Teaching SPAM and Spyware at the University of Calgary

John Aycock
Department of Computer Science
University of Calgary
Calgary, Alberta, Canada
Why Teach Spam & Spyware?

- Spam and spyware are legitimate areas of security research
- Spam and spyware are major problems for our computer-connected society
- Universities should produce graduates educated about, and able to help solve, society’s problems
Why Teach Spam & Spyware?

- Spam and spyware are legitimate areas of security research.
- Spam and spyware are major problems for our computer-connected society.
- Universities should produce graduates educated about, and able to help solve, society’s problems.

Why aren’t more universities teaching their students about this?
Why Spam and Spyware?

• They both start with the letter “S”
• Historical reasons
  – We already have a course on computer viruses and malware
• It’s about information
  – Stolen
  – Volunteered
  – Surrendered under false pretenses
About the Course

• First offered in fall 2005
• 13-week computer science course
• 150 minutes of lecture time/week
• Offered at 4th-year/senior undergraduate and graduate levels
• Hands-on approach taken; students write
  – Spamming and anti-spam software
  – Spyware and anti-spyware software
Why Hands-On?

I hear, and I forget.
I see, and I remember.
I do, and I understand.

- Anonymous
Course Admission

• No “sitting in” or auditing lectures; student identities verified by instructor

• Undergrad admission requirements:
  – GPA requirement
  – Computer Science students
  – 4th-year or higher
  – Admission essay

• Maximum of 16 students
Secure Lab Facility

• Secure environment created in part through lab protocol, legal agreement, law & ethics lecture content

• “Medium-security” facility
  – Separate locked room
  – Isolated network
  – Computers locked down, literally and figuratively

• SMTP servers, proxy server, DNS
Assignments

• One written ethics assignment
• Four programming assignments done in the secure lab:
  – Spyware - startup hooks, keylogging
  – Anti-spyware - detection, identification, removal
  – Spam - bulk mailing software
  – Anti-spam - filtering
• Pairs of offensive/defensive assignments
Conclusion

• Spam and spyware can be taught safely and effectively
• Spam and spyware should be taught
• “Education” isn’t only for end-users; the next generation of defenders needs to be educated too
Conclusion

• Spam and spyware can be taught safely and effectively
• Spam and spyware *should* be taught
• “Education” isn’t only for end-users; the next generation of defenders needs to be educated too

• For industry: our students are some of the best-trained in the world (hint, hint)
Teaching Spam and Spyware at the University of Calgary
John Aycock <aycock@cpsc.ucalgary.ca>