07- Intro to security, etc.

Lorrie Cranor and Blase Ur

February 4, 2014

05-436 / 05-836 / 08-534 / 08-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Today!

- Statistics: Non-independent data
- Discussion of course projects
- Intro to security
- IRB application procedure

Stats with non-independent data

Independence

- Why might your data in UPS experiments not be independent?
  - Non-independent sample (bad!)
  - The inherent design of the experiment (ok!)
- If you have two data points of ponies' race completion times (before and after some treatment), can you actually do a single test that assumes independence to compare conditions?

Non-independence

- Repeated measures (multiple measurements of the same thing)
  - e.g., before and after measurements of a pony's time to finish a race
- Paired t-test (two samples per participant, two groups)
- Repeated measures ANOVA (more general)

Non-independence

- For regressions, use a mixed model
  - "Random effects" based on hierarchy/group
- Case 1: Many measurements of each pony
- Case 2: The ponies have some other relationship. e.g., there are 100 ponies each trained by one of 5 trainers. The identity of the trainer might impact a whole class of ponies' performance.

Discussion of projects

Intro to security

Computer security

- Key properties include:
  - Confidentiality (information isn't disclosed)
  - Integrity (information isn't changed)
  - Availability (information can be accessed)
- Other properties might be desirable:
  - Access control, Anonymity, Auditability, Authenticity, Privacy, Secrecy,…

What could go wrong?

- Attackers exploit bugs
  - Software/hardware bugs
  - Humans (social engineering)
  - Unintended characteristics (e.g., side channels, poor sources of randomness)

The Morris Worm

- Released in 1988, its stated purpose was to measure the size of the Internet
- Exploited three bugs:
  - An issue with debug in sendmail
  - Buffer overrun in fingerd
  - Remote logins using .rhost files
- Author was the first indicted under the Computer Fraud and Abuse Act of 1986
  - Where is he now?

Modeling our system

- What are our assets, and what is their cost?
  - What is the cost of an outage?
- What is the overall architecture?
- How does the system communicate?
- What humans are involved?
- How valuable is this system to attackers?
  - How valuable is it to us?
- What are we worried about?

Modeling the attacker

- What type of action will they take?
  - Passive (look, but don’t touch)
  - Active (look and inject messages)
- How sophisticated are they?
- How much do they care?
  - How much time will they spend?
- How much do they already know?
  - External / internal attacker?

Group exercise in attacker modeling

- Think about the security of a home
- Come up with at least two attacker models that lead to totally different ways of architecting security for the home
  - Be able to explain your attacker model
  - What is the threat you're worried about?
  - What is your defense?

Defending against attackers

- Legal or policy threats, but no “security”
- Strong “walls”
  - Cryptography, firewalls, etc.
- Redundancy
  - Multiple backup systems
- Detection
  - Intrusion detection systems
- Offense / counterattack

Allocating your resources

- It is impossible to stop everything
  - Time
  - Cost
  - People
  - You probably have better things to do
- What are the most likely threats?
- What are the possible consequences?
- What are relatively simple defenses?

Institutional Review Board (IRB)

IRB process

- Is it research? Are there human subjects?
- Full review vs. expedited vs. exempt
- Fill out and submit protocol
  - Include all study materials (e.g., surveys)
  - Include recruitment text and/or poster
  - Leave plenty of time