Introduction to the course
CYBR (IA) - Capstone

Dr. Hale
University of Nebraska at Omaha

Welcome to ~~IASC~~ CYBR 4580

What is this class?

Short story:
We will be making stuff and/or breaking stuff.

What is this class?

Long story:
This may very well be the most challenging course you've had at UNO. It is meant to be.

- You will feel great when you create something new and/or exercise your muscles at systematically breaking something.
- You are about to be 'let loose' on the world of Cybersecurity. This class is for you to prove to yourself and the world that you are ready.
- I'm here for you and want you to know that.
    - Open door policy
    - Weekly meeting updates once the projects start
    - Open questions any time of day (via slack or email) – I'll respond when I can

What is this class?

Long(er) story:

- You will be a member of team
- You will pick a ‘track’ – development oriented or assessment oriented
    - Both tracks are equally ‘difficult’ and will require roughly the same amount of your time (a lot).
    - Both tracks will require both technical skill and writing prowess. Part of being a professional isn’t just being the best, brightest technical mind in the room, but being able to communicate that with others
- You will follow an agile methodology and create both technical artifacts (code and tests) but also documentation (system architecture designs, use cases, etc)

Who am I

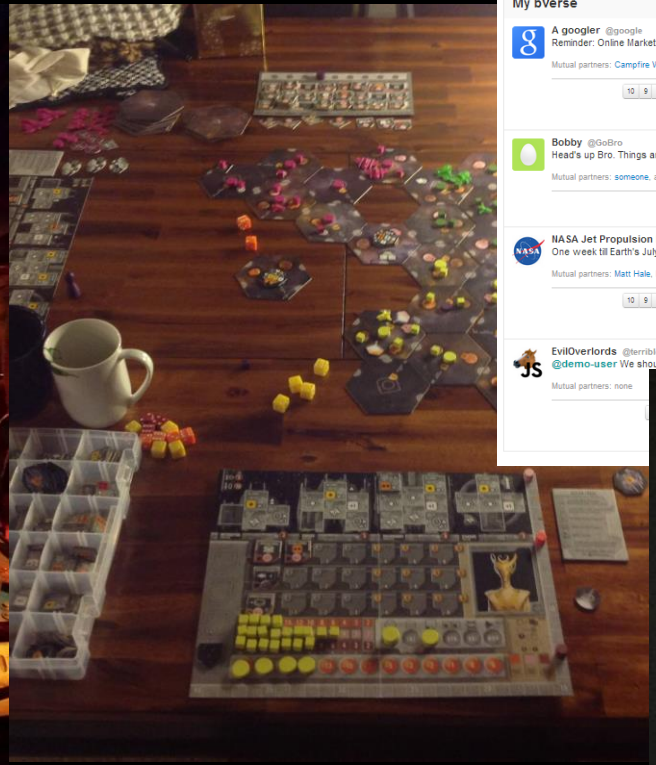
- I'm a nerd, a philosopher, an artist, a board gamer, and a software engineer.
- I'm here to challenge you. Life is meaningless if you never know (and push) your limits. 'Non est ad astra mollis e terris via' – (There is no easy way from the earth to the stars) – Seneca

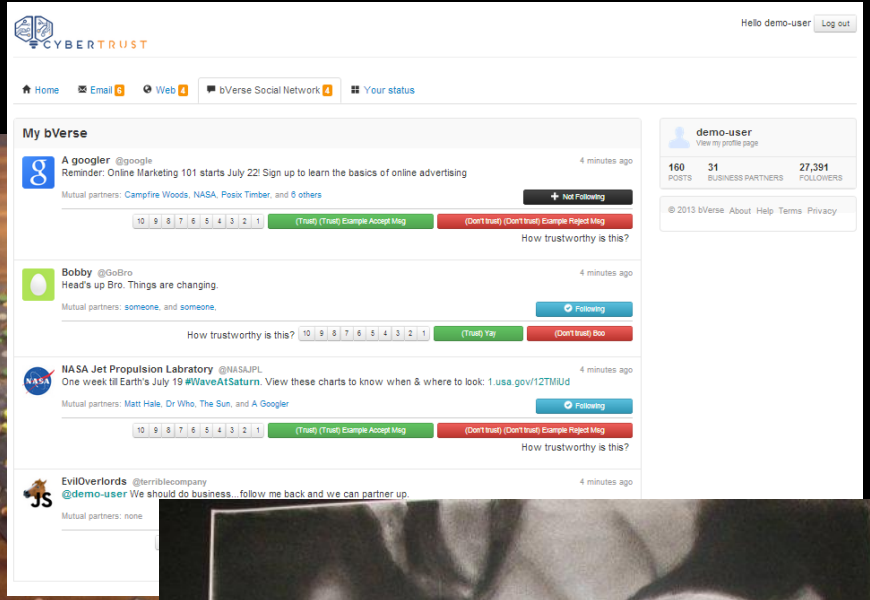
and Why should you trust me?

- I've made stuff (mostly highly interactive and visual web apps).
- I've also helped students make stuff and seen the looks of pride on their faces when they make stuff they never thought they could make.
- I believe in you and want to see you succeed.

Who am I


KEEP
CALM
AND
DON'T




CYBERTRUST
Hello demo-user
Log out
Home
Email 5
Web 4
bVerse Social Network 4
Your status
My bVerse
A googler @google
4 minutes ago
Reminder: Online Marketing 101 starts July 22! Sign up to learn the basics of online advertising
Mutual partners: Campfire Woods, NASA, Posix Timber, and 6 others
Not Following
How trustworthy is this?
(Trust) (Trust) Example Accept Msg
(Don't trust) (Don't trust) Example Reject Msg
Bobby @GoBro
4 minutes ago
Head's up Bro. Things are changing.
Mutual partners: someone, and someone.
Following
How trustworthy is this?
(Trust) Yay
(Don't trust) Boo
NASA Jet Propulsion Labratory @NASAJPL
4 minutes ago
One week till Earth's July 19 #WaveAtSaturn. View these charts to know when & where to look: 1.usa.gov/12TMIJd
Mutual partners: Matt Hale, Dr Who, The Sun, and A Googler
Following
How trustworthy is this?
(Trust) (Trust) Example Accept Msg
(Don't trust) (Don't trust) Example Reject Msg
EvilOverlords @terriblecompany
4 minutes ago
@demo-user We should do business...follow me back and we can partner up.
Mutual partners: none
demo-user
View my profile page
160 POSTS
31 BUSINESS PARTNERS
27,391 FOLLOWERS
© 2013 bVerse About Help Terms Privacy

Who are you?

- Something quirky about yourself
- Something you find interesting
- What motivates you?

- What do you want to do after you graduate?

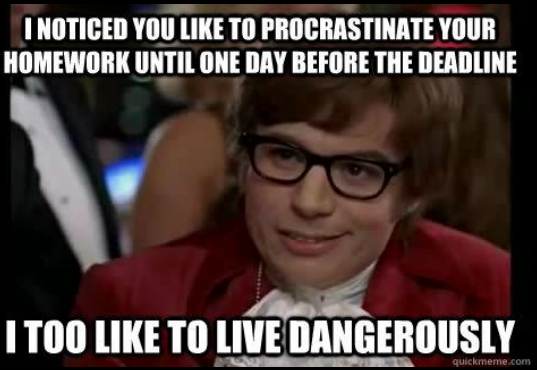
Ok so what will we cover?

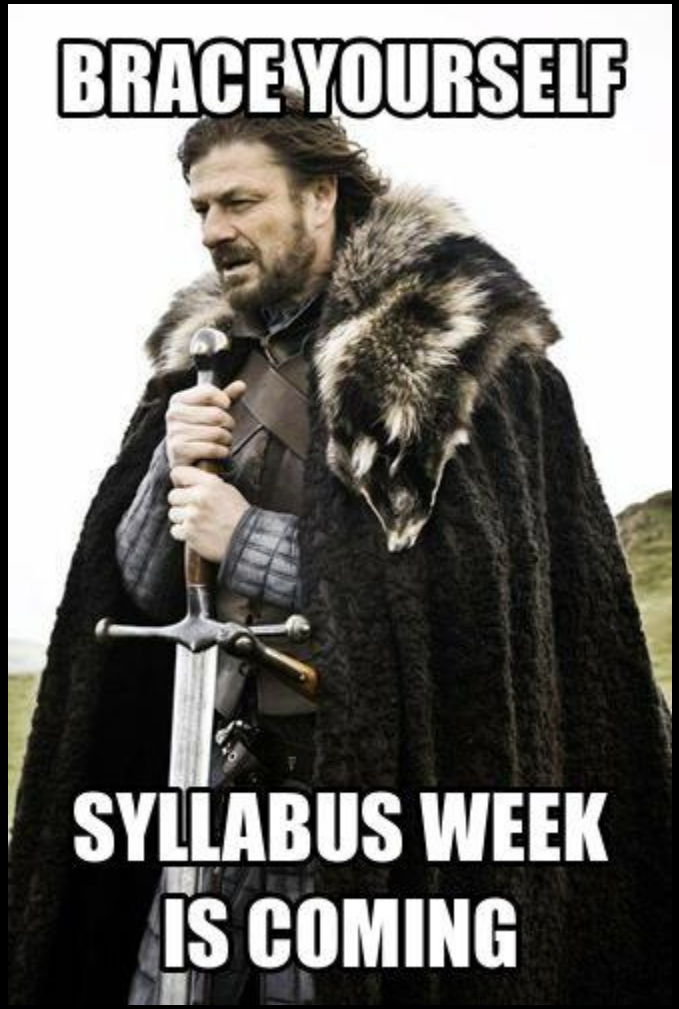
- Software engineering principles
  - Software architecting
  - Software design principles (including security)
  - Security in the SDLC (Software Development Lifecycle)
- Certification and assessment standard (review and apply)
  - Security controls, countermeasures, etc
  - NIST SP800-53, FIPS200, 800-33, etc
- Test driven development and assessment
  - Unit testing
  - Blackbox testing
  - Assessment tools
- Collaboration
  - Methods and frameworks
  - Tools

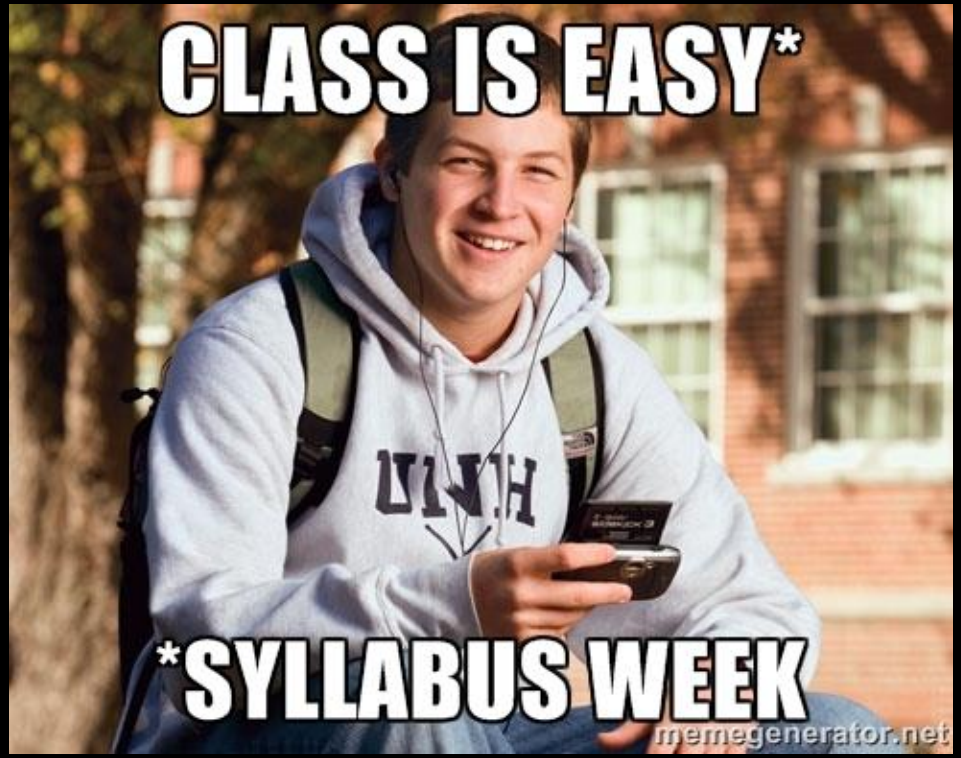
Foreword:

What to expect from this class

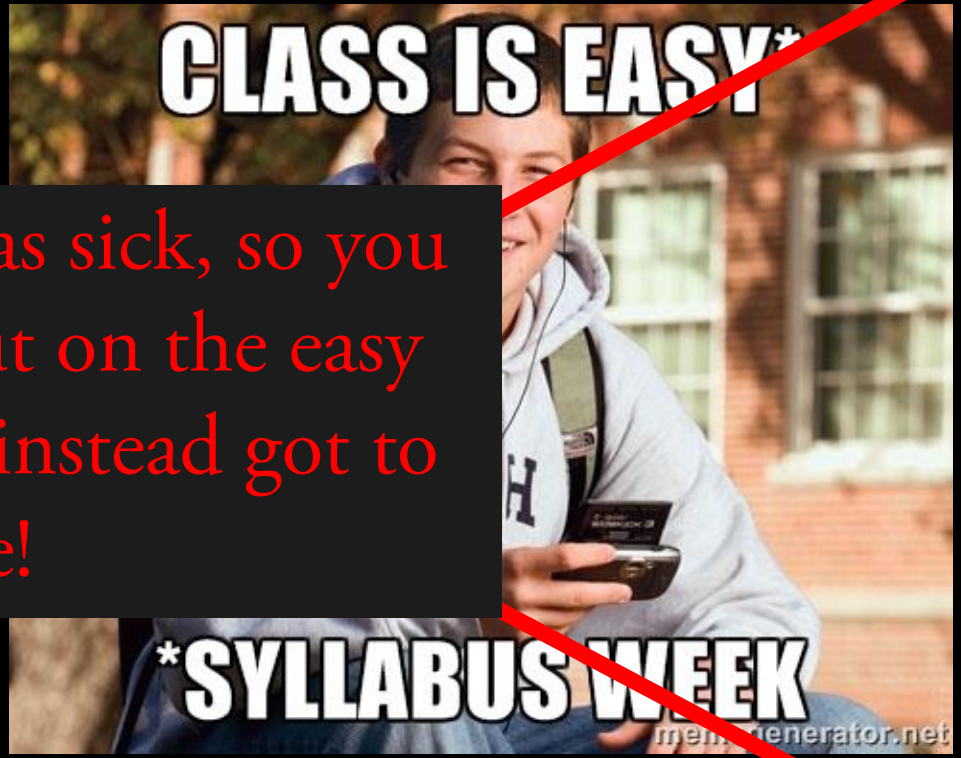
- Mostly project development and lab time with a bit of lecture
- A few step-by-step tutorials
- Some review content and materials in different areas
- No tests
- Lots of projects (don't procrastinate)
- self-referential (bad) humor in slides







Hint: Syllabus time



Sadly I was sick, so you missed out on the easy class and instead got to stay home!

Hint: Syllabus time

Today's Class: Not spending the entire class on the syllabus

Foreword: what is this class, who am I, who are you, what we will cover
Content Part 1: State of the world we live in
- Statistics: threat vectors and vulnerabilities
- Web apps, native apps, hybrid apps, oh my (architectures)
- Wearables and IoT
- SCADA

Intermission: (I'll try to give you all a 5-10min break roughly in the middle of class)
Hands-on: TBA
Content Part 2: What you can do about it
- Build better, safer, software
- Help make existing software safer by identifying (and reporting/mitigating)

Part1:

State of the world

Lets talk about a little about web apps and security.

citibank

twitter

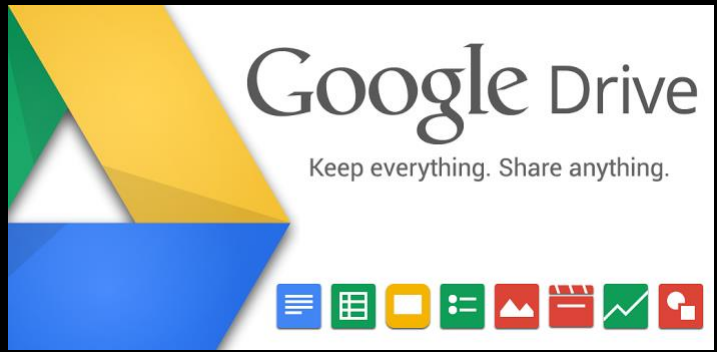
Insta

Gmail by Google

(nearly) All companies have a web app.
You probably use them, daily.

Dropbox

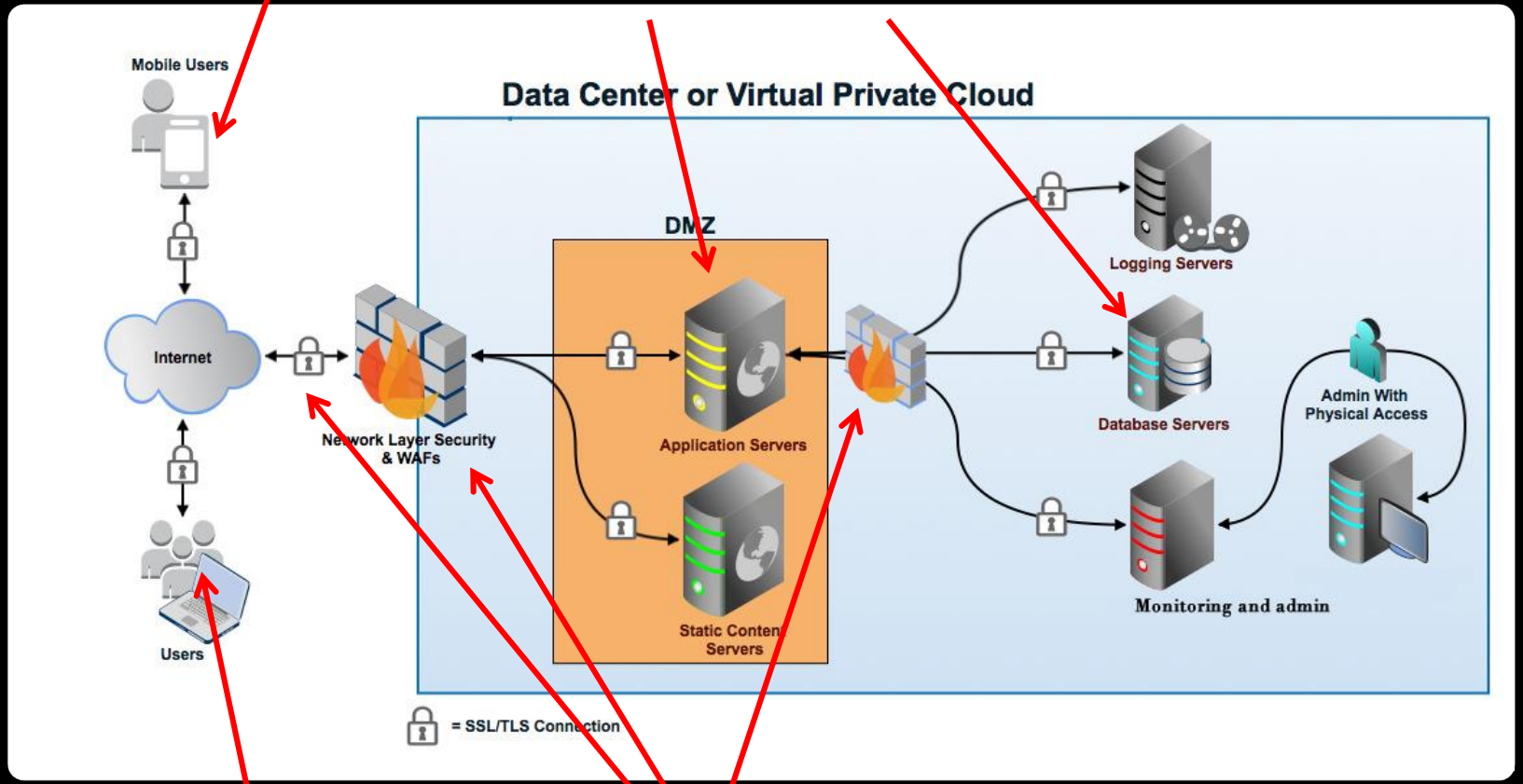
foursquare



Also you

Where developers should actually focus on security

Typical Web Application Architecture



You

What most companies think "security" means

As a user, you expect web apps to be:

fast, responsive, always available, and secure

Percentage of tested apps with vulnerabilities

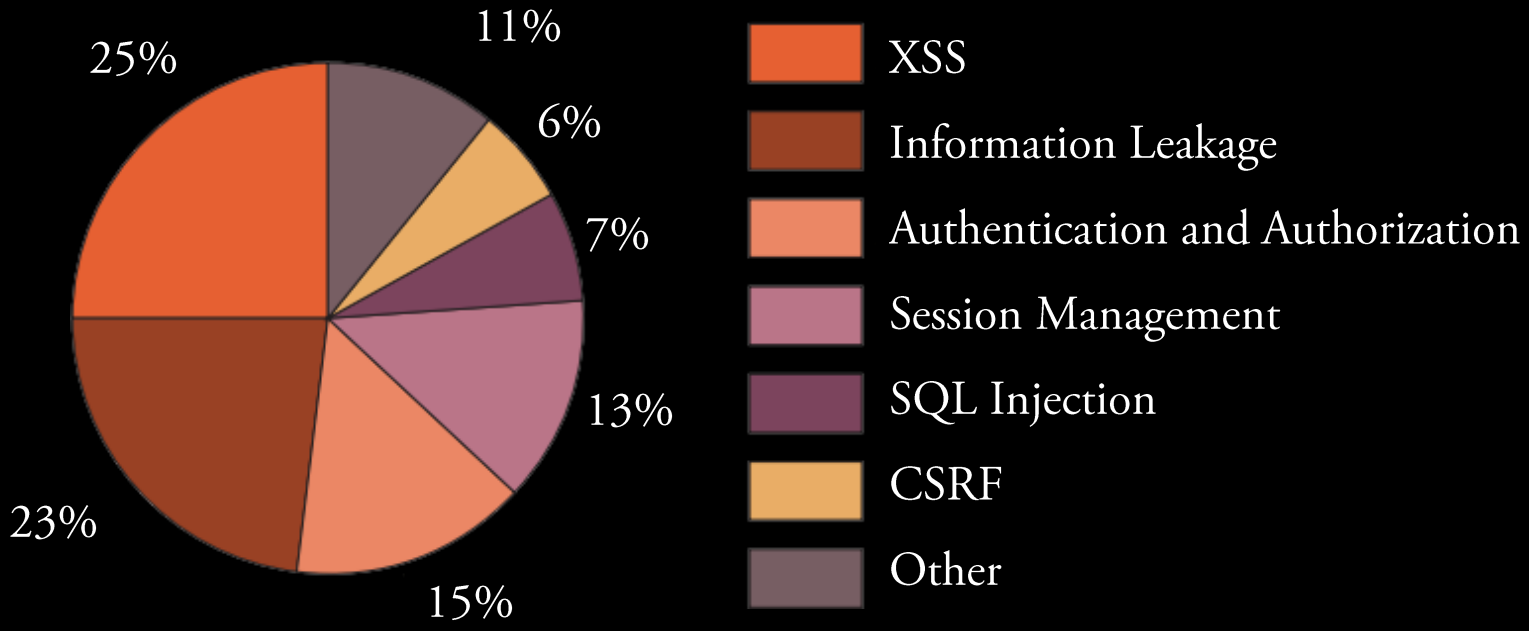
Despite your expectations…

96% of web applications have vulnerabilities*

Median number of vulnerabilities per app

Cenzic Application Vulnerability Trends Report : 2014

*…at the application level



*Cenzic Application Vulnerability Trends Report : 2014

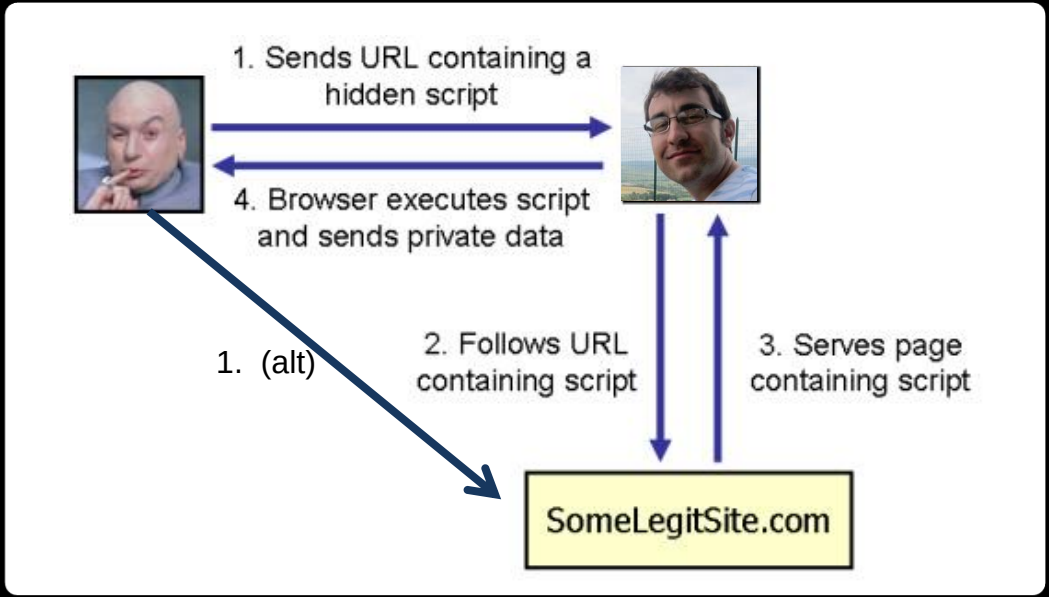
The basic principle behind all web application attacks…

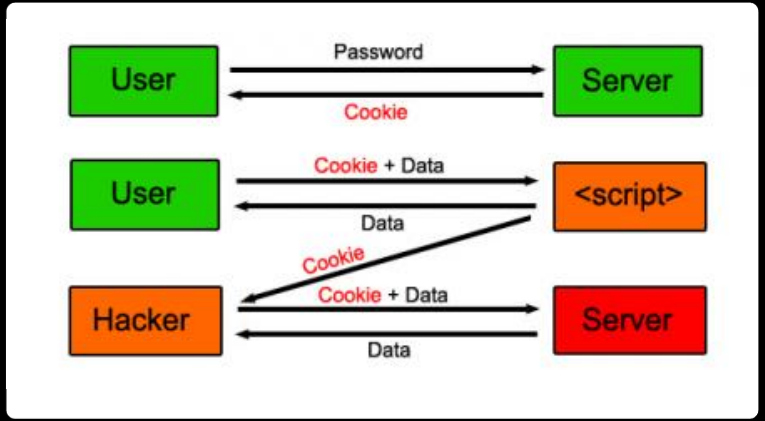
…make the web application do something it was never intended to do.

aka…user input is evil.

Ex: XSS

Allows attackers to inject malicious scripts into web pages and have it executed in another user's browser. Usually to capture some user information.





Ex: Defending against XSS (serverside)

(The problem children)

HTML Entities	
Character	**Encoding**
<	< or <
>	> or >
&	& or &
"	" or "
'	' or '
(	&#40;
)	&#41;
#	&#35;
%	&#37;
;	&#59;
+	&#43;
-	&#45;

Filter and validate all user input before accepting it.
Encode and escape special characters as HTML.

Never trust user input or display raw submissions.

Ex: Defending against XSS (client-side)

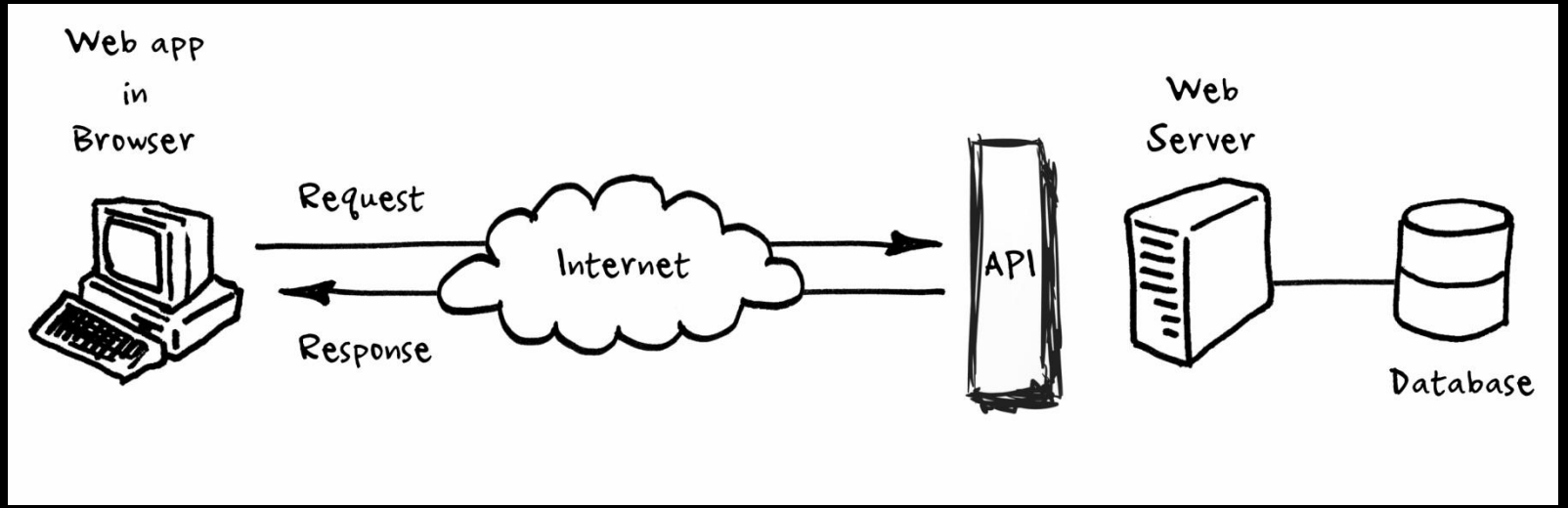
Use Content-Security-Policy

```
Content-Security-Policy: default-src: 'self'; script-src: 'self' somedomain.com
```

Ex: Defending against XSS

Use well tested frameworks

Unique opportunities (and security challenges) arise with modern web concepts like REST, client-side MVC, and mobile apps.



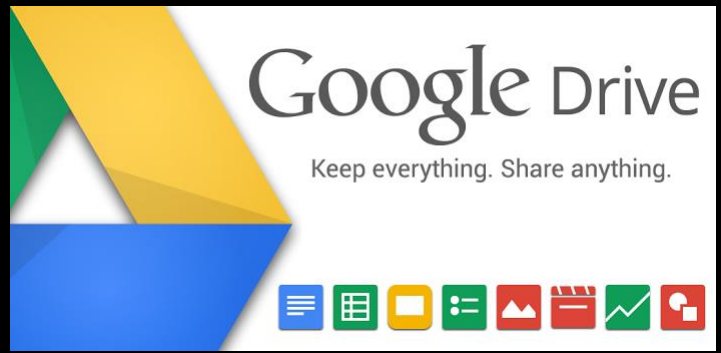
REST: REpresentational State Transfer
(GET/POST/PUT/DELETE requests drive your application)

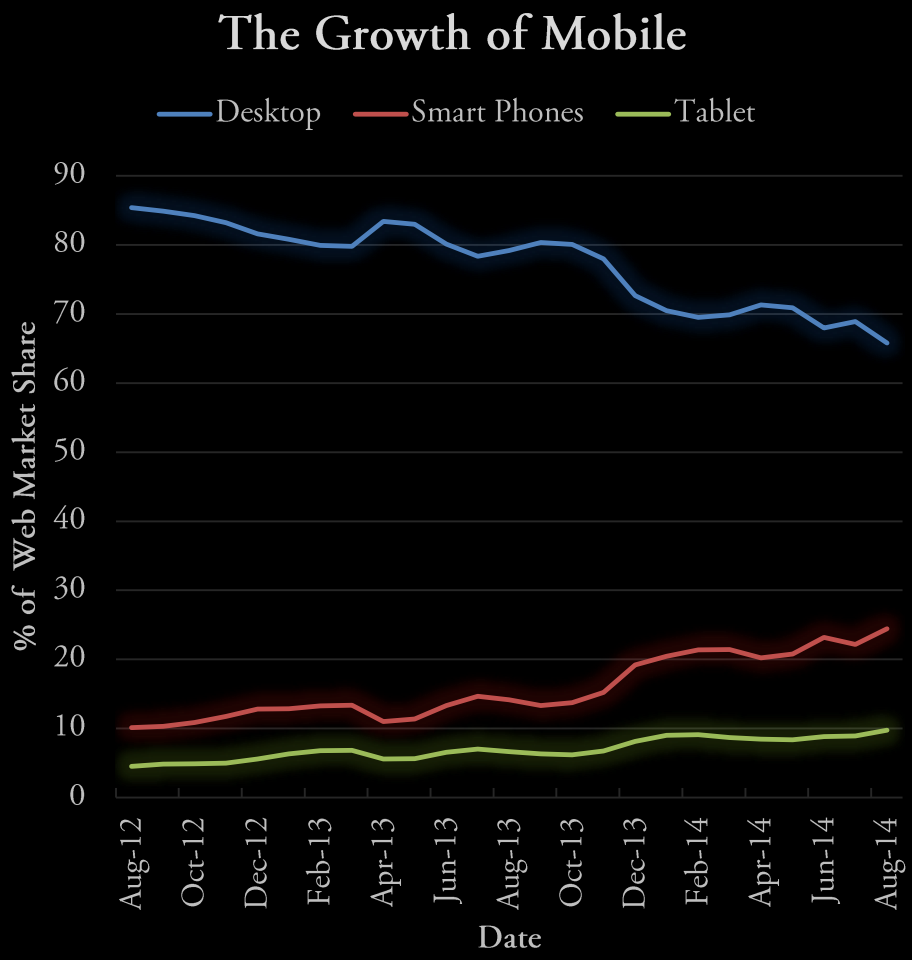
Data is exposed using a REST-ful API
Asynchronous AJAX callbacks used to dynamically load data into the application on the client-side.

