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, 11/18

- Lab #2
  - Due Monday, 11/21
- Second security review & current event due 12/2
  - Extra credit for every week early

Experiments at Indiana University

[Jagatic et al.]

Experiments at Indiana University

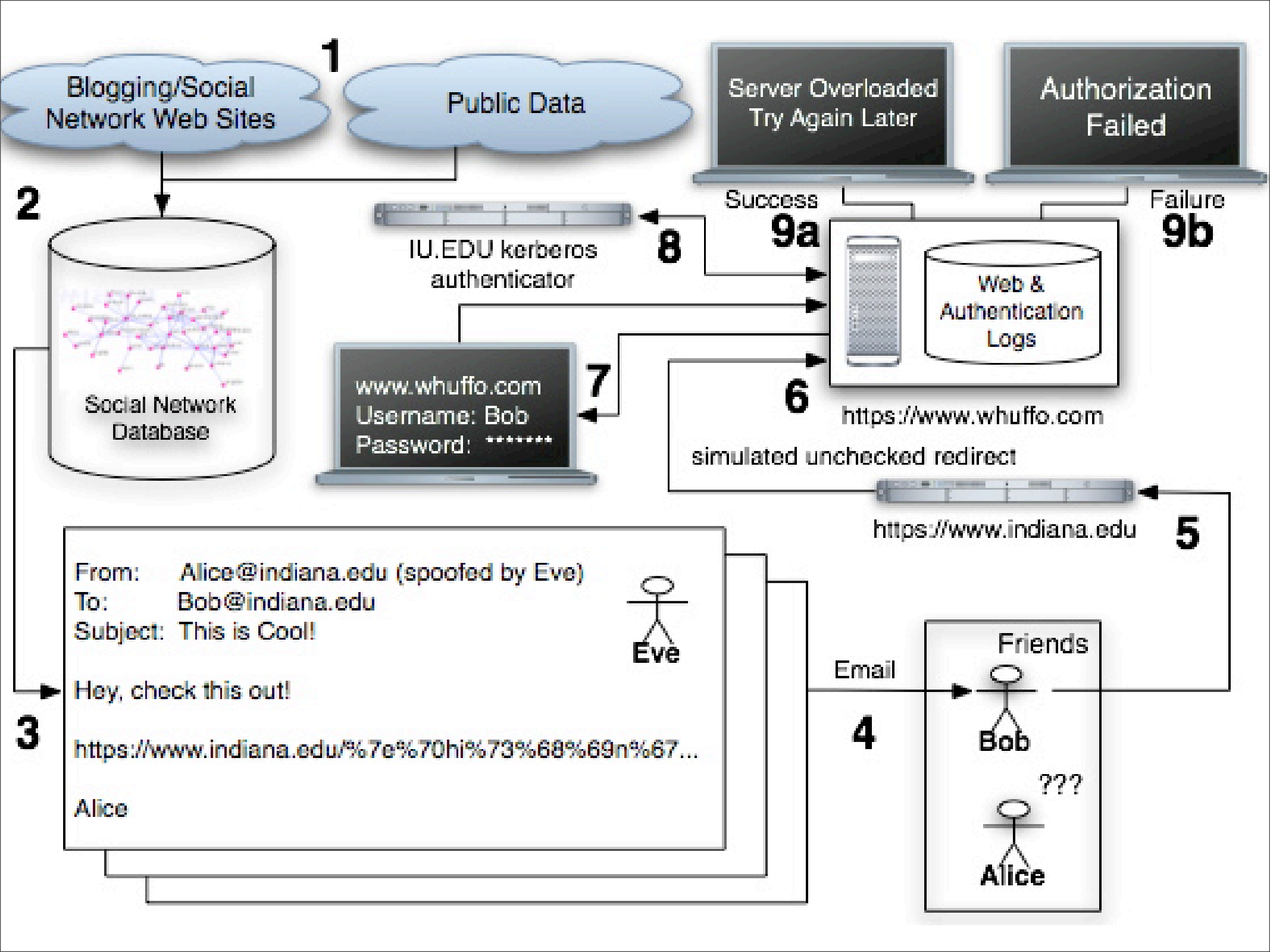
[Jagatic et al.]

