CSE 484 (Winter 2010)

User Authentication
+
Other 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

- User authentication
- Phishing

Password Managers

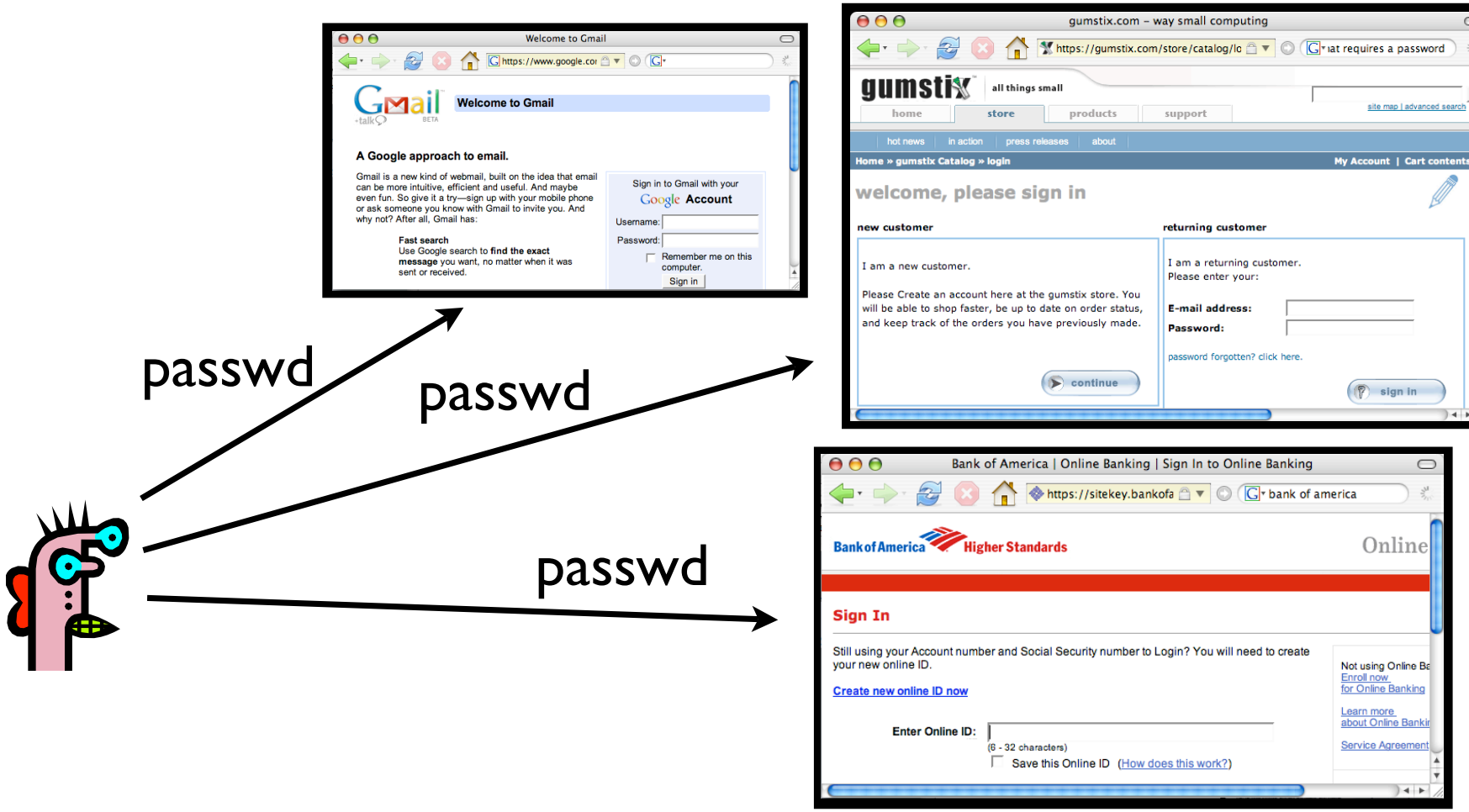
- Idea: Software application that will store and manage passwords for you.
  - You remember one password.
  - Each website sees a different password.
- Examples: PwdHash (Usenix Security 2005) and Password Multiplier (WWW 2005).

