CSE 484 (Winter 2011)

User Authentication + Human Aspects

Tadayoshi Kohno

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

Goals for Today

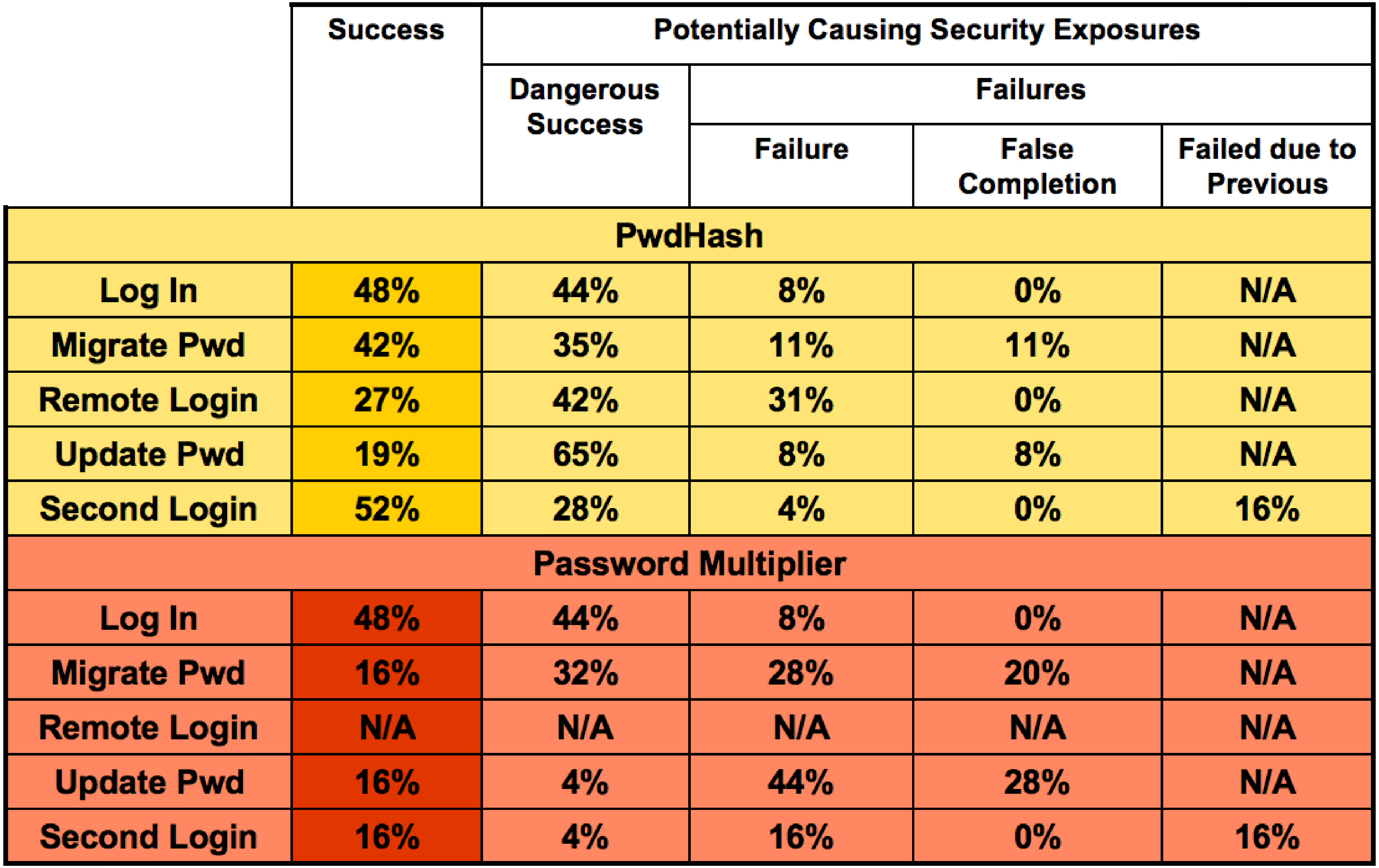
- Continue user authentication
- Other human aspects

- Lab 3: Still plan to announce today.

- Future guest lectures
  - Feb 23: Bryan Parno: Trusted Computing
  - Feb 25: John John: Botnets
  - March 4: Jaeyeon Jung: Mobile Device security/ privacy
  - March 7: Jake Appelbaum: Anonymity and censorship

[Chiasson, van Oorschot, Biddle]

Task completion results



	Success	Potentially Causing Security Exposures			
		Dangerous Success	Failures		
			Failure	False Completion	Failed due to Previous
PwdHash					
Log In	48%	44%	8%	0%	N/A
Migrate Pwd	42%	35%	11%	11%	N/A
Remote Login	27%	42%	31%	0%	N/A
Update Pwd	19%	65%	8%	8%	N/A
Second Login	52%	28%	4%	0%	16%
Password Multiplier					
Log In	48%	44%	8%	0%	N/A
Migrate Pwd	16%	32%	28%	20%	N/A
Remote Login	N/A	N/A	N/A	N/A	N/A
Update Pwd	16%	4%	44%	28%	N/A
Second Login	16%	4%	16%	0%	16%

http://www.scs.carleton.ca/~schiasso/Chiasson_UsenixSecurity2006_PwdManagers.ppt

Problem: Transparency

- Unclear to users whether actions successful or not.
    - Should be obvious when plugin activated.
    - Should be obvious when password protected.
- Users feel that they should be able to know their own password.

Problem: Mental model

Users seemed to have misaligned mental models

- Not understand that one needs to put "@@" before *each* password to be protected.
- Think different passwords generated for each session.
- Think successful when were not.
- Not know to click in field before Alt-P.
- PwdHash: Think passwords unique to them.

HCI is important!

