CSE 484 and CSE M 584 (Winter 2009)

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 ...

Administrivia

- Final on March 18
  - Closed notes; closed electronic devices
- Today:
  - Human aspects of security (beyond just usability)
- Next week:
  - Research presentations
    - Valuable practice for presenters
    - Opportunity to hear about emerging directions

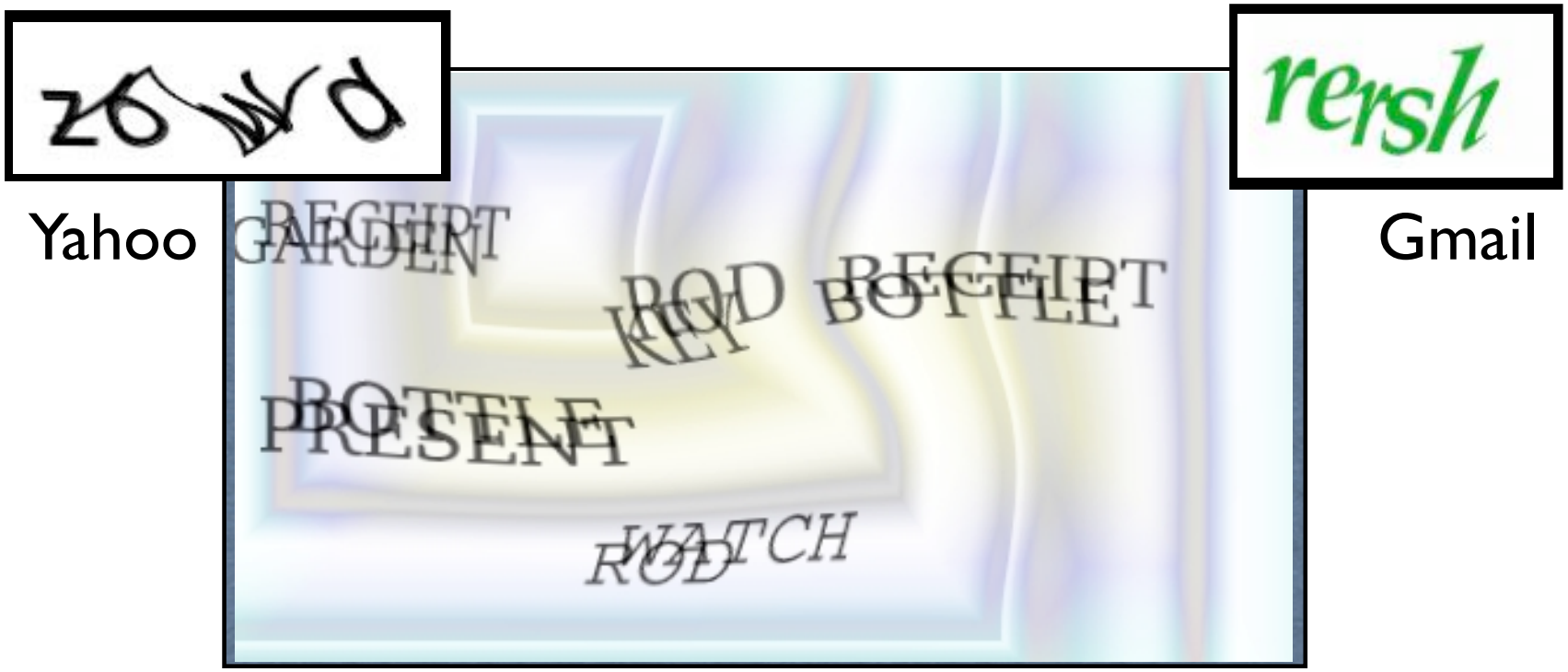
Next week

- Mon:
  - How to 0wn the Internet in Your Spare Time
  - Spamalytics: An Emperical Analysis of Spam Marketing Conversion
  - Why Phishing Works
  - Tor: Second-generation Onion Router
- Wed:
  - RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads
  - Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-power Defenses
  - Improving Wireless Privacy with an Identifier-Free Link Layer Protocol

