CSE 484 / CSE M 584 (Autumn 2011)

Human Factors in Security (cont.)

Daniel Halperin
Tadayoshi Kohno

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

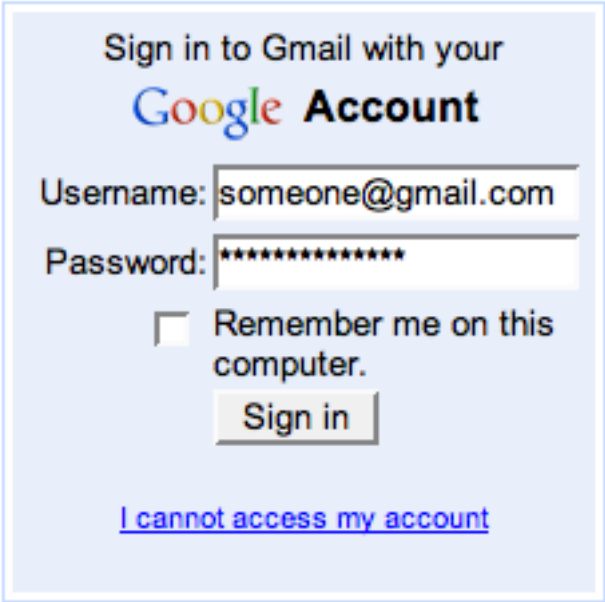
Updates, 11/16

- Lab #1 grades on Catalyst; other grades soon
- Lab #2
  - Due ~~Friday~~ **next Monday, 11/21**
- Second security review & current event due 12/2
  - Extra credit for every week early

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)

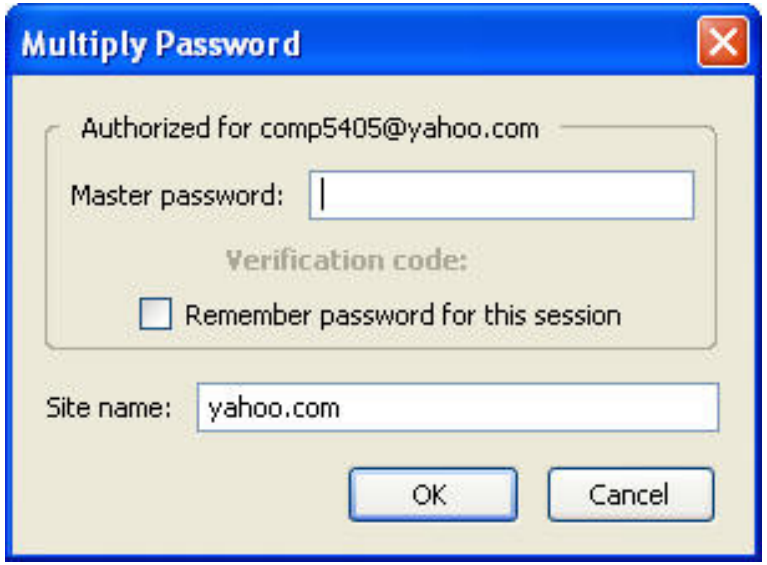
PwdHash



@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd,domain)

Password Multiplier



Activate with Alt-P or double-click

sitePwd = Hash(username, pwd, domain)

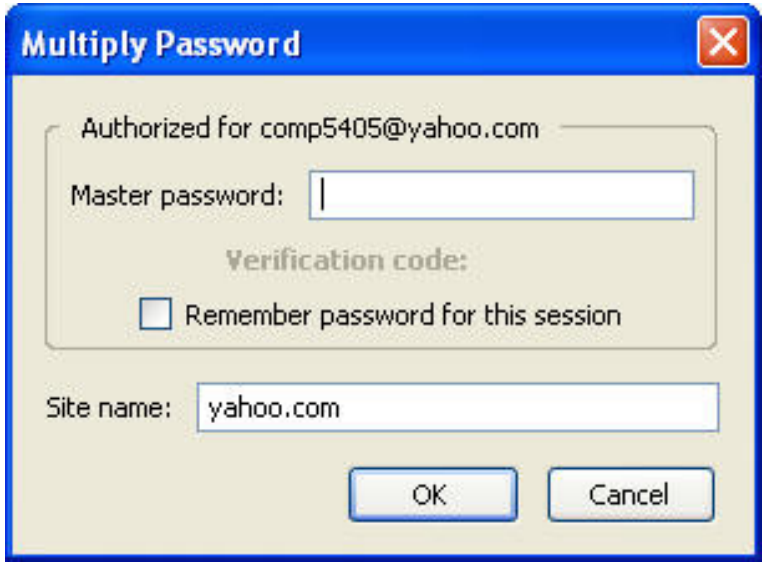
Both solutions target simplicity and transparency.