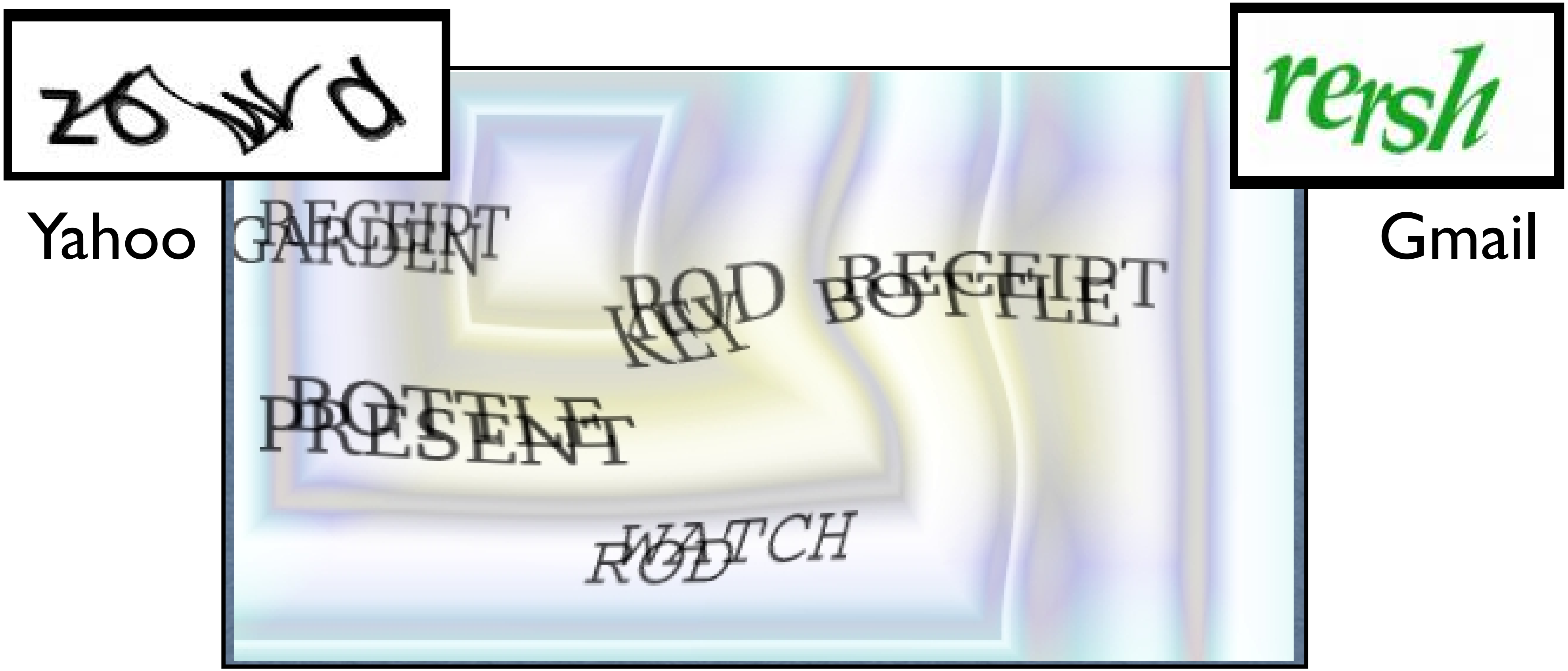
When “nothing works”

- Tendency to try all passwords
  - A poor security choice.
  - May make the use of PwdHash or Password Multiplier *worse* than not using any password manager.
- Usability problem leads to security vulnerabilities.

Human Verification

- Problem:
  - Want to make it hard for spammers to automatically create many free email accounts
  - Want to make it difficult for computers to automatically crawl some data repository
- Need a method for servers to distinguish between
  - Human users
  - Machine users
- Approach: CAPTCHA
  - Completely Automated Public Turing Test to Tell Computers and Humans Apart

