COMP 4384 Software Security

Module 0: *Course Overview*

Ahmed Tamrawi

atamrawi atamrawi.github.io ahmedtamrawi@gmail.com

B.Eng. Computer Engineering
(Class of 2007)

M.Sc. Computer Engineering
(Class of 2011)

Ph.D. Computer Engineering
(Class of 2016)

Secure Programming

Static Program Analysis

Data & Pattern Mining

Software Analysis & Security

Quantum Physics

Biology

Astronomy

Bug finding and Malware detection

Build System Analysis

Abstractions and Symbolic Evaluations

Medium

High Scalability

Building bigger, faster, more reliable websites.

Quora

Your best source for knowledge.

Smarter Every Day

YouTube

twitter

رؤيا

3Blue1Brown

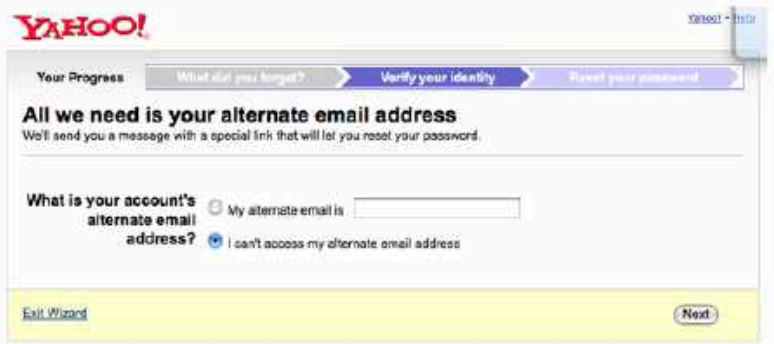
Quantamagazine

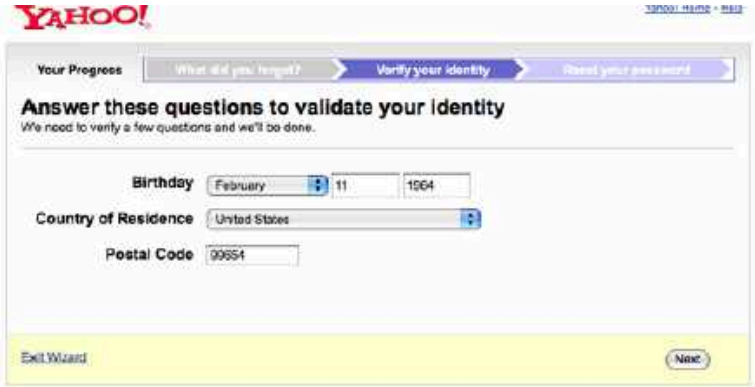
Your turn!

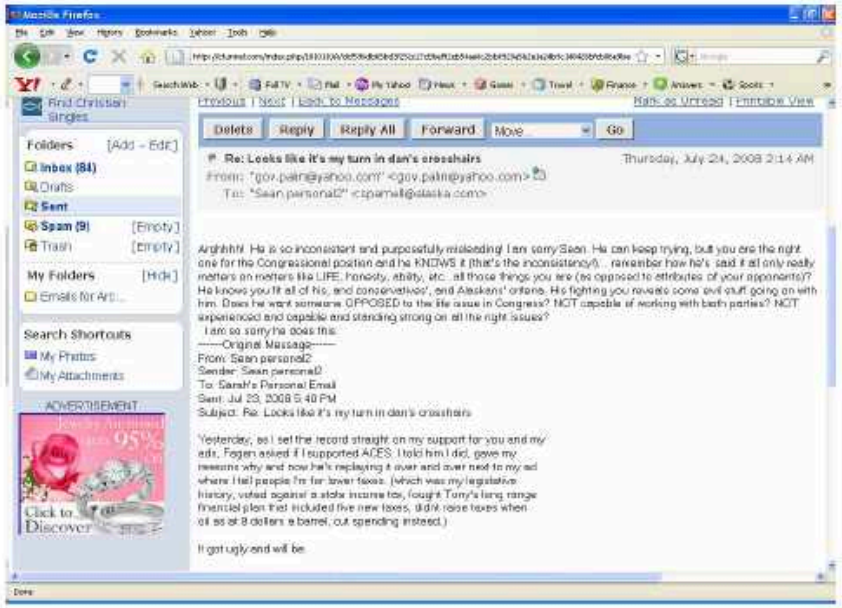
- *Name*
- *Undergraduate major and/or current work.*
- *Something about you*
  - *Food you like.*
  - *Programming languages you used.*
  - *Open source projects you contributed to.*
- *What do you think of this course?*
- *What are your goals after graduation?*

