

CSE 484 / CSE M 584 (Spring 2012)

User Authentication

Tadayoshi Kohno

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

Goals for Today

- ◆ User Authentication
- ◆ Lab 2 due this Friday

Authentication by Handwriting

[Ballard, Monroe, Lopresti]

- ◆ Maybe a computer could also forge some biometrics

graphic language target	crisis management target	solo concert target
graphic language human forgery	crisis management human forgery	solo concert human forgery
graphic language generative forgery	crisis management generative forgery	solo concert generative forgery

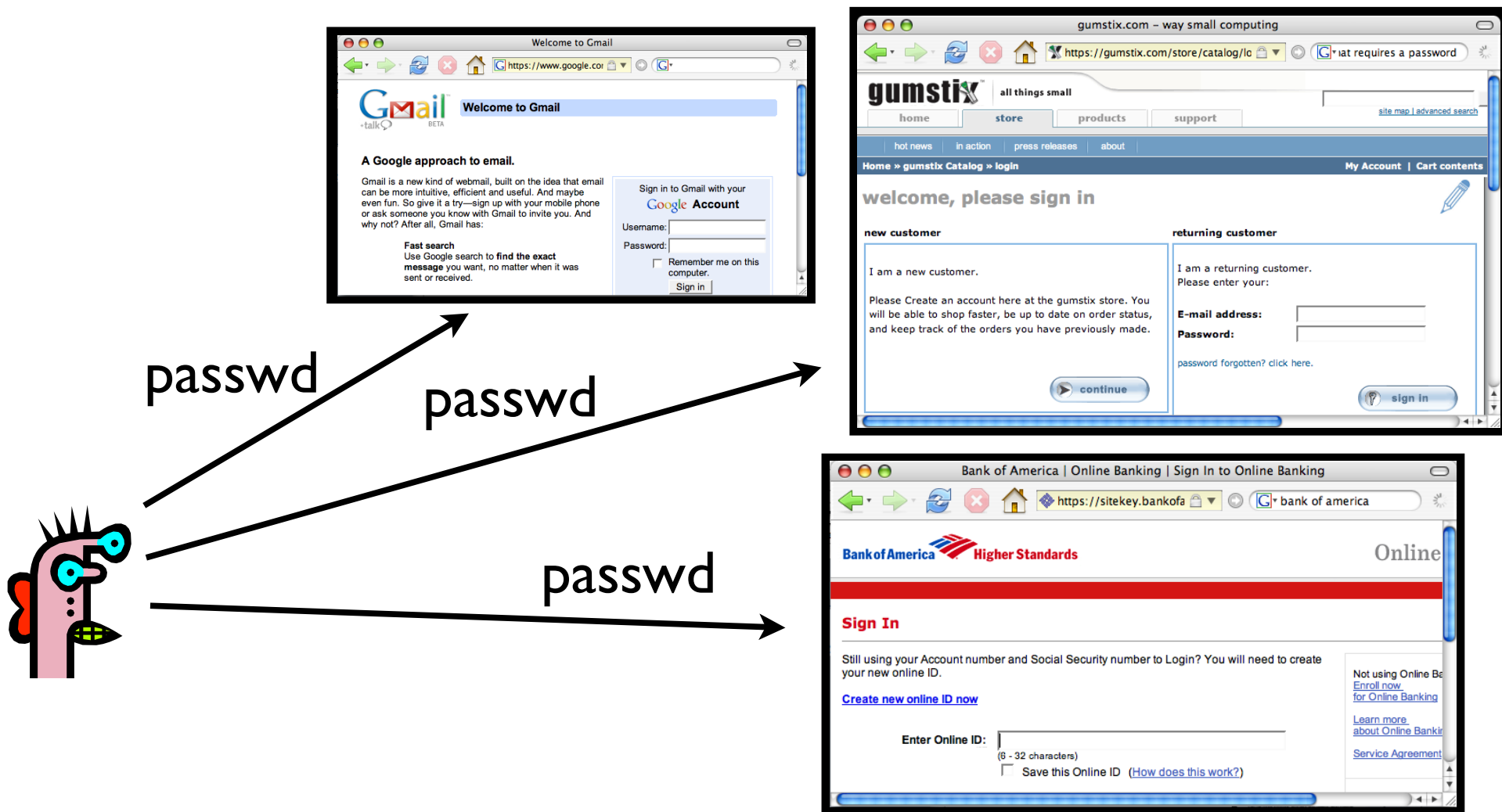
Generated by computer algorithm trained on handwriting samples

