Prolog to Lecture 16
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Security Evaluations and the US Government

- The US government runs lots of computers and networks
- It’s a big, obvious target
  - And does get attacked a lot
- We obviously want its systems to be secure
- How to evaluate their system security?

Something That Didn’t Work

- FISMA (Federal Information Security Management Act of 2002)
- Result of law intended to improve security of government systems
  - Passed in 2002
- Required NIST to set standards
- Other gov’t agencies needed to document what they did to meet them

What Happened With FISMA

- Turned into an exercise in generating reports
- All agencies had to do was write lengthy reports
- Small companies went into business writing the reports
- But most government systems’ security was not actually improved

What’s the Lesson For Us?

- Not just that government tends to useless bureaucracy
- Rather, be sure to ask for the right thing from security reviews
- What you really want is to know whether you’re secure
- And what to do to become more so

What Was the Problem With FISMA?

- Did not force agencies to actually improve security
  - You just had to write reports
- Did not focus on practical methods of improving security
- Did not take into account dynamic and changing nature of threats

How Can You Do Better?

- If you're involved in a security evaluation, keep your eye on the ball
- Look at things that strongly affect real security
  - In ways relevant to your situation
- Consider the real threats you're facing
- Think about and report on where the system needs to be improved

The New Government Approach

- FISMA 2.0
- Passed by House of Representatives (2012)
- Intended to place more emphasis on actually securing systems
  - Automated security reporting
  - Mandating security requirements in contracts
  - Continuous security monitoring
  - Legislates federal CTO