CSE 484 / CSE M 584 (Winter 2013)

Authentication

Tadayoshi Kohno

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

Goals for Today

- Authentication (continued)
- Lab 2 deadline extended (TBD; abstract.cs down)
- **Tentative** plan still the same:
  - HW3 out tomorrow
  - Lab3 out on Monday

- Available to help write Android malware?

- (Our goal is, ultimately, to develop better ways to detect malware. But we need some great, clever examples of malware to begin with.)

Biometric Error Rates (Adversarial)

- Want to minimize "fraud" and "insult" rate
  - "Easy" to test probability of accidental misidentification (fraud)
  - But what about adversarial fraud
- An adversary might try to steal the biometric information
  - Malicious fingerprint reader
    - Consider when biometric is used to derive a cryptographic key
  - Residual fingerprint on a glass

Voluntary: Making a Mold

[Matsumoto]

Put the plastic into hot water to soften it.

Press a live finger against it.

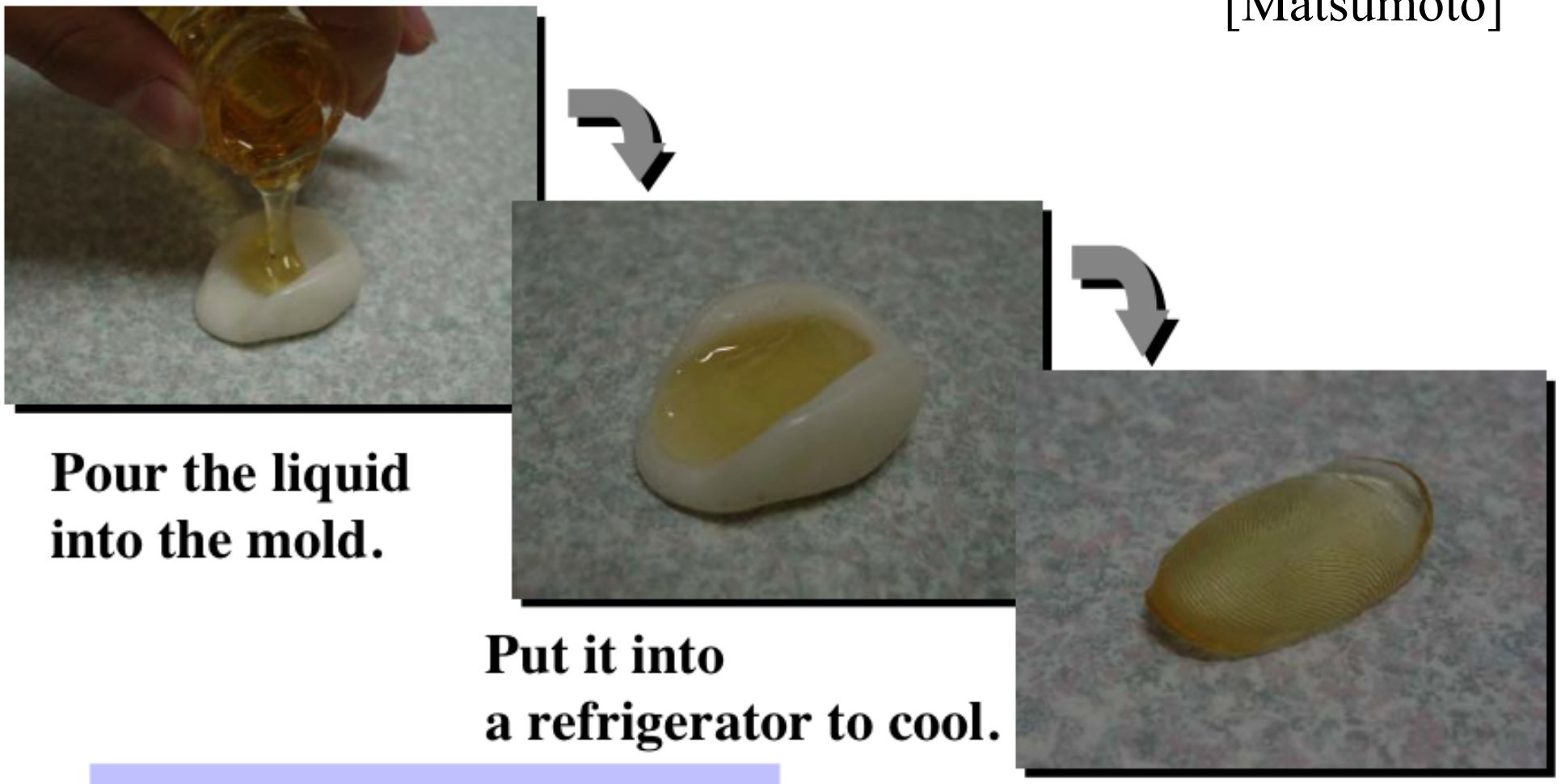
The mold

It takes around 10 minutes.

http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Voluntary: Making a Finger

[Matsumoto]



Pour the liquid into the mold.

Put it into a refrigerator to cool.

It takes around 10 minutes.

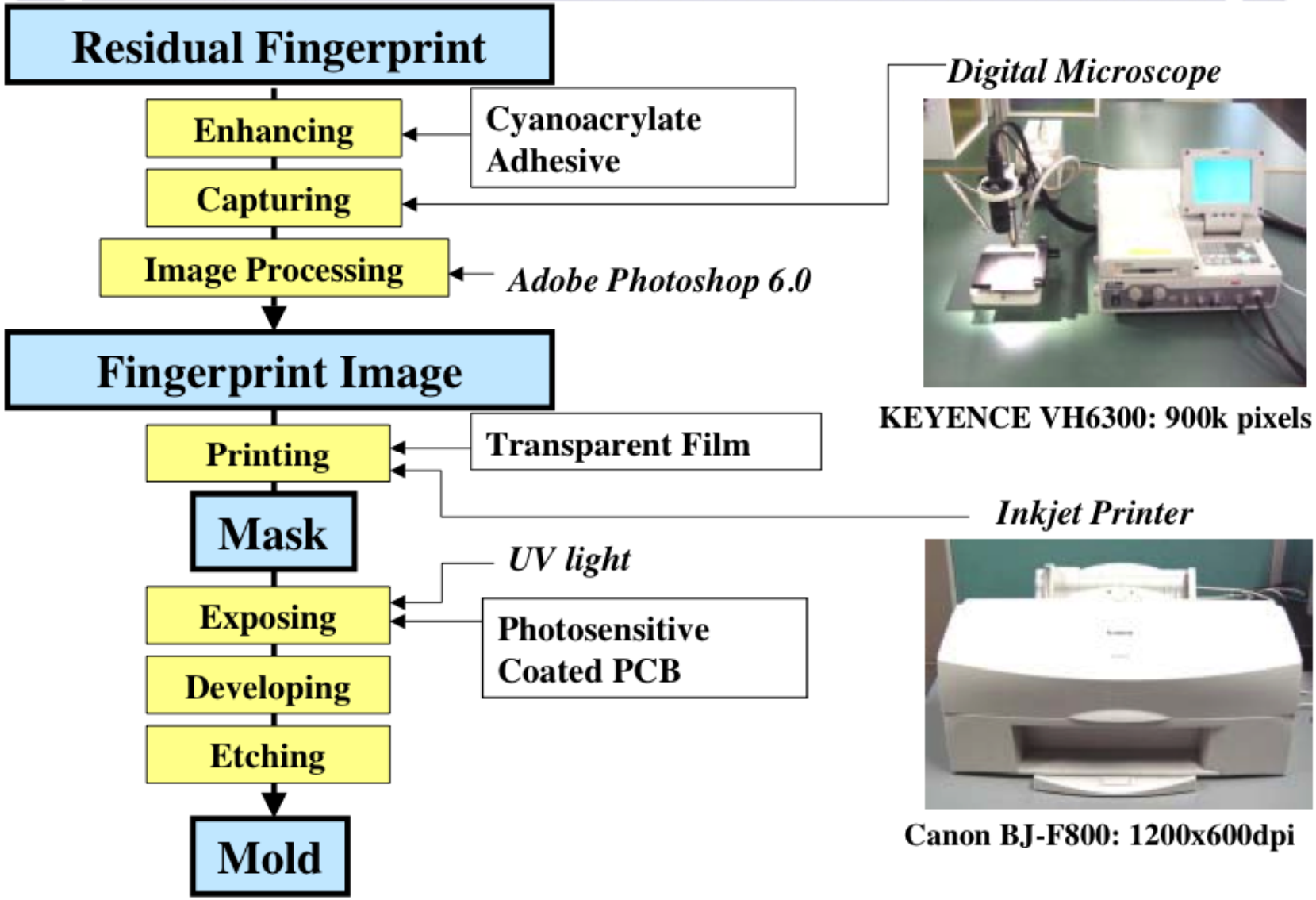
The gummy finger

http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

This **did** fool early desktop fingerprint readers

Involuntary

[Matsumoto]