CAPTCHAs

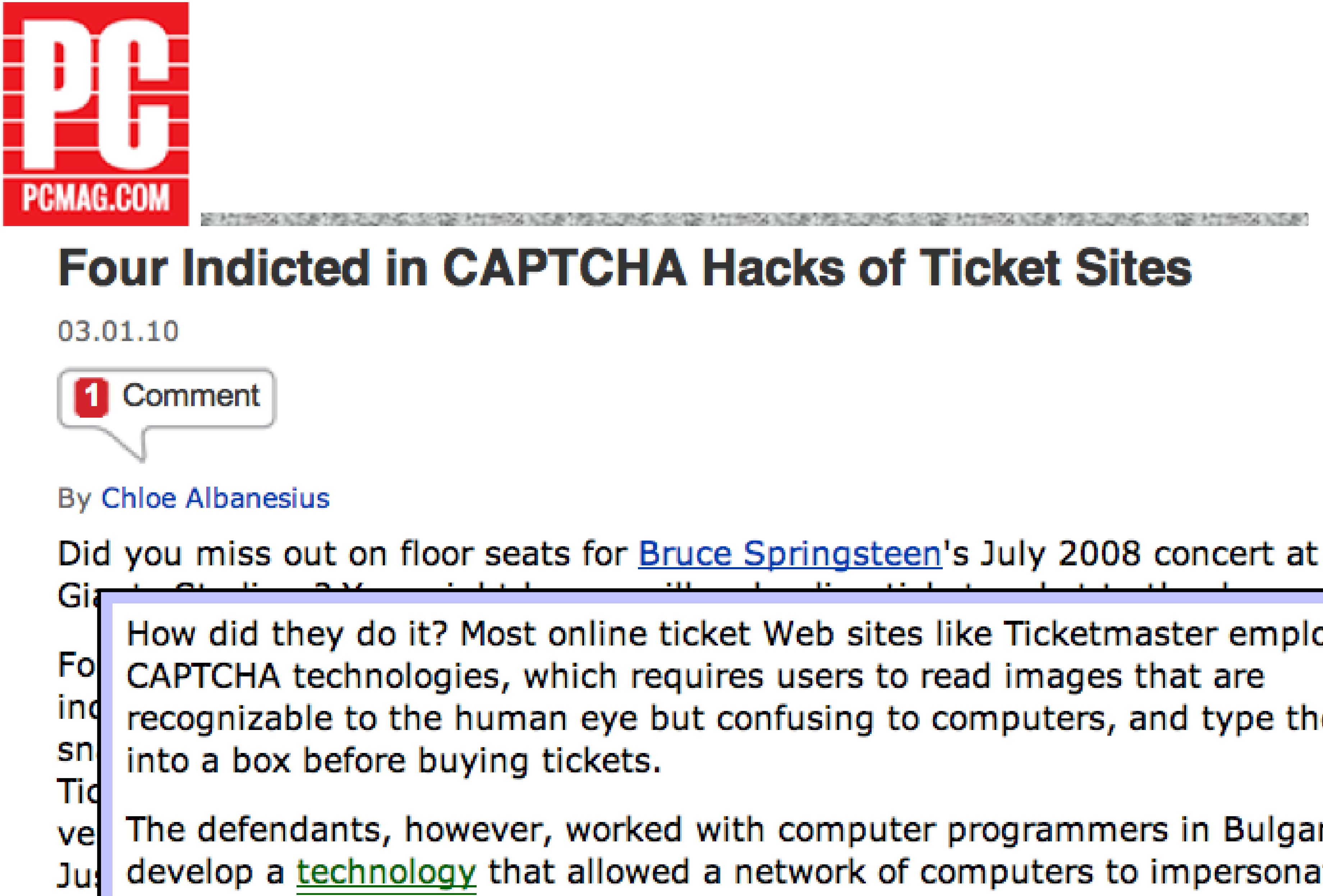


Yahoo

Gmail

captcha.net

Idea: “easy” for humans to read words in this picture, but “hard” for computers



PCMAG.COM

Four Indicted in CAPTCHA Hacks of Ticket Sites

03.01.10

1 Comment

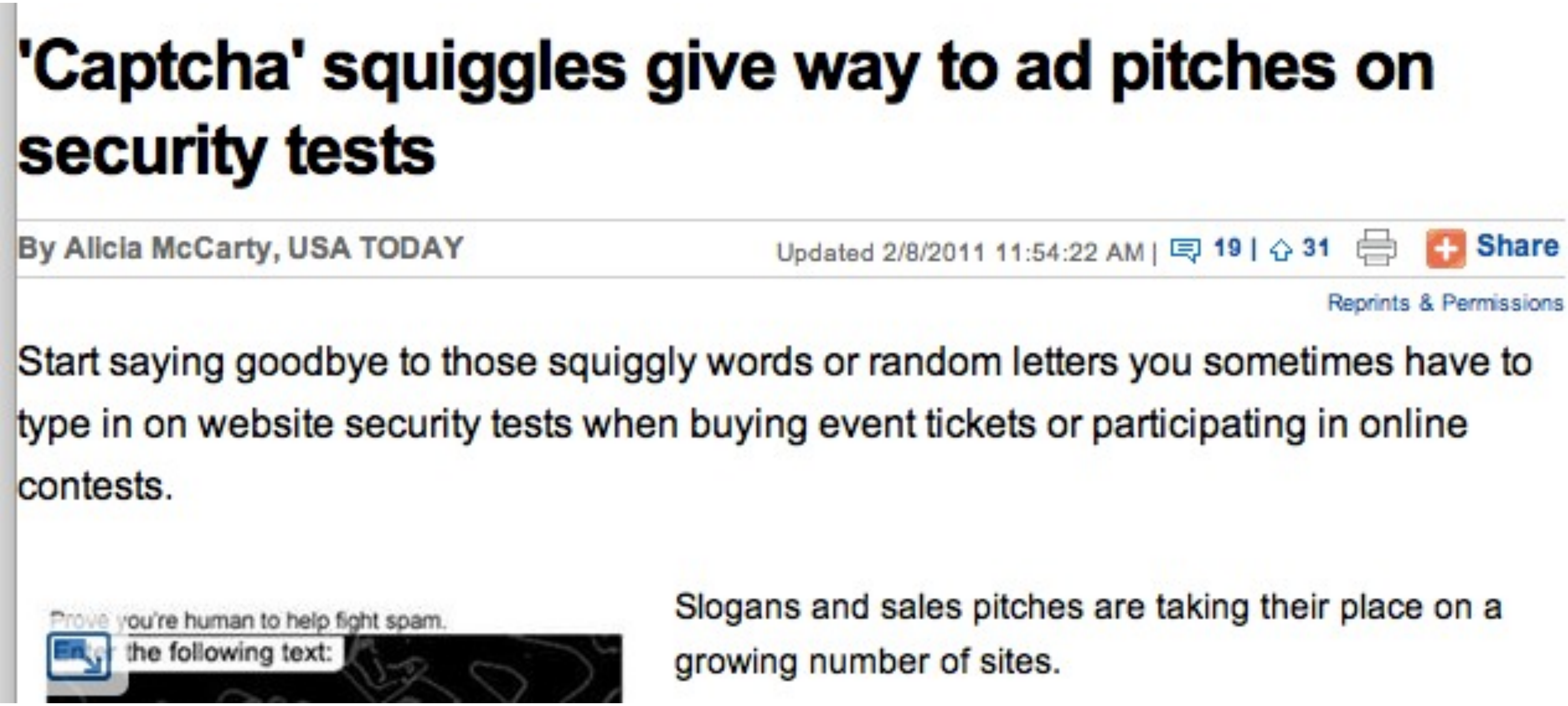
By Chloe Albanesius

Did you miss out on floor seats for Bruce Springsteen's July 2008 concert at Gia

Fo
inc
sn
Tic
ve
Jus

How did they do it? Most online ticket Web sites like Ticketmaster employ CAPTCHA technologies, which requires users to read images that are recognizable to the human eye but confusing to computers, and type them into a box before buying tickets.

The defendants, however, worked with computer programmers in Bulgaria to develop a technology that allowed a network of computers to impersonate individual visitors to online ticket vendors. The ticket vendors did not immediately recognize the purchases as computer-generated, so these "CAPTCHA Bots" let Wiseguy Tickets to flood ticket vendors as soon as tickets went on sale and purchase tickets faster than any human.



'Captcha' squiggles give way to ad pitches on security tests

By Alicia McCarty, USA TODAY

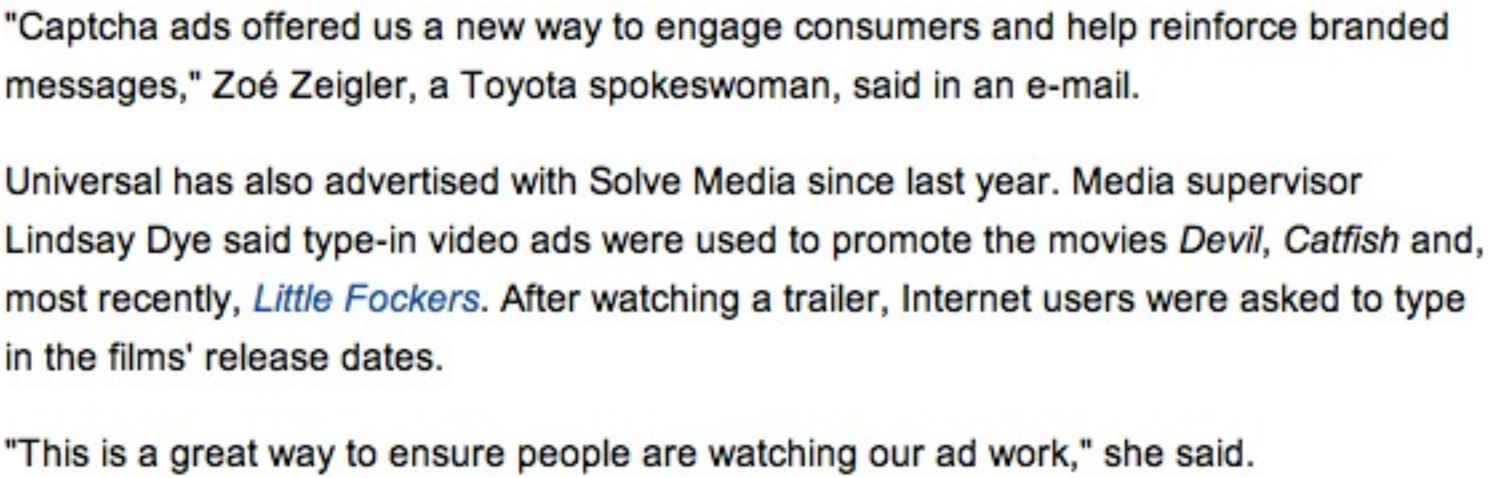
Updated 2/8/2011 11:54:22 AM | 19 | 31 Share

Reprints & Permissions

Start saying goodbye to those squiggly words or random letters you sometimes have to type in on website security tests when buying event tickets or participating in online contests.

Prove you're human to help fight spam.
Enter the following text:

Slogans and sales pitches are taking their place on a growing number of sites.