- 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


1
Blogging/Social Network Web Sites
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!
Eve
Hey, check this out!
https://www.indiana.edu/%7e%70hi%73%68%69n%67...
Alice
3
Email
4
Friends
Bob
???
Alice

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

More Details

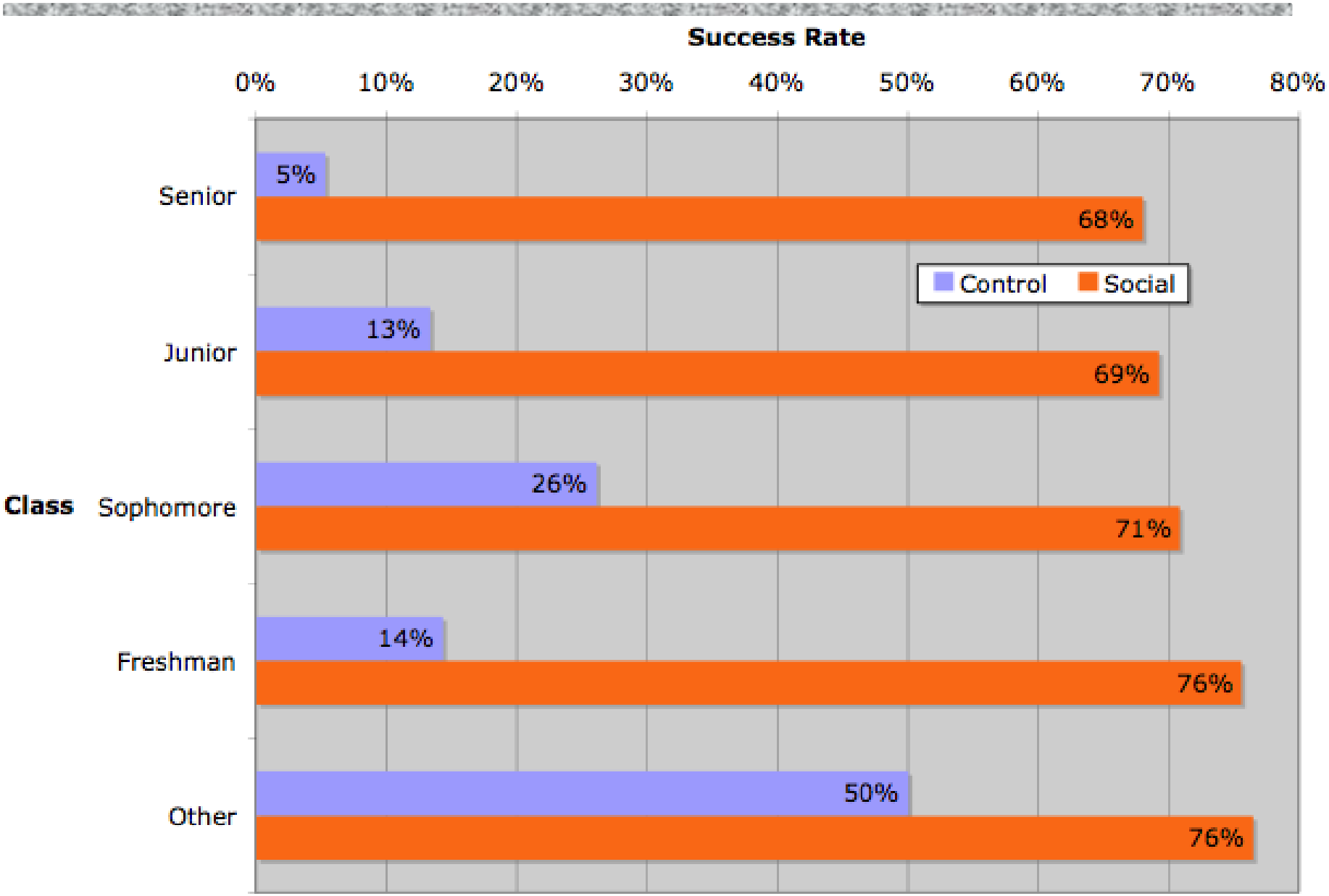
- Control group: 15 of 94 (16%) entered personal information
- Social group: 349 of 487 (72%) entered personal information