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

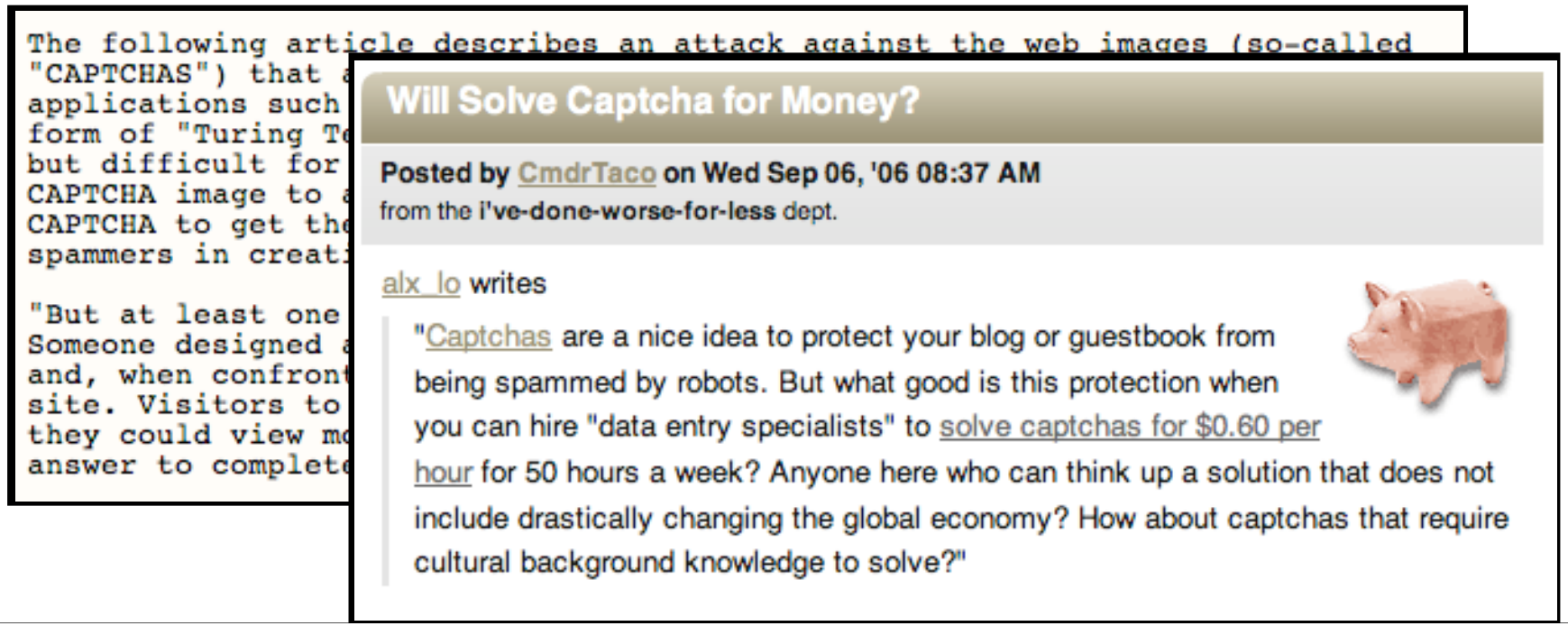
CAPTCHAs



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



Social Engineering & Phishing

- Create a bank page advertising an interest rate slightly higher than any real bank; ask users for their credentials to initiate money transfer
  - Some victims provided their bank account numbers to "Flintstone National Bank" of "Bedrock, Colorado"
  - http://www.antiphishing.org/Phishing-dhs-report.pdf
- Exploit social network
  - Spoof an email from a Facebook or MySpace friend
  - In a West Point experiment, 80% of cadets were deceived into following an embedded link regarding their grade report from a fictitious colonel

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
  - Males more likely to do this if email is from a female