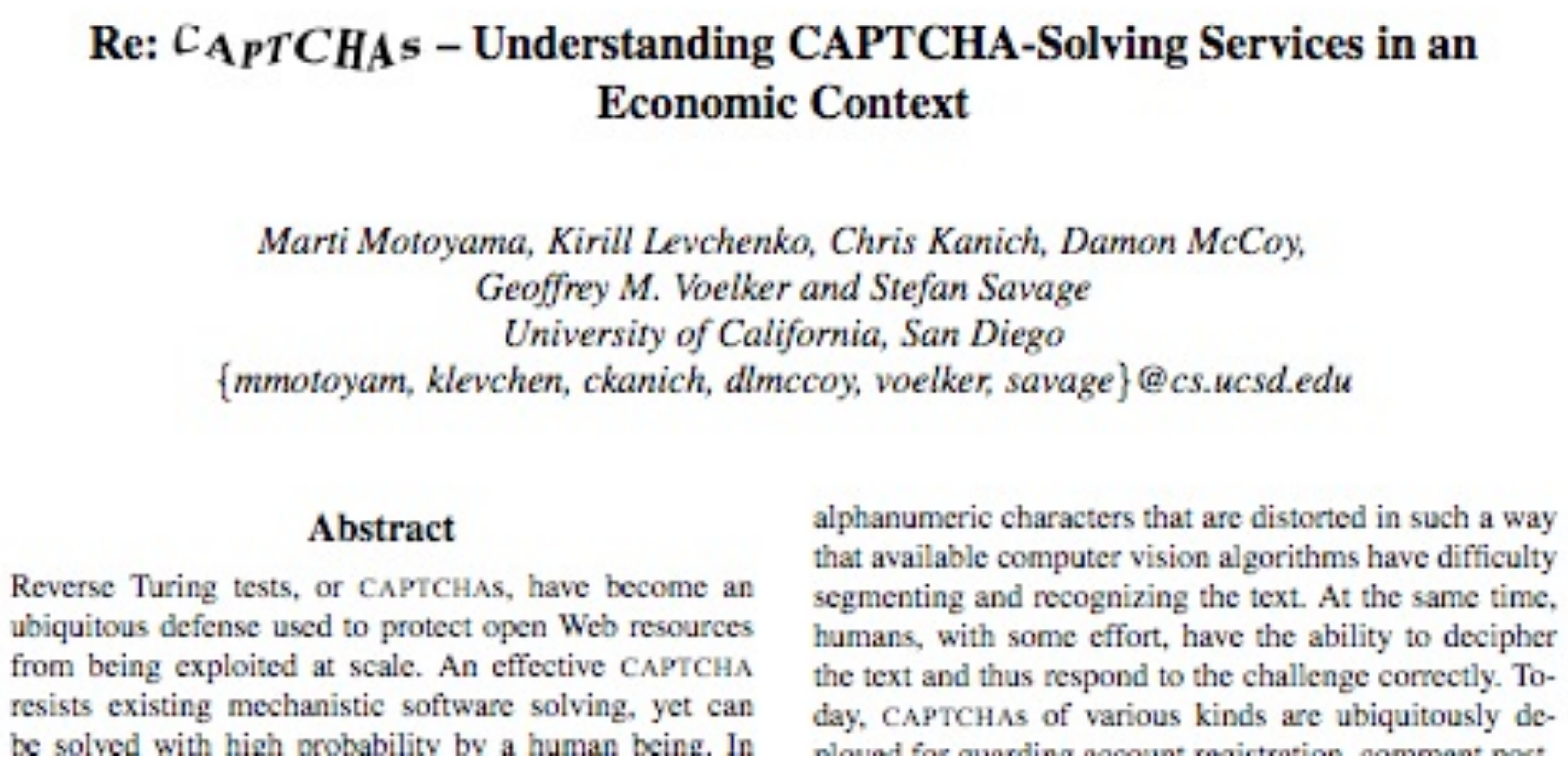
"Captcha ads offered us a new way to engage consumers and help reinforce branded messages," Zoé Zeigler, a Toyota spokeswoman, said in an e-mail.

Universal has also advertised with Solve Media since last year. Media supervisor Lindsay Dye said type-in video ads were used to promote the movies *Devil*, *Catfish* and, most recently, *Little Fockers*. After watching a trailer, Internet users were asked to type in the films' release dates.

"This is a great way to ensure people are watching our ad work," she said.

Detour (Later)

- Detour through the slides for this paper:
  - http://cseweb.ucsd.edu/~savage/papers/UsenixSec10.pdf



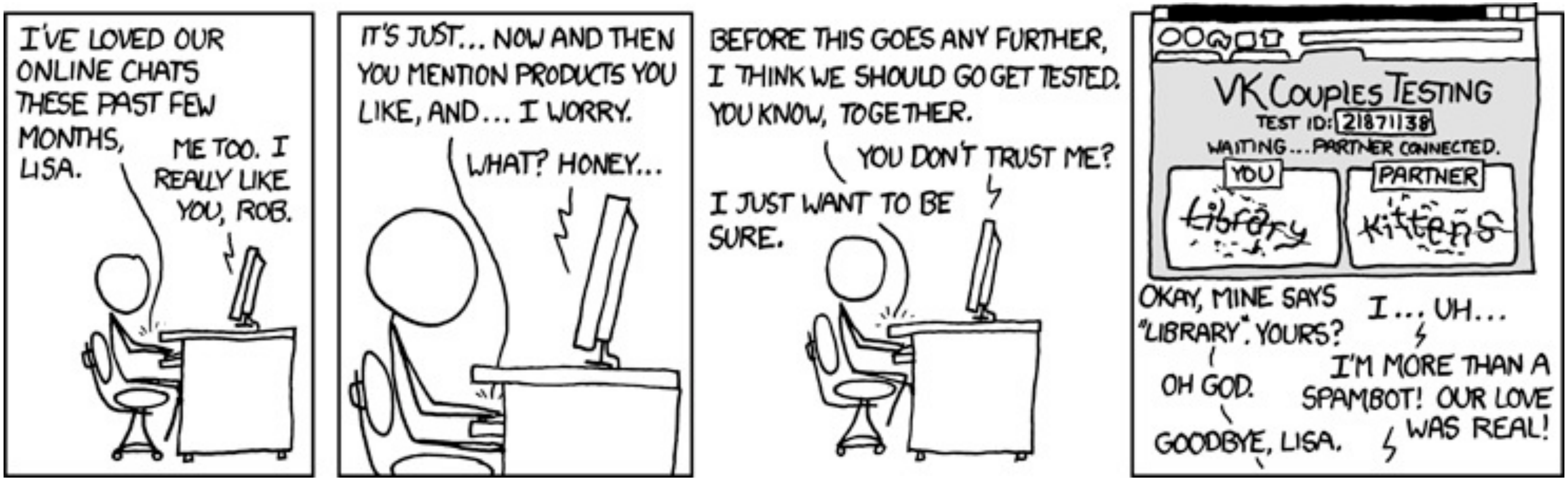
Re: CAPTCHAs – Understanding CAPTCHA-Solving Services in an Economic Context

