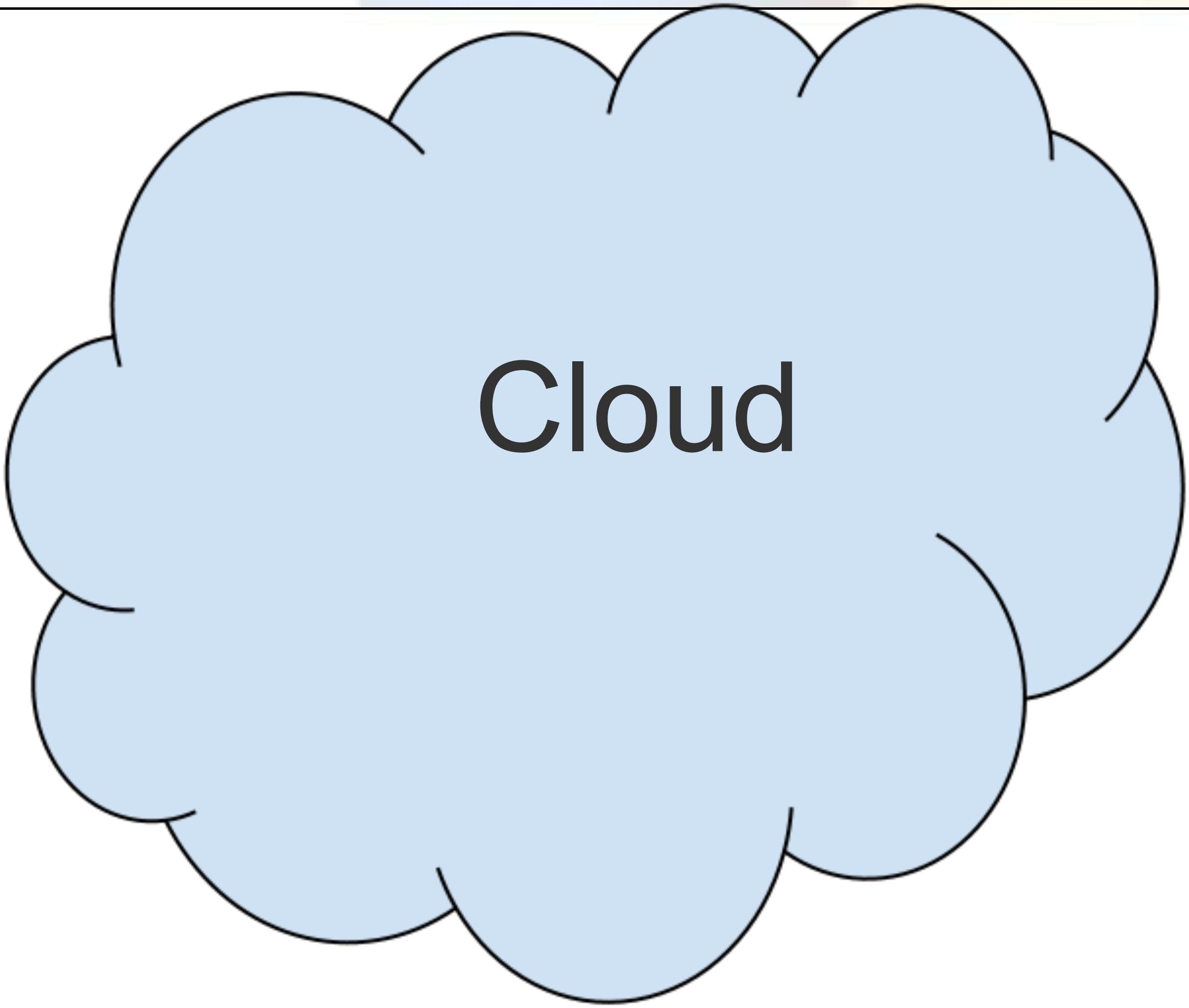
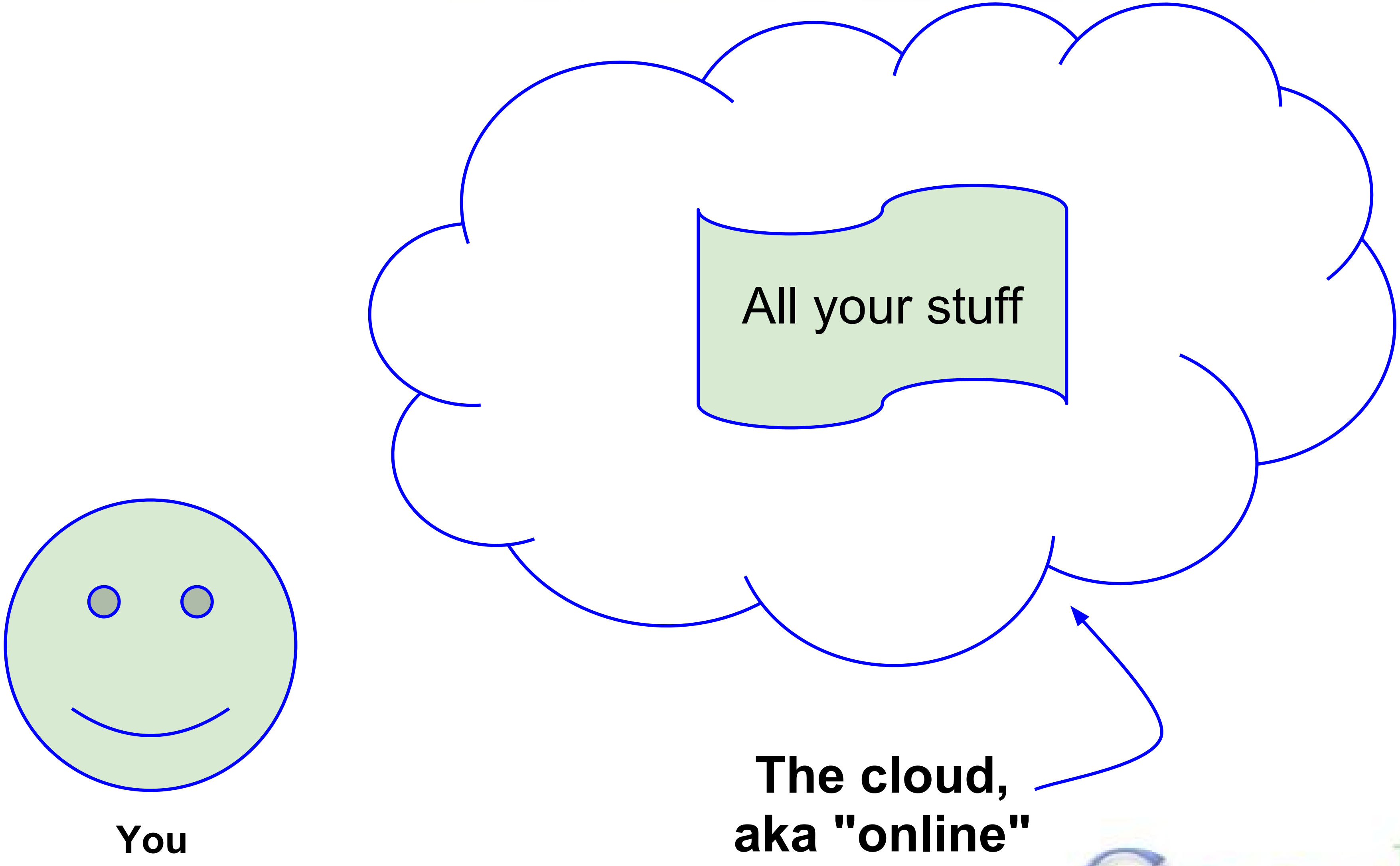
Security and Privacy at Scale