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

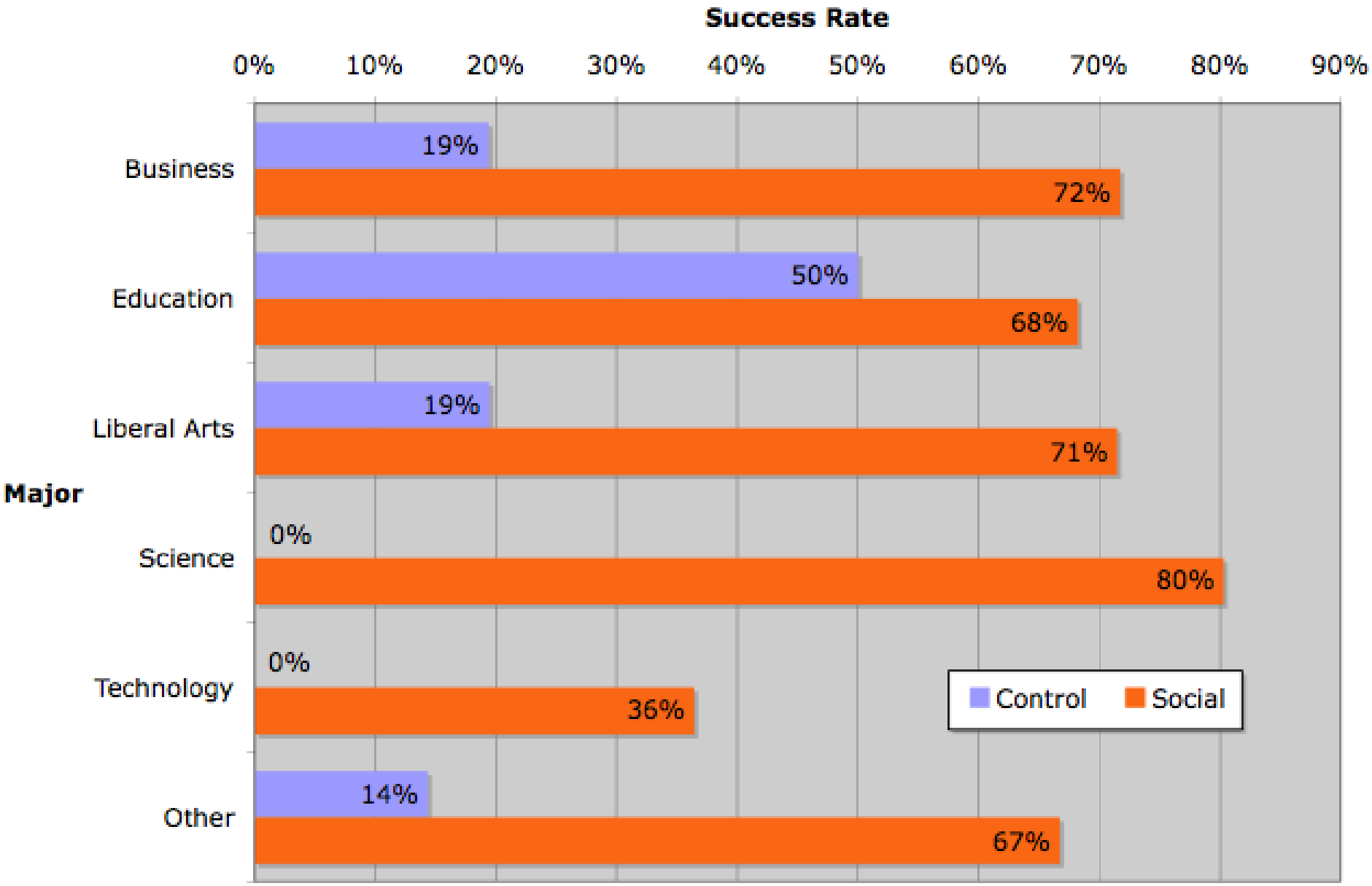
More Details