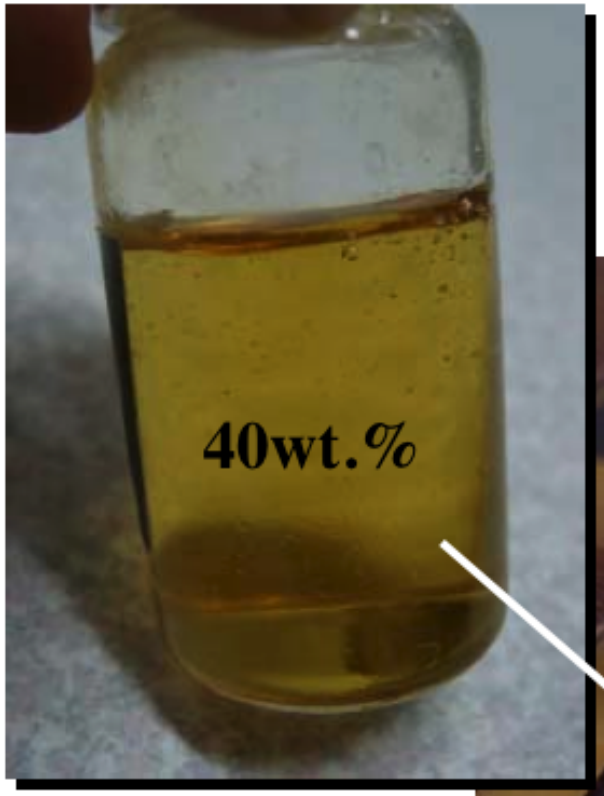


http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

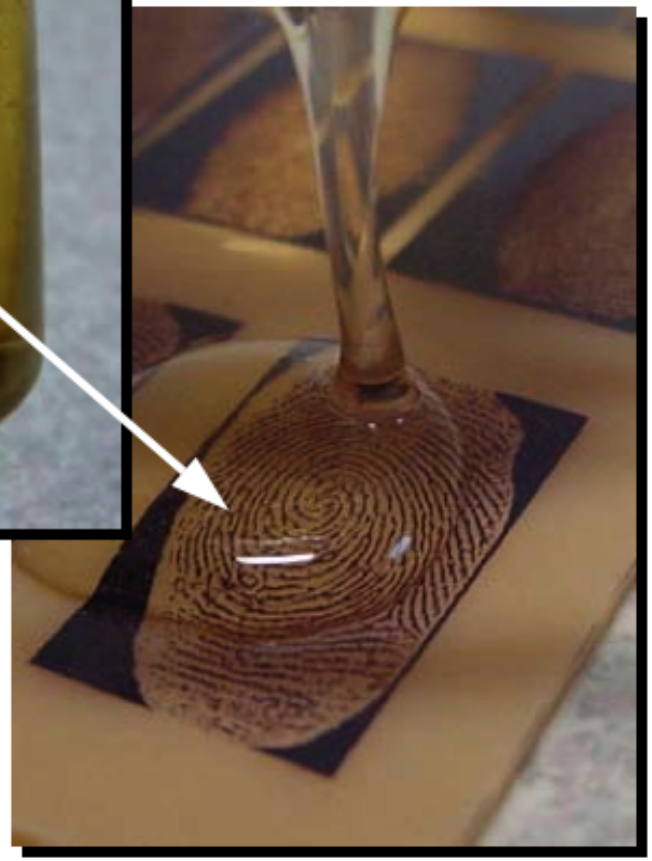
Involuntary

[Matsumoto]

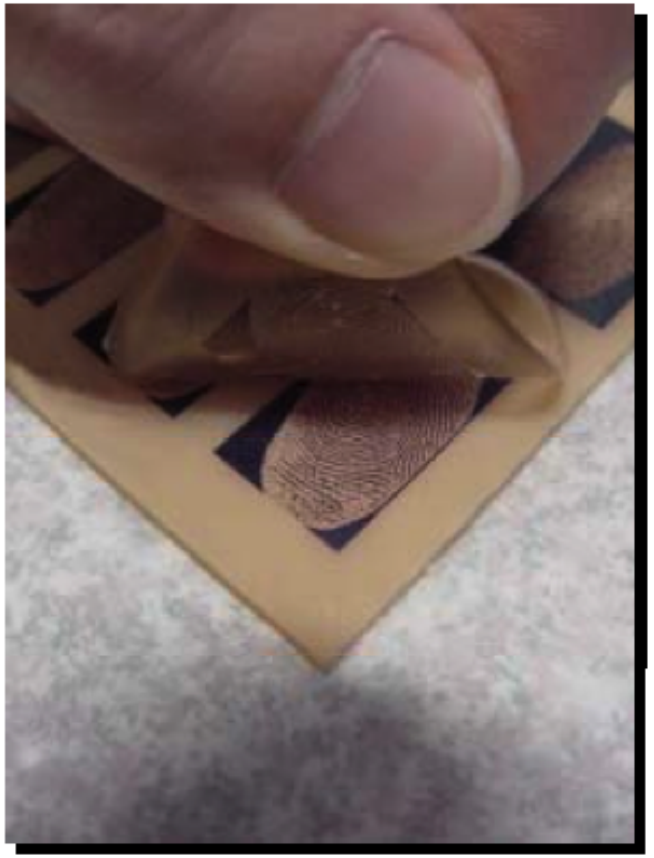
Gelatin Liquid



Drip the liquid onto the mold.



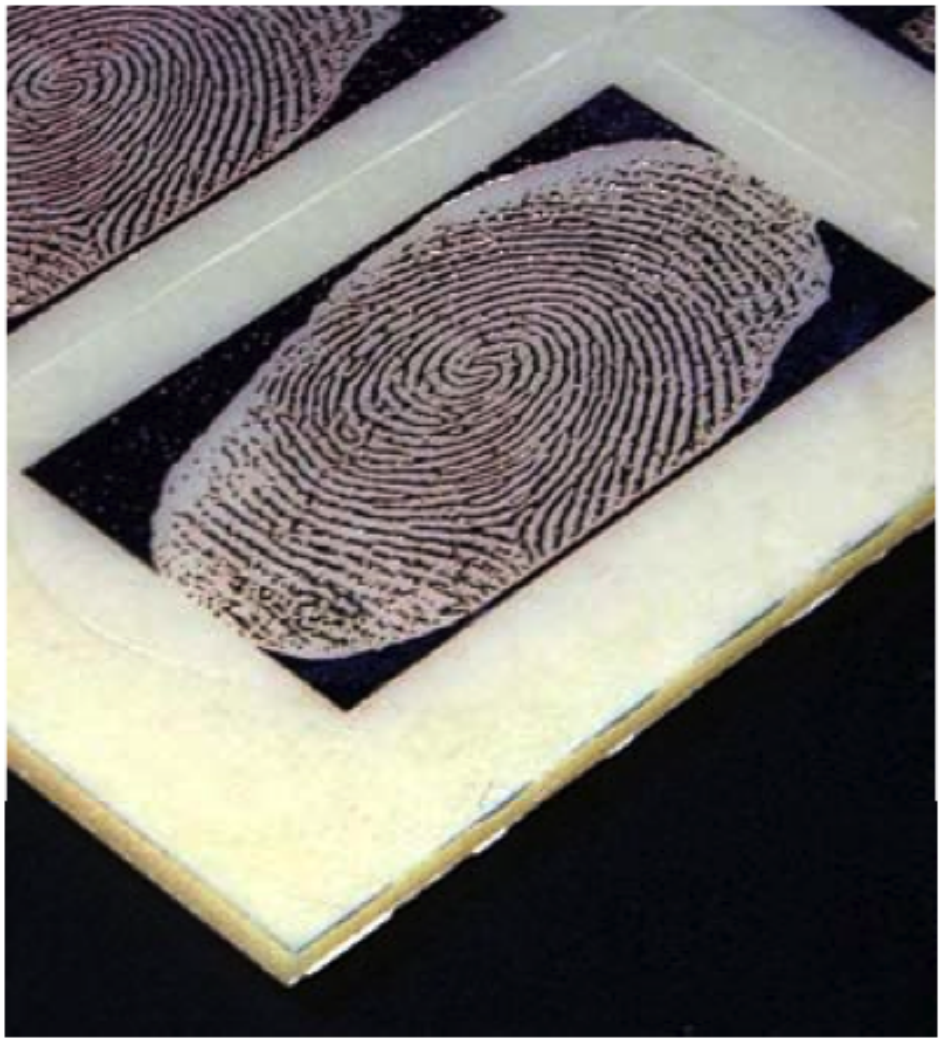
Put this mold into a refrigerator to cool, and then peel carefully.