DARPA *is investing billions of dollars into Securing Software*

APAC	*Automated Program Analysis for Cybersecurity*
VET	*Vetting Commodity IT Software and Firmware*
HACMS	*High Assurance Cyber Military Systems*
STAC	*Space/Time Analysis for Cybersecurity*
CASE	*Cyber Assured Systems Engineering*
CHESS	*Computers and Humans Exploring Software Security*
ARCOS	*Automated Rapid Certification Of Software*







Sarah Palin Email Hack

https://www.wired.com/2008/09/palin-e-mail-ha/

bitcoin Introduction Resources Innovation Participate About English

Android Security Vulnerability

11 August 2013

What happened

We recently learned that a component of Android responsible for generating secure random numbers contains critical weaknesses, that render all Android wallets generated to date vulnerable to theft. Because the problem lies with Android itself, this problem will affect you if you have a wallet generated by any Android app. An incomplete list would be Bitcoin Wallet, blockchain.info wallet, BitcoinSpinner and Mycelium Wallet. Apps where you don't control the private keys at all are not affected. For example, exchange frontends like the Coinbase or Mt Gox apps are not impacted by this issue because the private keys are not generated on your Android phone.

What is being done

Updates are being prepared for the following wallet apps:

- **Bitcoin Wallet**: Update has been prepared and is in beta testing now. Learn more.
- **BitcoinSpinner**: Update is being prepared.
- **Mycelium Wallet**: Update v0.6.5 can be installed from Google Play or mycelium.com.
- **blockchain.info**: Update is being prepared.

What you should do

In order to re-secure existing wallets, key rotation is necessary. This involves generating a new address with a repaired random number generator and then sending all the money in your wallet back to yourself. If you use an Android wallet then we strongly recommend you to upgrade to the latest version available in the Play Store as soon as one becomes available. Once your wallet is rotated, you will need to contact anyone who has stored addresses generated by your phone and give them a new one.

If you use Bitcoin Wallet by Andreas Schildbach, key rotation will occur automatically soon after you upgrade. The old addresses will be marked as insecure in your address book. You will need to make a fresh backup.