Human Factors in User Authentication

Passwords

The problem

Alice needs passwords for all the websites that she visits



Possible solutions

- **Easy to remember:** Use **same password** on all websites. Use “**weak**” password.
 - Poor security (don't share password between bank website and small website)
- **More secure:** Use **different, strong passwords** on all websites.
 - Hard to remember, unless write down.



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

Facebook founder Mark Zuckerberg 'hacked into emails of rivals and journalists'

By MAIL FOREIGN SERVICE

Last updated at 2:09 AM on 06th March 2010



Business Insider claimed he then told a friend how he had hacked into the accounts of Crimson staff.

Facebook
been a
account

He allegedly told the friend that he used TheFacebook.com to search for members who said they were Crimson staff.

The CB
social r
at least
of artic

Then, he allegedly examined a report of failed logins to see if any of the Crimson members had ever entered an incorrect password into TheFacebook.com.

As part
detailin
magaz
evidenc

In the instances where they had, Business Insider claimed that Zuckerberg said he tried using those incorrect passwords to access the Crimson members' Harvard email accounts.

In two instances, the magazine claimed, he succeeded - and was able to read emails between Crimson staff discussing the possibility of writing an article on the accusations surrounding him.

'In other words,' Business Insider claimed, 'Mark appears to have used private login data from TheFacebook to hack into the separate email accounts of some TheFacebook users'.

Classroom Survey

Who here...

- repeats 1 password across many sites?
- uses 1 password with site-specific variations?
- uses 2 passwords, one low-security and one high-security for special sites?
- uses truly unique passwords for special sites?
- uses a truly unique password on every site?
- Does something else?

Password managers

- Password managers handle creating and “remembering” strong passwords
- Potentially:
 - Easier for users
 - More secure
- Examples:
 - PwdHash (Usenix Security 2005)
 - Password Multiplier (WWW 2005)

PwdHash



@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd, domain)

Prevent phishing attacks

Password Multiplier



Activate with Alt-P or double-click

sitePwd = Hash(username, pwd, domain)

Both solutions target simplicity and transparency.

Usenix 2006: Usability testing

HCI is important!

- Are these programs **usable**? If not, what are the problems?
- Two main approaches for evaluating usability:
 - **Usability inspection** (no users)
 - Cognitive walk throughs
 - Heuristic evaluation
 - **User study**
 - **Controlled experiments**
 - Real usage