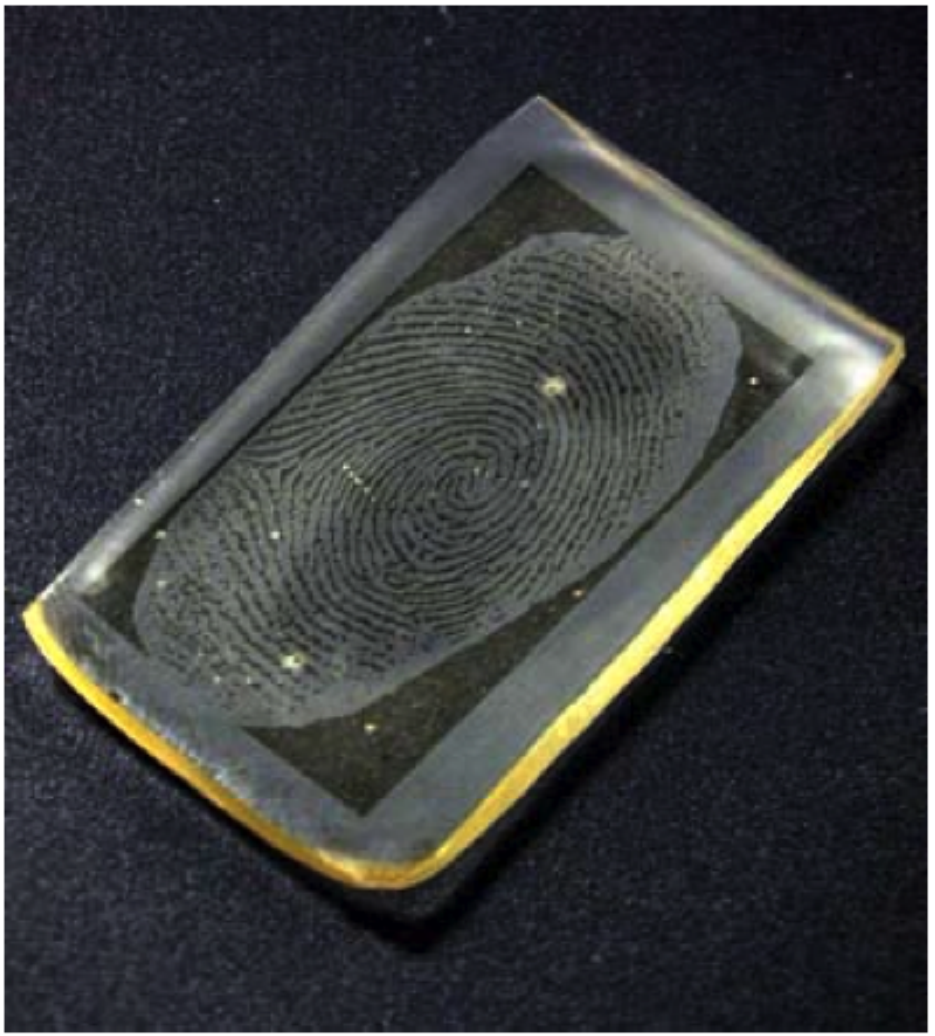


http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Involuntary

[Matsumoto]





http://web.mit.edu/6.857/OldStuff/Fall03/ref/gummy-slides.pdf

Questions

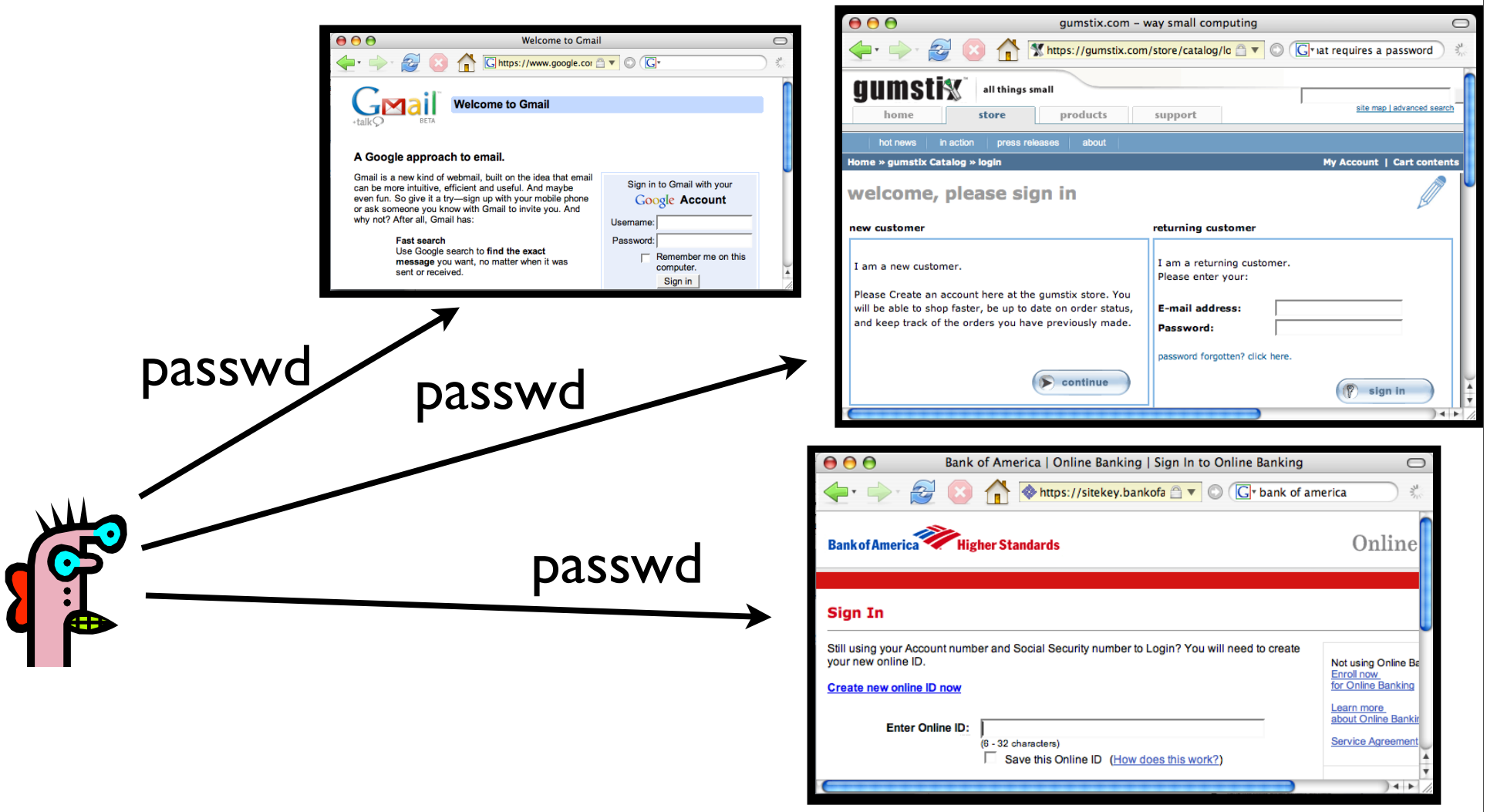
- Q1. Have you ever knowingly used a biometric system in the past?
- Q2. Having now heard about biometrics, when / where / how would you like to see biometrics used?
- Q3. Having now heard about biometrics, when / where / how would you like to **not** see biometrics used?
- Q4. What are the biggest advantages of biometrics?
- Q5. What are the biggest disadvantages of biometrics?

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.