Geetanjali Sampemane
geta@google.com



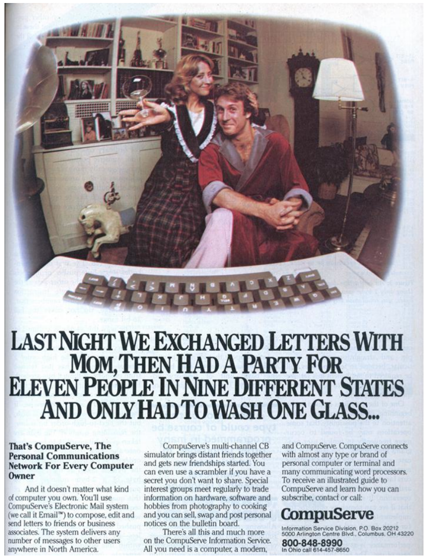
Cloud

All your stuff is online



Cloud v0?

- Shared multi-user computing: Multics, Unix, VMS, ...
- Online user communities: Plato, BBS, AOL...
- Large-scale scientific computing: supercomputers, grids, high-performance clusters,...
- "Thin clients"
- Utility computing



LAST NIGHT WE EXCHANGED LETTERS WITH MOM, THEN HAD A PARTY FOR ELEVEN PEOPLE IN NINE DIFFERENT STATES AND ONLY HAD TO WASH ONE GLASS...

That's CompuServe, The Personal Communications Network For Every Computer Owner

And it doesn't matter what kind of computer you own. You'll use CompuServe's Electronic Mail system (we call it Email™) to compose, edit and send letters to friends or business associates. The system delivers any number of messages to other users anywhere in North America.

CompuServe's multi-channel CB simulator brings distant friends together and gets new friendships started. You can even use a scrambler if you have a secret you don't want to share. Special interest groups meet regularly to trade information on hardware, software and hobbies from photography to cooking and you can sell, swap and post personal notices on the bulletin board.

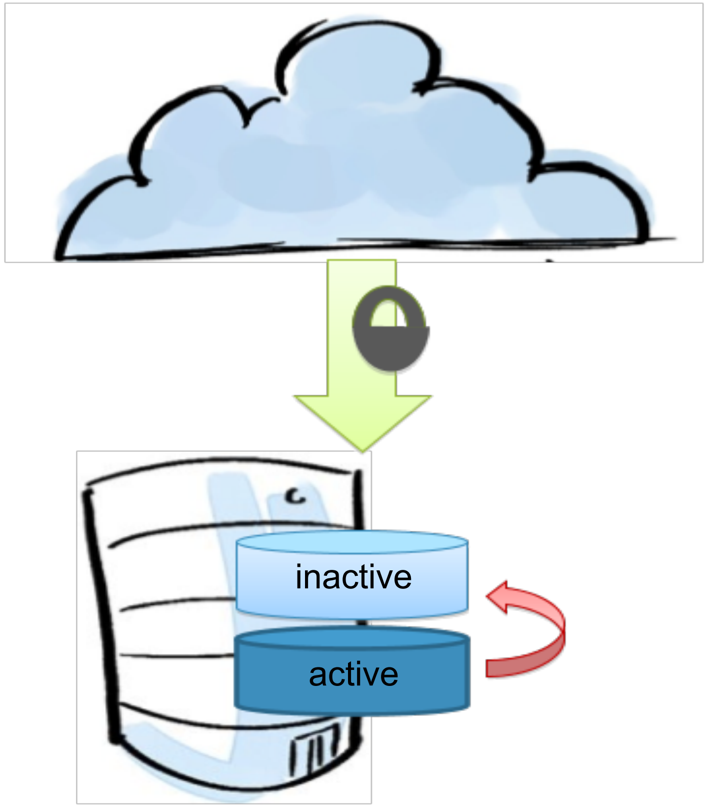
There's all this and much more on the CompuServe Information Service. All you need is a computer, a modem, and CompuServe. CompuServe connects with almost any type or brand of personal computer or terminal and many communicating word processors. To receive an illustrated guide to CompuServe and learn how you can subscribe, contact or call:

CompuServe

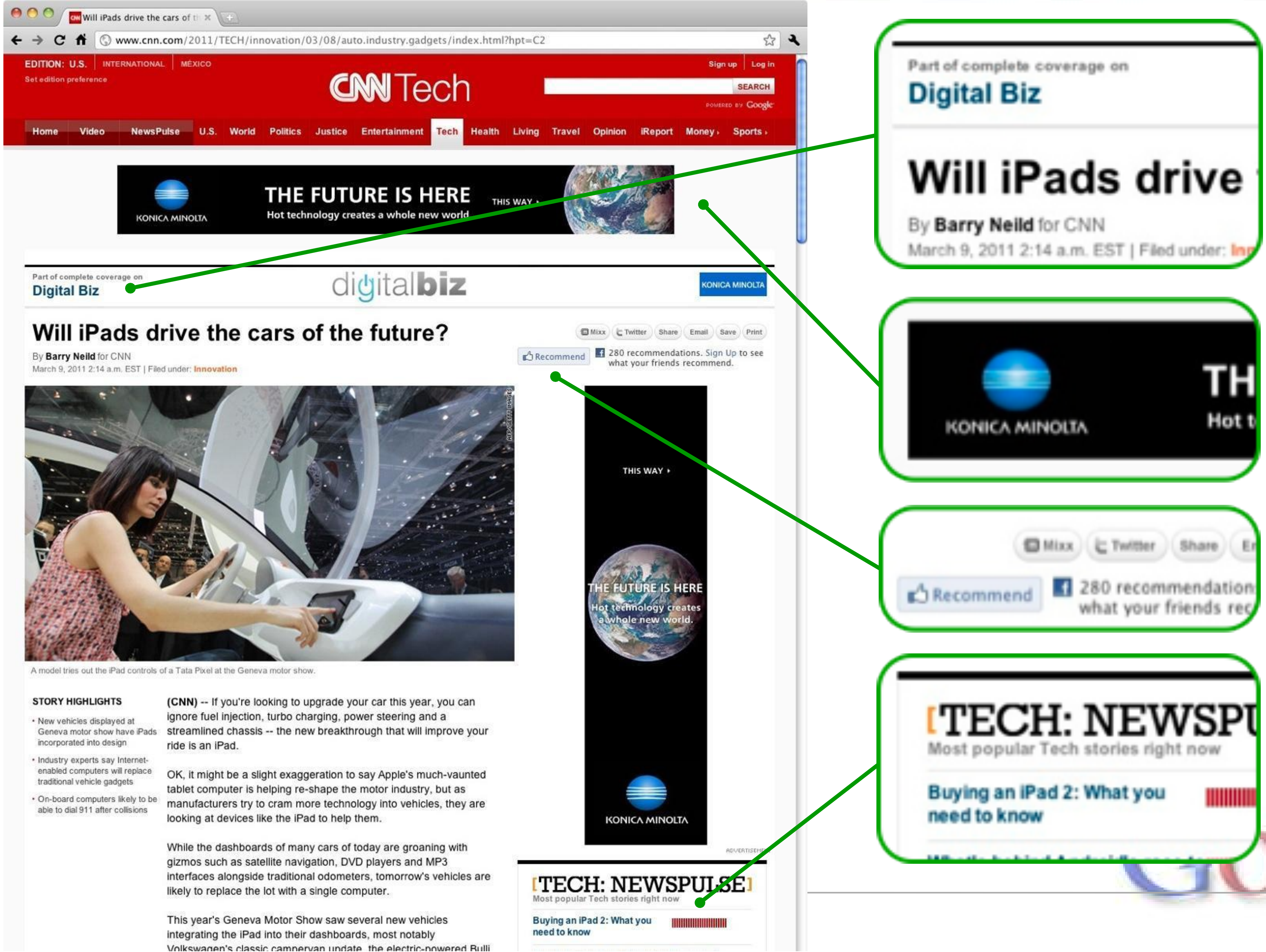
Information Service Division, P.O. Box 20212
5000 Arlington Centre Blvd., Columbus, OH 43220
800-848-8990
In Ohio call 614-457-8650

Cloud characteristics

- High availability, no planned downtime
- Dynamic software on clients and servers
- Store, process and combine user data
- Users expect anytime/anywhere access



The Cloud has many Parties



Part of complete coverage on
Digital Biz

Will iPads drive the cars of the future?

280 recommendations. Sign Up to see what your friends recommend.

By **Barry Neild** for CNN
March 9, 2011 2:14 a.m. EST | Filed under: Innovation

A model tries out the iPad controls of a Tata Pixel at the Geneva motor show.

STORY HIGHLIGHTS

- New vehicles displayed at Geneva motor show have iPads incorporated into design
- Industry experts say Internet-enabled computers will replace traditional vehicle gadgets
- On-board computers likely to be able to dial 911 after collisions

(CNN) -- If you're looking to upgrade your car this year, you can ignore fuel injection, turbo charging, power steering and a streamlined chassis -- the new breakthrough that will improve your ride is an iPad.

OK, it might be a slight exaggeration to say Apple's much-vaunted tablet computer is helping re-shape the motor industry, but as manufacturers try to cram more technology into vehicles, they are looking at devices like the iPad to help them.

While the dashboards of many cars of today are groaning with gizmos such as satellite navigation, DVD players and MP3 interfaces alongside traditional odometers, tomorrow's vehicles are likely to replace the lot with a single computer.

This year's Geneva Motor Show saw several new vehicles integrating the iPad into their dashboards, most notably Volkswagen's classic campervan update, the electric-powered Bulli