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

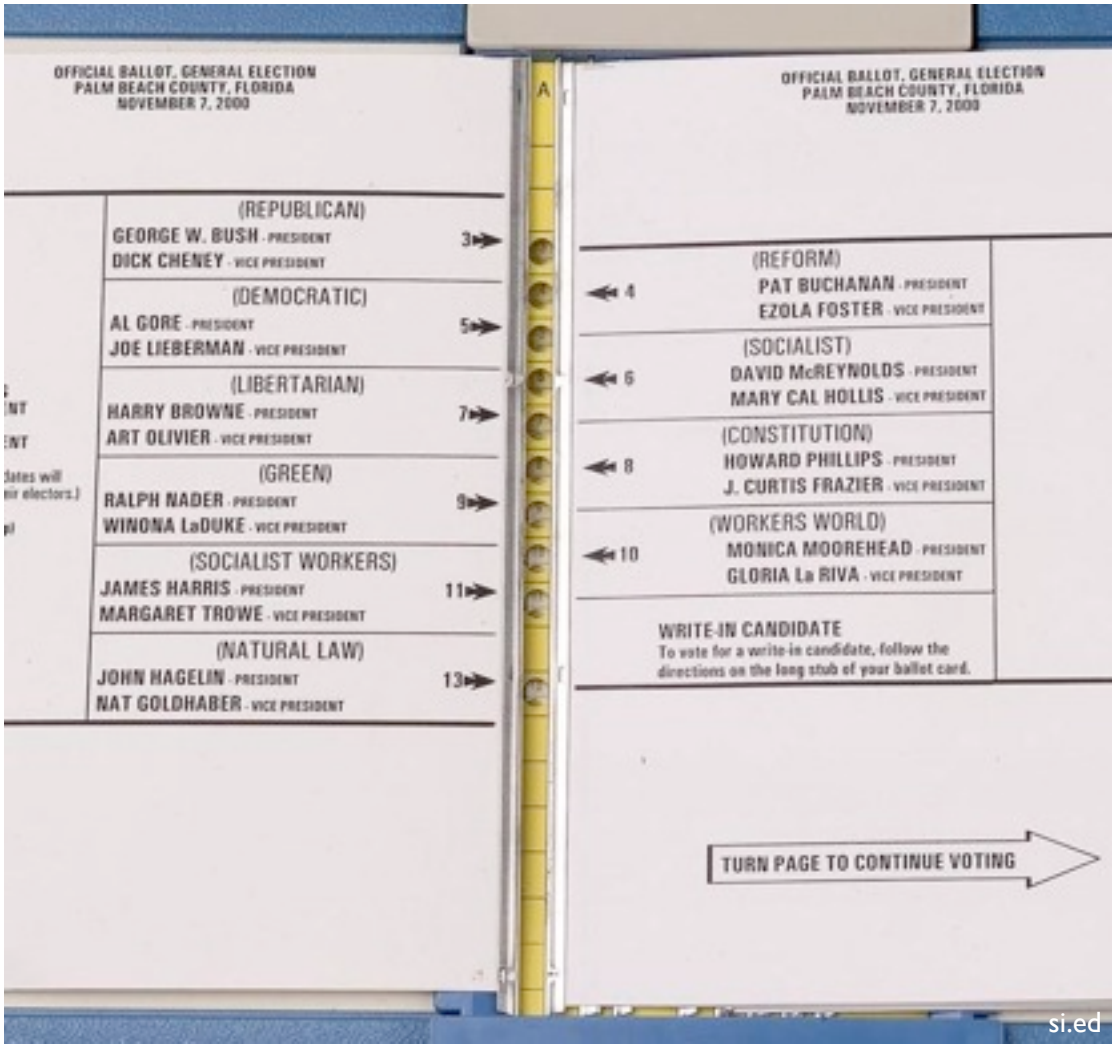
More Details (Class Year)



