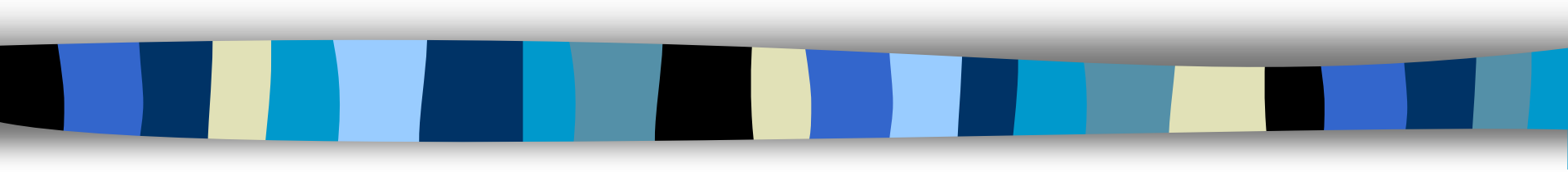
Information Security
CS 526
Topic 9-A



Secure Software: Market Failure

Why Software Has (or appear to have) So Many Bugs?

- Software is complicated, and created by human
- Software is no more buggy, is just more targeted?
- Unique nature of software
  - Near-zero marginal cost
- Market failure for secure software
  - Market failure: a scenario in which individuals' pursuit of self-interest leads to bad overall outcomes
    - i.e., cannot leave it to free market could lead to bad outcome
  - Typical reasons for market failure: Information asymmetries, externalities, public goods
  - Market failure for secure software means that vendor lack incentives to produce higher quality software.
- Materials in this and the next few slides from “Geekonomics: The Real Cost of Insecure Software” by David Rice

Evidence of Market Failure: Guy Kawasaki: "**The Art of Innovation**"

- Don't worry, be crappy.
  - An innovator doesn't worry about shipping an innovative product with elements of crappiness if it's truly innovative.

- Churn, baby, churn.
  - I'm saying it's okay to ship crap--I'm not saying that it's okay to stay crappy. A company must improve version 1.0 and create version 1.1, 1.2, ... 2.0. This is a difficult lesson to learn because it's so hard to ship an innovation; therefore, the last thing employees want to deal with is complaints about their perfect baby. Innovation is not an event. It's a process.

Reasons Why Vendors Lack Incentive to Produce More Secure Software

- Cash flows when product starts shipping.
- Market dominance is key to success
  - being first often means becoming de facto standard
- Users cannot just vote for security with their money.
  - lack of measurement for security
- No liability.
- Bugs can be patched with little cost. No expensive recall.
- Thorough testing is inefficient. Let the users test it and fix only the bugs that affect users

The Perversity of Patching

- Releasing a patch costs little
- Buggy software can force users to upgrade
  - Achieving market dominance means competing with previous versions
  - Stop releasing patches for old versions can force users to upgrade
- Patching provide an opportunity of offering new licensing terms

Coming Attractions …

- Symbolic execution