[TECH: NEWSPULSE]
Most popular Tech stories right now

Buying an iPad 2: What you need to know

Content provider

Ad network

Social sharing

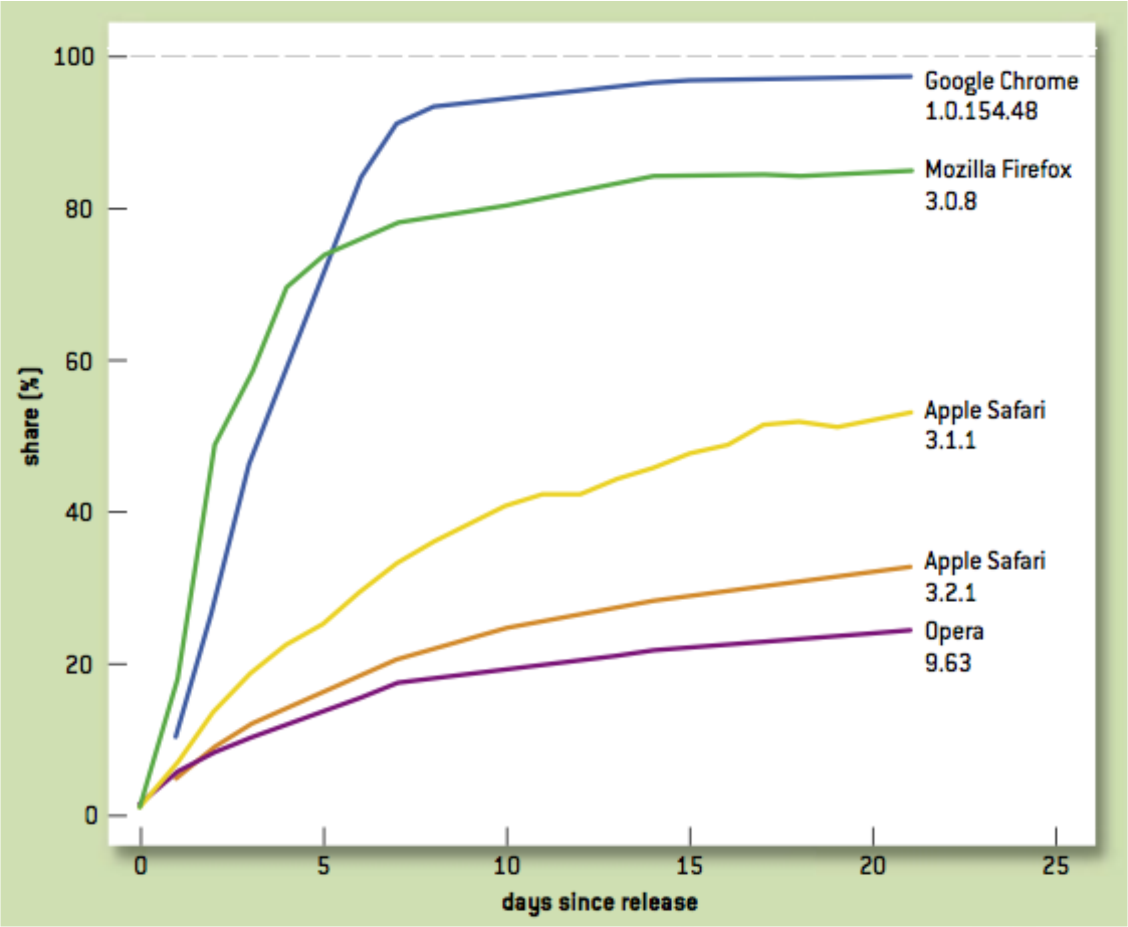
Affiliated sites

Has to work at scale.

- New types of services
- Hundreds of millions of users
- All over the world
- Fast

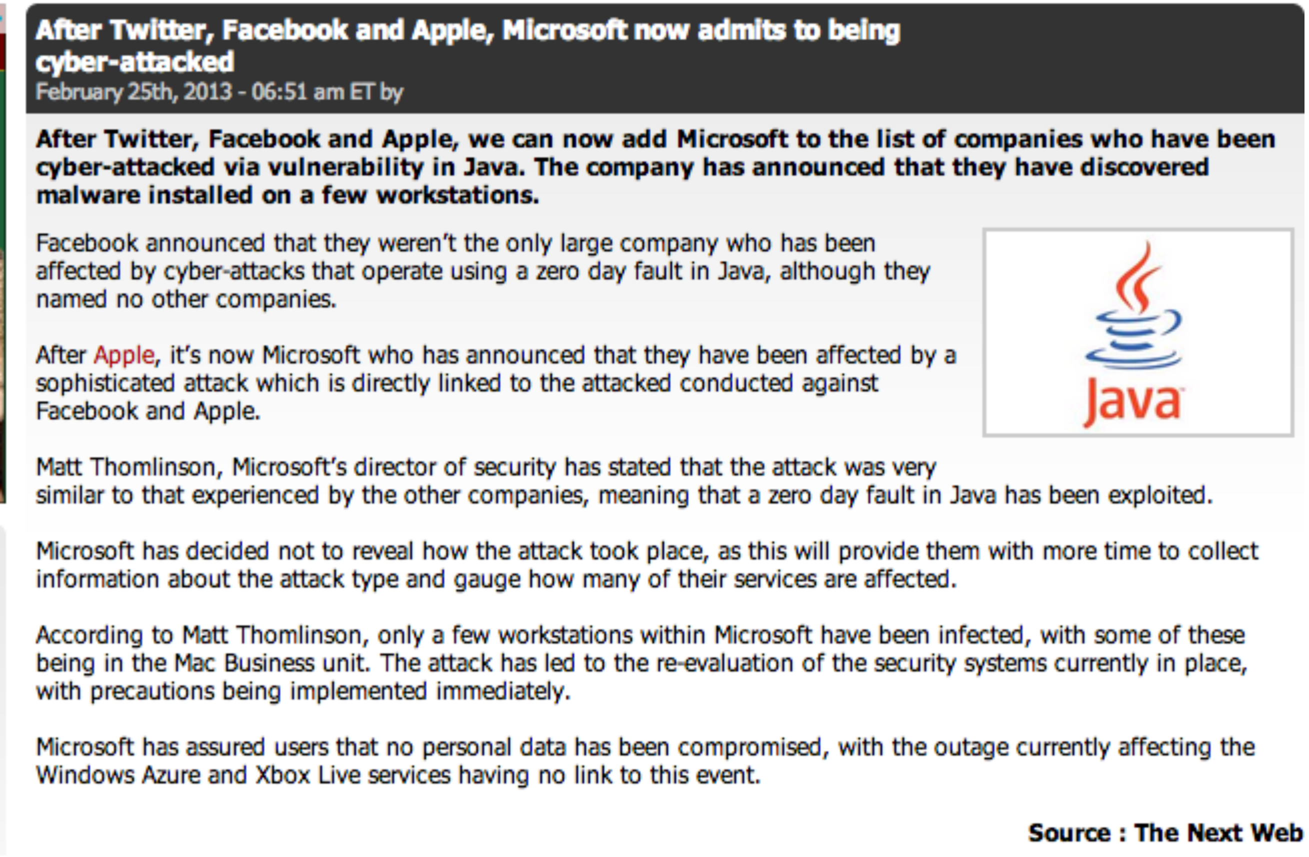
New opportunities

- Fast software updates
- Use data for defence
- Scale
- Automate management



New challenges

- Big target: attractive to sophisticated attackers
- No downtime
- Scale
- Usability



After Twitter, Facebook and Apple, Microsoft now admits to being cyber-attacked

February 25th, 2013 - 06:51 am ET by

After Twitter, Facebook and Apple, we can now add Microsoft to the list of companies who have been cyber-attacked via vulnerability in Java. The company has announced that they have discovered malware installed on a few workstations.