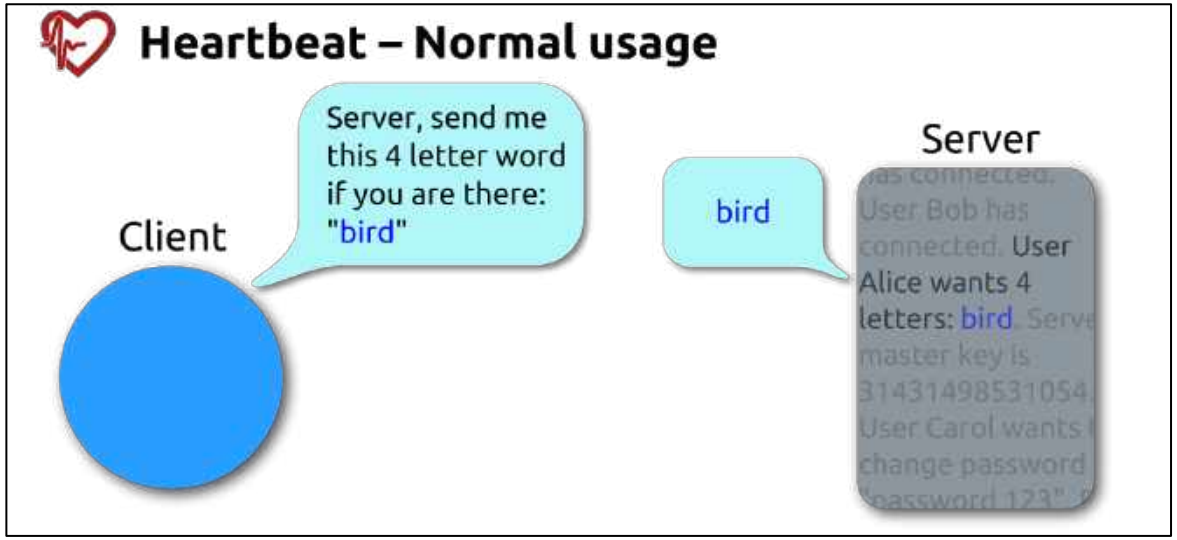
This notice last updated: Sun Aug 12 02:45:00 UTC 2013

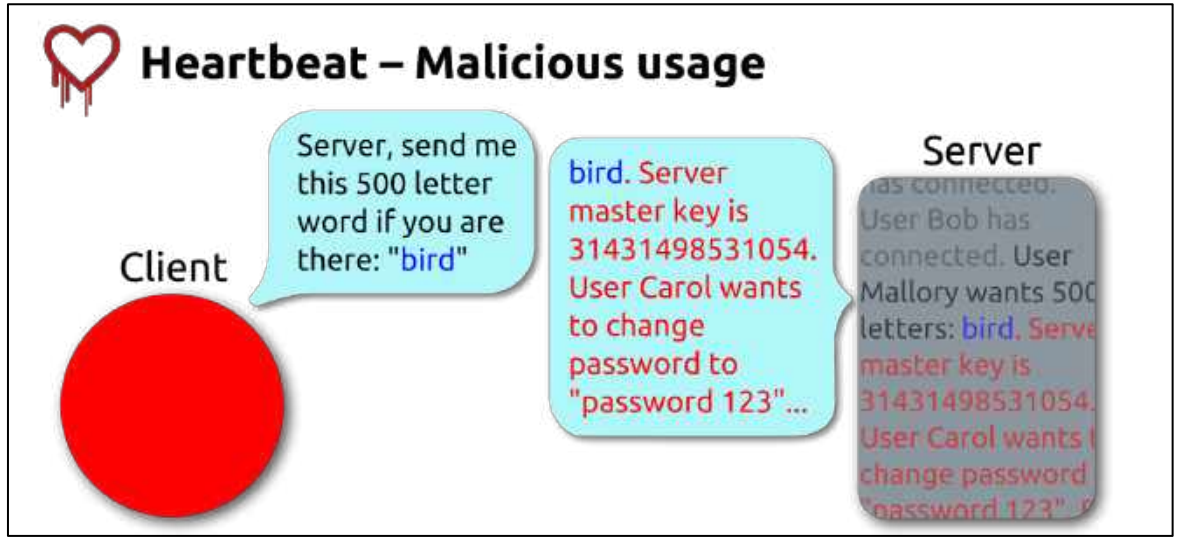
Android Random Number Flaw Results in Bitcoin Thefts

https://nakedsecurity.sophos.com/2013/08/12/android-random-number-flaw-implicated-in-bitcoin-thefts