This work stresses
need to observe real users

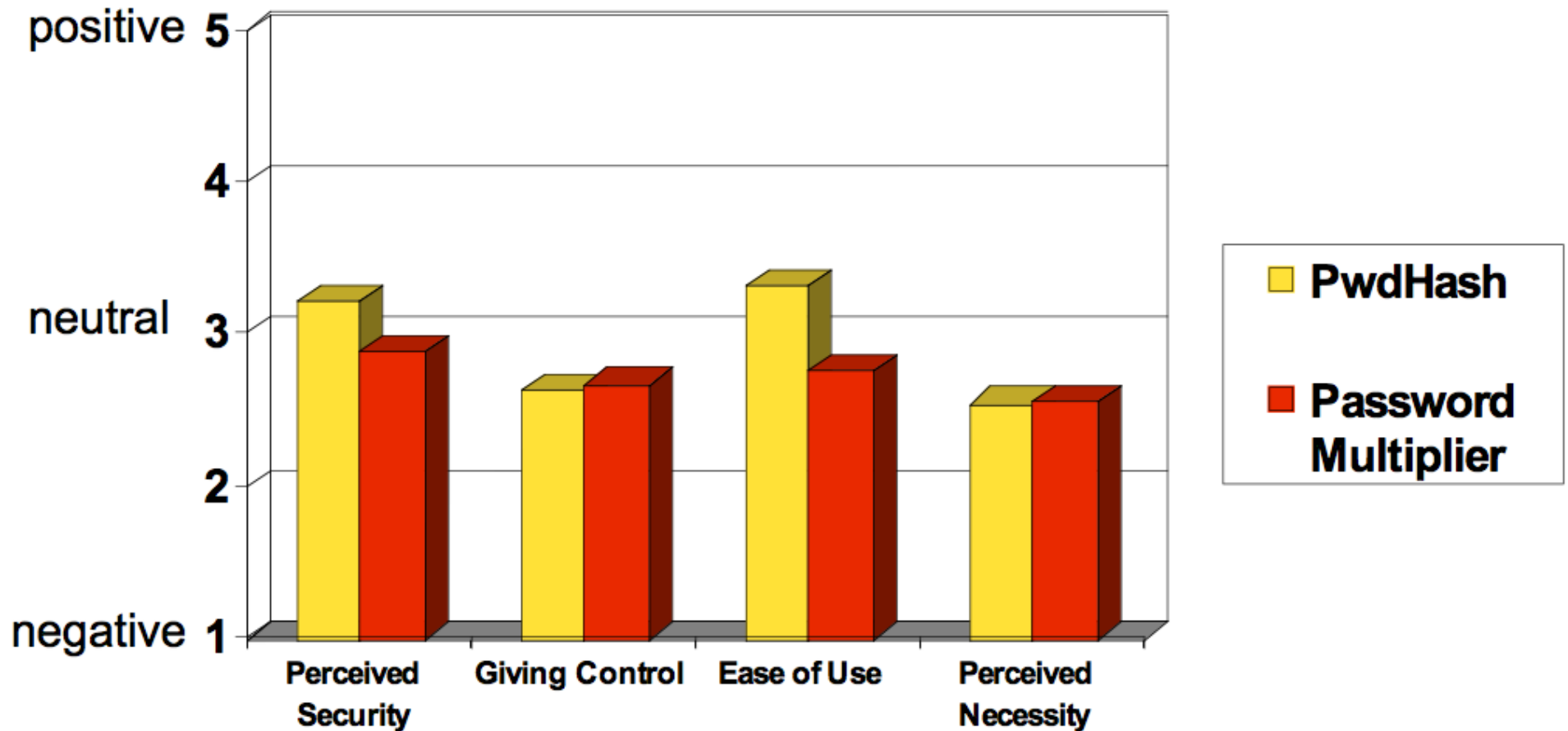
Study details

- 26 participants, across various backgrounds (4 technical)
- Five assigned tasks per plugin
- Data collection
 - Observational data (recording task outcomes, difficulties, misconceptions)
 - Questionnaire data (initial attitudes, opinions after tasks, post questionnaires)

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%

Questionnaire responses



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 Factors in User Authentication

