CSCI 476
COMPUTER SECURITY

FOCUS ON SOFTWARE SECURITY

WHAT IS THIS COURSE ABOUT?

- Software security
- Not
  - Network or perimeter security
  - Operating system security
  - Cryptography (well, maybe some)
- Why software security generally sucks
- What does it mean to be secure in software
- How do you create secure software
- How do you know its secure

WHY SHOULD YOU CARE?

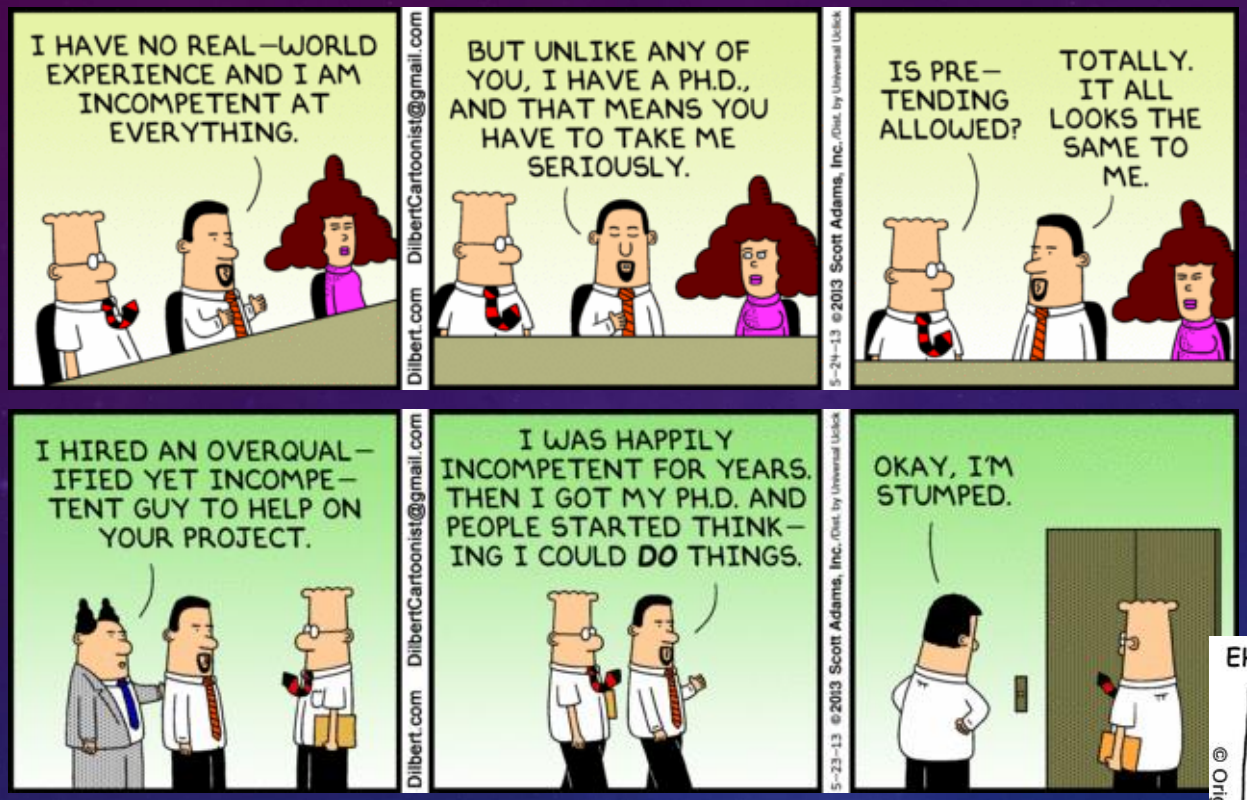
- If you don't, hopefully you will lose every software development job you ever get
  - But you won't
- Software that meets functional requirements, but doesn't protect itself, its data and its environment is bad software and it is dangerous
- Increasingly, the security of a software product is as important as the functional characteristics
- Remember the term - Unlimited Liability
- Compliance
- Software security is the responsibility of the developer

SO WHO AM I?