HEART BLEED BUG

Major OpenSSL Sequrity Leak

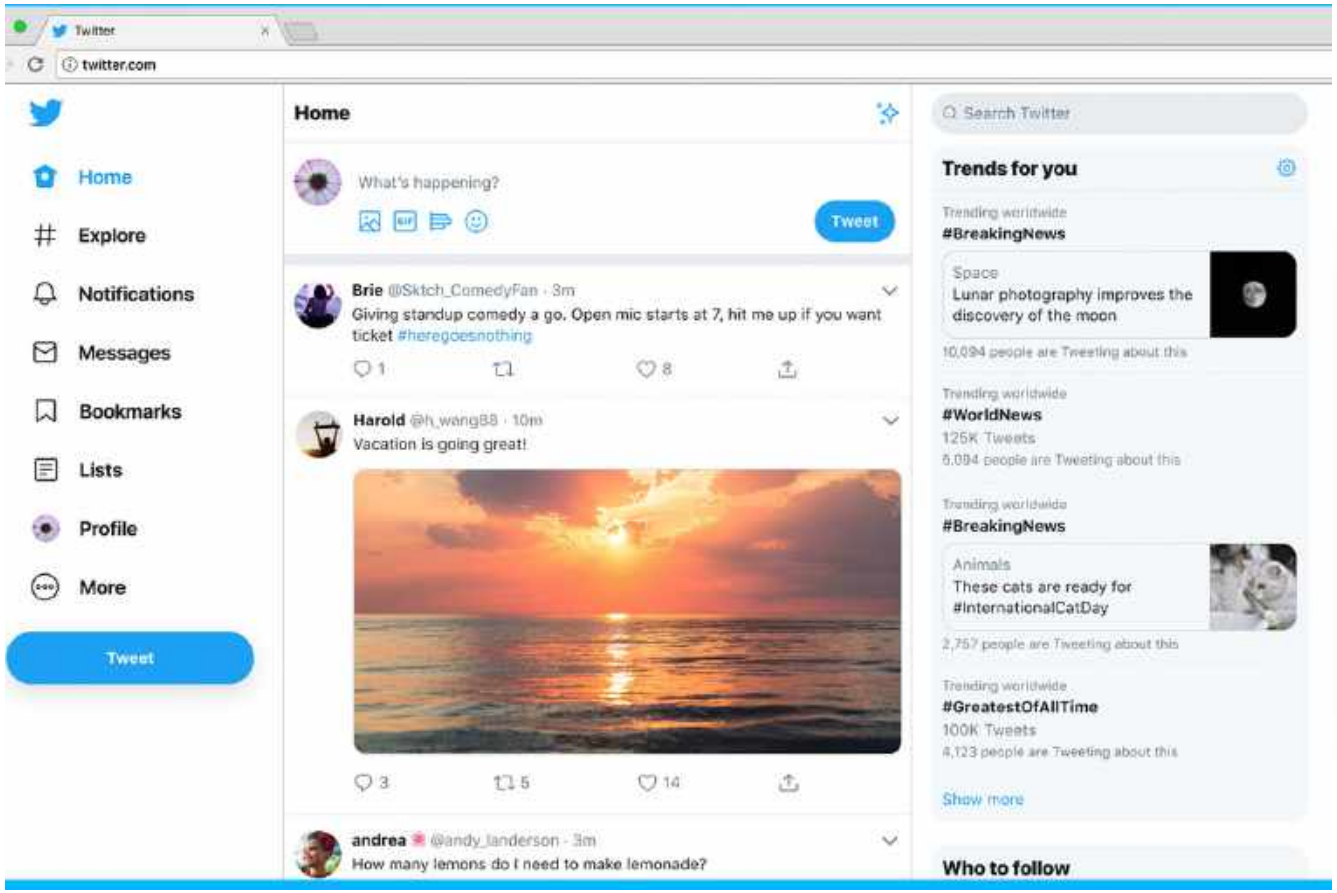




https://heartbleed.com/

https://en.wikipedia.org/wiki/2012_LinkedIn_hack

Twitter Worm



https://www.pcworld.com/article/163054/twitter_mikeyy_worm_stalkdaily.html

WannaCry Ransomeware

http://www.wired.co.uk/article/wannacry-ransomware-virus-patch/

Old Systems Break Operations (2017)