More Details

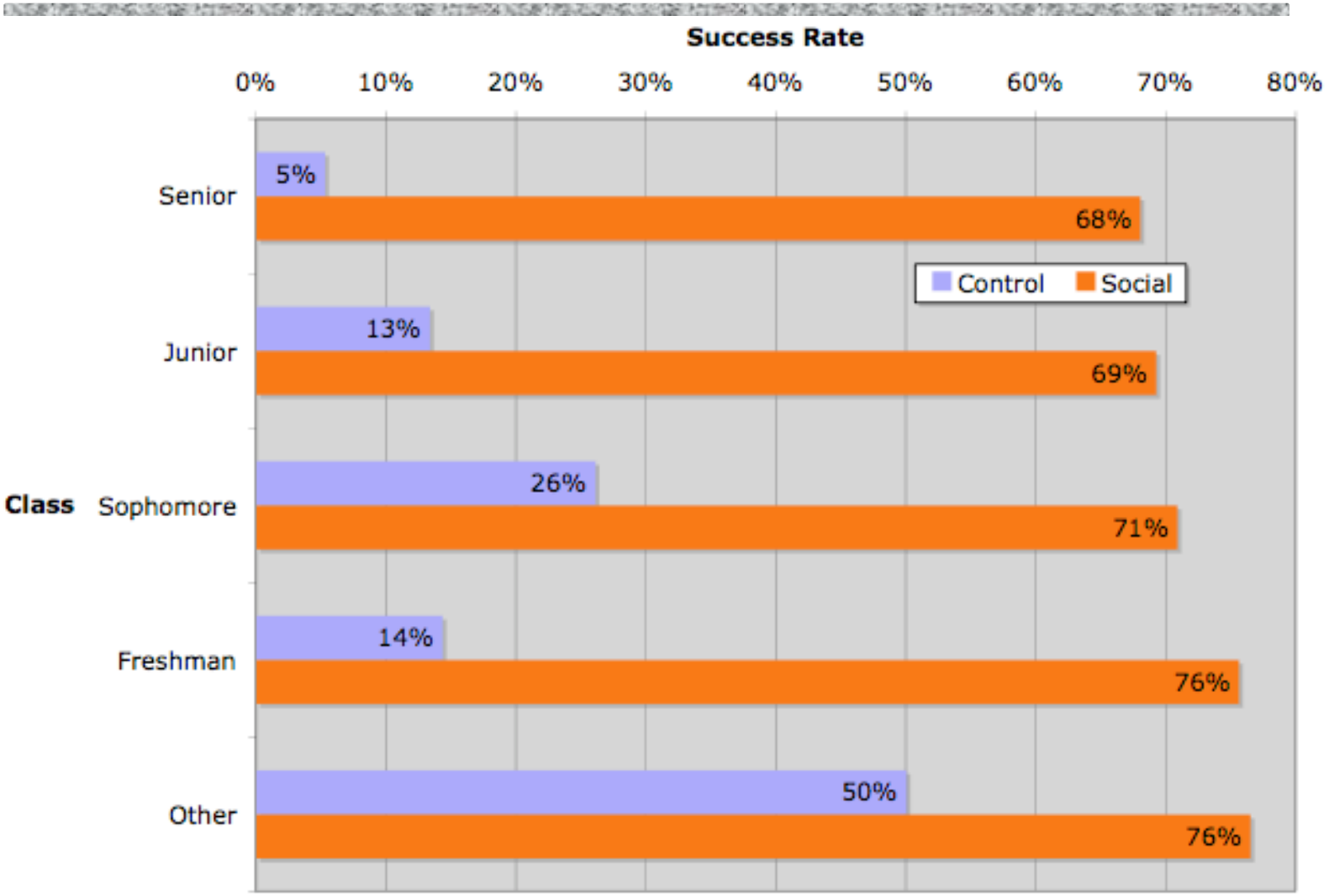
- Control group: 15 of 94 (16%) entered personal information
- Social group: 349 of 487 (72%) entered personal information