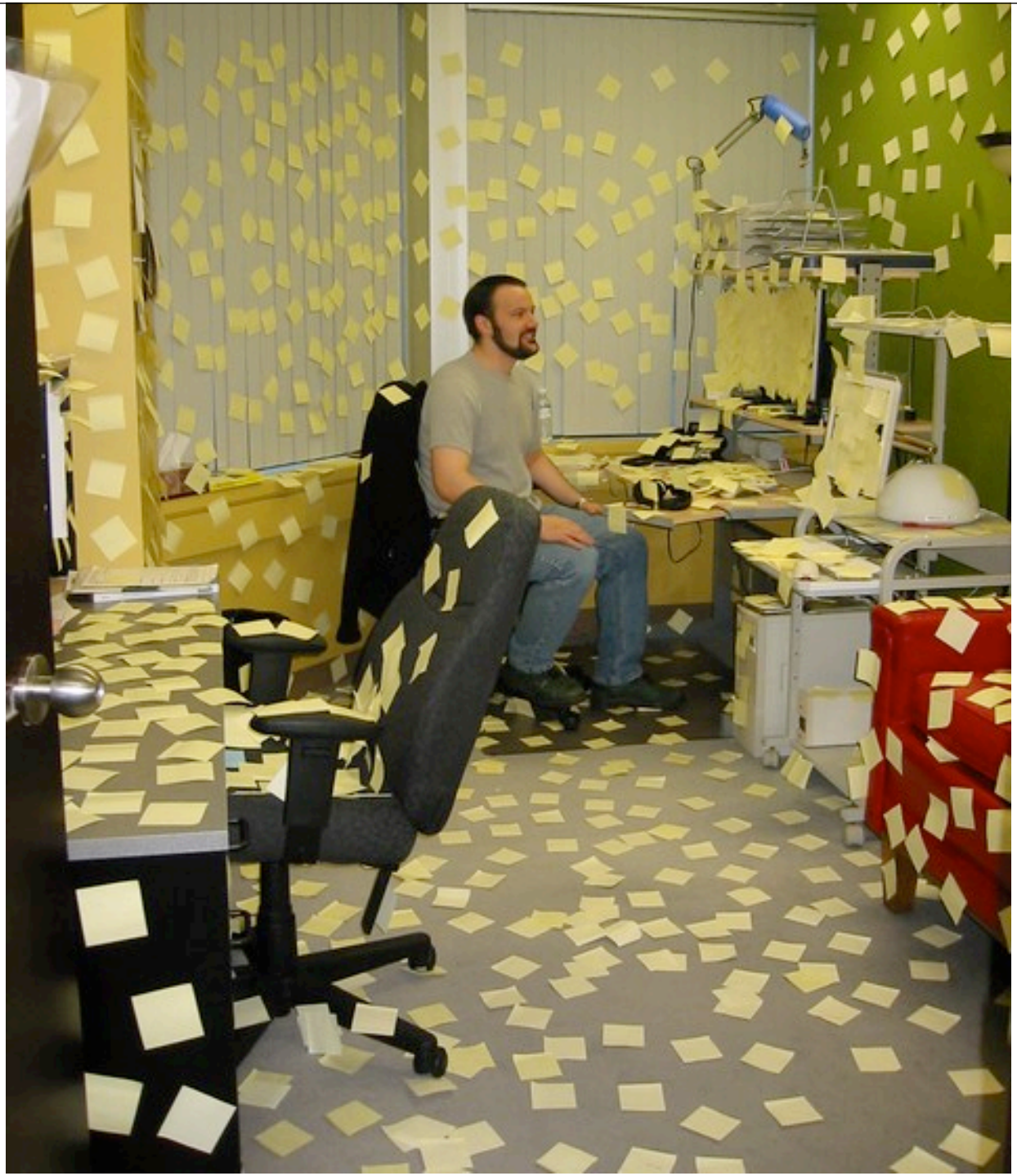


Image from http://www.interactivetools.com/staff/dave/damons_office/

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

Co

Faceb
been a
accoun

The CE
social n
at leas
of artic

As part
detailin
magaz
eviden

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

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

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.

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 (Last Time, Just a Reminder)

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)

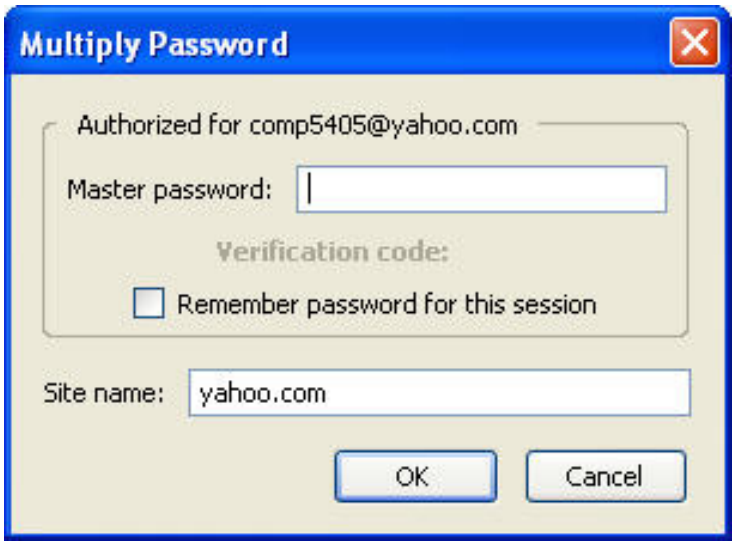
PwdHash

@@ 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 Security 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

[Chiasson, van Oorschot, Biddle]

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)

[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.
  - Big theme in course: sometimes things designed to increase security can also increase other risks

Questions

- Q1. What usable security features have you encountered in the past?
- Q2. What security features could have been more usable?

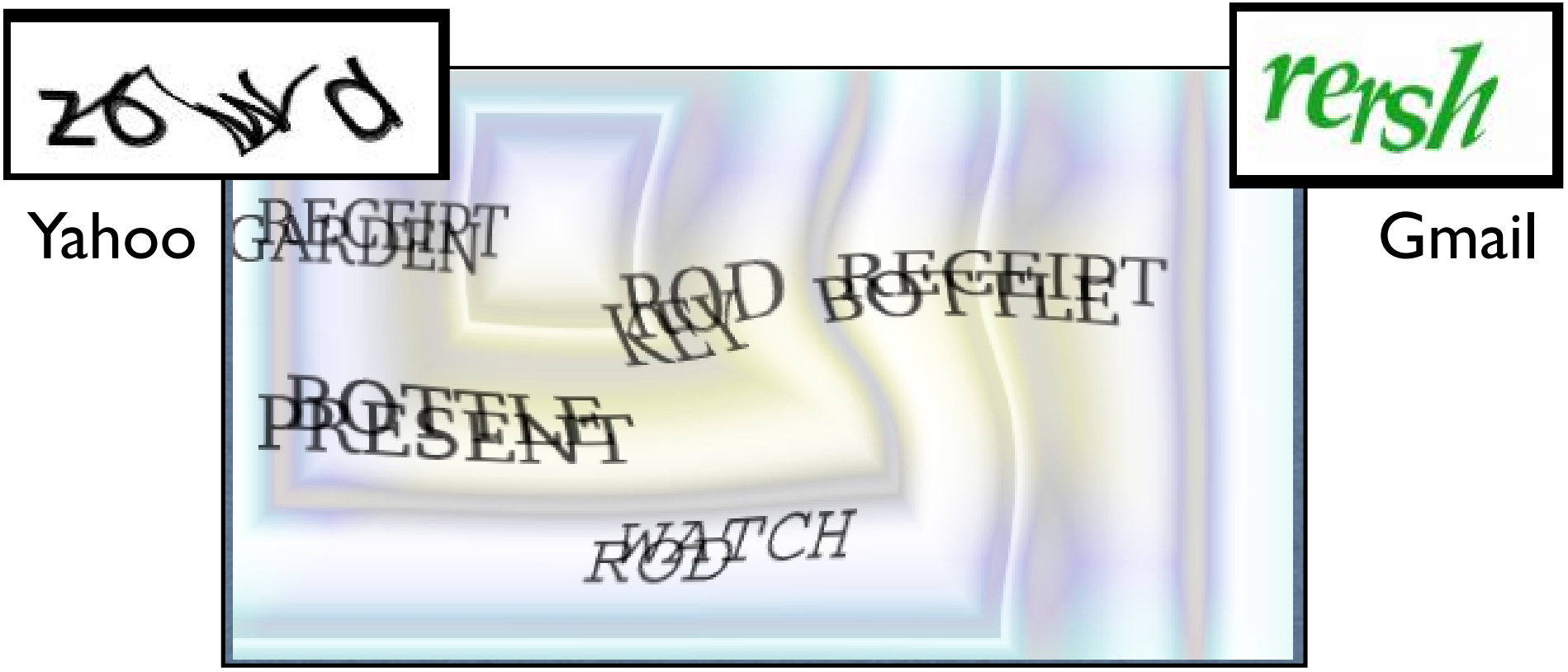
Human Factors in User Authentication

CAPTCHAs

Human Verification

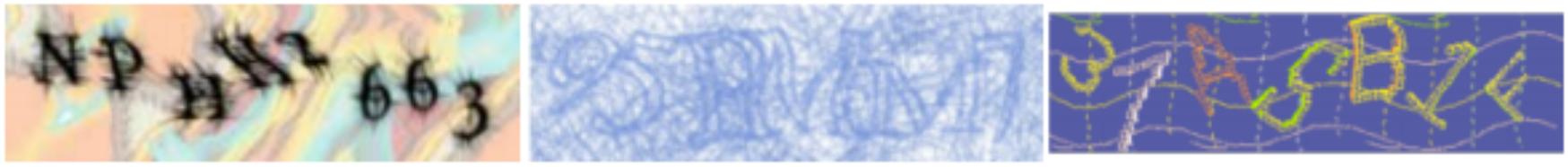
- Problem:
  - Want to make it hard for spammers to automatically create many free email accounts
  - Want to make it difficult for computers to automatically crawl some data repository
- Need a method for servers to distinguish between
  - Human users
  - Machine users
- Approach: CAPTCHA
  - Completely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

CAPTCHAs



captcha.net

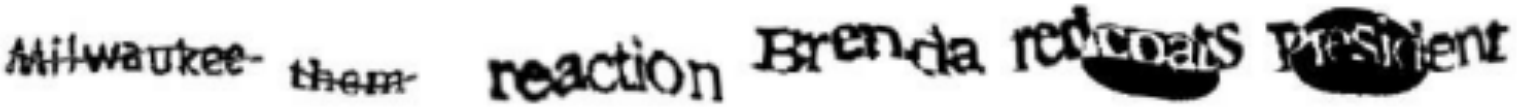
Idea: “easy” for humans to read words in this picture, but “hard” for computers



(a) Aol. (b) mail.ru (c) phpBB 3.0

(d) Simple Machines Forum (e) Yahoo! (f) youku

Figure 1: Examples of CAPTCHAs from various Internet properties.



