# What am I Doing? Comprehension and Authentiation

Steven M. Bellovin
http://www.cs.columbia.edu/~smb

# Premise: Systems Confuse Users

- People don’t always realize when they’re authenticating
- People don’t realize to whom they’re authenticating
- People don’t realize the implications of authentication
- If you try to explain it, people *still* won’t understand

# Don’t Blame the Users!

“If we assume that the people who use technology are stupid (‘Bubbas’) then we will continue to design poorly conceived equipment, procedures, and software, thus leading to more and more accidents, all of which can be blamed upon the hapless users rather than the root cause – ill-conceived software, ill-conceived procedural requirements, ill-conceived business practices, and ill-conceived design in general.”

– Don Norman, December 2003

# When Do You Authenticate?

- Thought experiment: what is the difference between a nym and a tracking cookie?
- Answer: user knowledge and user consent
- If your browser is trackable by a web site, you have logged in with a nym – but you probably don't know it and you certainly didn't consent

# Where Do You Authenticate?

- You authenticate to most sites you visit
- You authenticate to every embedded third-party image or IFRAME
- Phishing!
    - (Need I say more?)

# Implications of Authentication

- What happens when you authenticate?
- What access rights do you now have?
- What rights have you given away?

# It’s Not Just Authentication

- Users don’t understand computer systems in general
- Things that are obvious to us aren’t obvious to most people – and they don’t want to be bothered to figure them out
- (One doctor I know firmly believes that programmers are *explicitly* trained to ignore user needs, as opposed to what they think users should want)

# Are Systems Better if they do Less?

“It was so simple, especially compared to the old days of buying PCs when I had all sorts "choices" that gave me a headache.”

– Adam Lashinsky, “Confessions of a Mac switcher”

March 2011

# Let’s Look at Facebook

- I won’t bother to explain what Facebook is…
- Users can share information selectively – but do they know how?
- What do you think…?

# A Facebook Privacy Study

- Joint work with Michelle Madejski and Maritza Johnson
- Compare people's attitudes and beliefs about their privacy settings to reality
- Details: http://mice.cs.columbia.edu/getTechreport.php?techreportID=1459&format=pdf&

# Methodology

- 65 Columbia undergraduate volunteers
- By restricting enrollment to Columbia students, we could study “network” permissions
- Also looked at “stranger”, “friend”, and “friend of friend” permissions
- (Yes, we got IRB approval)

# Stages

- Survey of Facebook experience and user privacy attitudes: what do people think about privacy on Facebook?
- Intentions: what do people think their settings should be for 12 different classes of information (religious, political, drugs, sex, family, etc.)
- Automated search for violations
- Confirmation by users

# Attitudes

- Most people cared about privacy
- Most said they understood things like reputational threats
- Most said that media coverage made them double-check their settings, but they didn’t change things
- Virtually everyone (62/65) thought their settings correctly reflected their attitudes and intentions

# Intentions

- No surprises in intentions
- People often wanted to hide things like drug and alcohol use, even from friends (but if you don't want anyone to see it, why put it on Facebook at all?)
- Some categories correlated well (e.g., personal, family, academic, work, interests)

# The Facebook App

- Ran an app as an outsider, as a Columbia person, and as a friend (participants were required to "friend" a study account)
- The app tried to auto-classify content based on keywords, then tried to access the content
- These results were compared with the user's attitude for that type of content

# Confirmation

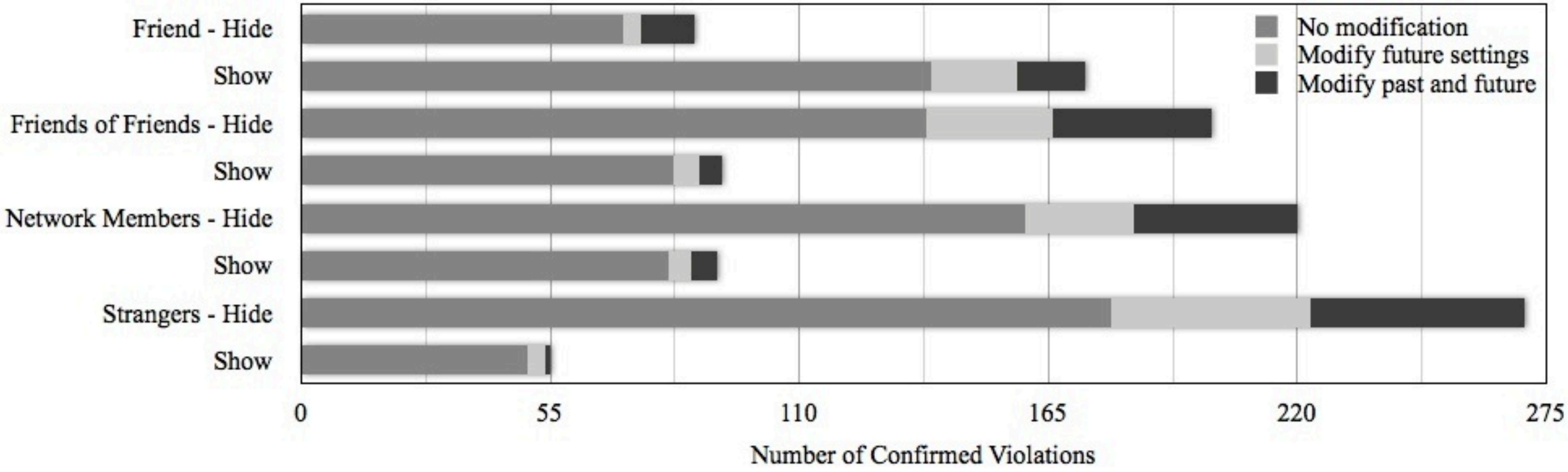
- Our simple-minded classifier could only handle about half of the items found – which means that error rates could be higher than we observed

- We asked people to confirm the accuracy of the classification, and then react to how its setting compared with their attitudes

# Results

- ~94% of users had "show" violations: they were exposing information they said they wanted to hide
  - Obviously, a serious privacy problem
- ~85% of users had "hide" violations: they were hiding things they wanted people to see
  - This is a Facebook utility problem

# People Wouldn't Fix Mistakes



# Generalizing…

- Computer scientists understand access control
  - Even we don't get it right. (How many world-writable files are under my home directory?)
- Normal people don't understand it
- If it's too complicated, people *won't* use it

# Authentication

- People have very little understanding of authentication technologies
- As a result, they fight the rules, even when the rules are designed for their own protection
- For more complex scenarios (e.g., PKI), confusion is nearly total

# Failures

- PKI – no one understands it
- Single sign-on – probably, no one understands it, but it's never caught on. (Why not?)
- Tokens – inconvenient, especially if you need many of them
- Passwords – need I explain?
- But everyone understands physical locks and keys…

# What Should be Done?

- Pay attention to cognitive models
- Make it easy to do the right thing
- Ask what will happen if everyone adopts the idea – does it scale cognitively?