Scalable Web Software

CS193S - Jan Jannink - 2/09/10

Weekly Syllabus

1. Scalability: *(Jan.)*
2. Agile Practices
3. Ecology/Mashups
4. Browser/Client
5. Data/Server: *(Feb.)*
6. **Security/Privacy**
7. Analytics*
8. Cloud/Map-Reduce
9. Publish APIs: *(Mar.)* *
10. Future

* assignment due

Recent Quotes & Events

- "Don't do it, if you really need privacy"
- "Privacy is no longer a social norm"
- 32 million username/passwords taken
- Top 25 dangerous programming errors
- China web censorship in the news
- Google privacy principles announced

This Relates to Scalability?

- Security constrains usability
  - usability improves adoption
- Flexible privacy is extremely confusing
  - does it do what users want?
  - do users know what they really want?
  - confusion hurts word of mouth

Real World Privacy

- Physical limitations to potential attacks
  - location limits pool of attackers
- Psychological limitations
  - out of sight, out of mind
- The web blows these limitations up

Some Common Passwords

1. 123456
2. 12345
3. 123456789
4. password
5. iloveyou
6. princess
7. 1234567
8. rockyou
9. 12345678
10. abc123

Why this is not Simple

- Some Solutions
  - banned password list
  - password requirements & policy
- Drawbacks
  - users demand control
  - only victims recognize threats

Pretty Unscalable Privacy

- Almost 20 years of PGP & 10 of GPG
    - no universal service has emerged
- Contrast with protocols like HTTP
    - lack of awareness
    - explanation requires sophistication
    - maintenance requires dedication

Trust him with your Cash?

Why Entrust our Identities?

- We did it a little bit at a time
- Herd mentality
- The past has been whitewashed away
- Wait a minute, my profile isn’t my ID…
- Nothing too bad can happen…

Historical Perspective

- Internet was a research tool
    - simple collegial rules applied
    - hypergrowth started before the web
- Internet is the first global culture
    - web culture is developing bottom up
    - amalgam of every human culture

The New Wild West

- Internet territory is still being settled
- Perceived anonymity is declining
- Web wants to free information
- Information very public and permanent
- No divide between haves and have nots

Scaling Security & Privacy

- Users can not help
- Power law of intrusion attempts
- Influential unusual internet subcultures
- Computational obscurity
- Distance based privacy models
- Include self/developers in models

Observe Execs

- Apple's stance is most consistent
- Microsoft's antipiracy is antisecurity
  - auto upgrade IE6 no questions asked
- Google always assumes user openness
- Facebook makes the biggest flip flops

Practical Privacy Principles

- Everything I link to directly sees me
- I am discoverable (public profile)
- I have personas (work, home, play)
- Others' use of my information
    - generally out of my control
    - but based on mutual trust

Obfuscation

- Security through obscurity fails
  - eventually
- How to set hurdles high enough
  - assume the worst
- The internet is the biggest pond
  - who are the security sharks?

Desperadoes & Authority

- You will be pwned
  - Black hats, security agencies
- You will be prodded
  - DDoS, spam, phishing
- You will be punked
  - Something Awful, 4chan

Agile Response

- User readable agreements & policy
- Add security audits into release process
    - attacks increase as a service grows
- Know of relevant internet law
    - DMCA safe harbor provisions
    - Patriot act

Worth Checking Out

- Google privacy principles
  - http://googleblog.blogspot.com/2010/01/googles-privacy-principles.html
- 25 Dangerous Programming Errors
  - http://cwe.mitre.org/top25/
- Chilling Effects
  - http://www.chillingeffects.org/

Q & A Topics

- Is there intuitive privacy & security?
- Out of band attacks
  - finding coincidental information
- Social engineering
  - phishing