PwdHash

@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd,domain)

Password Multiplier



Activate with Alt-P or double-click

sitePwd = Hash(username, pwd, domain)

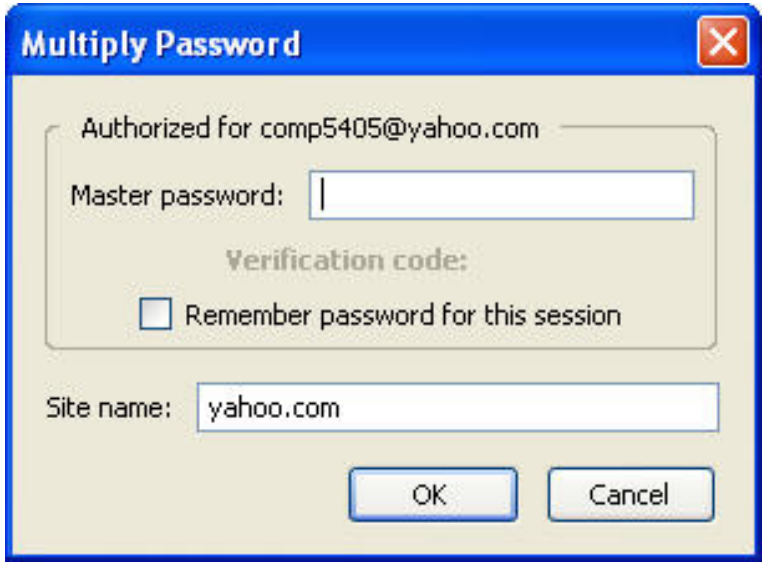
Both solutions target simplicity and transparency.

PwdHash

@@ in front of passwords to protect; or F2

sitePwd = Hash(pwd,domain)

Password Multiplier



Activate with Alt-P or double-click

sitePwd = Hash(username, pwd, domain)

Both solutions target simplicity and transparency.

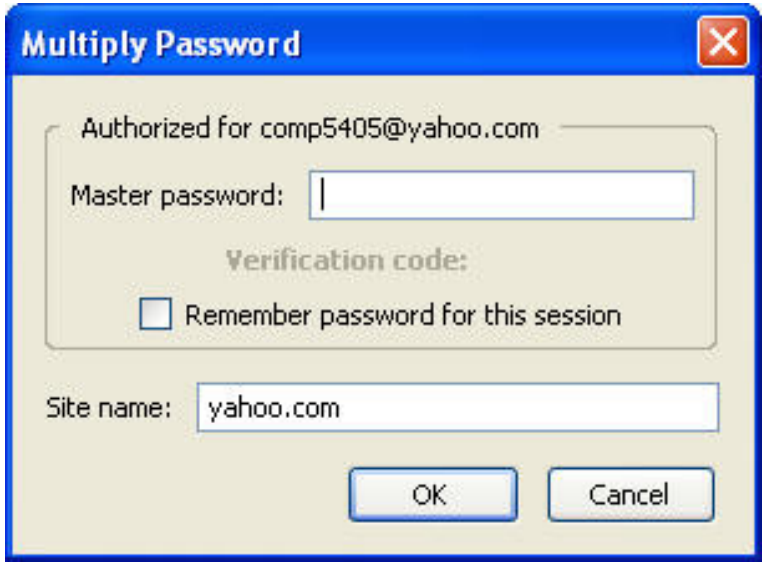
PwdHash

@@ 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

- 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

Usenix 2006: Usability testing

- 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

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

[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]