CAPTCHAs

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

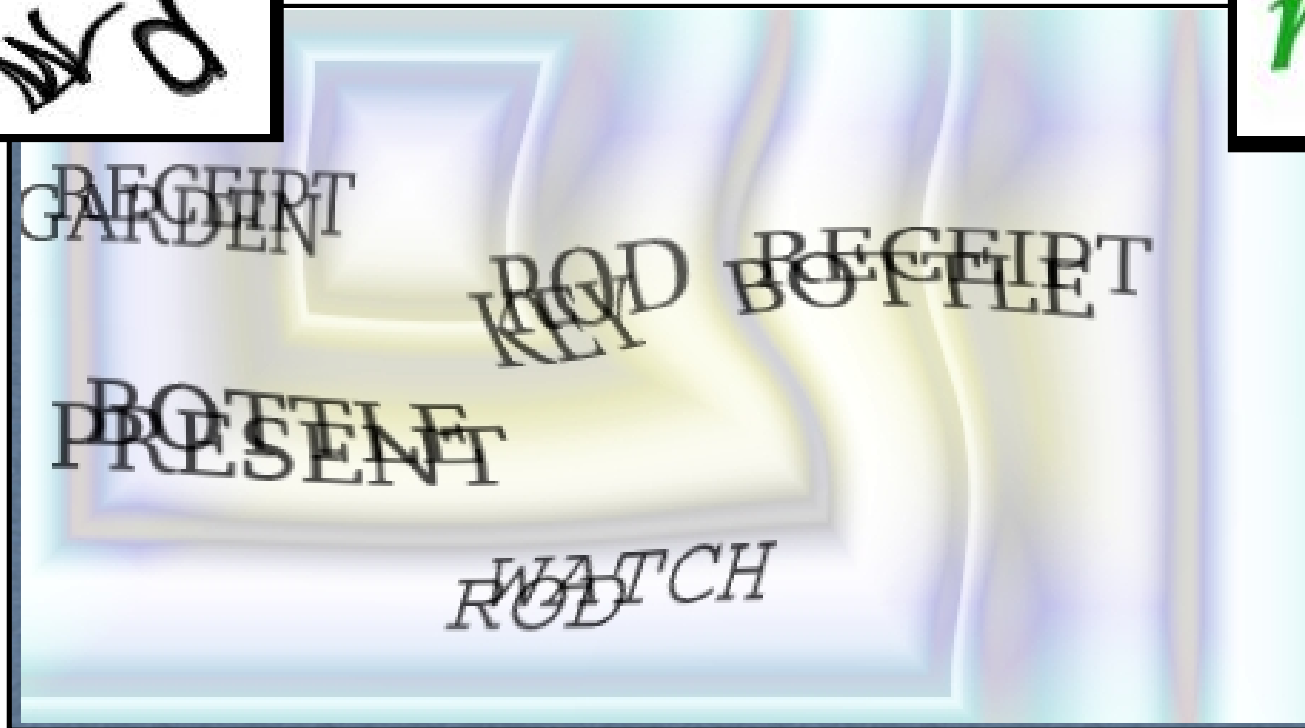
CAPTCHAs



Yahoo



Gmail



captcha.net

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

Four Indicted in CAPTCHA Hacks of Ticket Sites

03.01.10



By [Chloe Albanesius](#)

Did you miss out on floor seats for [Bruce Springsteen](#)'s July 2008 concert at
Gi...





For
inc
sn
Tid
ve
Ju

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.
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