Network Tab REST DEMO
http://jsonplaceholder.typicode.com/

Lets talk a little about the different types of mobile apps.

(nearly) All companies have a mobile app.
You probably use them, daily.





Face reality as it is, not as it was or as you wish it to be

- Jack Welch (former GM CEO)

As a user, you expect mobile apps to be:

fast, responsive, connected, and secure

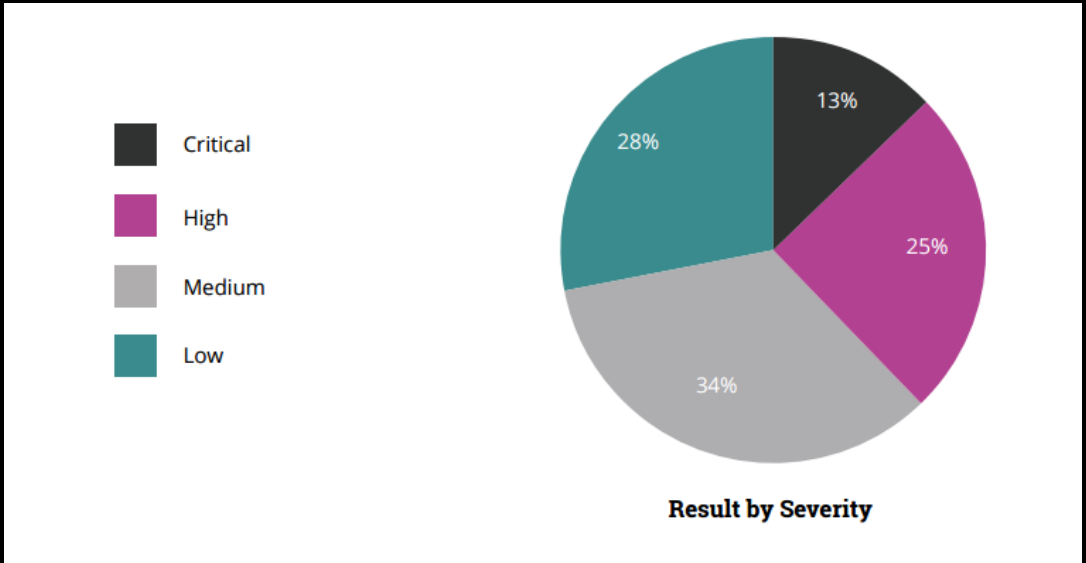
Despite your expectations…

Most mobile applications have vulnerabilities*

*9.041 Vulnerabilities per app on average

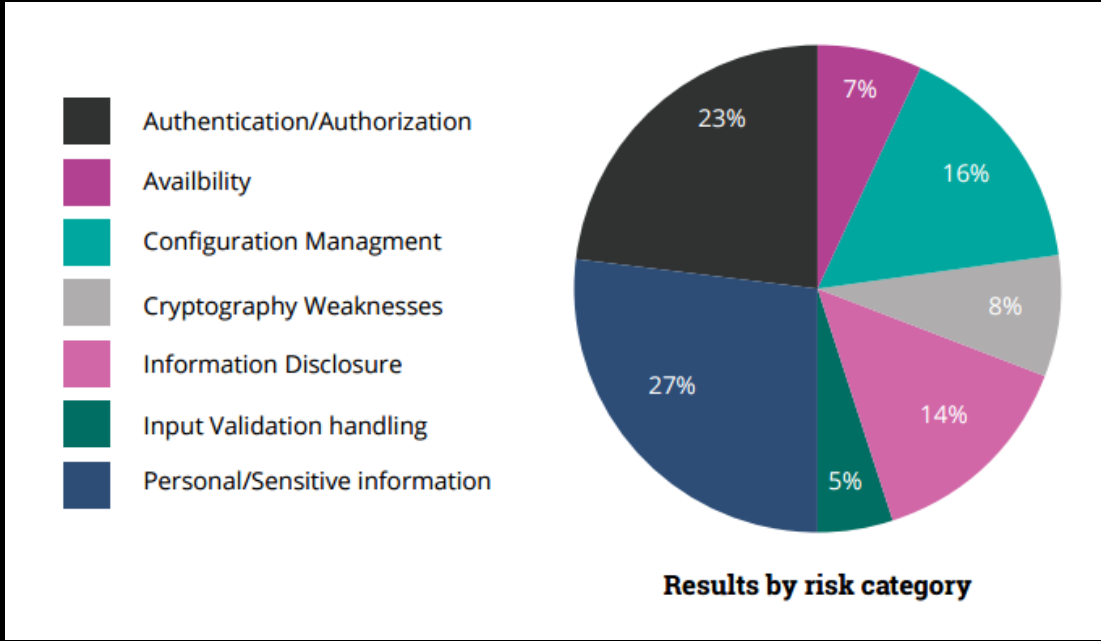
CheckMarx appsec labs 2014-2015 The State of Mobile Application

…decomposition by criticality



CheckMarx appsec labs 2014-2015 The State of Mobile Application Security

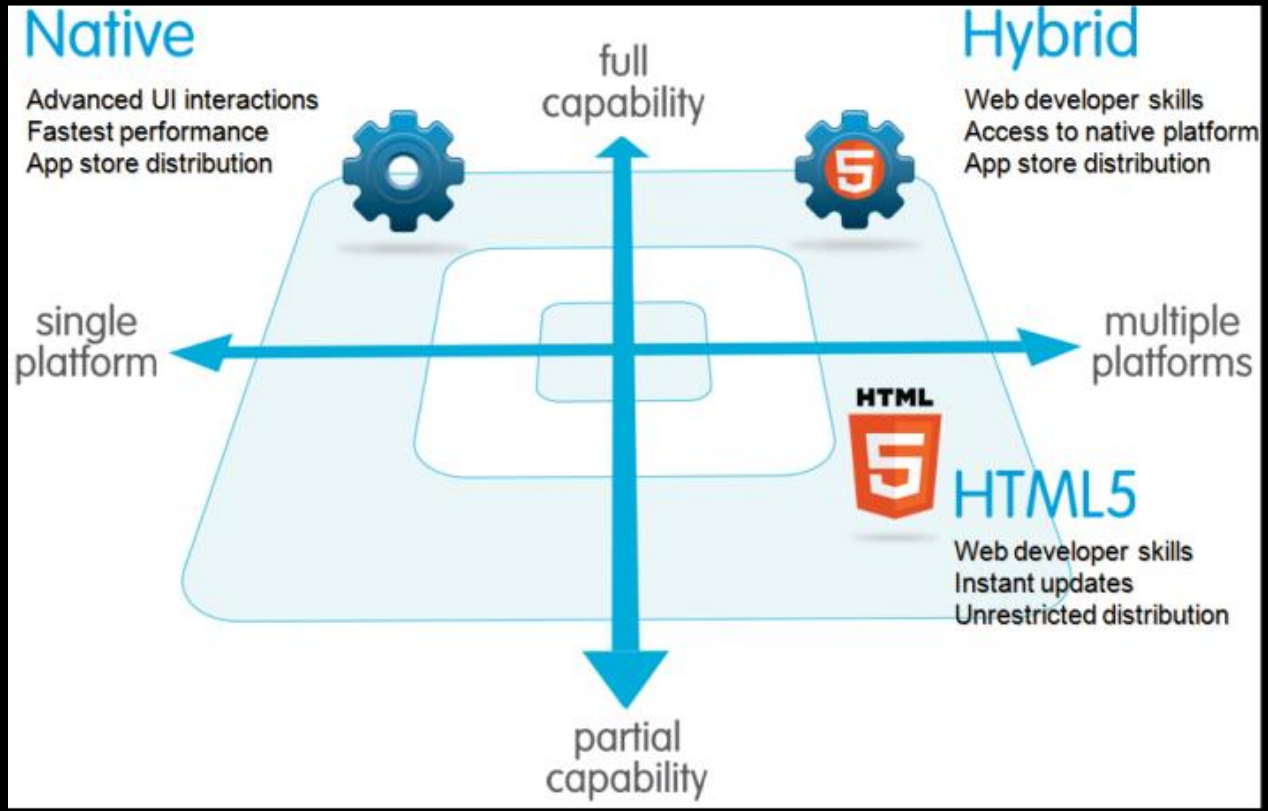
…decomposition by type



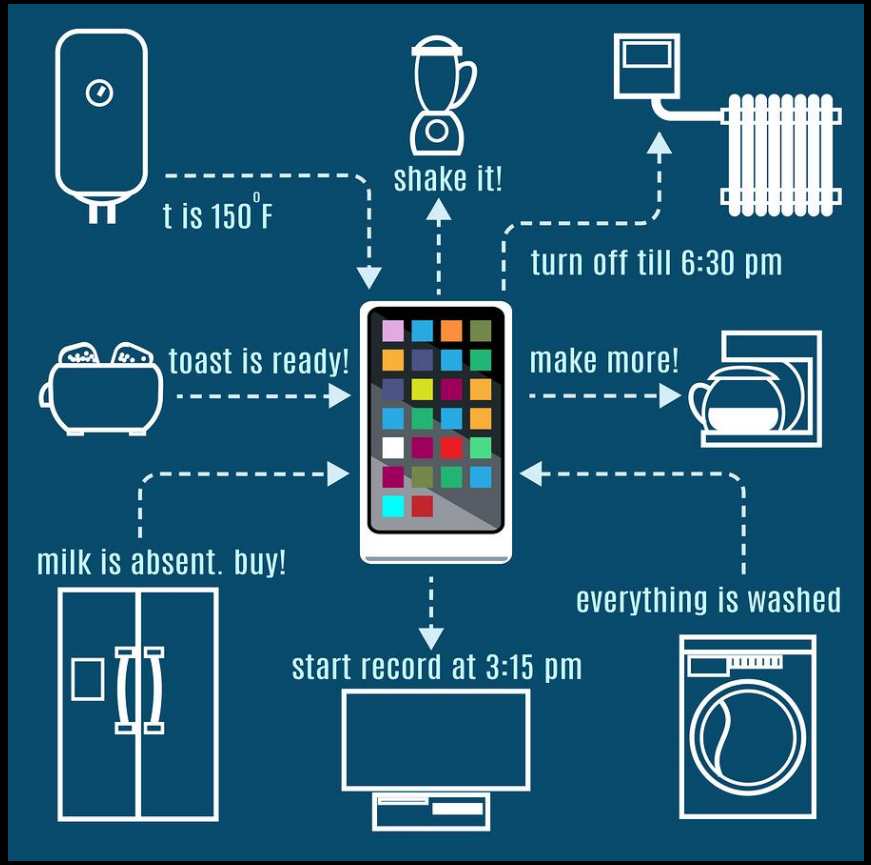
CheckMarx appsec labs 2014-2015 The State of Mobile Application Security