Facebook announced that they weren't the only large company who has been affected by cyber-attacks that operate using a zero day fault in Java, although they named no other companies.

After Apple, it's now Microsoft who has announced that they have been affected by a sophisticated attack which is directly linked to the attacked conducted against Facebook and Apple.

Matt Thomlinson, Microsoft's director of security has stated that the attack was very similar to that experienced by the other companies, meaning that a zero day fault in Java has been exploited.

Microsoft has decided not to reveal how the attack took place, as this will provide them with more time to collect information about the attack type and gauge how many of their services are affected.

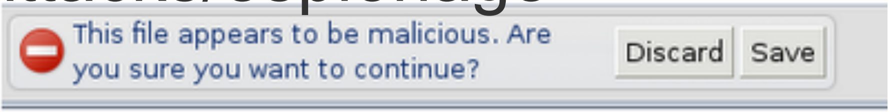
According to Matt Thomlinson, only a few workstations within Microsoft have been infected, with some of these being in the Mac Business unit. The attack has led to the re-evaluation of the security systems currently in place, with precautions being implemented immediately.

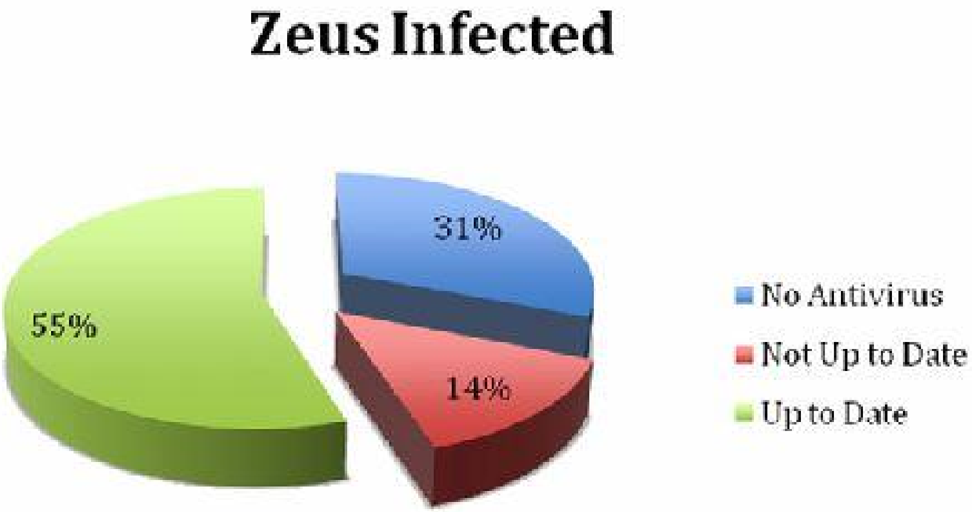
Microsoft has assured users that no personal data has been compromised, with the outage currently affecting the Windows Azure and Xbox Live services having no link to this event.