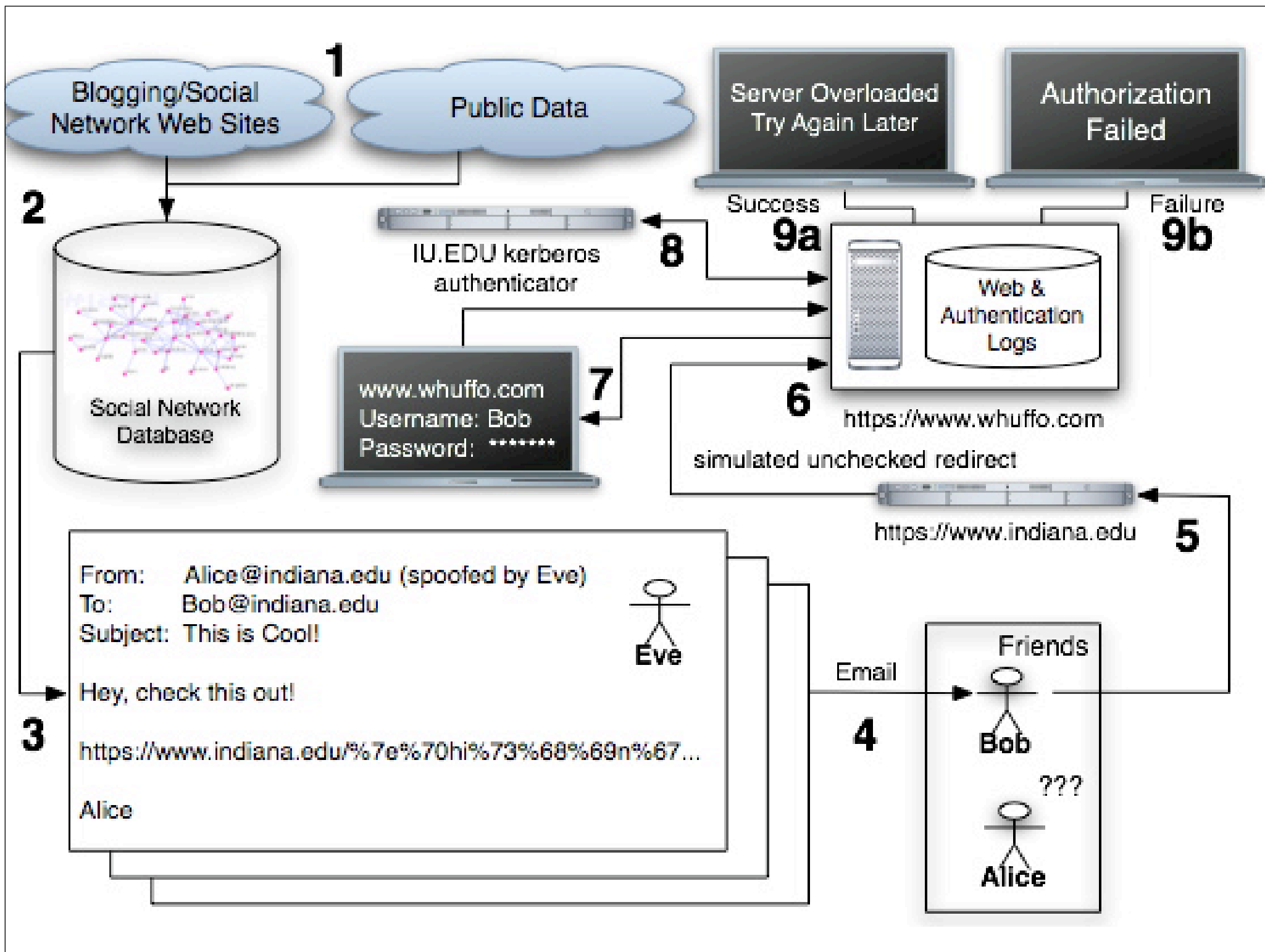
Phishing

- ◆ “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



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