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

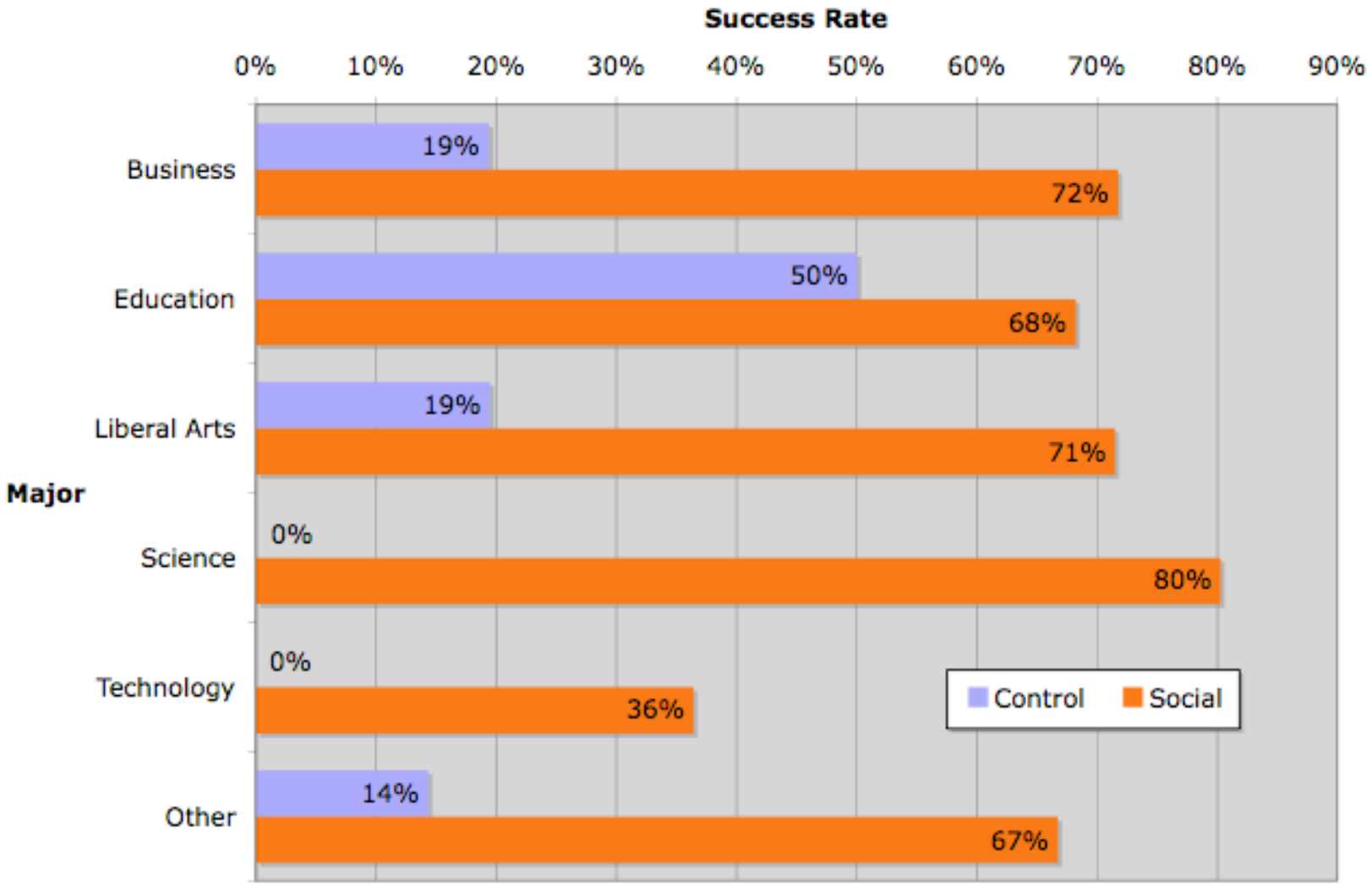
More Details

	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



Seven Stages of Grief

[according to Elizabeth Kübler-Ross]

- Shock or disbelief
- Denial
- Bargaining
- Guilt
- Anger
- Depression
- Acceptance

Victims' Reactions (1)

[Jagatic et al.]

- Anger
  - Subjects called the experiment unethical, inappropriate, illegal, unprofessional, fraudulent, self-serving, useless
  - They called for the researchers conducting the study to be fired, prosecuted, expelled, or reprimanded
- Denial
  - No posted comments included an admission that the writer had fallen victim to the attack
  - Many posts stated that the poster did not and would never fall for such an attack, and they were speaking on behalf of friends who had been phished

Victims' Reactions (2)

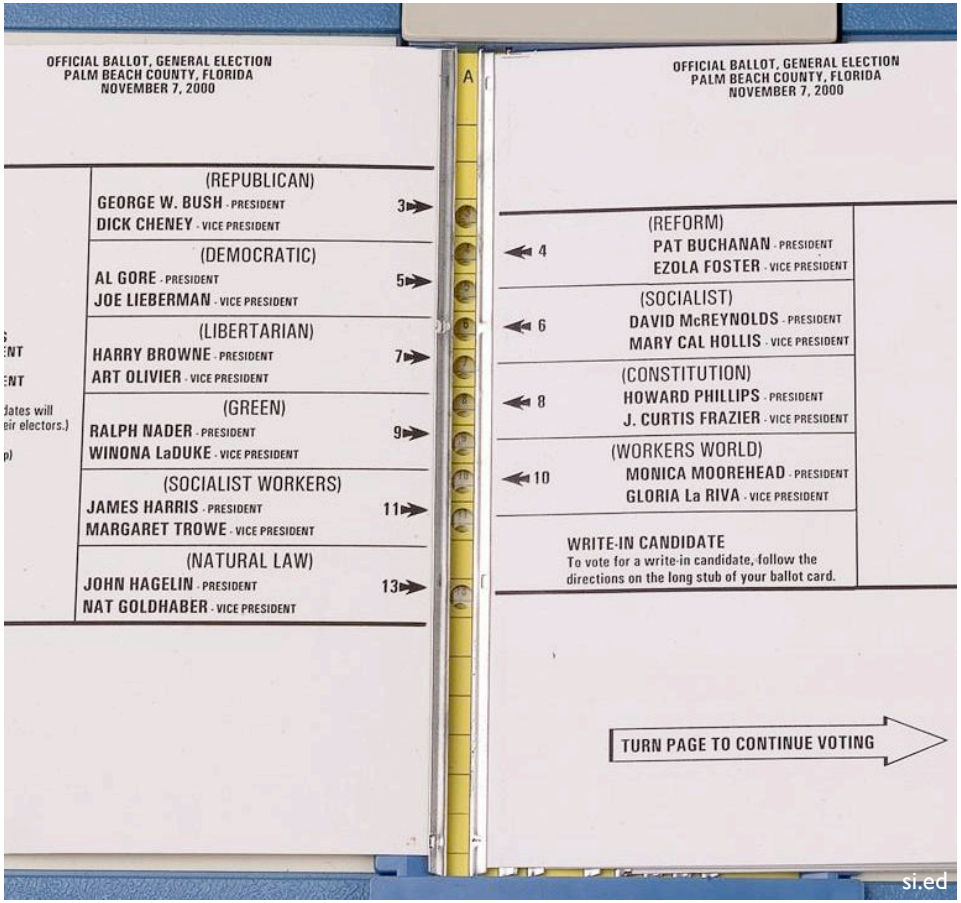
[Jagatic et al.]