Key ideas

- User remembers a single password
- Password managers
  - On input: (1) the user's single password and (2) information about the website
  - Compute: Strong, site-specific password
- Goal: Avoid problems with passwords

The problem

Alice needs passwords for all the websites that she visits



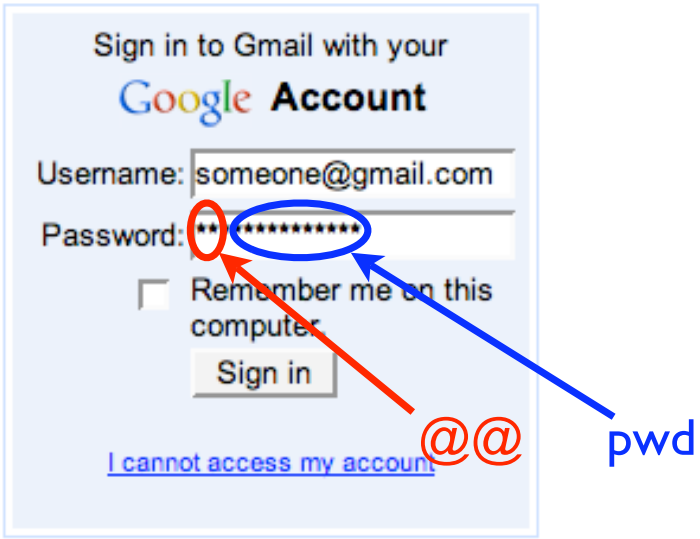
Possible solutions

- 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.

Alternate solution: 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

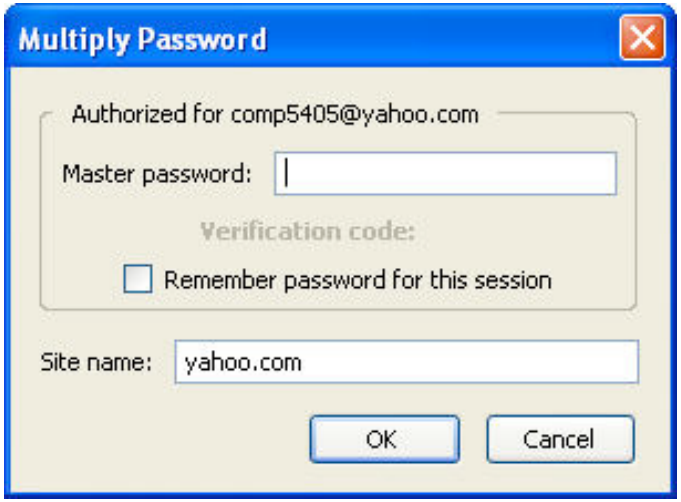


@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd,domain)

Prevent phishing attacks

Password Multiplier



Active with Alt-P or double-click

sitePwd = Hash(usrname, 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 paper 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]