There are three main types of mobile apps

Landscape of types



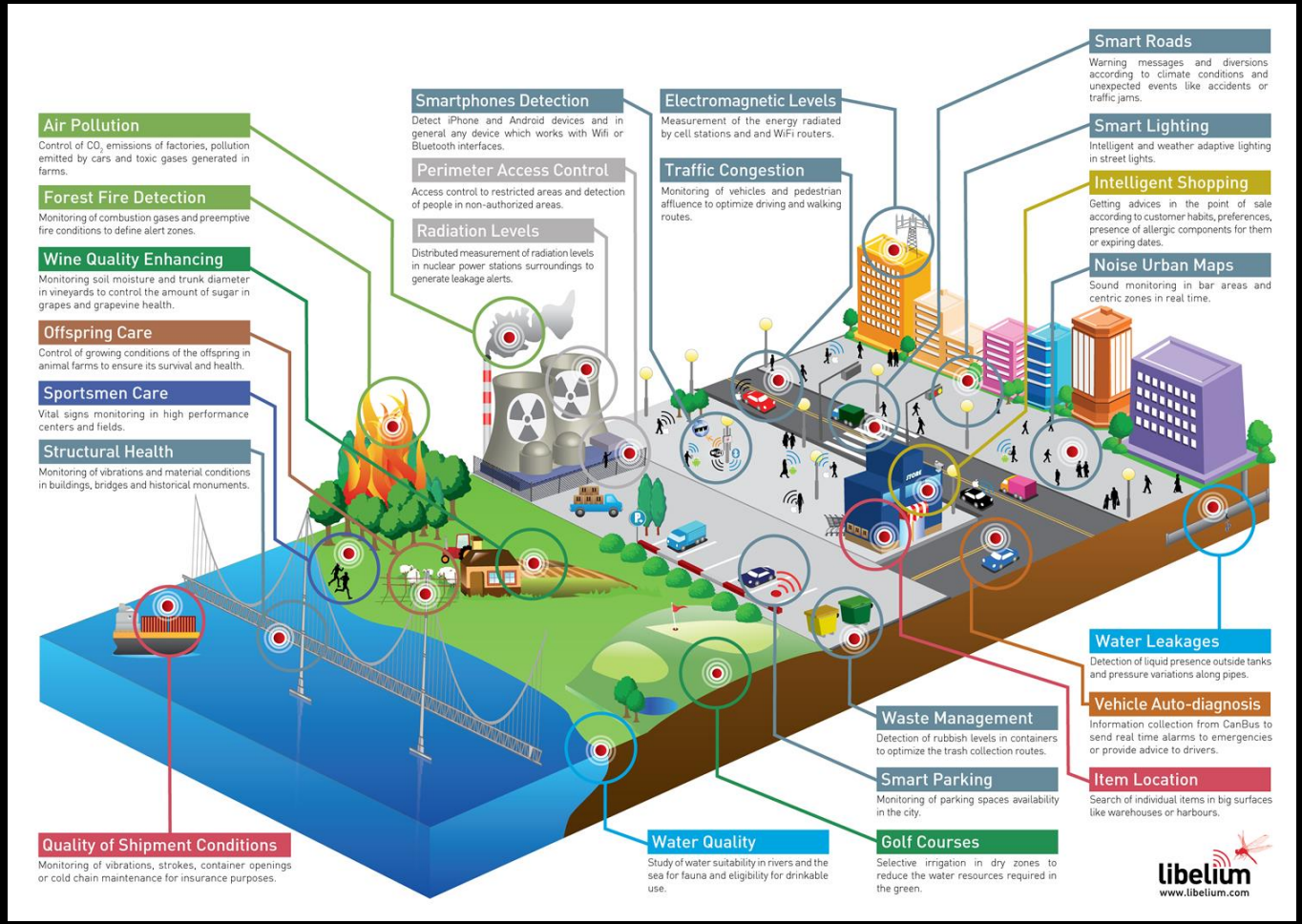
Lets talk about a little about IoT security.



What is the internet of things and why should you care?

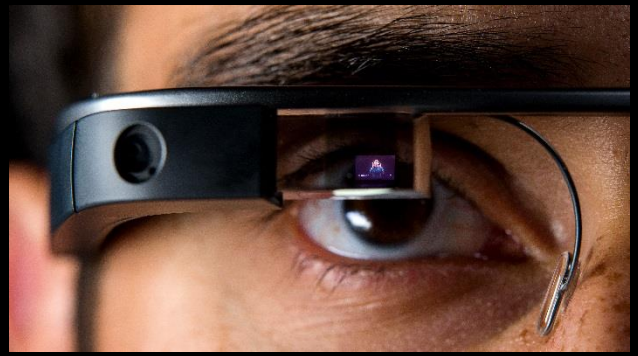
What is the internet of things?

Sensors
Embedded
Everywhere



What is the internet of things?

fitbit surge™



GLASS

Including on your wrist, in your clothes, on your face…

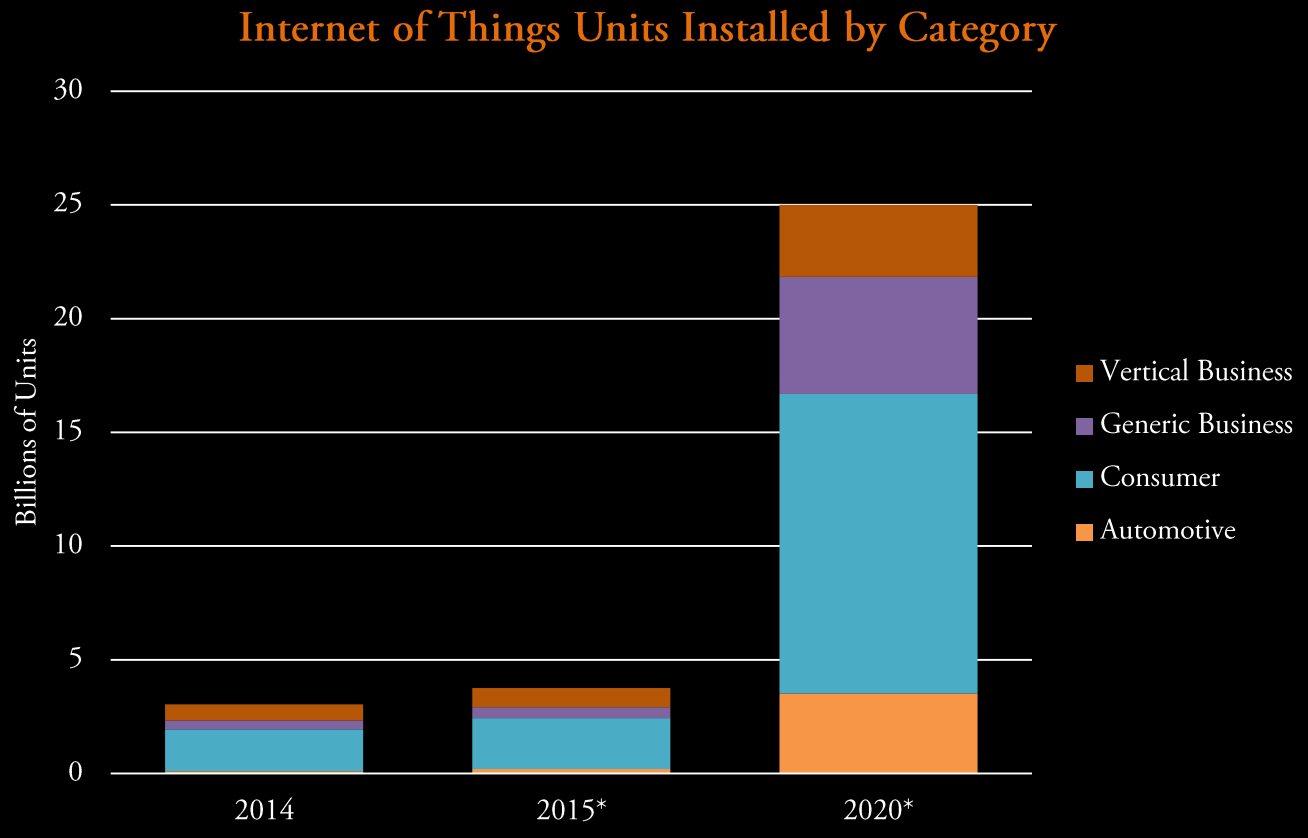
NIKEFUEL

UP by JAWBONE™

What is the internet of things?

And lots of:

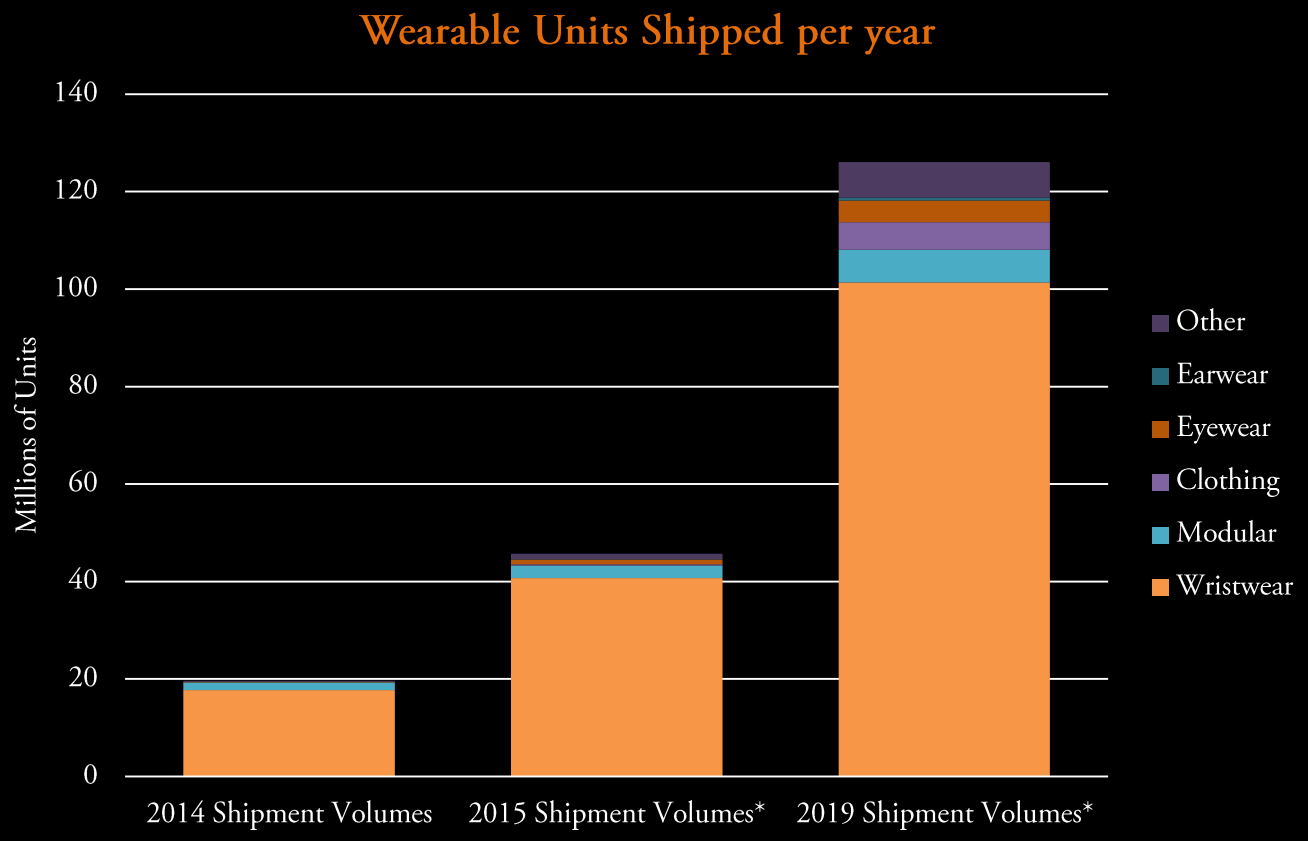
An Idea of Scale (IoT)