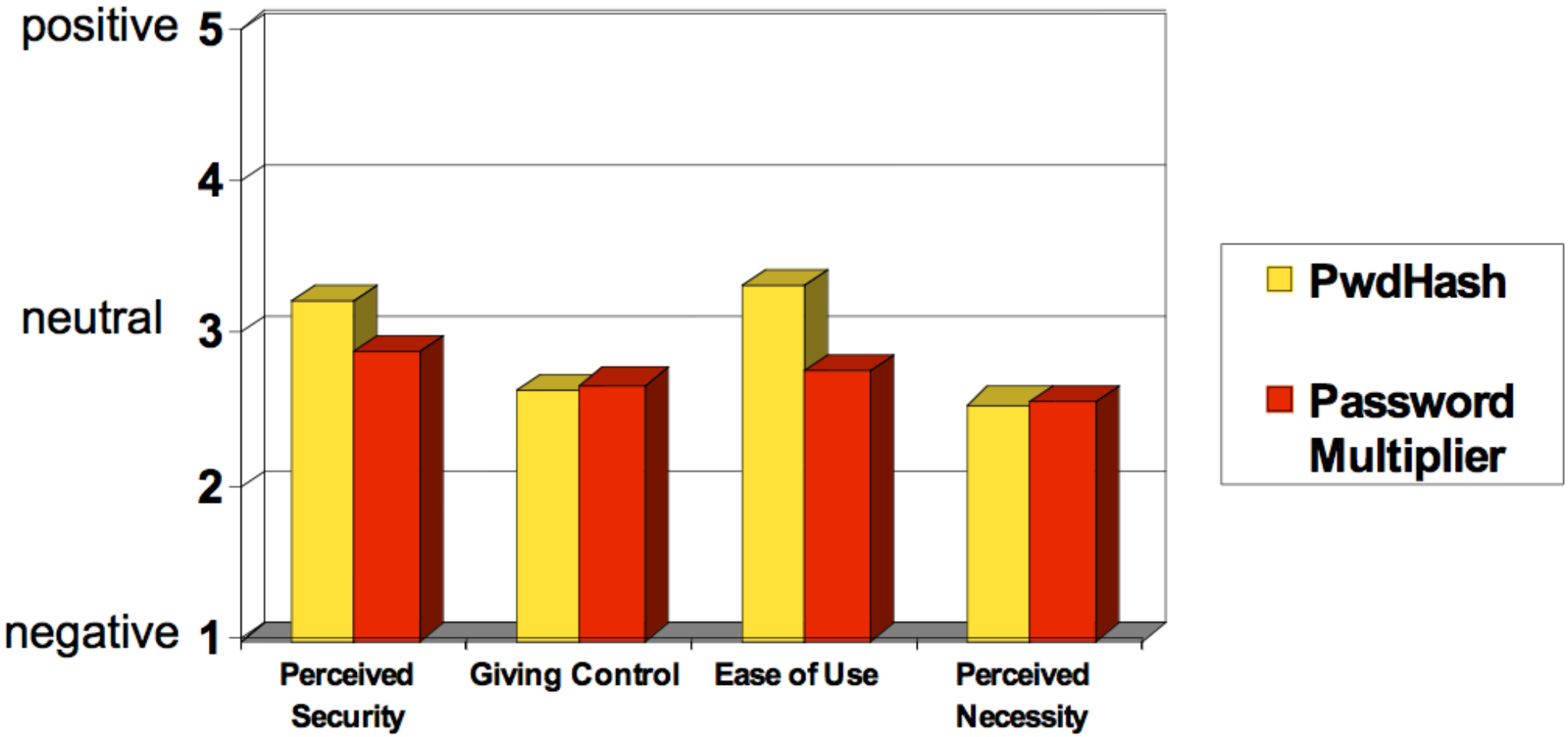
Task completion results

	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.

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.