- Gary Harkin
  - harkin@cs.montana.edu
  - 31 years at MSU
  - 8+ years in industry (Right Now Technologies, Oracle, Security Innovation)
  - Currently at Security Innovation as a Software Security Consultant
- Since I'm fully employed, I will not be on campus except for the class, unless you ask.
- I promise to check my email at least weekly

- Office/Desk/Closet – unknown at this point
- I may have to travel on business for up to a week at a time
- Hopefully, we can work out some system to make up the time

WHAT DO YOU CALL ME?



How about Gary?

MY APPROACH

- I’m not a retailer trying to sell you a nifty something, I’m your guide to an auto-didactic experience
- There’s no text because I don’t see the need to have you buy a $100 book that covers 20% of the material
- It’s all online
- I would like the course to be laboratory driven, but that is not going to be practical
- I don’t have the time or resources to grade HW
  - But I will assign lots of it
- You will get out of the course what you put in
- I’m going to have to give grades … humbug

MY APPROACH

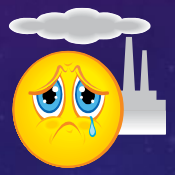
- I don't know what you don't know – so ask
- The only stupid question is the one I can't answer
- I encourage you to learn from each other
  - I don't encourage workload sharing

TOPICS TO COVER

- Software security
  - What
  - Why
  - How
- Vulnerabilities or most of them
- Securing coding principles
- The Secure Development Lifecycle (SDL)
- Threat Modeling

TOPICS TO COVER

- Some cryptography
- Tools for penetration testing
- Time available
  - 1.25 x 2 x 14 = 35 hours --- not enough
  - 80 hours is closer to what is needed



SYLLABUS

- A moveable feast (sorry Ernest)
- Here's what we are going to try
  - SQL Injection (no good reason except it's easy to understand)
    - How it happens
    - The consequences
    - How attackers find it
      - There are other names, most not civil
      - Tools they might use
    - What you, as a developer, are obligated to do to prevent it
      - Coding
      - Testing

SYLLABUS

- Continuing
  - A taxonomy of computer security
  - Some more vulnerabilities
    - The intricacies
    - Practical issues of dealing with them
    - How to attack the vulnerability
  - The Secure Development Lifecycle
  - Threat modeling
  - Whatever we can fit in
- Somewhere in here, a mid-term and a final

RESOURCES

- If you want a textbook to pack around
  - Introduction to Computer Security, Bishop (he has a 2014 release)
- Decent software security books
  - Building Secure Software, Viega and McGraw
  - Exploiting Software, Hoglund and McGraw
  - How to Break Software Security, Whittaker and Thompson
  - How to Break Web Software, Andrews and Whittaker
  - 24 Deadly Sins of Software Security, Howard, LeBlanc and Viega

RESOURCES

- Hacking
  - Hacking: The Art of Exploitation, Erickson
  - The Web Application Hackers Handbook, Stuttard and Pinto
  - Hacking Exposed: Web Applications, Scambray, Liu and Sima
  - Counter Hack Reloaded: A Step-by-step …, Skoudis and Liston
  - http://www.sans.edu/research/book-reviews/article/security-books-best
  - http://www.ivizsecurity.com/blog/security-books/
  - Penetration Testers Open Source Toolkit, Faircloth, Hurley and Varsalone
  - Gray Hat Hacking: The Ethical Hacker's Handbook, Harris

RESOURCES

- Web sites
  - www.owasp.org
  - www.sans.org
  - www.securityinnovation.com
  - www.elite-hackers.com
  - hacking-tutorial.com
  - www.evilzone.com
  - www.hackaday.com
  - www.hackinthebox.com
  - hackthissite.com

RESOURCES

- Blogs and feeds
  - blog.securityinnovation.com/blog/
  - nakedsecurity.sophos.com
  - krebsonsecurity.com
  - www.Kaspersky.com
  - www.schneier.com
  - www.veracode.com/blog
- Feeds
  - www.krebsonsecurity.com
  - www.dankaminsky.com
  - www.stillsecureafteralltheseyears.com