Source : The Next Web

Threats we see

1. Authentication
2. Malware
3. Attacks on SSL/network
4. Vulnerabilities in Web Apps
5. Insider attacks/espionage

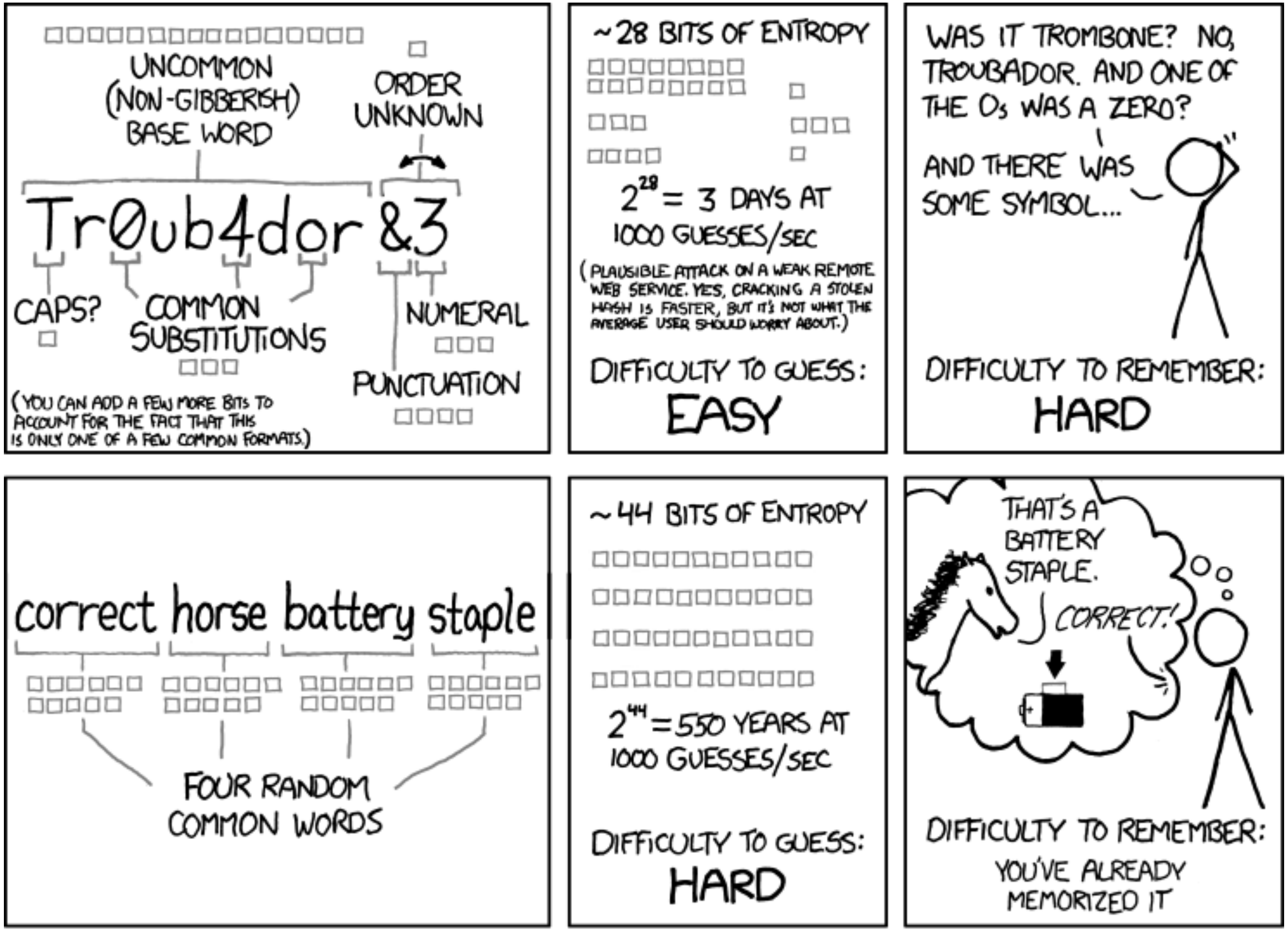

This file appears to be malicious. Are you sure you want to continue?



User authentication is hard!

"On the Internet, nobody knows you're a dog."

Passwords have problems

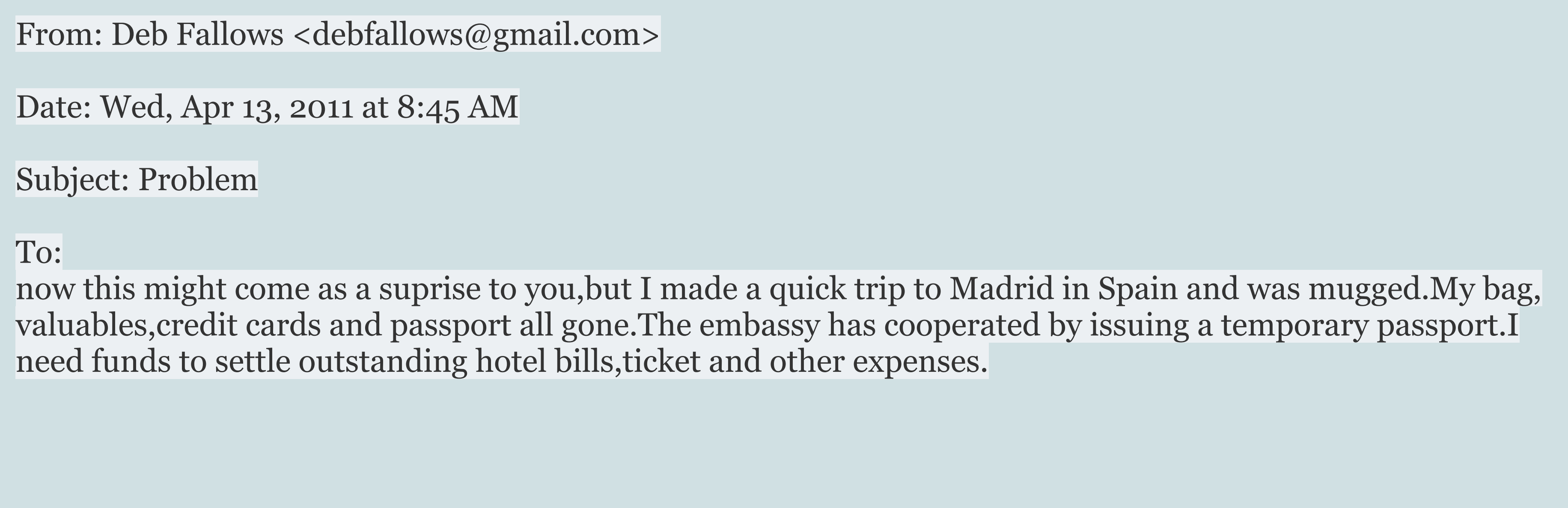

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Most common attacks on passwords

- Phishing attacks, keyloggers, server compromise
- Password re-use
- Security Q&A or secondary email

Account hijackings: statistically small, but devastating to user (tens of thousands per day)



From: Deb Fallows <debfallows@gmail.com>

Date: Wed, Apr 13, 2011 at 8:45 AM

Subject: Problem

To:
now this might come as a suprise to you,but I made a quick trip to Madrid in Spain and was mugged.My bag, valuables,credit cards and passport all gone.The embassy has cooperated by issuing a temporary passport.I need funds to settle outstanding hotel bills,ticket and other expenses.

The Official Google Blog

Insights from Googlers into our products, technology, and the Google culture.