NHS cyber-attack: GPs and hospitals hit by ransomware

13 May 2017

Share

Attacks can Cause Physical Damage (2014)

BBC | Sign in | News | Sport | Weather | iPlayer | TV | Radio

NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Education | Entertainm

Technology

Hack attack causes 'massive damage' at steel works

22 December 2014 | Technology

AFP

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

Nobody can Keep Online Records Safe (2015)

Forbes / Tech

The Little Black Book of Billionaire Secrets

JUN 11, 2015 @ 02:12 PM 15,154 VIEWS

Federal Union Says OPM Data Breach Hit Every Single Federal Employee

Known Good Practice Ignored (2015)

NEWS

TalkTalk discloses possible breach, admits some data not encrypted

A woman walks past a company logo outside a TalkTalk building in London, Britain October 23, 2015. *Credit: REUTERS/Stefan Wermuth*

MORE LIKE THIS

TalkTalk hit by data breach and ransom demand

Police arrest 15-year-old in TalkTalk hack

UK police arrest third person in TalkTalk breach investigation

on IDG Answers

How is data stored and accessed in the cloud?

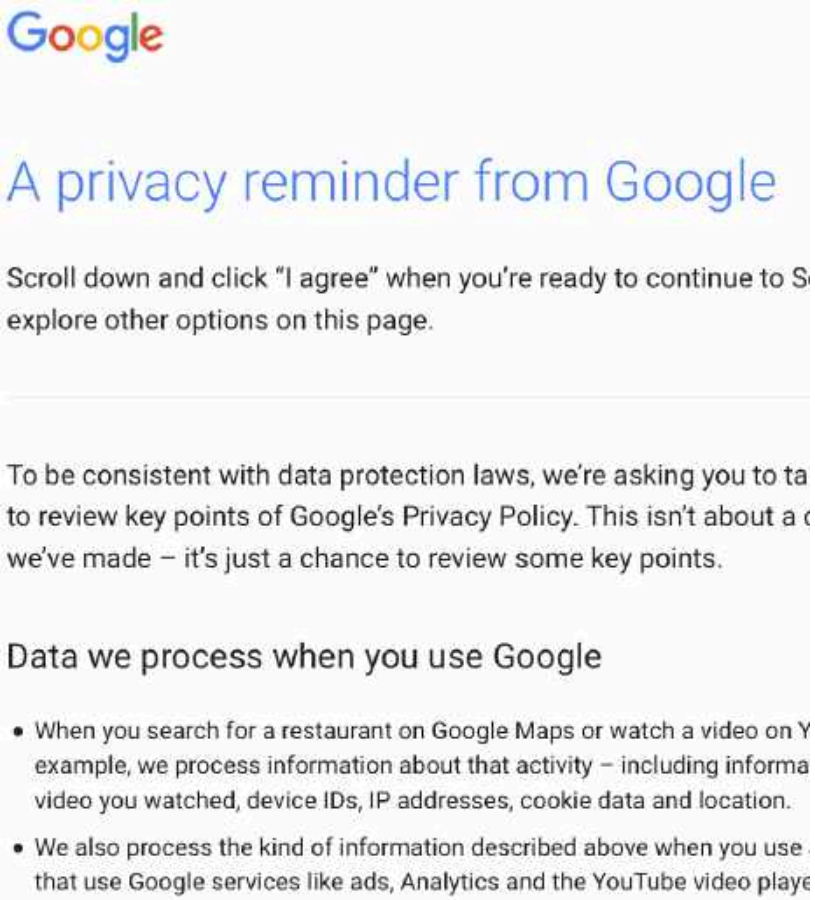
IoT Easily raises a DDoS Botnet Army (2016)

Cost Estimates are Difficult

But it’s agreed they’re increasing. . .

Cyber Warfare is Real

Privacy is being Eroded



Google

A privacy reminder from Google

Scroll down and click "I agree" when you're ready to continue to S
explore other options on this page.