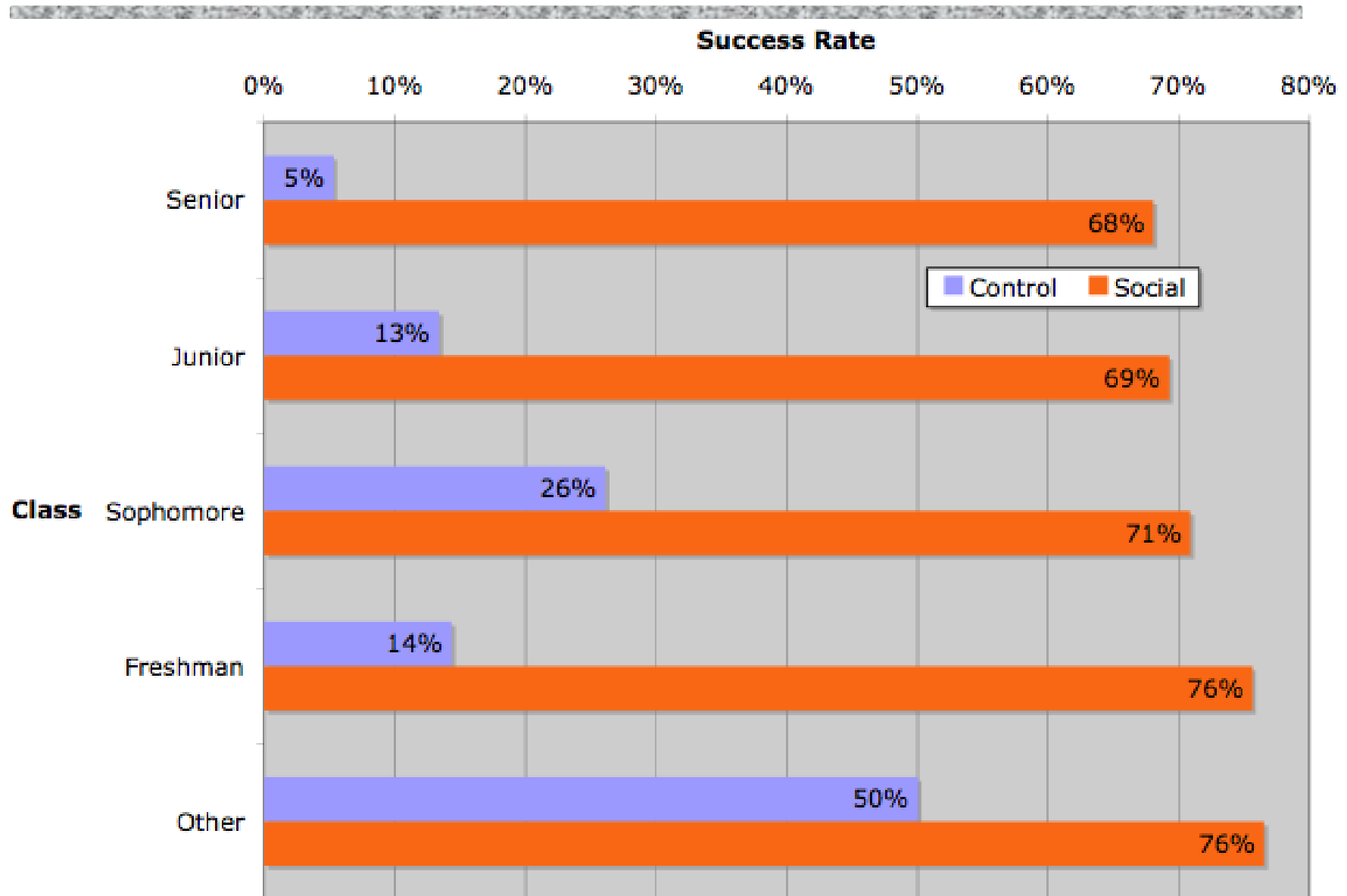
- ◆ Control group: 15 of 94 (16%) entered personal information
- ◆ Social group: 349 of 487 (72%) entered personal information