*Marti Motoyama, Kirill Levchenko, Chris Kanich, Damon McCoy,
Geoffrey M. Voelker and Stefan Savage
University of California, San Diego
{mmotoyam, klevchen, ckanich, dlmccoy, voelker, savage}@cs.ucsd.edu*

Abstract

Reverse Turing tests, or CAPTCHAs, have become an ubiquitous defense used to protect open Web resources from being exploited at scale. An effective CAPTCHA resists existing mechanistic software solving, yet can be solved with high probability by a human being. In

alphanumeric characters that are distorted in such a way that available computer vision algorithms have difficulty segmenting and recognizing the text. At the same time, humans, with some effort, have the ability to decipher the text and thus respond to the challenge correctly. Today, CAPTCHAs of various kinds are ubiquitously deployed for guarding account registration, comment post


I'VE LOVED OUR ONLINE CHATS THESE PAST FEW MONTHS, LISA.
ME TOO. I REALLY LIKE YOU, ROB.
IT'S JUST... NOW AND THEN YOU MENTION PRODUCTS YOU LIKE, AND... I WORRY.
WHAT? HONEY...
BEFORE THIS GOES ANY FURTHER, I THINK WE SHOULD GO GET TESTED. YOU KNOW, TOGETHER.
YOU DON'T TRUST ME?
I JUST WANT TO BE SURE.
VK Couples Testing
TEST ID: 21871138
WAITING... PARTNER CONNECTED.
YOU
Library
PARTNER
Kittens
OKAY, MINE SAYS "LIBRARY". YOURS?
I... UH...
OH GOD.
I'M MORE THAN A SPAMBOT! OUR LOVE WAS REAL!
GOODBYE, LISA.

Phishing

- "The Emperor's New Security Indicators"
  - http://www.usablesecurity.org/emperor/emperor.pdf
- "Why Phishing Works"
  - http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf

- In one study: 27 out of 27 people entered personal information if HTTPS was changed to HTTP (no SSL)
- Other security indicators not very effective (lock icons, ...)
- If a site looks "professional", people likely to believe that it is legitimate

Experiments at Indiana University

[Jagatic et al.]

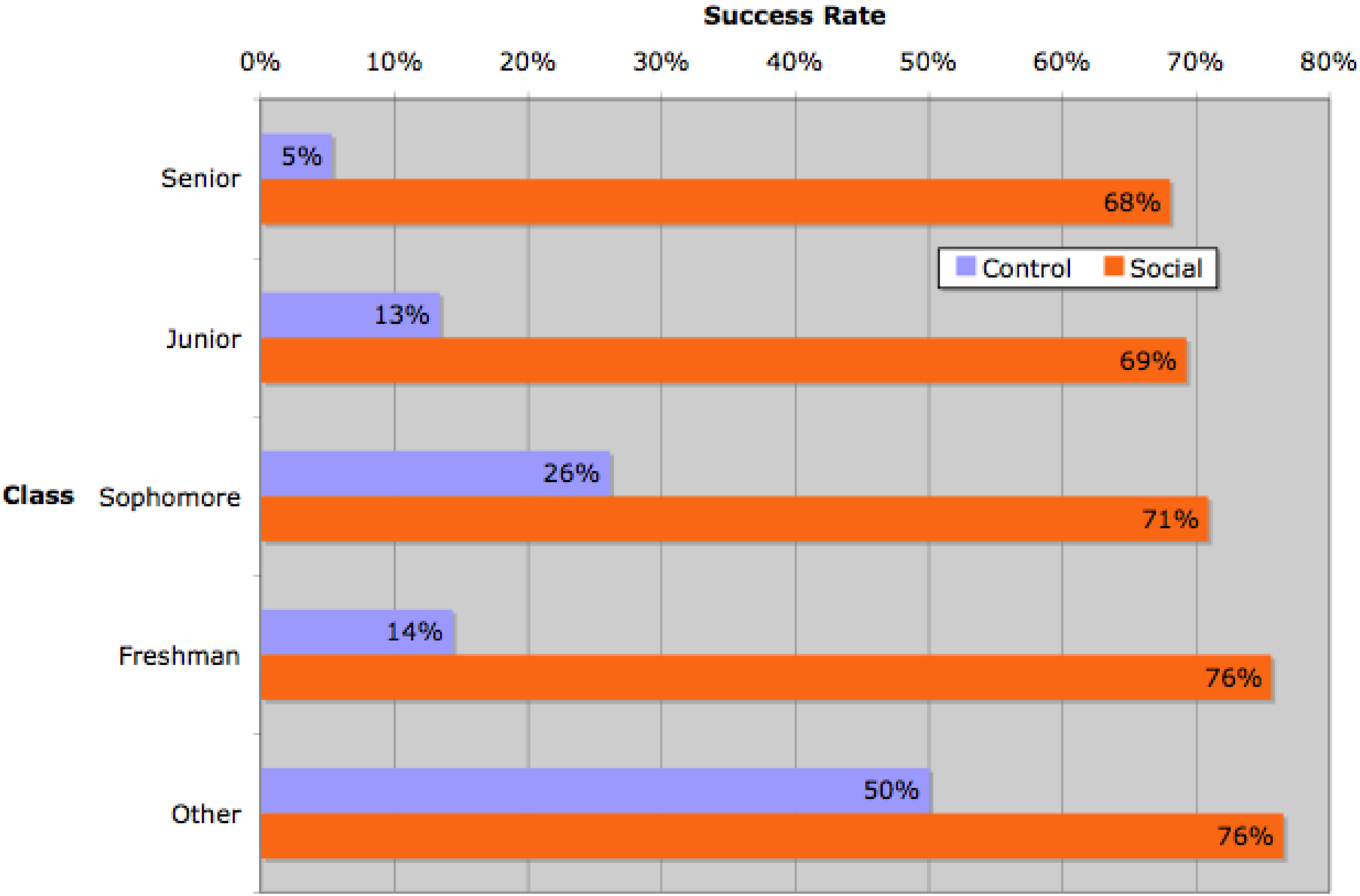
- Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
- Sent 921 Indiana University students a spoofed email that appeared to come from their friend
- Email redirected to a spoofed site inviting the user to enter his/her secure university credentials
  - Domain name clearly distinct from indiana.edu
- 72% of students entered their real credentials into the spoofed site