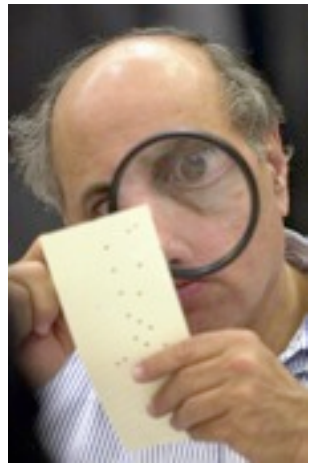
More Details (Major)



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

SSL/TLS

XSS

RSA

Buffer overflows

Phishing

Spyware

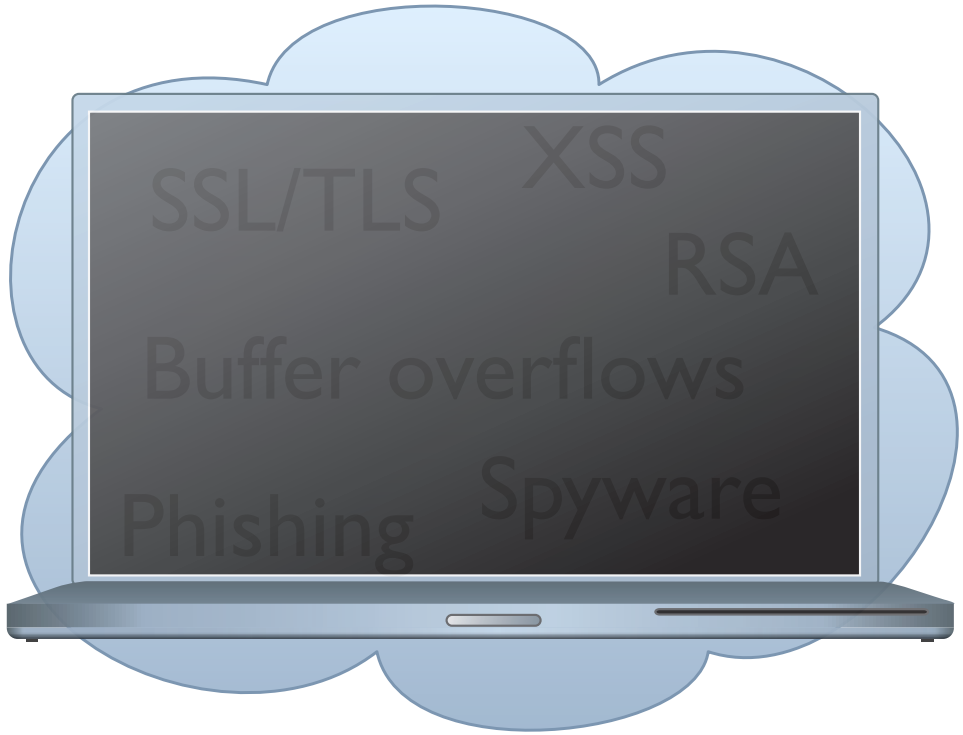
Too complex, hidden, no intuition.