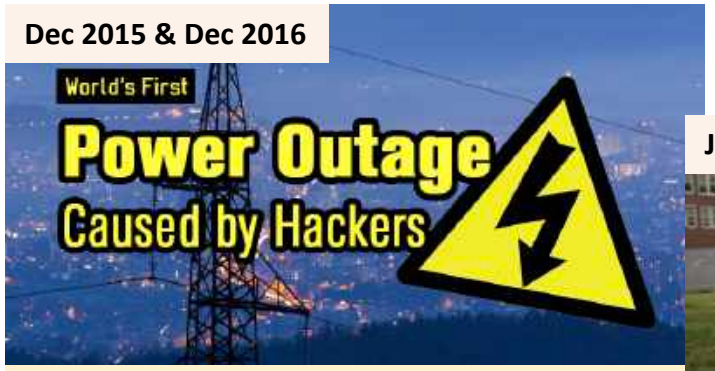
To be consistent with data protection laws, we're asking you to ta
to review key points of Google's Privacy Policy. This isn't about a c
we've made – it's just a chance to review some key points.

Data we process when you use Google

- When you search for a restaurant on Google Maps or watch a video on Y
example, we process information about that activity – including informa
video you watched, device IDs, IP addresses, cookie data and location.
- We also process the kind of information described above when you use
that use Google services like ads, Analytics and the YouTube video playe

But maybe there is hope. . .

Dec 2015 & Dec 2016



Ukraine power grid attacks

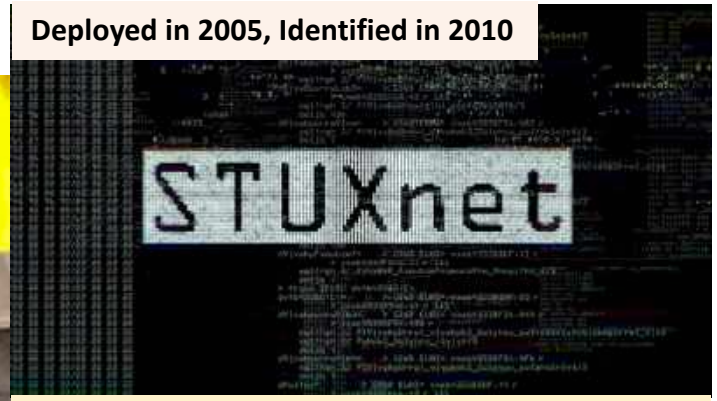
July 21, 2015

Jeep remotely hijacked

November 29, 2011

HP printers remotely set on fire

Deployed in 2005, Identified in 2010



STUXnet Worm

{ Complex Software }

Although software development practice has *advanced rapidly* in recent years, common practice hasn't

Many programs are still **buggy**, **late**, and **over budget**, and many **fail** to satisfy the needs of their users

IT'S IN THE SYLLABUS

This message brought to you by every instructor that ever lived.

WWW.PHDCOMICS.COM

Software Security COMP4384

Instructor: Ahmed Tamrawi

Fall 2020, Revision 1

E-mail: ahmedtamrawi@gmail.com Web: https://atamrawi.github.io/teaching/comp4384_fall20

Private Meetings: Available upon request Class: Tuesdays,Thursdays 12:50 – 2:05pm

This course syllabus should be interpreted as a contract of understanding between students, teaching assistants, and the instructor. By participating in the course you are agreeing to this understanding. Please review this document carefully and inform the instructor of any concerns. Revisions to this document will be made as needed then posted and announced in class.

Course Description

Software is pervasive, and for better or worse it now controls our daily lives. Almost every recent computer security issue has been rooted in software, so it is critical to develop and maintain secure software. This course provides a foundation for building secure software by applying the principles and the practices of secure programming. Secure software is the umbrella term used to describe software that is engineered such that it continues to function correctly under malicious attack. To write secure software, software practitioners need to write programs in a defensive fashion, to avoid vulnerabilities that can be exploited by attackers and use security features provided by libraries, such as authentication and encryption, appropriately and effectively. Specific course topics will include: operating systems and applications security, web security, secure design and development, malware, algorithmic complexity and side channel attacks, an introduction software analysis and penetration testing, among other topics.