June 2011

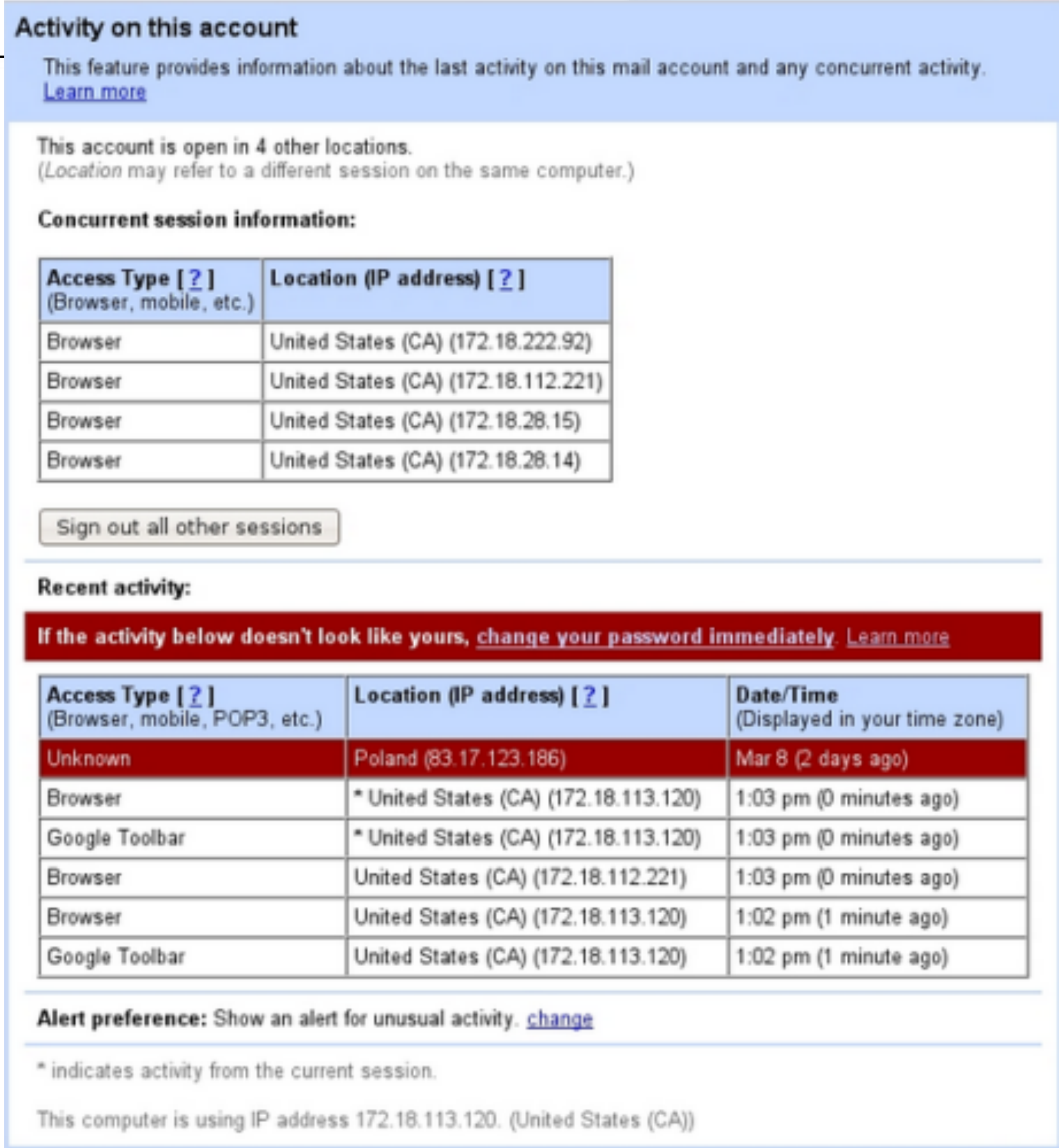
...

Bad actors take advantage of the fact that most people aren’t that tech savvy—hijacking accounts by using malware and phishing scams that trick users into sharing their passwords, or by using passwords obtained by hacking other websites. Most account hijackings are not very targeted; they are designed to steal identities, acquire financial data or send spam. But some attacks are targeted at specific individuals.

Through the strength of our cloud-based security and abuse detection systems, we recently uncovered a campaign to collect user passwords, likely through phishing. This campaign, which appears to originate from Jinan, China, affected what seem to be the **personal Gmail accounts of hundreds of users including, among others, senior U.S. government officials**, Chinese political activists, officials in several Asian countries (predominantly South Korea), military personnel and journalists.

...

Account heuristics



Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. Learn more

This account is open in 4 other locations.
(*Location* may refer to a different session on the same computer.)

Concurrent session information:

Access Type [?] (Browser, mobile, etc.)	**Location (IP address) [?]**
Browser	United States (CA) (172.18.222.92)
Browser	United States (CA) (172.18.112.221)
Browser	United States (CA) (172.18.28.15)
Browser	United States (CA) (172.18.28.14)

Recent activity:

If the activity below doesn't look like yours, change your password immediately. Learn more

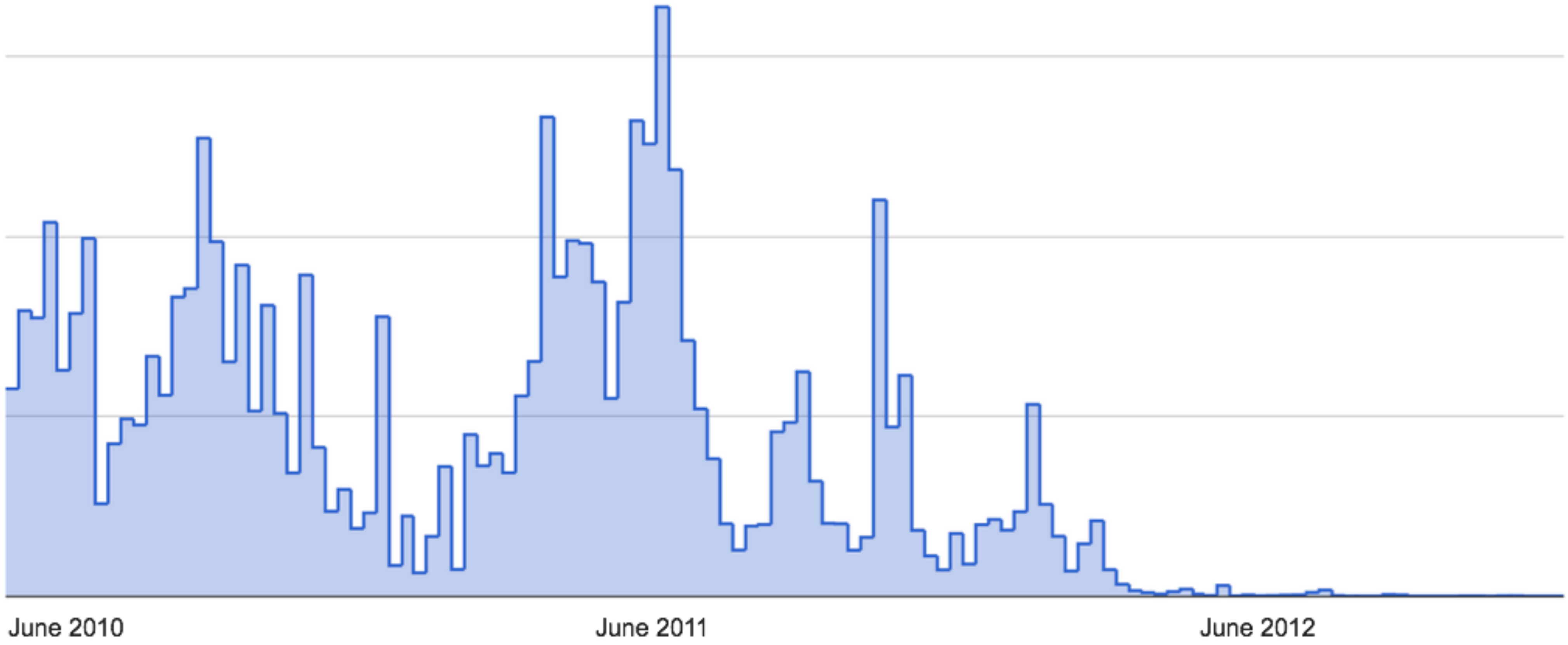
Access Type [?] (Browser, mobile, POP3, etc.)	**Location (IP address) [?]**	**Date/Time** (Displayed in your time zone)
Unknown	Poland (83.17.123.186)	Mar 8 (2 days ago)
Browser	* United States (CA) (172.18.113.120)	1:03 pm (0 minutes ago)
Google Toolbar	* United States (CA) (172.18.113.120)	1:03 pm (0 minutes ago)
Browser	United States (CA) (172.18.112.221)	1:03 pm (0 minutes ago)
Browser	United States (CA) (172.18.113.120)	1:02 pm (1 minute ago)
Google Toolbar	United States (CA) (172.18.113.120)	1:02 pm (1 minute ago)