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

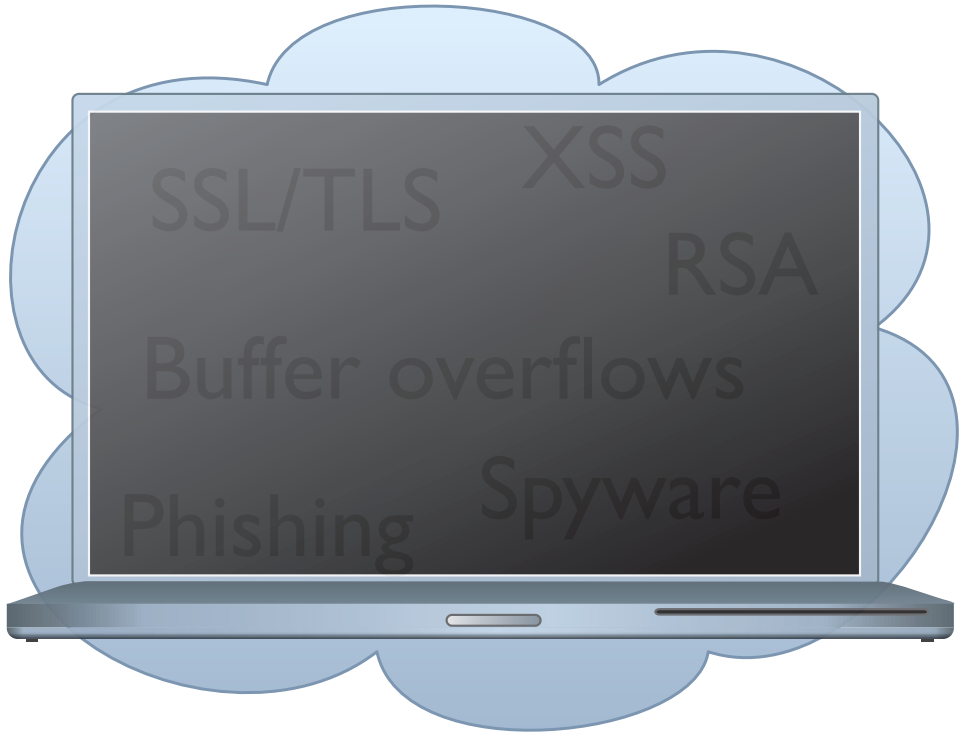
- Mismatch between perception of technology and what really happens
  - Public keys?
  - Signatures?
  - Encryption?
  - Message integrity?
  - Chosen-plaintext attacks?
  - Chosen-ciphertext attacks?
  - Password management?
  - …

Issue #2: Who's in Charge?