This course provides students with a unique experience to hone their software development and software security skills in a hands-on and fast paced environment. Course materials are designed to prepare students for the workforce with practical skills while also providing a solid foundation to continue learning and research beyond the course.

If you do not feel my goals for the course align well with your personal goals, but you need to take this course anyway to satisfy a degree requirement, you should meet with me to figure out a way to make this course useful for satisfying your personal goals.

Expected Background & Prerequisites

Students entering this course are expected to be comfortable reading, designing, and writing *C* and *Java* programs that involve code distributed over many modules. Students are expected to have some familiarity with web applications and database concepts. You should be comfortable learning how to use new programming language features and APIs by reading their documentation (or source code when no documentation is available), and not be surprised when solving programming assignments that require you to seek documentation beyond what was provided in class.

Required Materials

We will closely follow the textbook from:

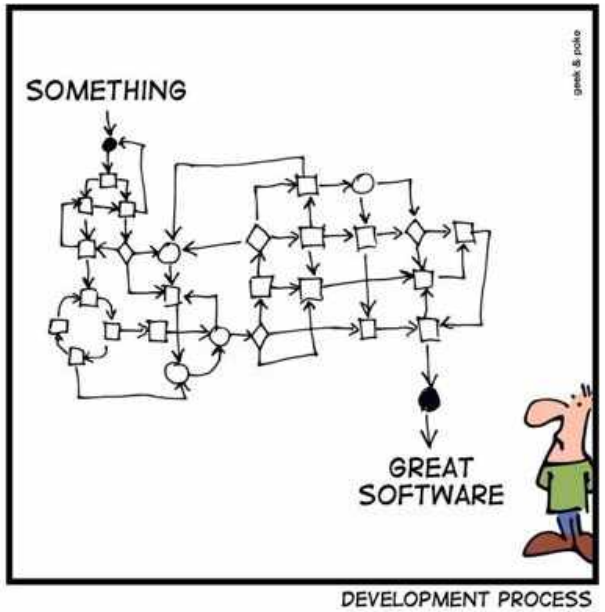
- [B1] Michael Goodrich and Roberto Tamassia 's *"Introduction to Computer Security,"* 1st Edition.

However, we will have several readings from many other resources including:

- [B2] Dieter Gollmann's *"Computer Security,"* 3rd Edition.
- [B3] Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies 's *"Security in Computing,"* 5th Edition.
- [B4] Brian Chess and Jacob West 's *"Secure Programming with Static Analysis,"* 1st Edition.
- [B5] Greg Hoglund, Gary McGraw 's *"Exploiting Software How to Break Code,"* 1st Edition.

1 / 4

Goal of the Class



Improve your ability to create **secure software** that will continue to work under **malicious attack** by understanding **secure development practices** and common **vulnerabilities** and **malicious attacks**

My **Real Goal** for Lectures

Provide **context** and **meaning** for the things you have or will later **learn on your own**

Ethical Concerns

- Disclaimer: The content in this course was created for educational purposes only.
- Consider the consequences of your actions. *Remember that every action may have unforeseeable consequences.*

```java
public class COMP4384 {

        public static void main(String[] args) {
                print("Hello");

                /*
                 * TODO: print World in unicode
                 * \u002A\u002F\u0070\u0072\u0069\u006E\u0074\u0028\u0022\u0043\u0072\u0075\u0065\u006C\u0022\u0029\u003B\u002F\u002A
                 */
                print("World");
        }

        private static void print(String s){
                System.out.print(s + " ");
        }

}
```

https://gist.github.com/atamrawi/68d07594174960c7bc534a5c8b259b25