More Details

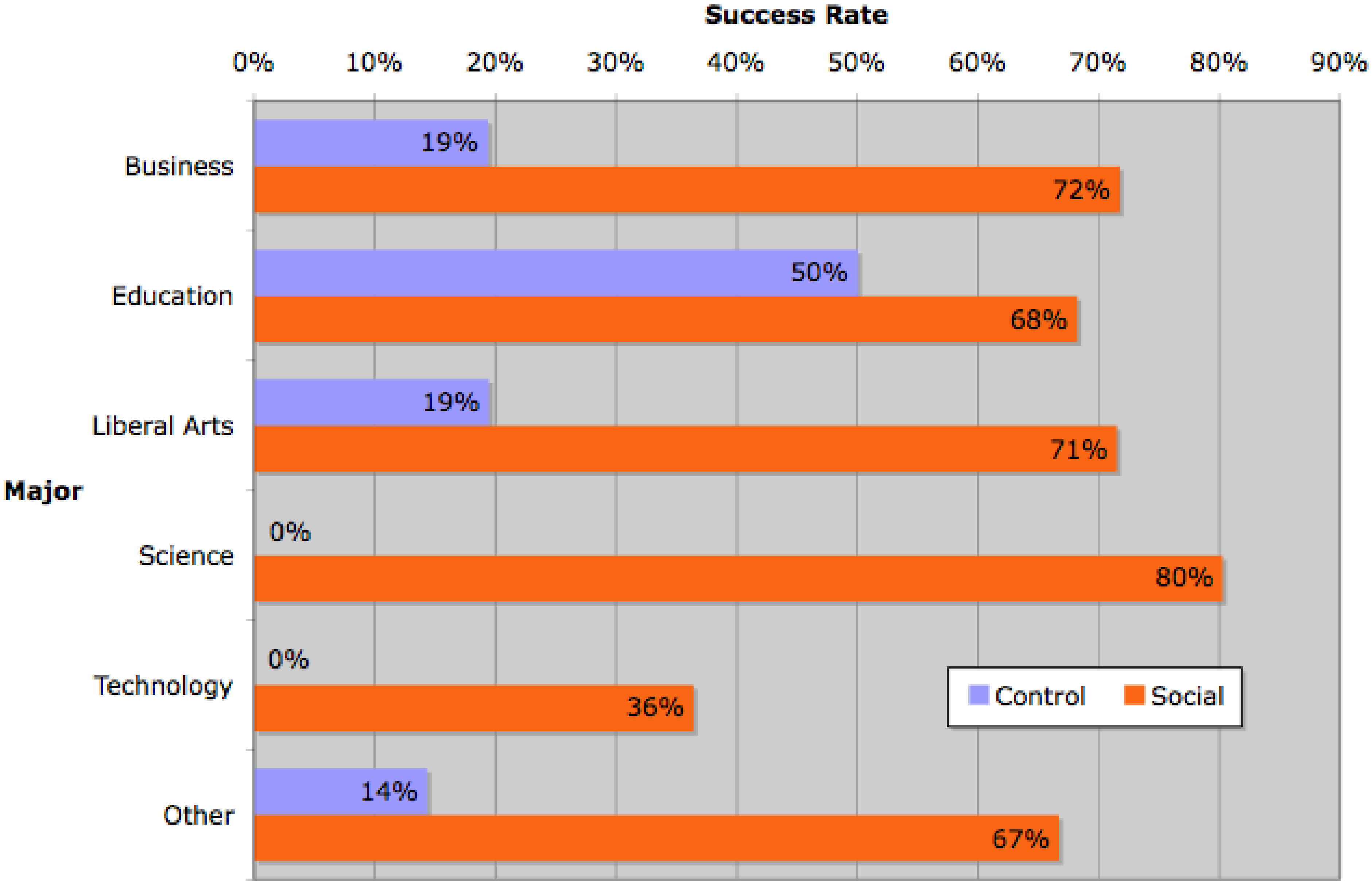
- Control group: 15 of 94 (16%) entered personal information
- Social group: 349 of 487 (72%) entered personal information

- 70% of responses within first 12 hours
- Adversary wins by gaining users’ trust

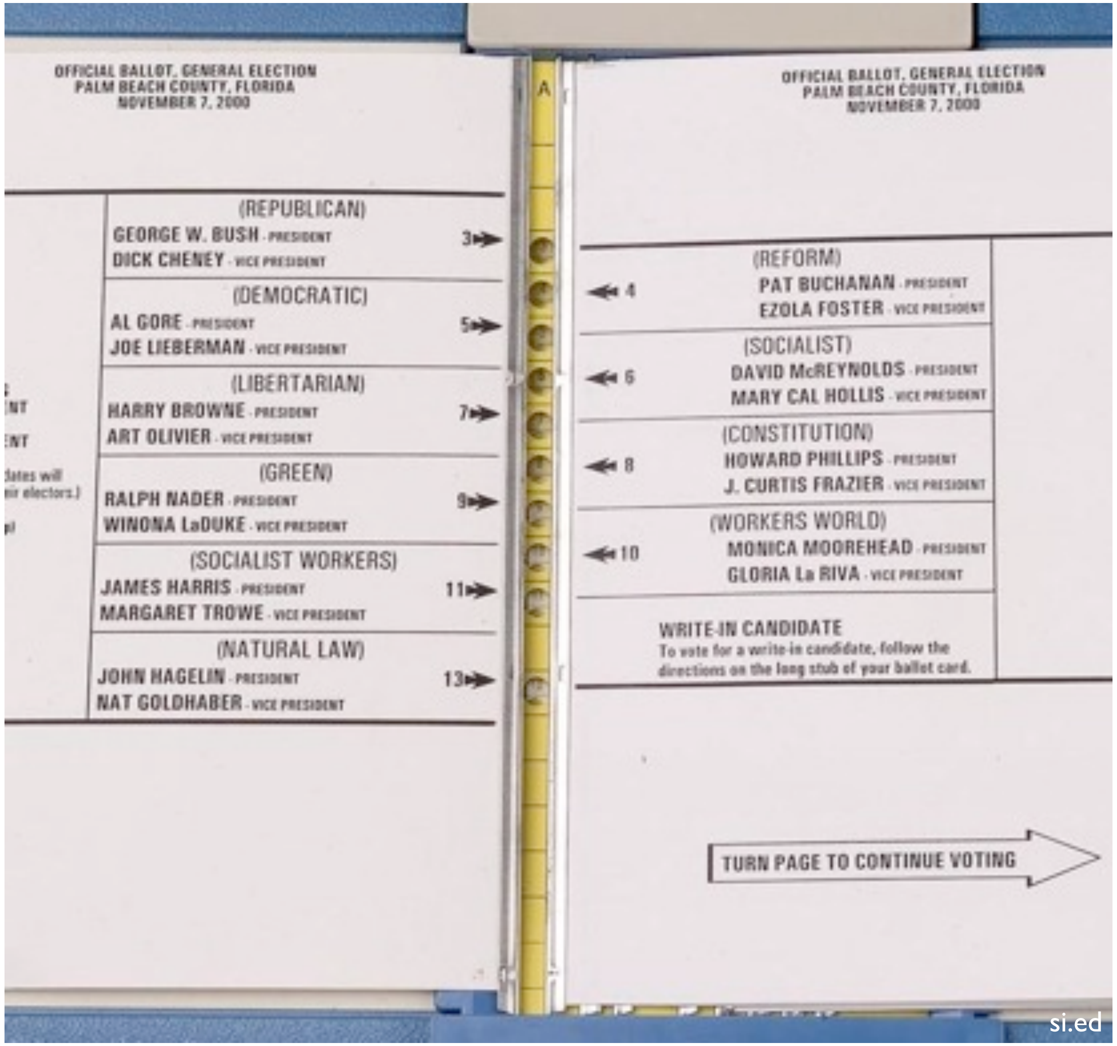
More Details



More Details



Poor Usability Causes Problems



OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT 3➤

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT 5➤

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT 7➤

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT 9➤

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT 11➤

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT 13➤

A

OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

◄4 (REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

◄6 (SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

◄8 (CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

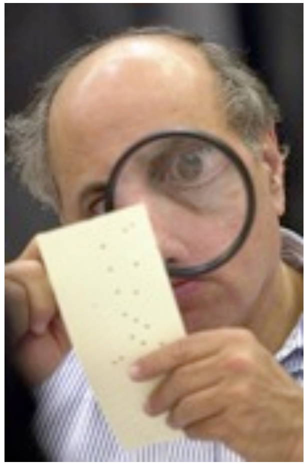
◄10 (WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