Real World

Complex, hidden, but *doctors manage*

Electronic World



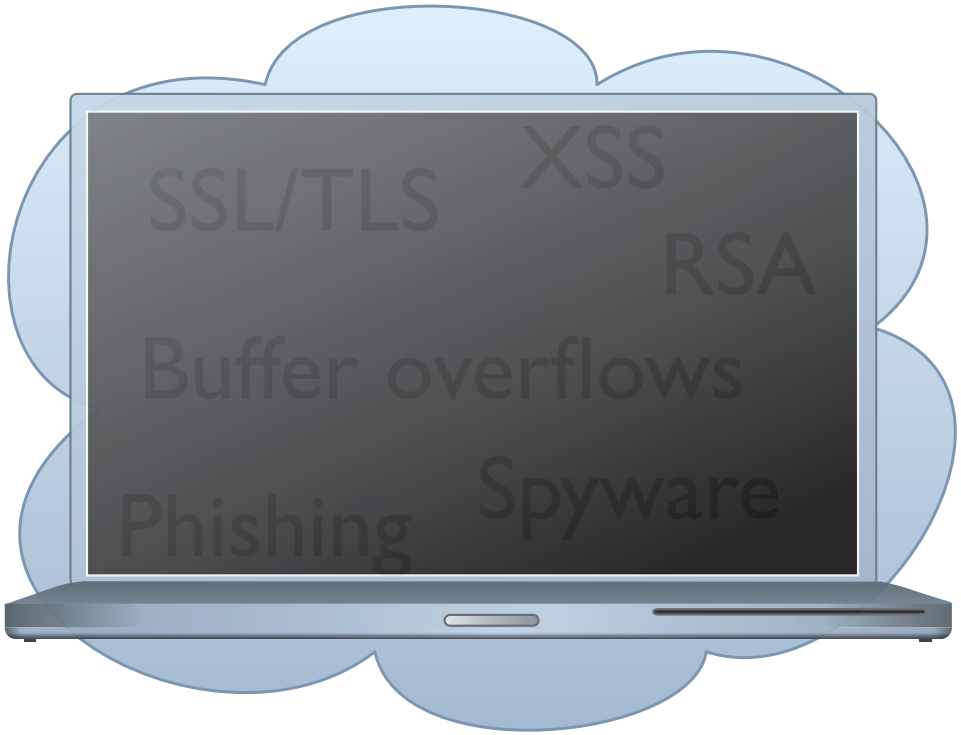
Complex, hidden, and *users manage*

Issue #2: Who's in Charge?

Real World

Complex, hidden, but *doctors manage*

Electronic World



Complex, hidden, and *users manage*

Issue #2: Who's in Charge?

Real World

Electronic World

Adversaries in the electronic world can be *intelligent*, *sneaky*, and *malicious*.

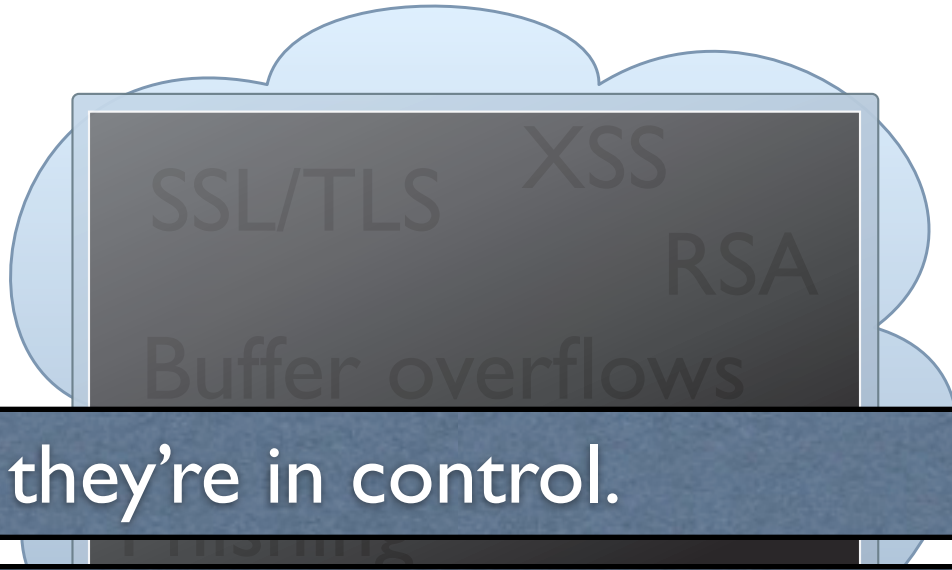
Complex, hidden, but *doctors manage*

Complex, hidden, and *users manage*

Issue #2: Who's in Charge?

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

Issue #3: Hard to Gage Risks

"It won't happen to me!"

Issue #3: Hard to Gage Risks

"It won't happen to me!" (Sometimes a reasonable assumption, sometimes not.)

Issue #3: Hard to Gage Risks

"It won't happen to me!" (Sometimes a reasonable assumption, sometimes not.)

"I remembered hearing about it and thinking that people that click on those links are stupid," she says. "Then it happened to me." Ms. Miller says she now changes her password regularly and avoids clicking on strange links. (Open Doors, by V. Vara, The Wall Street Journal, Jan 29, 2007)

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.

"
o
M
c
Street Journal, Jan 29, 2007)

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.

"
o
M
c
Street Journal, Jan 29, 2007)

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.

"
o
M
c
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