(a) Early 2008 (b) December 16th 2009 (c) January 24th 2010

Figure 2: Examples of CAPTCHAs downloaded directly from reCaptcha at different time periods.

Image from http://static.usenix.org/event/sec10/tech/full_papers/Motoyama.pdf

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 Gi

Fo
inc
sn
Tic
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.

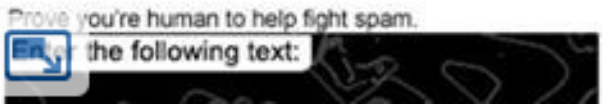
'Captcha' squiggles give way to ad pitches on security tests

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.



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.

Questions

- Q1. What do you like about CAPTCHAs?
- Q2. What do you dislike about CAPTCHAs?
- Q3. What properties of CAPTCHAs are valuable? (Related to Q1.)
- Q4. What properties of CAPTCHAs are "problematic"? (Related to Q2.)

- Q5. Should web sites use CAPTCHAs?

Caveats

- Usability challenges with visual impairments

Questions

- Q1. Suppose you are a spammer and want to create free accounts on Webmail Provider X, and Webmail Provider X uses CAPTCHAs during enrollment. How would you go about breaking those CAPTCHAs?

Caveats

- Researchers studying how to break CAPTCHAs
- Some attackers don't break CAPTCHAs; they hire or trick others
- Whole market set up around CAPTCHA solving

The following article describes an attack against the web images (so-called "CAPTCHAS") that are used to prevent robots from using certain web applications such as the creation of free e-mail accounts. The images are a form of "Turing Test", easy for a human user of normal ability to process, but difficult for a piece of software. The attack involves routing the CAPTCHA image to a page that advertises free porn. Users have to decode the CAPTCHA to get the advertised images and in doing so, unwitting assist spammers in creating bogus e-mail addresses.

"But at least one potential spammer managed to crack the CAPTCHA test. Someone designed a software robot that would fill out a registration form and, when confronted with a CAPTCHA test, would post it on a free porn site. Visitors to the porn site would be asked to complete the test before they could view more pornography, and the software robot would use their answer to complete the e-mail registration."

CAPTCHA-solving economies

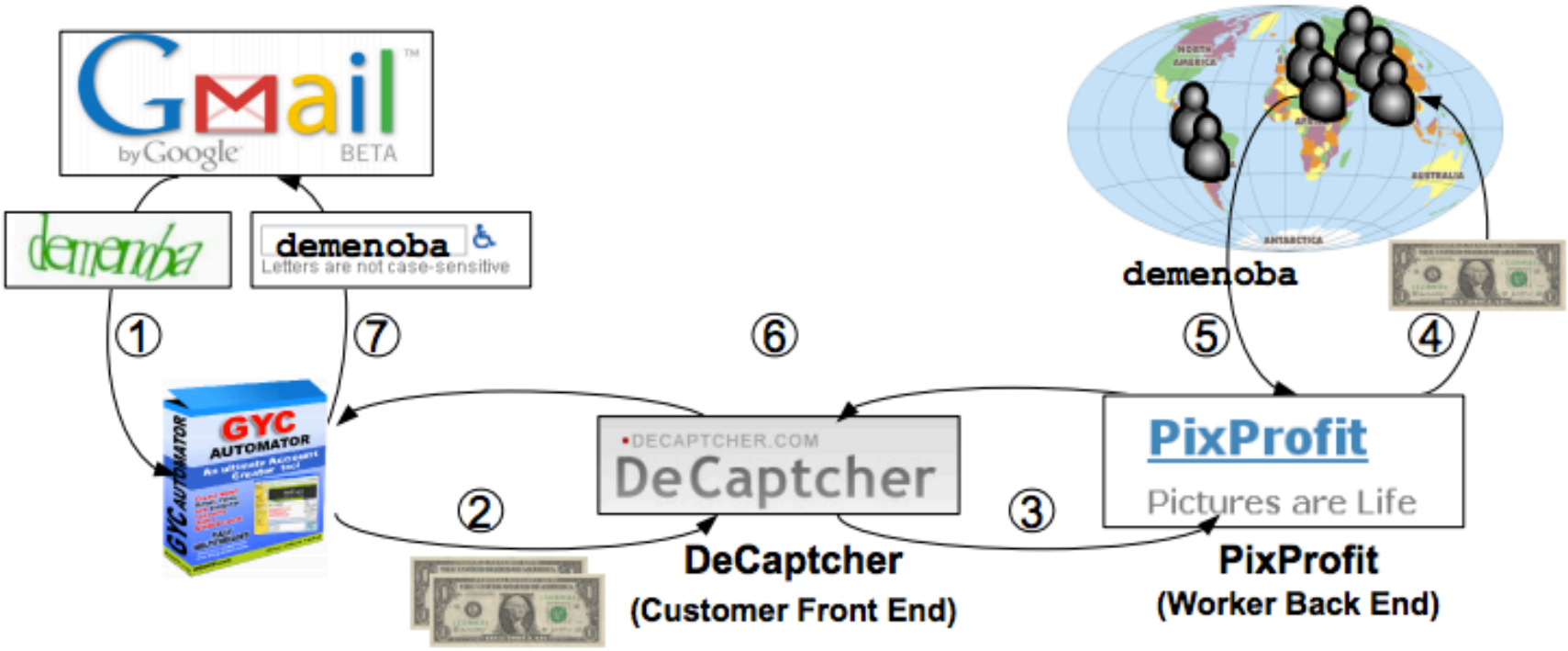


Figure 3: CAPTCHA-solving market workflow: ① GYC Automator attempts to register a Gmail account and is challenged with a Google CAPTCHA. ② GYC uses the DeCaptcher plug-in to solve the CAPTCHA at $2/1,000. ③ DeCaptcher queues the CAPTCHA for a worker on the affiliated PixProfit back end. ④ PixProfit selects a worker and pays at $1/1,000. ⑤ Worker enters a solution to PixProfit, which ⑥ returns it to the plug-in. ⑦ GYC then enters the solution for the CAPTCHA to Gmail to register the account.

Image from http://static.usenix.org/event/sec10/tech/full_papers/Motoyama.pdf

CAPTCHA-solving economies

Service	$/1K Bulk	Dates (2009–2010)	Requests	Responses
Antigate (AG)	$1.00	Oct 06 – Feb 01 (118 days)	28,210	27,726 (98.28%)
BeatCaptchas (BC)	$6.00	Sep 21 – Feb 01 (133 days)	28,303	25,708 (90.83%)
BypassCaptcha (BY)	$6.50	Sep 23 – Feb 01 (131 days)	28,117	27,729 (98.62%)
CaptchaBot (CB)	$1.00	Oct 06 – Feb 01 (118 days)	28,187	22,677 (80.45%)
CaptchaBypass (CP)	$5.00	Sep 23 – Dec 23 (91 days)	17,739	15,869 (89.46%)
CaptchaGateway (CG)	$6.60	Oct 21 – Nov 03 (13 days)	1,803	1,715 (95.12%)
DeCaptcher (DC)	$2.00	Sep 21 – Feb 01 (133 days)	28,284	24,411 (86.31%)
ImageToText (IT)	$20.00	Oct 06 – Feb 01 (118 days)	14,321	13,246 (92.49%)

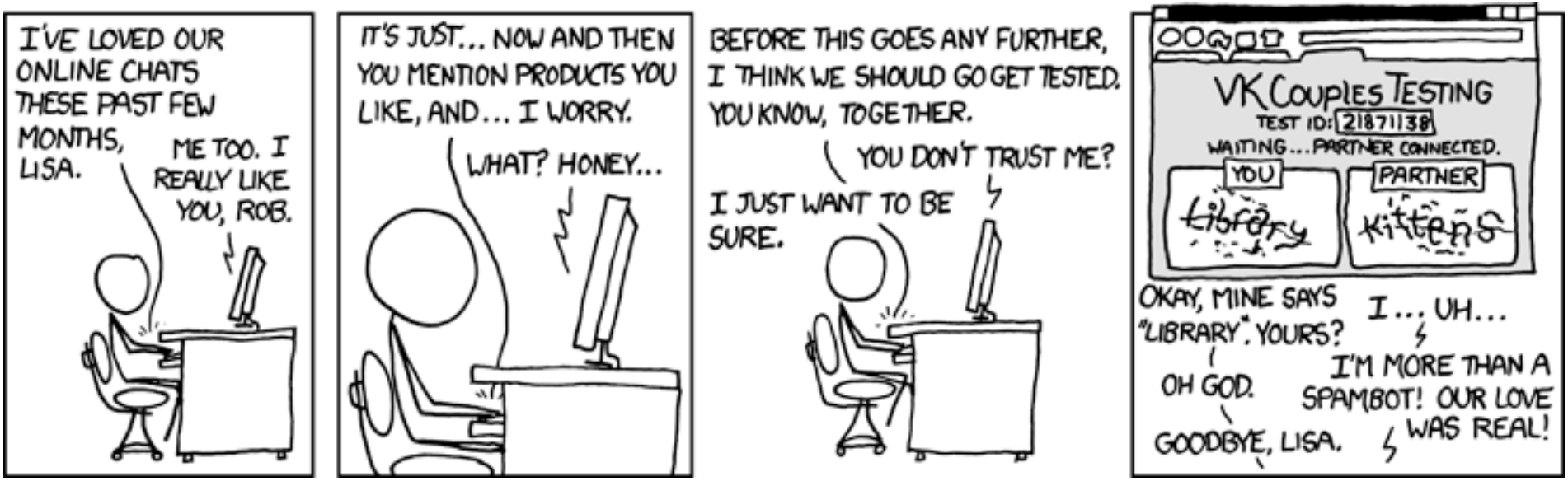
Table 1: Summary of the customer workload to the CAPTCHA-solving services.