TURN PAGE TO CONTINUE VOTING

si.ed

AP



Importance

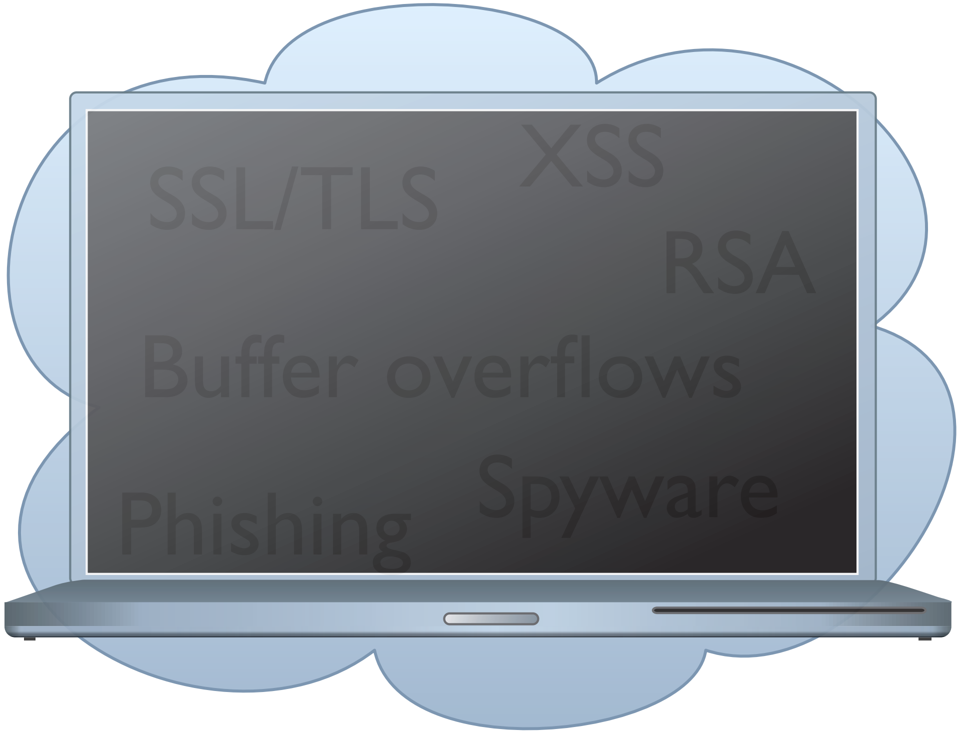
- Why is usability important?
  - People are the critical element of any computer system
    - People are the real reason computers exist in the first place
  - Even if it is **possible** for a system to protect against an adversary, people may use the system in other, **less secure** ways
- Next
  - Challenges with security and usability
  - Key design principles
  - New trends and directions

Issue #1: Complexities, Lack of Intuition

Real World

We can see, understand, relate to.

Electronic World



Too complex, hidden, no intuition.

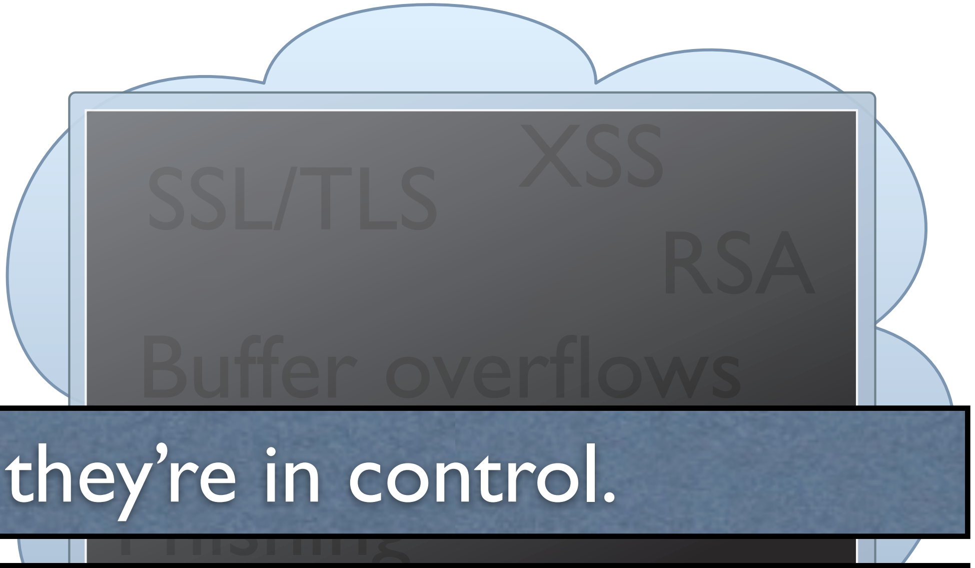
Issue #1: Complexities, Lack of Intuition

- Mismatch between perception of technology and what really happens
  - Public keys?
  - Signatures?
  - Encryption?
  - Message integrity?
  - Chosen-plaintext attacks?
  - Chosen-ciphertext attacks?
  - Password management?
  - …

Issue #2: Who's in Charge?

Real World

Electronic World



Users want to feel like they're in control.

Adversaries in the electronic world can be *intelligent*, *sneaky*, and *malicious*.