Alert preference: Show an alert for unusual activity. change

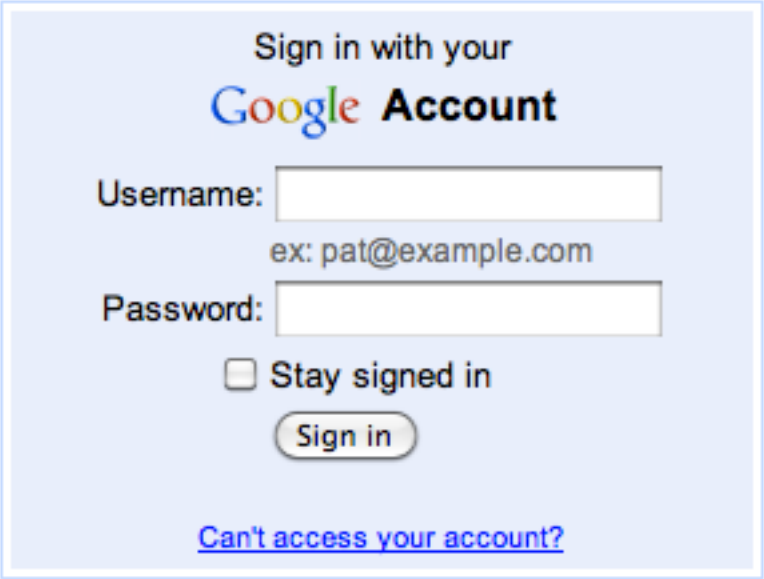
* indicates activity from the current session.

This computer is using IP address 172.18.113.120. (United States (CA))

Prevent spam from legit accounts



Two Step Authentication



Sign in with your

Google Account

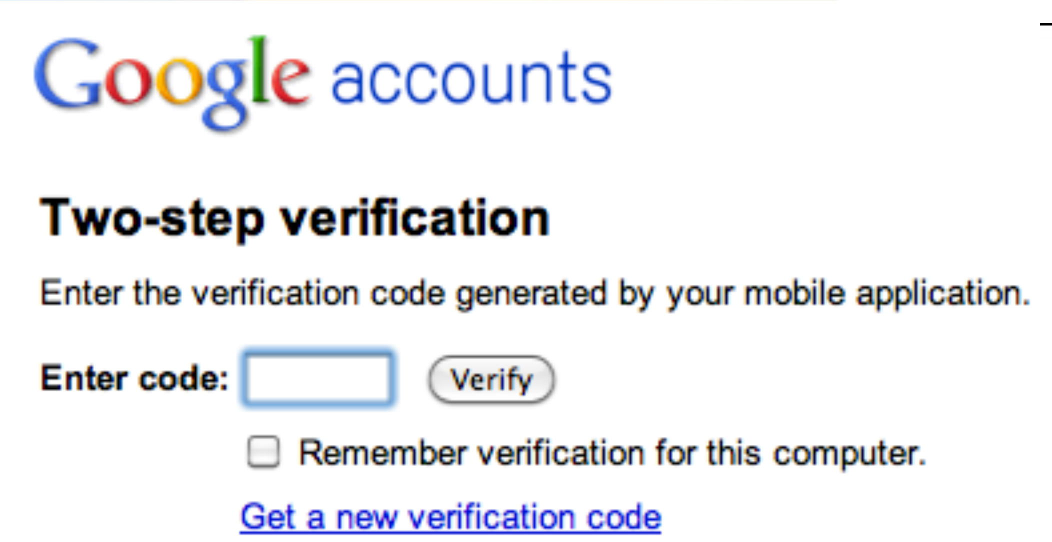
Username:

ex: pat@example.com

Password:

□ Stay signed in

Can't access your account?



Google accounts

Two-step verification

Enter the verification code generated by your mobile application.

Enter code:

□ Remember verification for this computer.

Get a new verification code

- Integrated two factor authentication system built into Google Apps.
- Password+code when signing in from new machine
- SMS or voice call or smartphone app or scratchcodes
- Defends well against password reuse, mildly against phishing and malware.

Device-based authorization

- "Bless" logins from personal/trusted devices
- Device can then access your data
- Use smartphone/smartcard as second channel
- Can revoke this delegation if needed
- Privacy-enhanced client certificates to preserve privacy

Grosse, Eric, and Mayank Upadhyay. "Authentication at Scale." IEEE Security & Privacy, Jan-Feb 2013.

Challenges

- Usability
- Apps which expect passwords
- Attackers use it too!

Parting thoughts

- Cloud provides new threats and new opportunities for security and privacy
- Usability and scale matter
- Experiments with new approach to user authentication

Questions?