Image from http://static.usenix.org/event/sec10/tech/full_papers/Motoyama.pdf

Language	Example	AG	BC	BY	CB	DC	IT	All
English	one two three	51.1	37.6	4.76	40.6	39.0	62.0	39.2
Chinese (Simp.)	一 二 三	48.4	31.0	0.00	68.9	26.9	35.8	35.2
Chinese (Trad.)	一 二 三	52.9	24.4	0.00	63.8	30.2	33.0	34.1
Spanish	uno dos tres	1.81	13.8	0.00	2.90	7.78	56.8	13.9
Italian	uno due tre	3.65	8.45	0.00	4.65	5.44	57.1	13.2
Tagalog	isá dalawá tatló	0.00	5.79	0.00	0.00	7.84	57.2	11.8
Portuguese	um dois três	3.15	10.1	0.00	1.48	3.98	48.9	11.3
Russian	один два три	24.1	0.00	0.00	11.4	0.55	16.5	8.76
Tamil	ஒன்று இரண்டு மூன்று	2.26	21.1	3.26	0.74	12.1	5.36	7.47
Dutch	een twee drie	4.09	1.36	0.00	0.00	1.22	31.1	6.30
Hindi	एक दो तीन	10.5	5.38	2.47	1.52	6.30	9.49	5.94
German	eins zwei drei	3.62	0.72	0.00	1.46	0.58	29.1	5.91
Malay	satu dua tiga	0.00	1.42	0.00	0.00	0.55	29.4	5.23
Vietnamese	một hai ba	0.46	2.07	0.00	0.00	1.74	18.1	3.72
Korean	일 이 삼	0.00	0.00	0.00	0.00	0.00	20.2	3.37
Greek	ένα δύο τρία	0.45	0.00	0.00	0.00	0.00	15.5	2.65
Arabic	واحد اثنين ثلاثة	0.00	0.00	0.00	0.00	0.00	15.3	2.56
Bengali	এক দুই তিন	0.45	0.00	9.89	0.00	0.00	0.00	1.72
Kannada	ಒಂದು ಎರಡು ಮೂರು	0.91	0.00	0.00	0.00	0.55	6.14	1.26
Klingon		0.00	0.00	0.00	0.00	0.00	1.12	0.19
Farsi	یک دو سه	0.45	0.00	0.00	0.00	0.00	0.00	0.08

Table 2: Percentage of responses from the services with correct answers for the language CAPTCHAs.

Image from http://static.usenix.org/event/sec10/tech/full_papers/Motoyama.pdf


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
PARTNER
library
kittens
OKAY, MINE SAYS "LIBRARY". YOURS?
I... UH...
OH GOD.
I'M MORE THAN A SPAMBOT! OUR LOVE WAS REAL!
GOODBYE, LISA.

Phishing

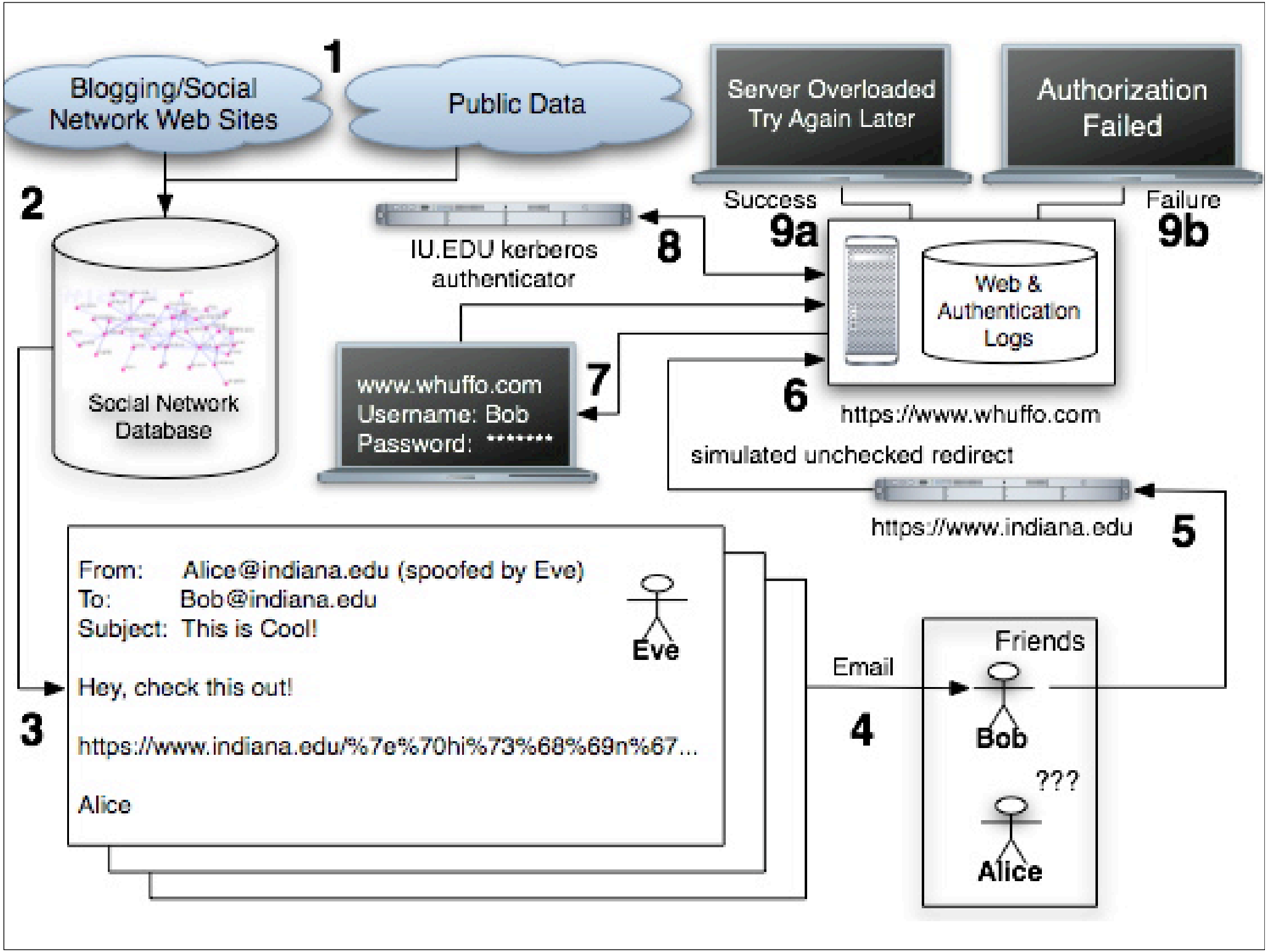
- "The Emperor's New Security Indicators"
  - http://www.usablesecurity.org/emperor/emperor.pdf
- "Why Phishing Works"
  - http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf

- 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

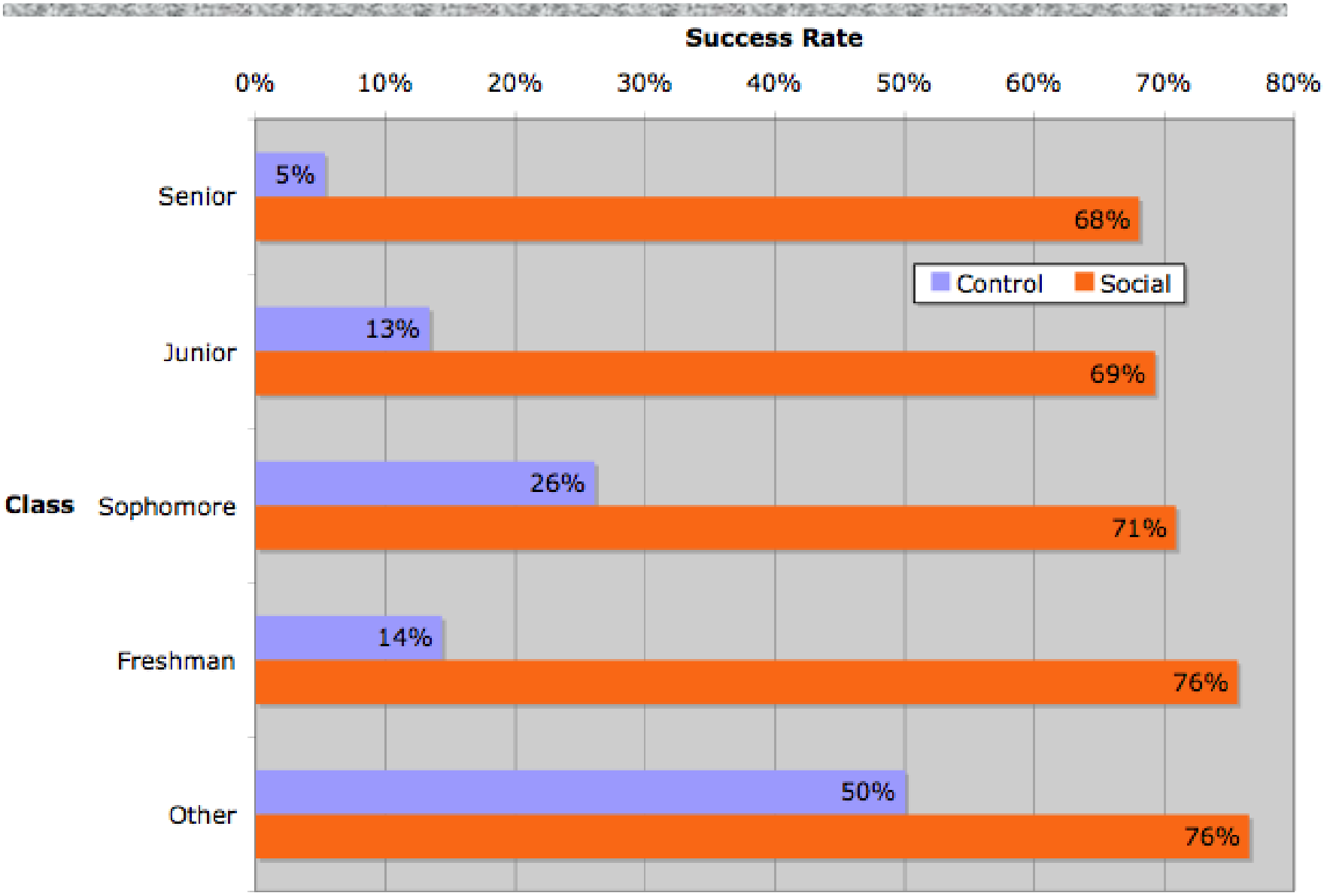

Blogging/Social Network Web Sites
1
Public Data
Server Overloaded Try Again Later
Authorization Failed
2
Success
9a
Failure
9b
IU.EDU kerberos authenticator
8
Web & Authentication Logs
Social Network Database
www.whuffo.com
Username: Bob
Password: *******
7
6
https://www.whuffo.com
simulated unchecked redirect
https://www.indiana.edu
5
From: Alice@indiana.edu (spoofed by Eve)
To: Bob@indiana.edu
Subject: This is Cool!
Hey, check this out!
https://www.indiana.edu/%7e%70hi%73%68%69n%67...
Alice
Eve
3
Email
4
Friends
Bob
???
Alice

More Details

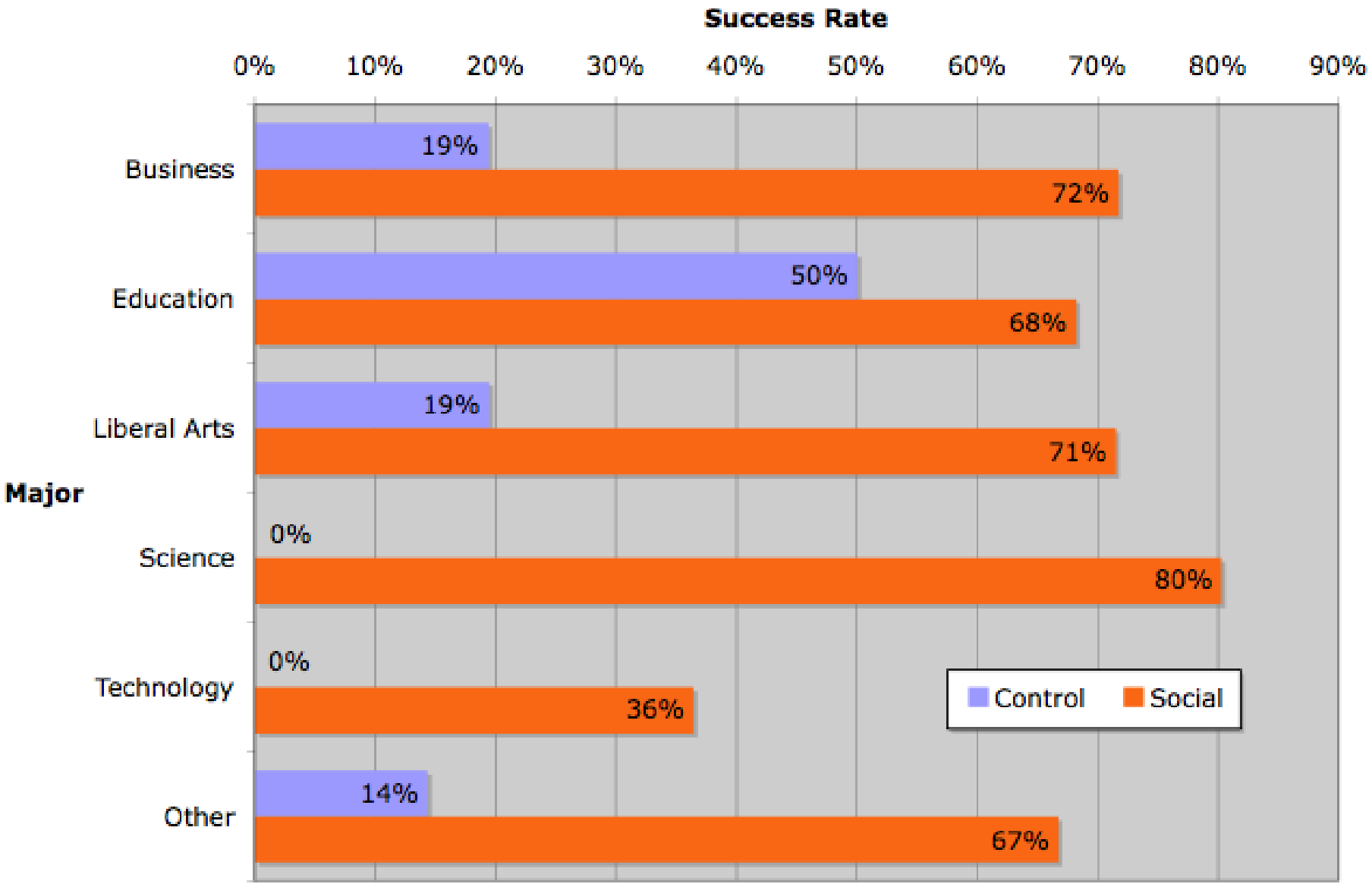
- Control group: 15 of 94 (16%) entered personal information
- Social group: 349 of 487 (72%) entered personal information

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

More Details (Class Year)