Complex, hidden, but *doctors manage*

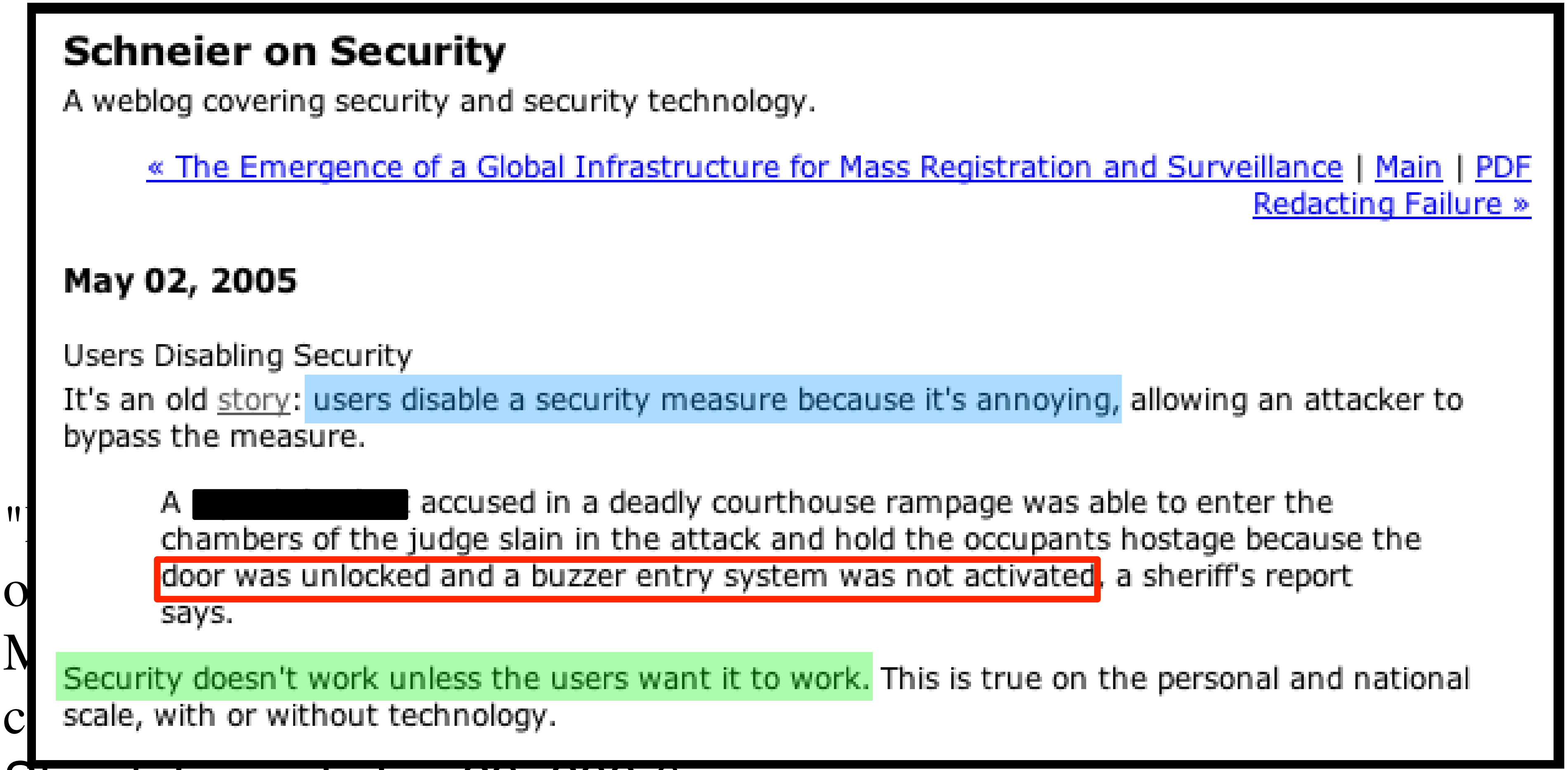
Complex, hidden, and *users manage*

Issue #2: Who’s in Charge?

- Systems developers should help protect users
  - Usable authentication systems
  - Red/green lights
- Software applications help users manage their applications
  - P3P for privacy control
  - PwdHash, Keychain for password management
  - Some say: Can we trust software for these tasks?

Issue #3: Hard to Gage Risks

"It won't happen to me!" (Sometimes a reasonable assumption, sometimes not.)



Schneier on Security

A weblog covering security and security technology.

« The Emergence of a Global Infrastructure for Mass Registration and Surveillance | Main | PDF Redacting Failure »

May 02, 2005

Users Disabling Security

It's an old story: users disable a security measure because it's annoying, allowing an attacker to bypass the measure.

> A [redacted] accused in a deadly courthouse rampage was able to enter the chambers of the judge slain in the attack and hold the occupants hostage because the door was unlocked and a buzzer entry system was not activated, a sheriff's report says.

Security doesn't work unless the users want it to work. This is true on the personal and national scale, with or without technology.

"I
o
M
c
Street Journal, Jan 29, 2007)

Issue #4: No Accountability

- Issue #3 is amplified when users are not held accountable for their actions
  - E.g., from employers, service providers, etc.
  - (Not all parties will perceive risks the same way)

Issue #5: Awkward, Annoying, or Difficult

- Difficult
  - Remembering 50 different, “random” passwords
- Awkward
  - Lock computer screen every time leave the room
- Annoying
  - Browser warnings, virus alerts, forgotten passwords, firewalls

- Consequence:
  - Changing user’s knowledge may **not** affect their behavior

Issue #6: Social Issues

- Public opinion, self-image
  - Only “nerds” or the “super paranoid” follow security guidelines
- Unfriendly
  - Locking computers suggests distrust of co-workers
- Annoying
  - Sending encrypted emails that say, “what would you like for lunch?”

Issue #7: Usability Promotes Trust

- Well known by con artists, medicine men
- Phishing
  - More likely to trust professional-looking websites than non-professional-looking ones

Response #1: Education and Training

- Education:
  - Teaching technical concepts, risks
- Training
  - Change behavior through
    - Drill
    - Monitoring
    - Feedback
    - Reinforcement
    - Punishment
- May be part of the solution - but not the solution

Response #2: Security Should Be Invisible

- Security should happen
  - Naturally
  - By Default
  - Without user input or understanding

- Recognize and stop bad actions
- Starting to see some invisibility
  - SSL/TLS
  - VPNs
  - Automatic Security Updates

See Dan Simon's slides: http://research.microsoft.com/projects/SWSecInstitute/slides/simon.ppt

Response #2: Security Should Be Invisible

- "Easy" at extremes, or for simple examples
  - Don't give everyone access to everything
- But hard to generalize
- Leads to things not working for reasons user doesn't understand
- Users will then try to get the system to work, possibly further reducing security
  - E.g., "dangerous successes" for password managers

See Dan Simon's slides: http://research.microsoft.com/projects/SWSecInstitute/slides/simon.ppt

Response #3: "Three-word UI:" "Are You Sure?"

- Security should be invisible
  - Except when the user tries something dangerous
  - In which case a warning is given

- But how do users evaluate the warning? Two realistic cases:
  - Always heed warning. But see problems / commonality with Response #2
  - Always ignore the warning. If so, then how can it be effective?

See Dan Simon's slides: http://research.microsoft.com/projects/SWSecInstitute/slides/simon.ppt

Response #4: Focus on Users, Use Metaphors

- Clear, understandable metaphors:
  - Physical analogs; e.g., red-green lights
- User-centered design: Start with user model
- Unified security model across applications
  - User doesn't need to learn many models, one for each application
- Meaningful, intuitive user input
  - Don't assume things on user's behalf
  - Figure out how to ask so that user can answer intelligently

See Dan Simon's slides: http://research.microsoft.com/projects/SWSecInstitute/slides/simon.ppt

Response #5: Least Resistance

- "Match the most comfortable way to do tasks with the least granting of authority"
  - Ka-Ping Yee, Security and Usability

- Should be "easy" to comply with security policy

- "Users value and want security and privacy, but they regard them only as secondary to completing the primary tasks"
  - Karat et al, Security and Usability