- Misunderstanding
  - Many subjects were convinced that the experimenters hacked into their email accounts. They believed it was the only possible explanation for the spoofed messages.
- Underestimation of privacy risks
  - Many subjects didn't understand how the researchers obtained information about their friends, and assumed that the researchers accessed their address books
  - Others, understanding that the information was mined from social network sites, objected that their privacy had been violated by the researchers who accessed the information that they had posted online

Social aspects

Slides based on Gaw et al's at CHI 2006: http://www.cs.princeton.edu/~sgaw/publications/presentations/CHI2006-sgaw.ppt

Poor Usability Causes Problems



AP

Importance

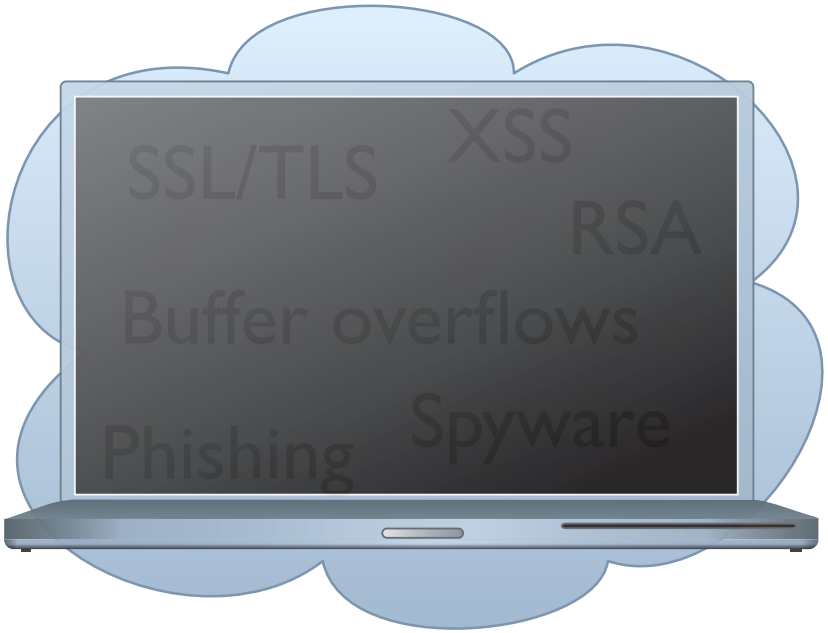
- Why is usability important?
  - People are the critical element of any computer system
    - People are the real reason computers exist in the first place
  - Even if it is **possible** for a system to protect against an adversary, people may use the system in other, **less secure** ways
- Today
 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

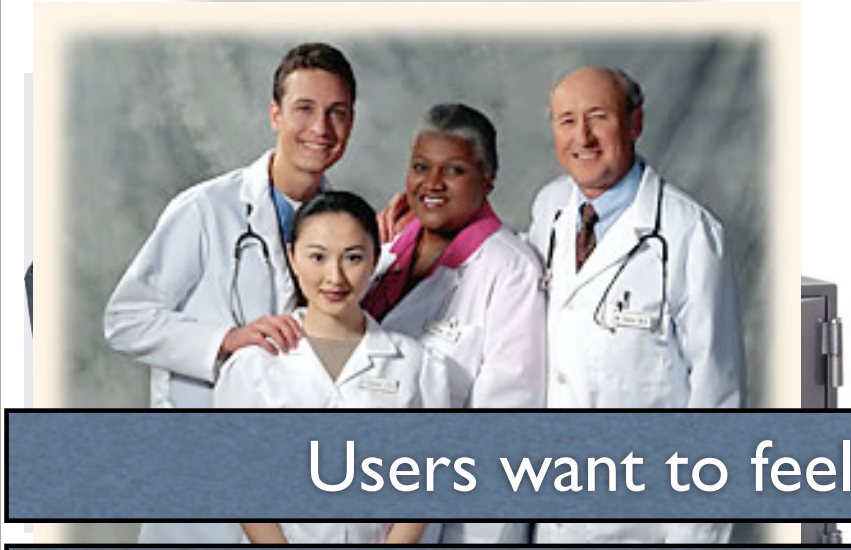
Issue #1: Complexities, Lack of Intuition

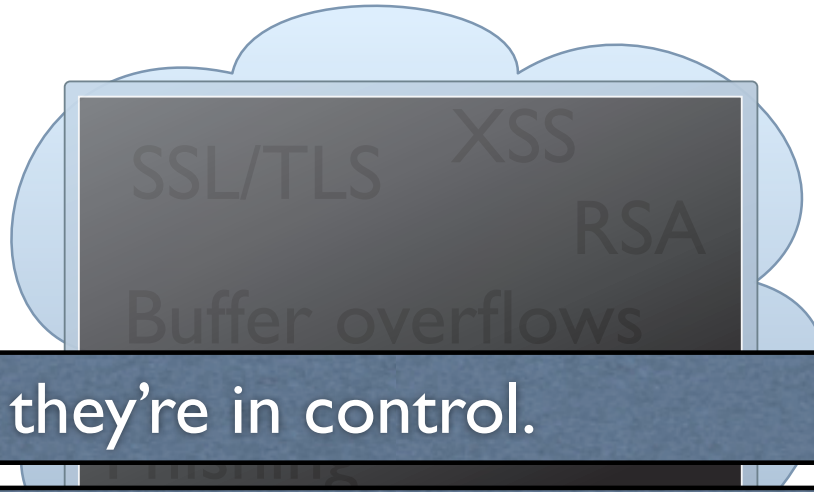
- Mismatch between perception of technology and what really happens
  - Public keys?
  - Signatures?
  - Encryption?
  - Message integrity?
  - Chosen-plaintext attacks?
  - Chosen-ciphertext attacks?
  - Password management?
  - ...