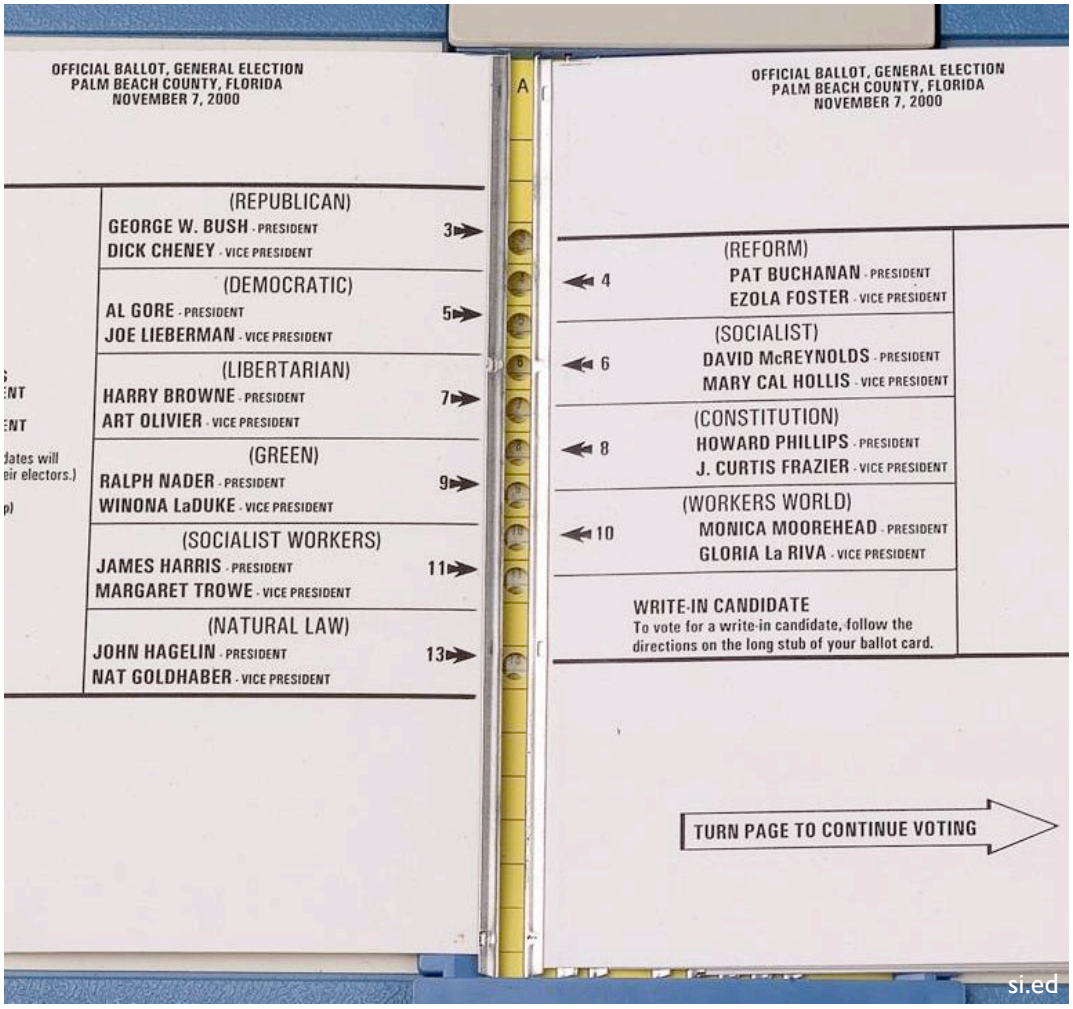
More Details (Major)



Questions

- Q. What are the root causes of usability issues in computer security?

Poor Usability Causes Problems



AP

Importance

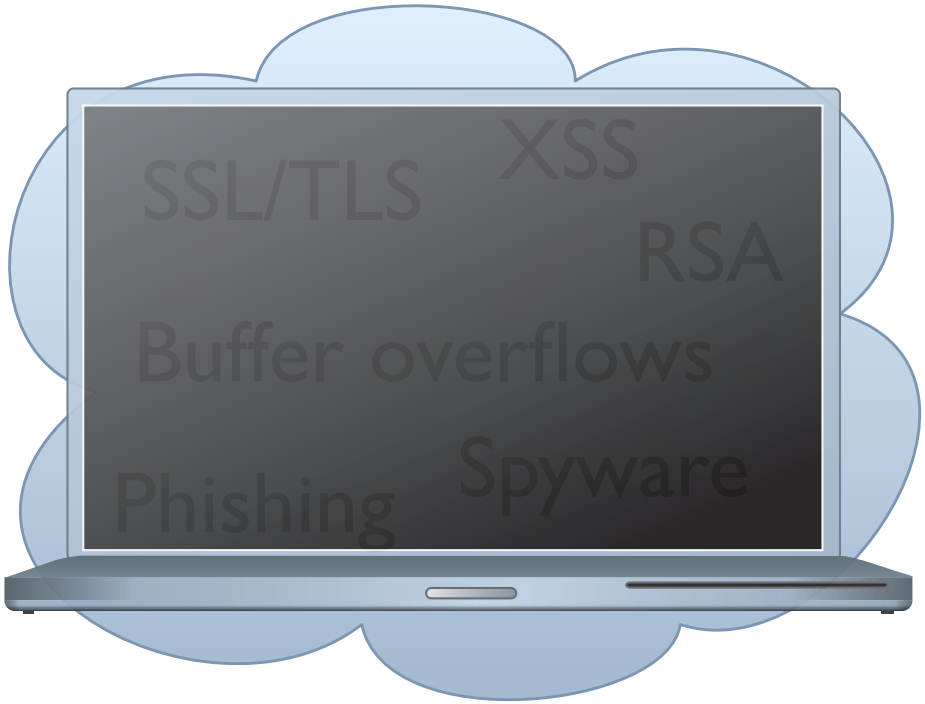
- Why is usability important?
  - People are the critical element of any computer system
    - People are the real reason computers exist in the first place
  - Even if it is **possible** for a system to protect against an adversary, people may use the system in other, **less secure** ways
- Next
  -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



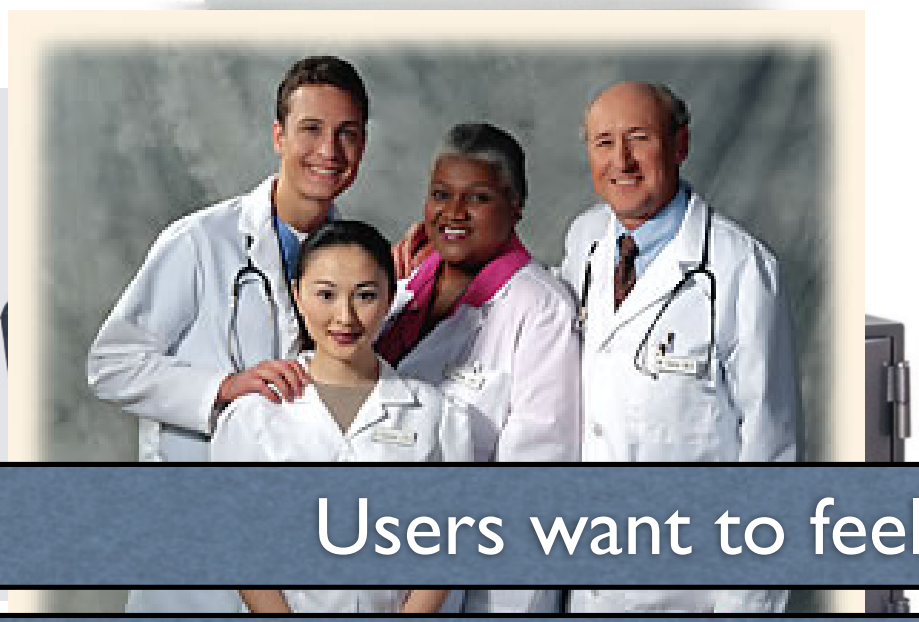
Too complex, hidden, no intuition.

Issue #1: Complexities, Lack of Intuition

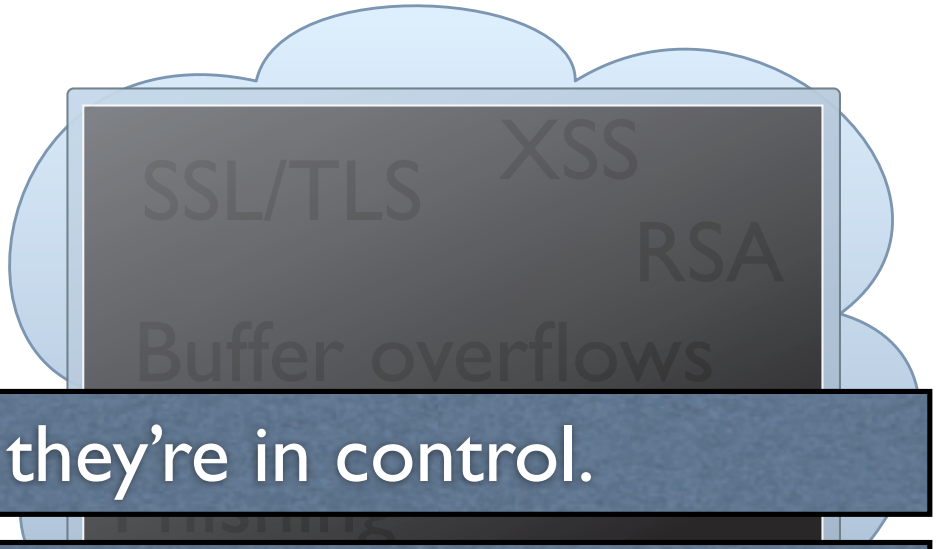
- Mismatch between perception of technology and what really happens
  - Public keys?
  - Signatures?
  - Encryption?
  - Message integrity?
  - Chosen-plaintext attacks?
  - Chosen-ciphertext attacks?
  - Password management?
  - …

Issue #2: Who's in Charge?

Real World



Electronic World



Users want to feel like they're in control.

Where analogy breaks down: *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
  - User-driven access control
    - http://www.franziroesner.com/pdf/udac-oakland2012.pdf
- 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)

- Also, recall that a user's poor security choices may affect **other** people
  - E.g., compromise account of user with weak password, then exploit a local (rather than remote) vulnerability to get root access

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

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
  - (User-driven access control)

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