* Forecasted figures

Source: Gartner: 4.9 Billion Connected "Things" will be in use by end of 2015, November, 2014

An Idea of Scale (Wearables)



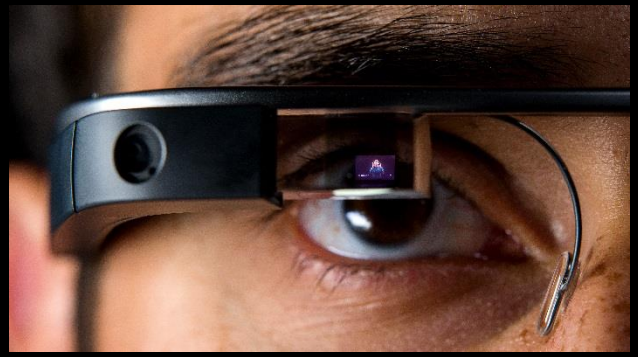
* Forecasted figures

Source: IDC Worldwide Quarterly Wearable Device Tracker, March 30, 2015

133.4% Growth from 2014 to 2015 (19.6M to 45.7M)

45.1% Five-year compound annual growth rate (19.6 to 126.1)

fitbit surge



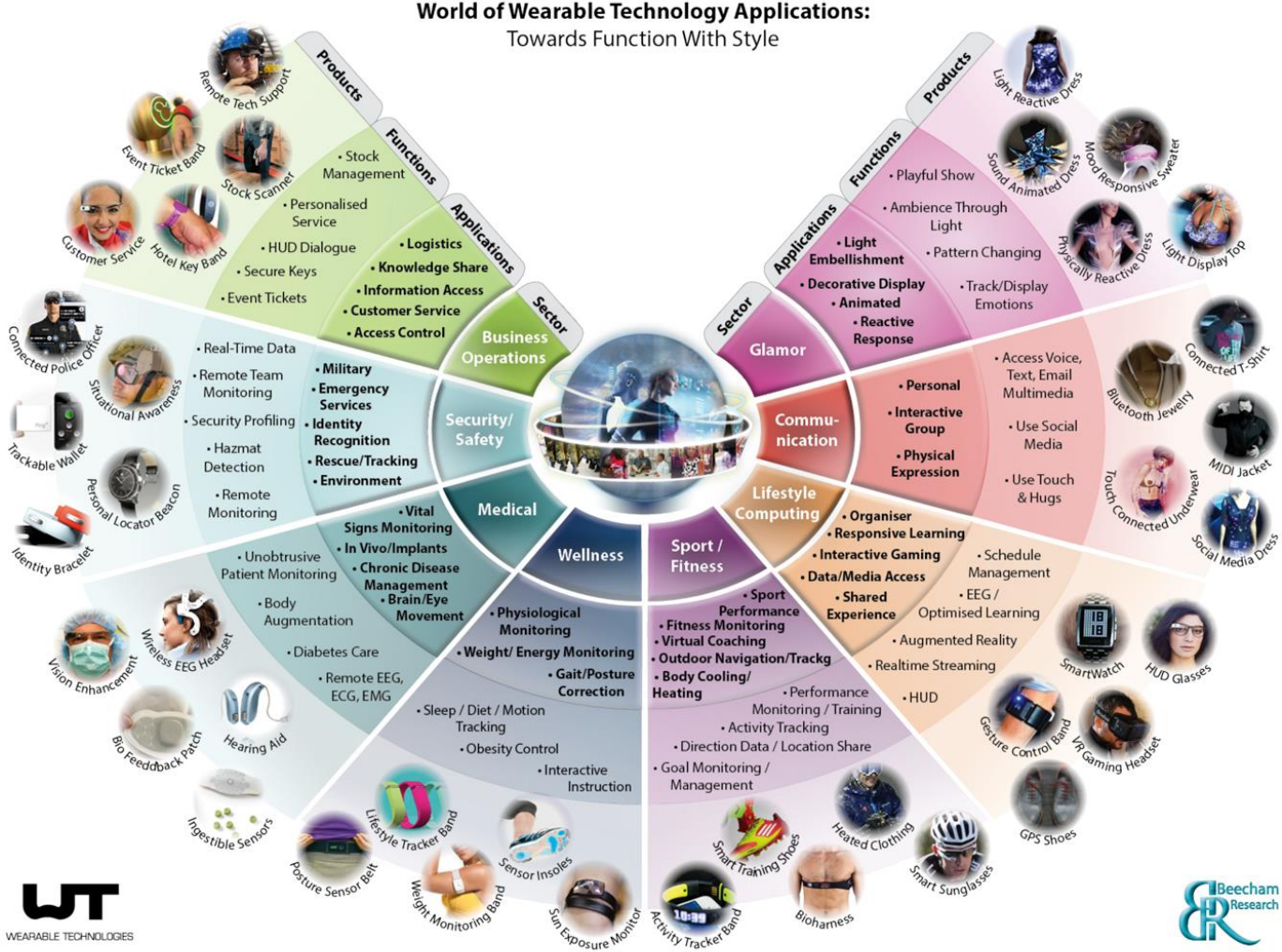
GLASS

…ok so what? its sleep and pedometer data.

NIKEFUEL

UP
by JAWBONE™

Not exactly.


World of Wearable Technology Applications:
Towards Function With Style
Products
Functions
Applications
Sector
Business Operations
Security/ Safety
Medical
Wellness
Sport / Fitness
Lifestyle Computing
Commu-nication
Glamor
Remote Tech Support
Event Ticket Band
Stock Scanner
Customer Service
Hotel Key Band
• Stock Management
• Personalised Service
• HUD Dialogue
• Secure Keys
• Event Tickets
• Logistics
• Knowledge Share
• Information Access
• Customer Service
• Access Control
Connected Police Officer
Situational Awareness
Trackable Wallet
Personal Locator Beacon
Identity Bracelet
• Real-Time Data
• Remote Team Monitoring
• Security Profiling
• Hazmat Detection
• Remote Monitoring
• Military
• Emergency Services
• Identity Recognition
• Rescue/Tracking
• Environment
Vision Enhancement
Wireless EEG Headset
Bio Feedback Patch
Hearing Aid
Ingestible Sensors
• Unobtrusive Patient Monitoring
• Body Augmentation
• Diabetes Care
• Remote EEG, ECG, EMG
• Vital Signs Monitoring
• In Vivo/Implants
• Chronic Disease Management
• Brain/Eye Movement
Posture Sensor Belt
Lifestyle Tracker Band
Weight Monitoring Band
Sensor Insoles
Sun Exposure Monitor
• Physiological Monitoring
• Weight/ Energy Monitoring
• Gait/Posture Correction
• Sleep / Diet / Motion Tracking
• Obesity Control
• Interactive Instruction
Activity Tracker Band
Bioharness
Smart Training Shoes
Heated Clothing
Smart Sunglasses
• Sport Performance
• Fitness Monitoring
• Virtual Coaching
• Outdoor Navigation/Trackg
• Body Cooling/ Heating
• Performance Monitoring / Training
• Activity Tracking
• Direction Data / Location Share
• Goal Monitoring / Management
GPS Shoes
Gesture Control Band
VR Gaming Headset
SmartWatch
HUD Glasses
• Organiser
• Responsive Learning
• Interactive Gaming
• Data/Media Access
• Shared Experience
• Schedule Management
• EEG / Optimised Learning
• Augmented Reality
• Realtime Streaming
• HUD
Touch Connected Underwear
Social Media Dress
Bluetooth Jewelry
MIDI Jacket
Connected T-Shirt
• Personal
• Interactive Group
• Physical Expression
• Access Voice, Text, Email Multimedia
• Use Social Media
• Use Touch & Hugs
Physically Reactive Dress
Light Display Top
Mood Responsive Sweater
Sound Animated Dress
Light Reactive Dress
• Playful Show
• Ambience Through Light
• Pattern Changing
• Track/Display Emotions
• Light Embellishment
• Decorative Display
• Animated
• Reactive Response
WEARABLE TECHNOLOGIES
Beecham Research
© 2014 Beecham Research Ltd. & Wearable Technologies AG

Why do apps use

?

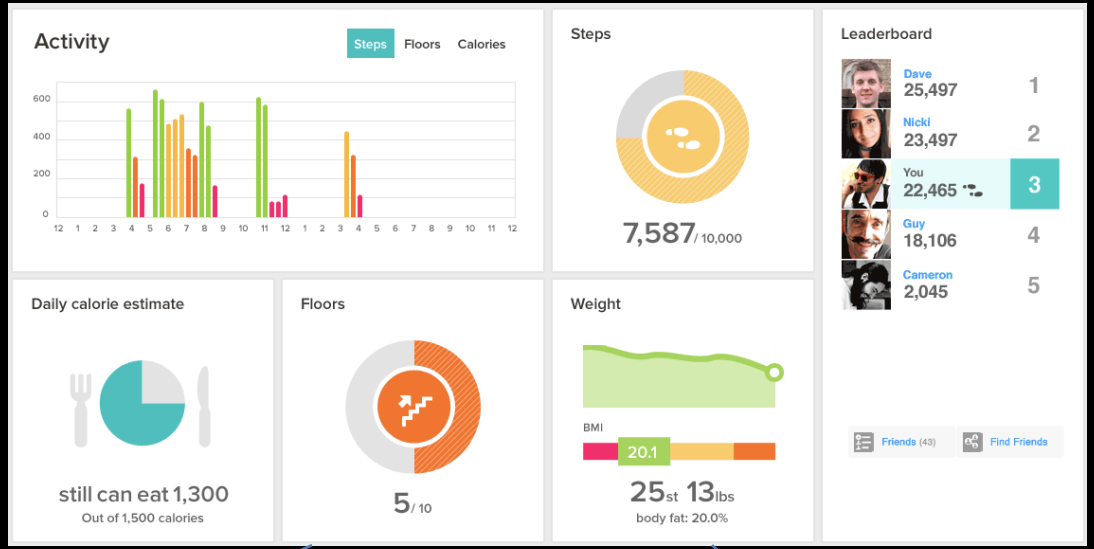
Better know the user*

*in whatever application

Mostly

-> Advertising and revenue generation

The possibilities:



Big data is also important for other sectors

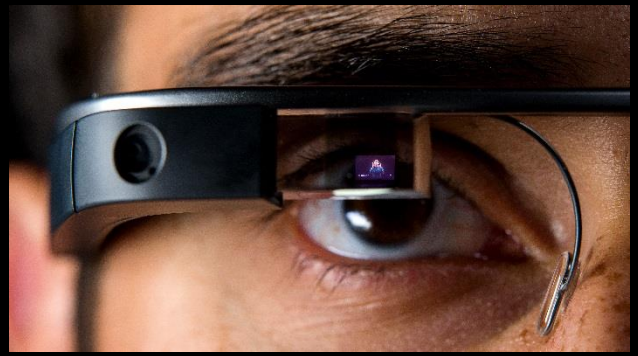
Medical -> patient well being & diagnosis

Military -> warfighter well being / operational intelligence

SITUATIONAL AWARENESS

Yeah it's important

fitbit surge™



GLASS

…there are many security challenges

NIKEFUEL

UP
by JAWBONE™

(in)security landscape

Domain security issues

User Awareness and Privacy Behaviors	Don't recognize data sensitivity or misuse May install malware or malicious apps Apps may be an invasion of privacy
Web Application	Standard Web attacks (XSS, SQL injection, CSRF, etc) Information Leakage (e.g. geotagging in social media) Secure data storage and acceptable data usage
Mobile Application	Third party tracking apps accessing data (stored/in-transit) Data encoding and transmission Resource consumption
Wearable Hardware	Physical tampering Data encoding and transmission Resource consumption

Inter-domain security issues

User Awareness and Privacy Behaviors

Web Application

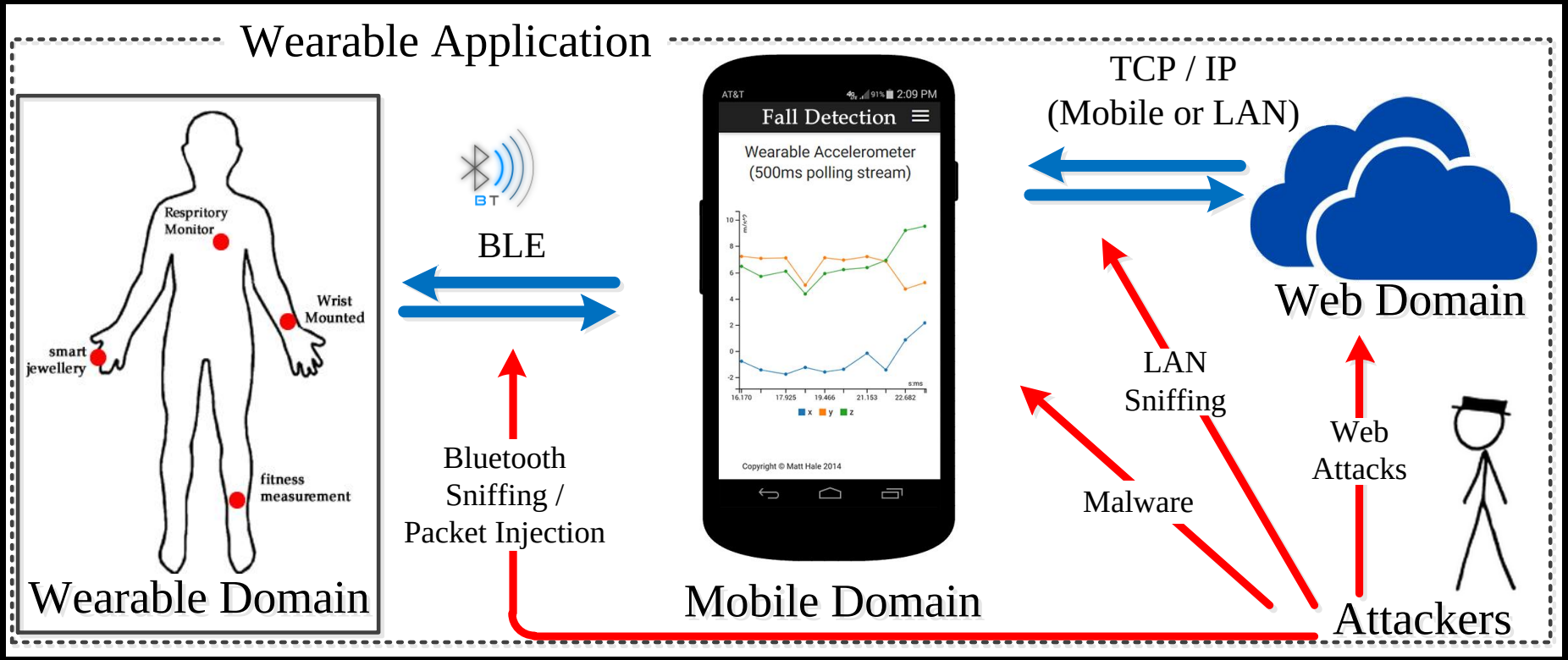
Insecure Wi-Fi or 4G
Lack of API Security (HTTPS/CORS/CSRF)

Mobile Application

Lack of over-the-air encryption
Man-in-the-middle attacks
Denial of service / Resource consumption

Wearable Hardware

Attack vectors for a typical app



Lets talk about a little about ICS/SCADA security.

Slides Credit: Bill Mahoney ©2016

A Control System

Sensor(s) +
Actuator(s) +
Controller(s)

SCADA(Supervisory control and data acquisition) or ICS (Industrial Control System) or DCS(Distributed Control System)?

NowaParts, people tend to say "SCADA" for anything related to Industrial Control Systems (ICS), but…

The key word in SCADA is "Supervisory." **This indicates that decisions are not directly made by the system.** SCADA systems are typically deployed across large geographical areas (e.g., electric grid).

DCS **provides real-time monitoring and control of a given process within a plant.** All major components of the system are usually confined to one or several facilities (e.g., Nuclear power plant).

There are several different types of control systems that are used to make, monitor, and move products. ICS refers to a broad set of control systems, which includes:

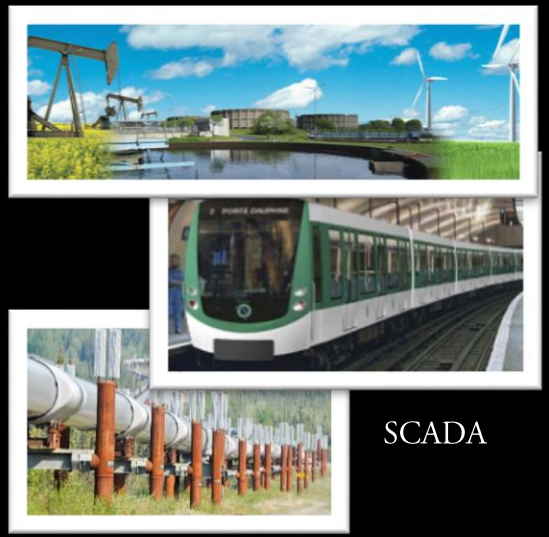
ICS (Industrial Control System)
=
IACS (Industrial Automation and Control System)
~=
SCADA (Supervisory Control and Data Acquisition)
~=
DCS (Distributed Control System)
~=
PCS (Process Control System)
~=
EMS (Energy Management System)
~=
SIS (Safety Instrumented Systems)

Industrial Automation (IACS)

Distributed Control (DCS)

Process Control (PCS)

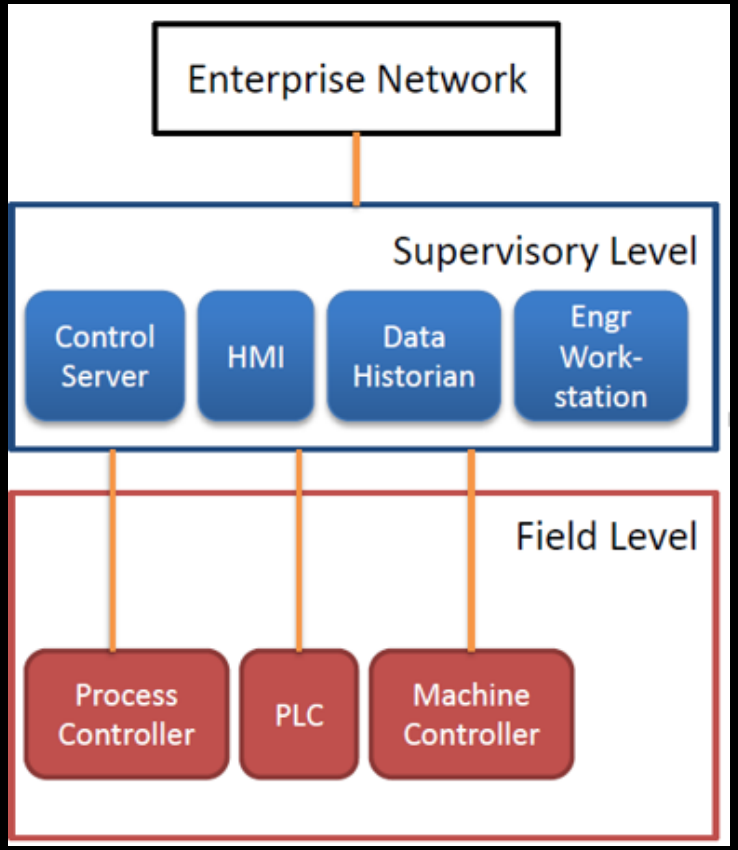
Energy Management System (EMS)



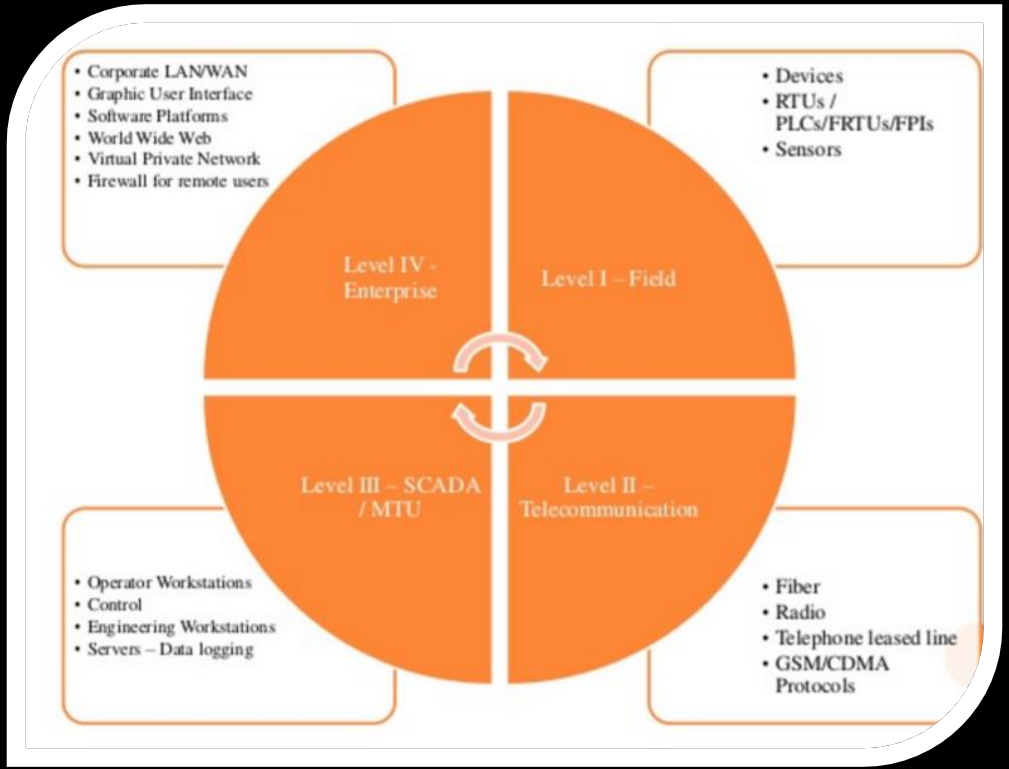
SCADA

Safety Instrumented System (SIS)