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*

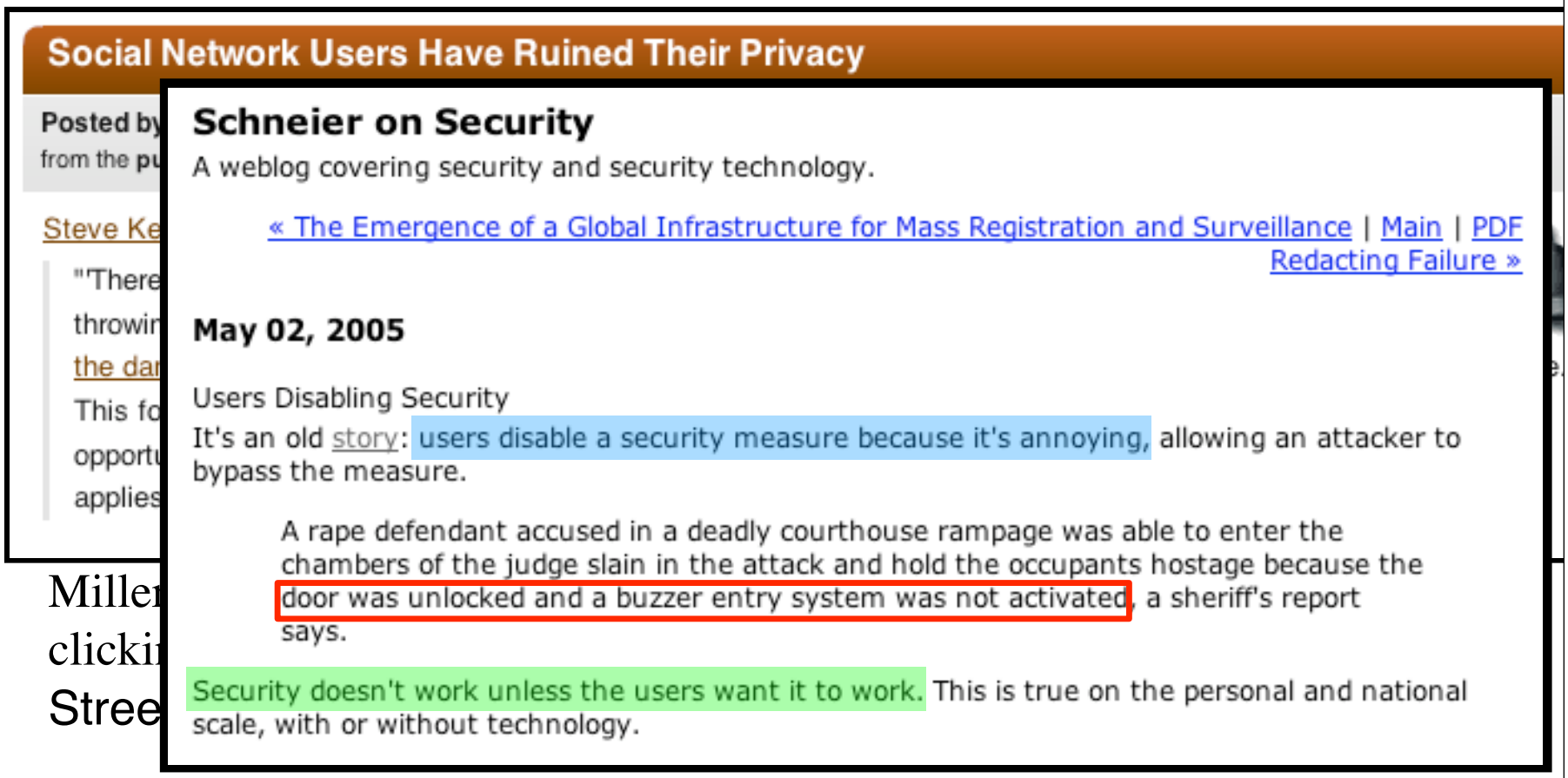
Complex, hidden, and *users manage*

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.)



Social Network Users Have Ruined Their Privacy

Posted by
from the pu

Steve Ke

"There
throwin
the dar
This fo
opportu
applies

Miller
clickin
Stree

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 rape defendant 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.

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

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, what's the point?