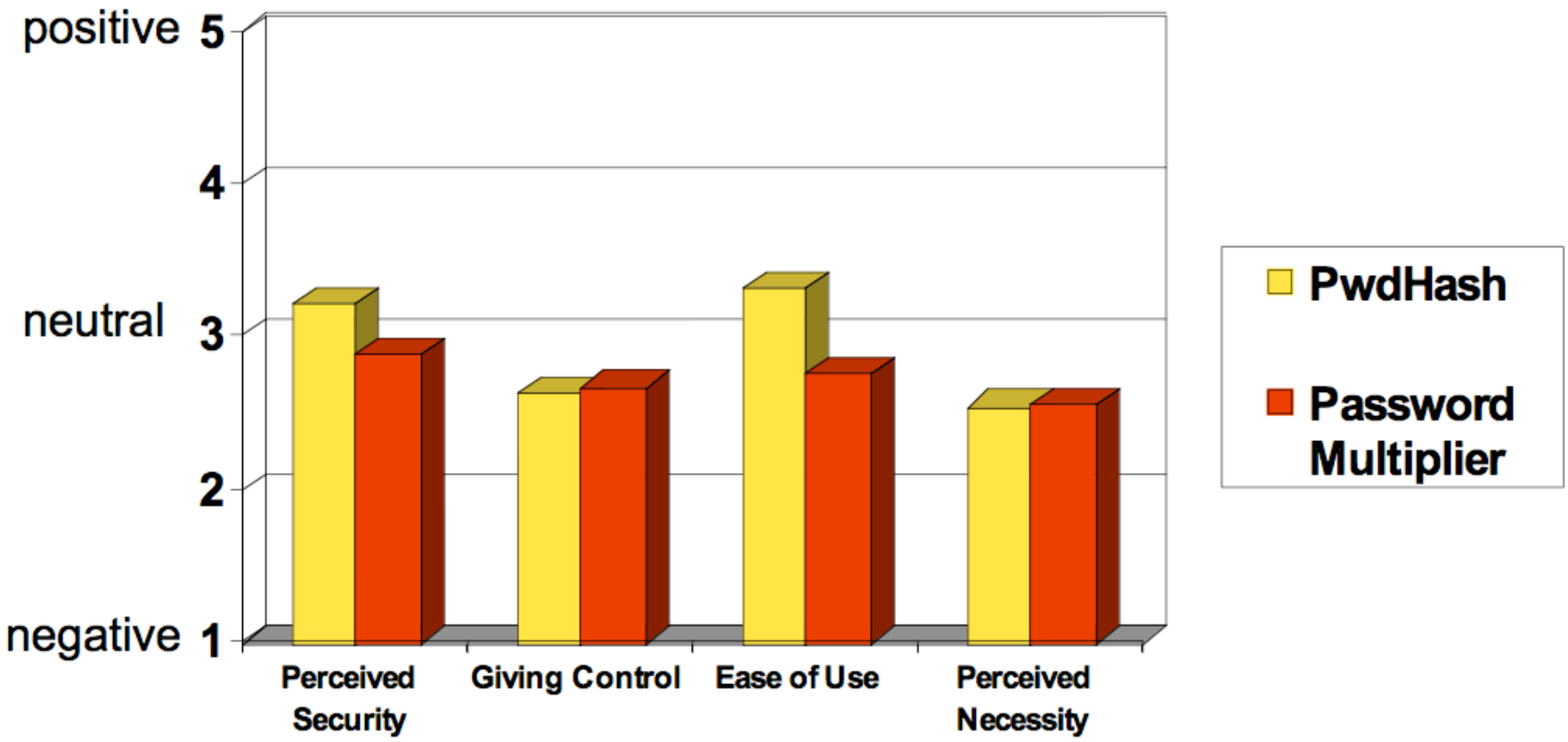
Task completion results

	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

[Chiasson, van Oorschot, Biddle]

Questionnaire responses



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.

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 r
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'.

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

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

Caveats

- Usability challenges with visual impairments
- Researchers studying how to break CAPTCHAs
- Some attackers don't break CAPTCHAs; they hire or trick others

PCMAG.COM

Four Indicted in CAPTCHA Hacks of Ticket Sites

03.01.10

1 Comment

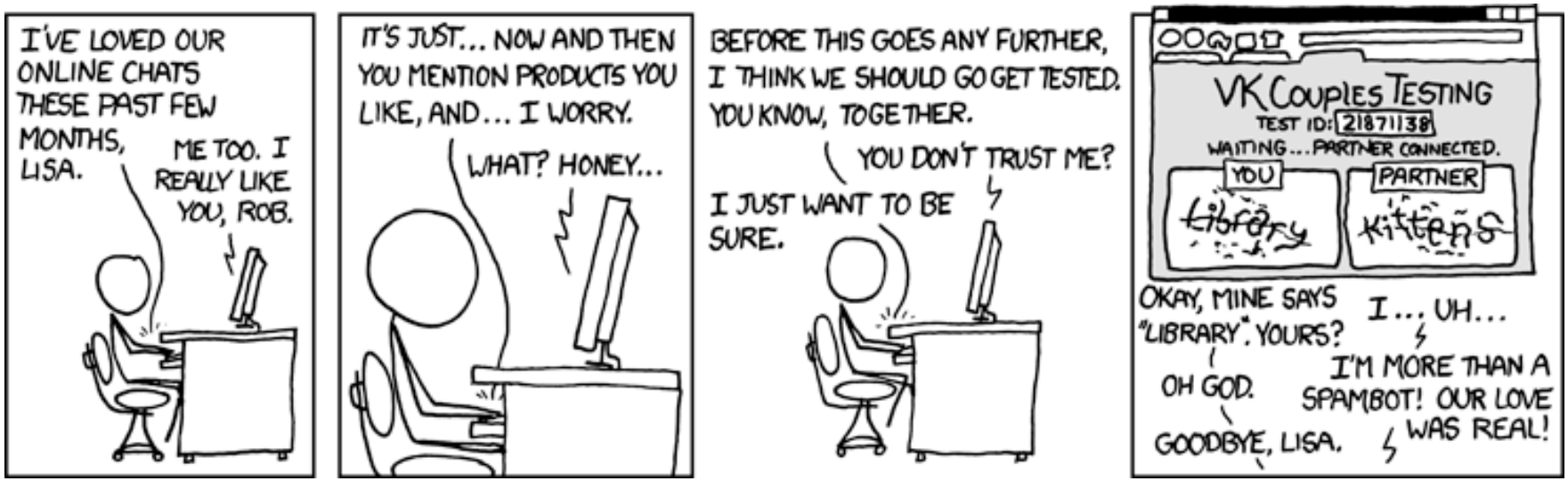
By Chloe Albanesius

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.