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

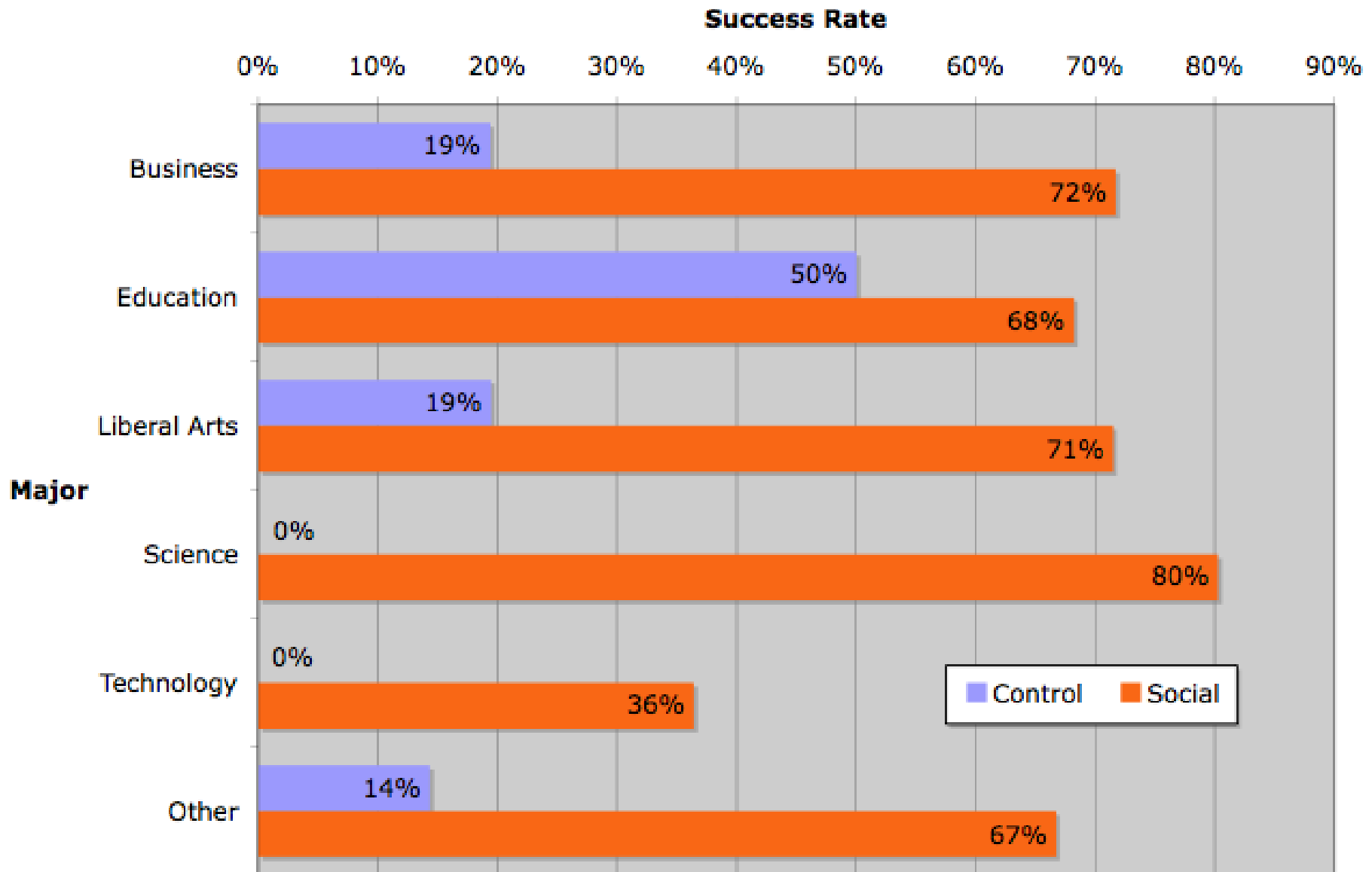
More Details

	To Male	To Female	To Any
From Male	53%	78%	68%
From Female	68%	76%	73%
From Any	65%	77%	72%

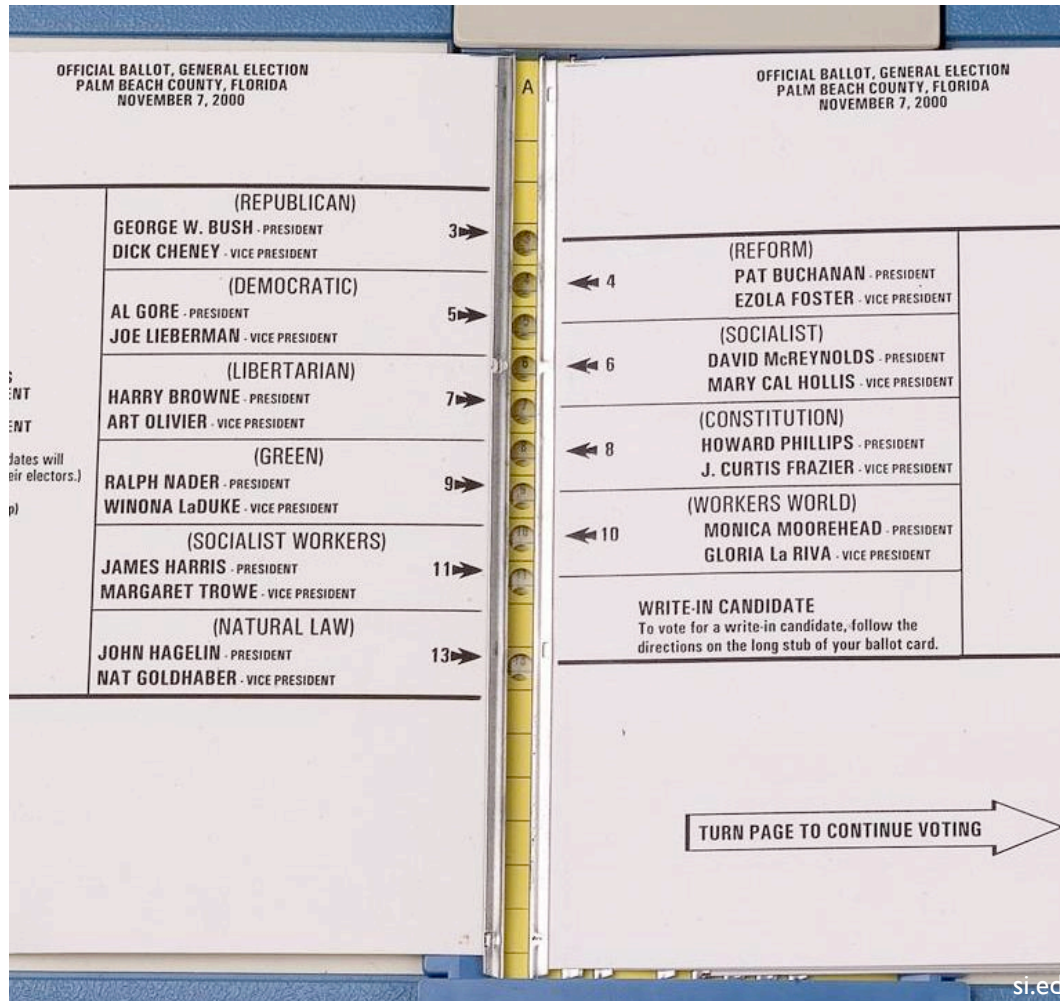
More Details (Class Year)