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

Response #4: Use Metaphors, Focus on Users

- 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

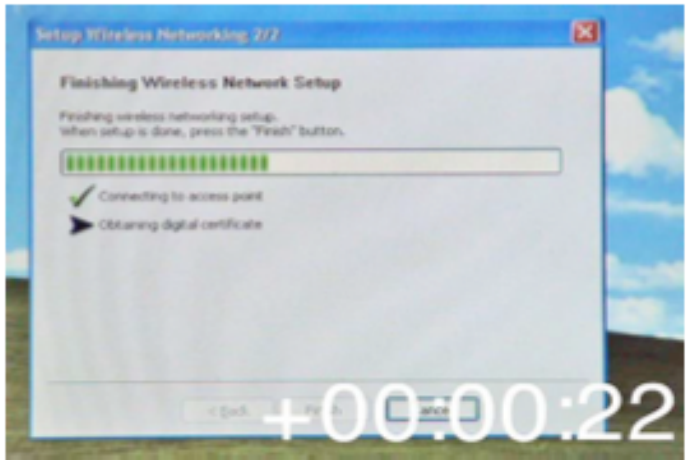
Response #5: Least Resistance

- "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

Application: Network in a Box

[Balfanz et al]

- Establishing cryptographic via IR bootstrap



ISP Ad Injection

ISP Traffic Modifications

ISPs Inserting Ads Into Your Pages

Posted by CmdrTaco on Sat Jun 23, '07 09:19 AM
from the **now-thats-just-slimey** dept.

TheWoozle writes

> "Some ISPs are resorting to a new tactic to increase revenue: inserting advertisements into web pages requested by their end users. They use a transparent web proxy (such as this

Comcast Forging Packets To Filter Torrents

Posted by kdawson on Tue Sep 04, 2007 03:56 PM
from the **could-be-actionable** dept.

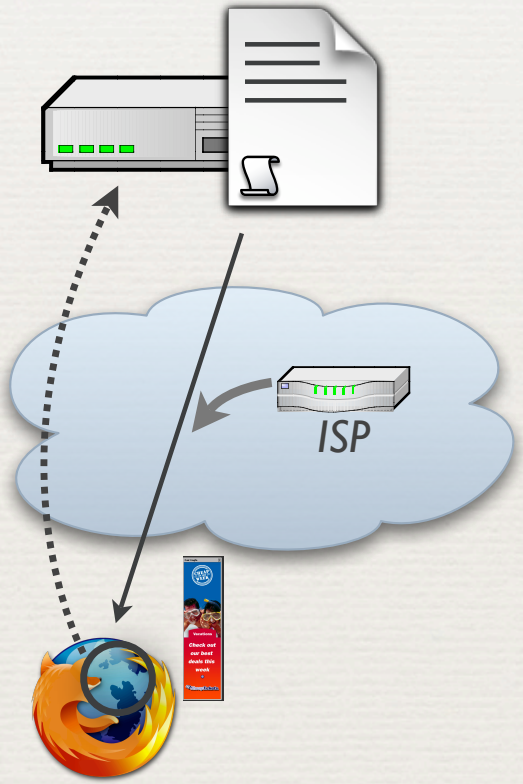
An anonymous reader writes

> "It's been widely reported by now that Comcast is throttling BitTorrent traffic. What has escaped attention is the fact that Comcast, like the Great Firewall of China uses forged TCP Reset (RST) packets to do the job. While the Chinese government can do what they want, it turns out that Comcast may actually be violating criminal impersonation statutes in states around the country. Simply put, while it's legal to block traffic on your network, forging data to and from customers is a big no-no."

- Reports of web page modifications
- Comcast forging packets in Bit torrent flows
- Is this really happening? How often?

Detecting Page Changes

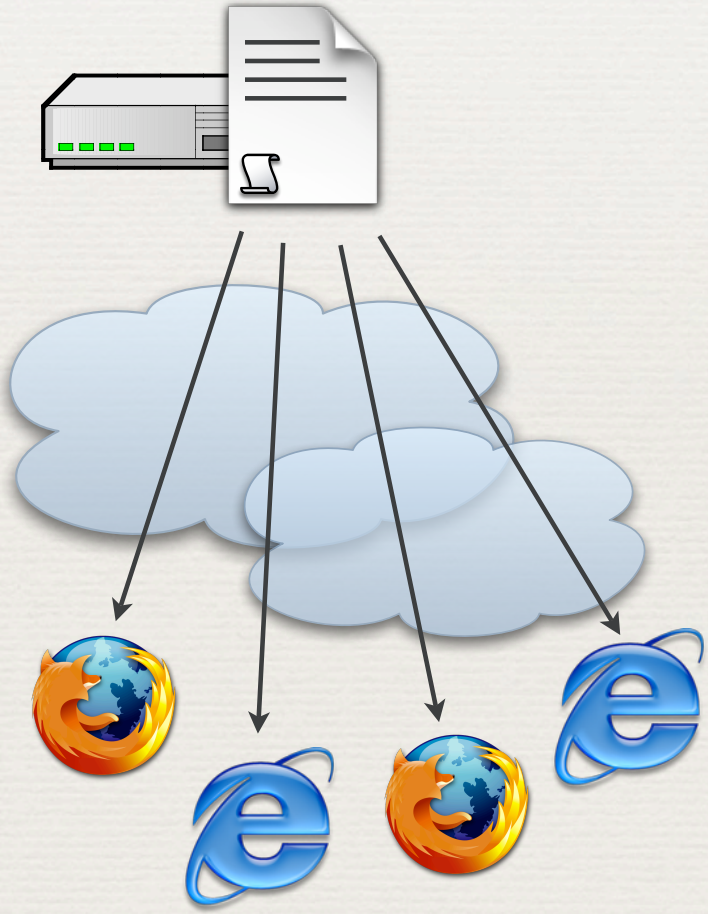
- Can detect with JavaScript
- Built a **Web Tripwire**:
  - Runs in client's browser
  - Finds most changes to HTML
  - Reports to user & server