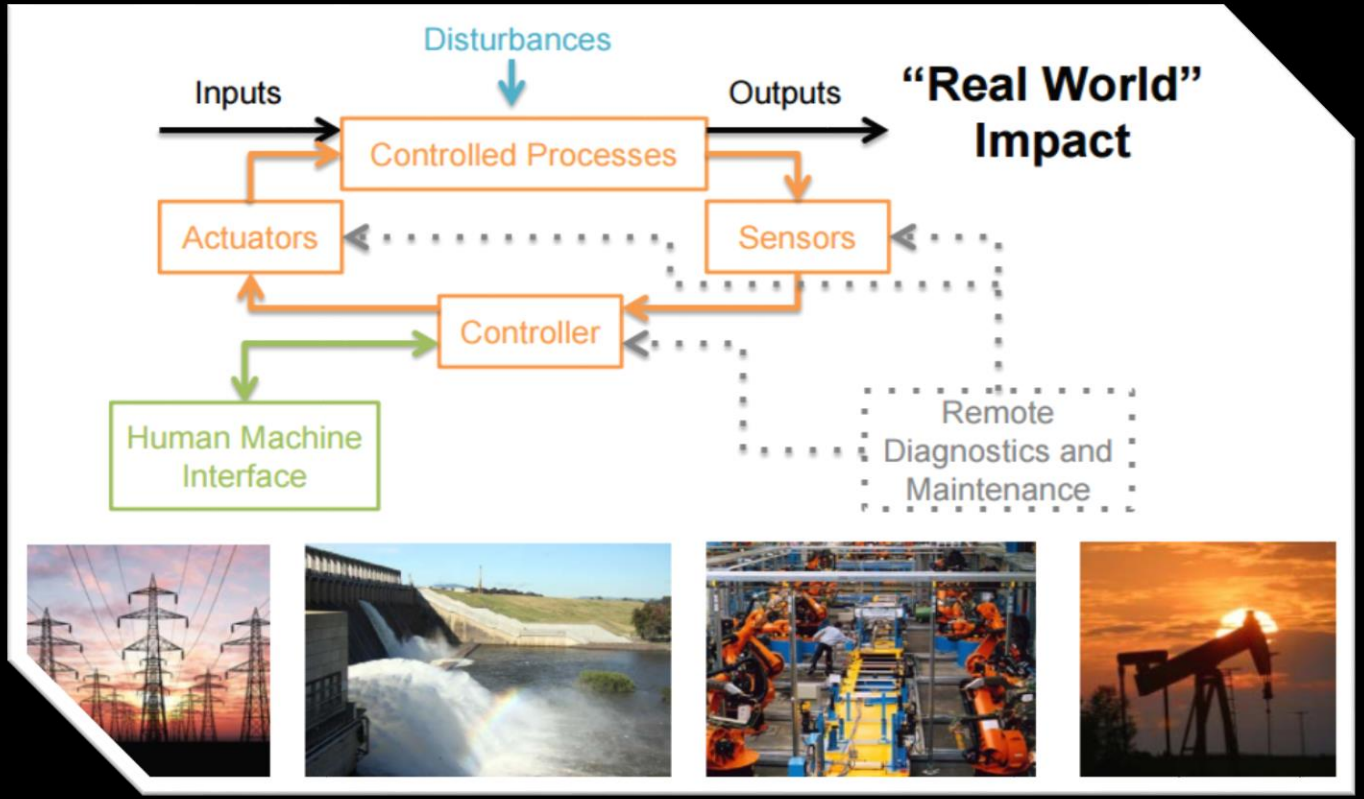
ICS Overview



SCADA Levels



Industrial Control Systems Overview



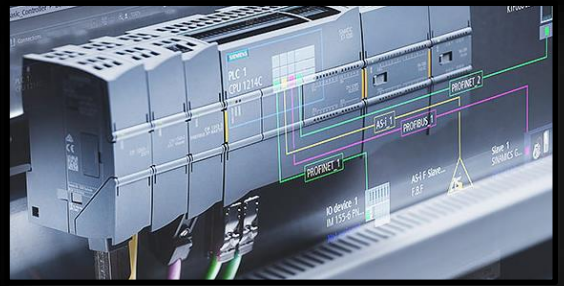
PLC—Programmable Logic Controller

What is a PLC?

PLC implements logic control functions by means of a program

A digitally operating electronic apparatus which uses a programming memory for the internal storage of instructions for implementing specific functions such as logic, sequencing, timing, counting and arithmetic to control through digital or analog modules, various types of machines or process.

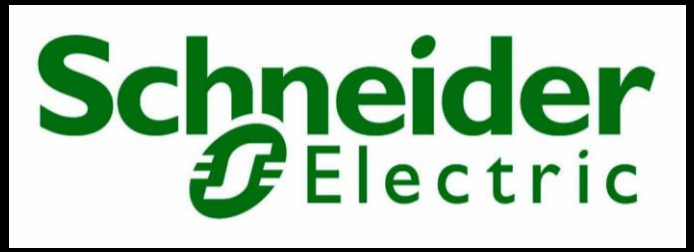
Definition according to NEMA standard ICS3-1978



PLC Vendors

Allen-Bradley

OMRON

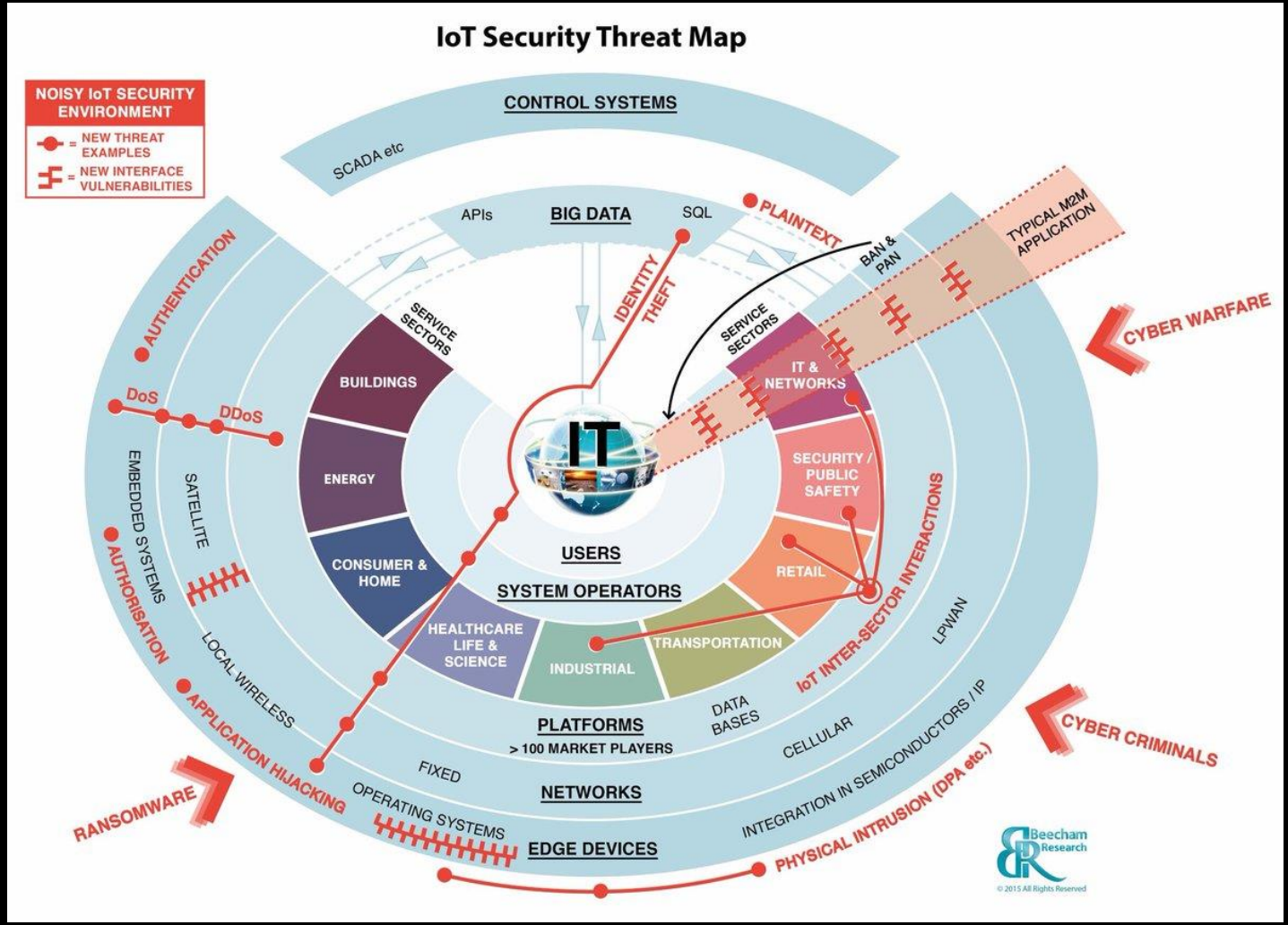


SIEMENS

Rockwell
Automation

Overview

Photo Credit:
Beecham Research
http://www.beechamresearch.com/download.aspx?id=43



Face reality as it is, not as it was or as you wish it to be
- Jack Welch (a favorite quote of mine obviously)

Reality: There are many security issues raised by a connected world

On that note …

Intermission

(a reminder for me to shut up)

Part2:

What you can do about it

But first…

The “Egg Drop”

Not that kind…

Here we go…

Split into groups of three and come up with a way to save an egg from breaking when dropped from a 7ft+ height.

You may use any materials on the table, but you are limited to 15 total items (4inches of tape = 1 item) – Choose Wisely.
You have 20 minutes – You get two eggs
(be careful with them during testing)

Some Takeaways:

Everyone has their own ideas for how to solve a problem

Working on a team requires collective vision and understanding

Development is iterative

Time and material resources are a big constraint

The thing you are trying to protect – needs to be well understood

Building software (e.g. web apps) isn't that different

We'll talk more about design and the benefits of software architecture for helping solve design problems next time

Back to…Part2:

What you ~~can~~ will do about it

Facing it:

Follow good coding practices, limit exposures, use good software engineering principles, pen test, identify mitigations,

Use what you've learned about in previous classes and what you will learn/reinforce and apply in here

I want to just spend the rest of class giving you a roadmap for the rest of the semester

Questions?

Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics

mlhale@unomaha.edu

Twitter: @mlhale_