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

More Details

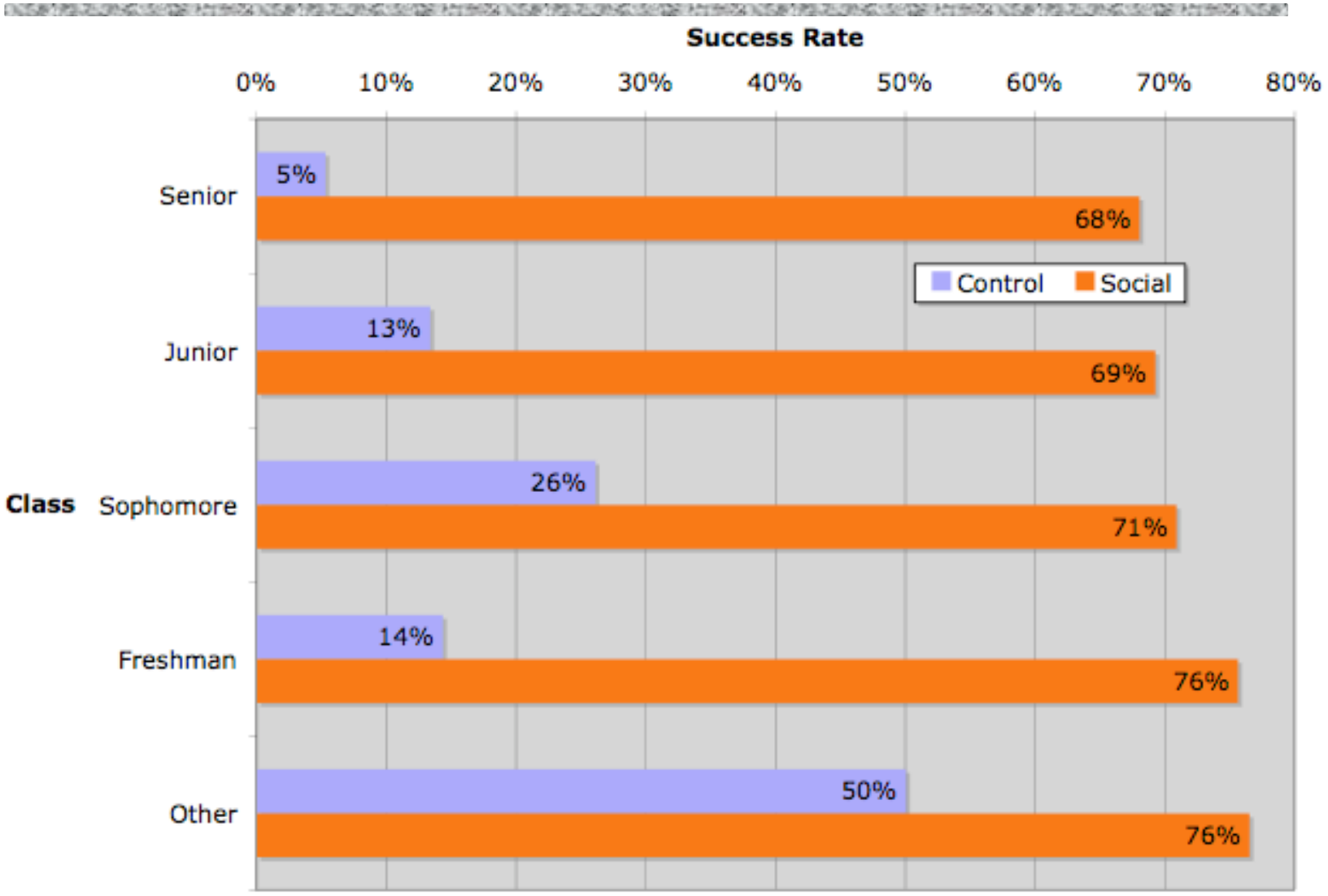
- Control group: 15 of 94 (16%) entered personal information
- Social group: 349 of 487 (72%) entered personal information

- 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



More Details