More Details (Major)



Poor Usability Causes Problems



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

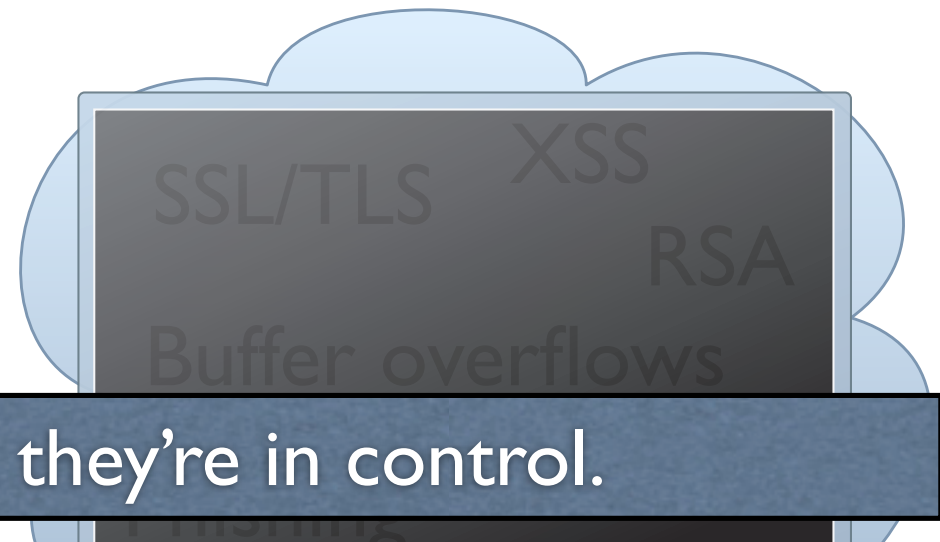
- ◆ Mismatch between perception of technology and what really happens
 - Public keys?
 - Signatures?
 - Encryption?
 - Message integrity?
 - Chosen-plaintext attacks?
 - Chosen-ciphertext attacks?
 - Password management?
 - ...

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.

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

Issues with Usability

1. Lack of intuition
 - See a safe, understand threats. Not true for computers
2. Who's in charge?
 - Doctors keep your medical records safe, you manage your passwords
3. Hard to gage risks
 - "It would never happen to me!"
4. No accountability
 - Asset-holder is not the only one you can lose assets
5. Awkward, annoying, or difficult
6. Social issues
7. Usability promotes trust

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

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

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?

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

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](#)