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

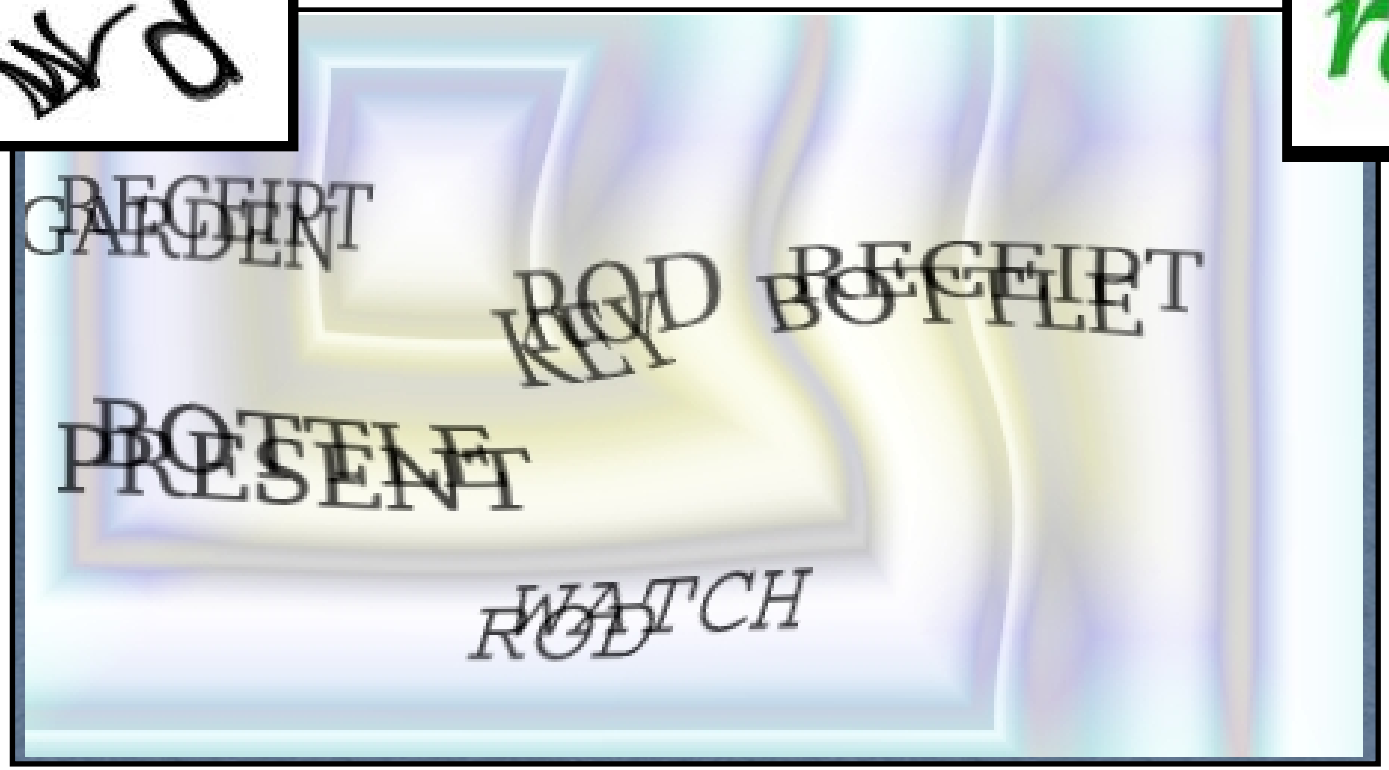
CAPTCHAs

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

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 Giants Stadium? You might have an illegal online ticket racket to thank.

Four men, operating under a company known as Wiseguy Tickets, were indicted Monday on charges that they used a complex computer program to snap up some of the best seats to popular events being sold on Ticketmaster, Tickets.com, MLB.com, MusicToday, and other online ticket vendors, and re-sell them at a hefty profit, according to the Department of Justice.

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.

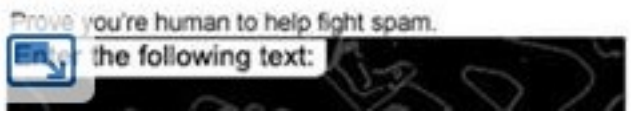
'Captcha' squiggles give way to ad pitches on security tests

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.

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.]

Experiments at Indiana University

[Jagatic et al.]

- Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster

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

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