37

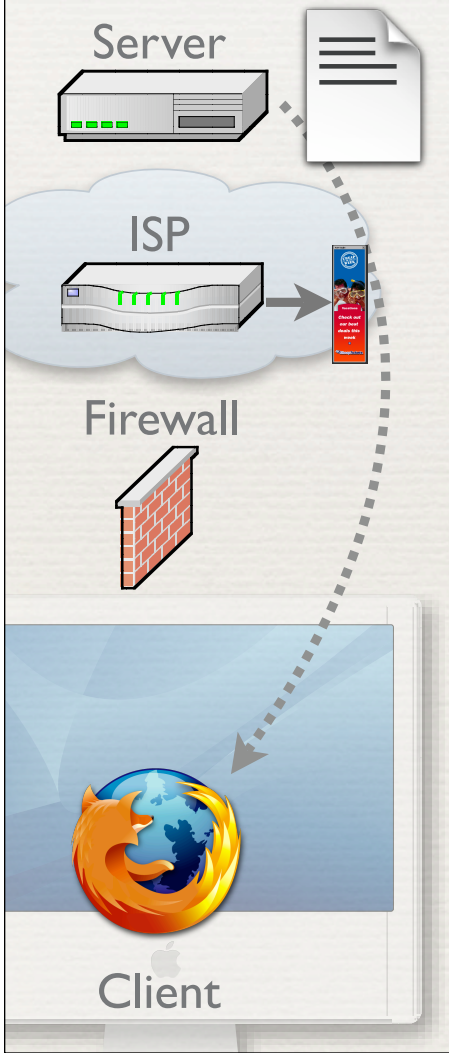
Attracting Visitors

- Wanted view of many clients on many networks
- Posted to **Digg**; Slashdotted
  - Visits from over 50,000 unique IP addresses



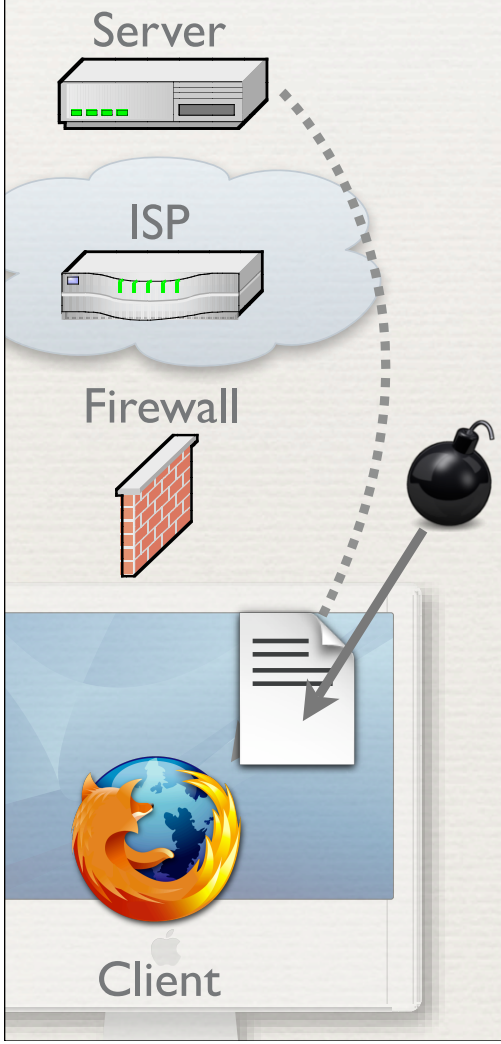
38

Really Happening



- 650+ clients saw changes (1.3%)
  - Many were client software
  - Some occurred in network
- 2.4% (16) of these were advertisement injections allegedly by multiple ISPs

Changes by Malware



- 650+ clients saw changes (1.3%)
  - Many were client software
  - Some occurred in network
- 2.4% of these were advertisement injections allegedly by multiple ISPs
- 2 cases of malware injection, most likely from other machines on local network

40