Building a fortress in a greenfield
My Research & Test Driven Development
SA: Guest Lecture

Dr. Hale
University of Nebraska at Omaha

Today's topics:

- A bit about me
  - Phishing: Cybertrust
    - Figure out how people fall prey to phishing attacks
    - Identify trust and suspicion cues to help them not get phished
  - Wearables: SecuWear
    - Target domain-spanning wearable security issues
    - Build a security toolkit
- Software Testing and Test driven development
  - Unit / integration / acceptance testing
  - Think-test-build-test-repeat
  - QUnit Demo

Cybertrust

Investigating what trust factors influence decision making with suspicious content

Previous Work Supported by AFOSR, currently continuing
Multiple papers: ICWS2015, SPE2014, HICSS2014, SPE2013, International Journal of Services Computing
Targeted Interventions Derived from Biomarkers of Cyber Trust

Nebraska University Center for Information Assurance

Matthew Hale

Software Engineering and Architecture Team

Rose Gamble, John Hale, Michael Haney, Charles Walter, Jessica Lin

Acknowledgement

This material is based on research sponsored in part by the Air Force Office of Scientific Research (AFOSR), under award number FA9550-12-1-0457. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views expressed in this talk are those of the author and do not reflect the official policy or position of the Department of Defense or U.S. Government.

Acknowledgement x2

Beginning in Early 2013, I started working on an AFOSR grant called CyberTrust

(actually, Targeted Interventions Derived from Biomarkers of Cyber Trust)

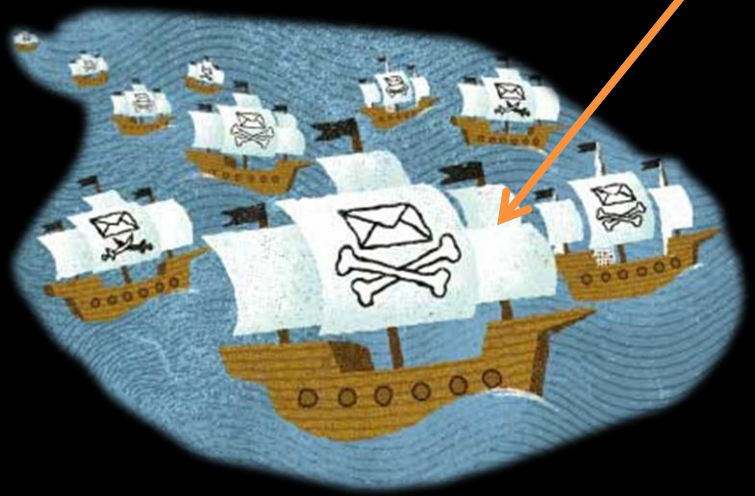
The CyberTrust grant was a multi-phase study that assesses what factors contribute to whether or not individuals trust content in online environments.

I’m working on a secure client-side web application that serves as a simulation platform for neuroscientists and psychologists to capture subject data about trust cues.

Why should you care?

Actual Facts

ARRRRRRR



156 Million

Phishing Emails

(Every Day)

Actual Facts

140 Million

Crash and burn at spam filters

ARRun it's the googles

But that means…

Actual Facts

CHARRRRRRRGE

16 Million

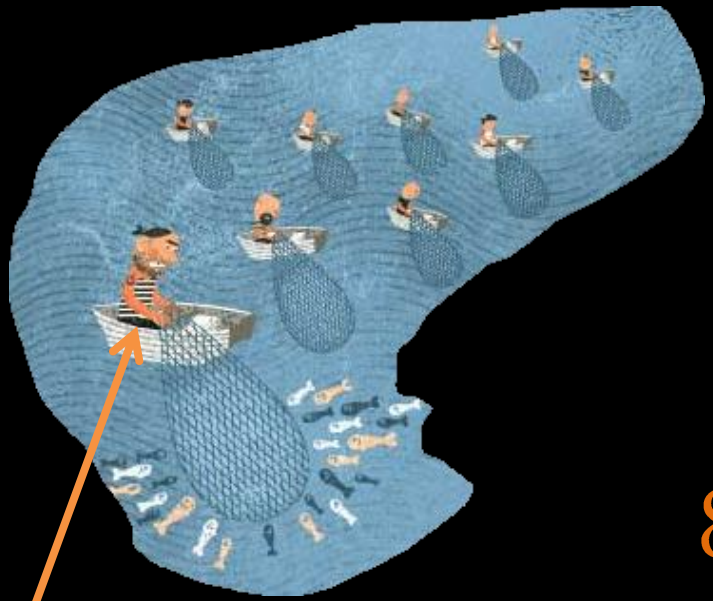
Make it through Filters

and…

8 Million

are actually opened

Actual Facts



800,000 (10%)

Links are clicked

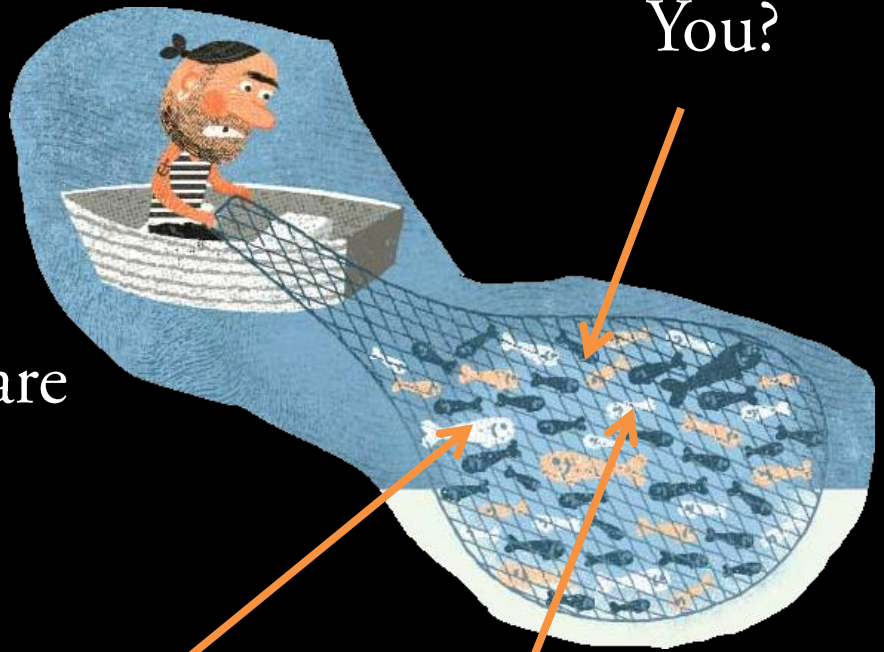
I have you now

Actual Facts

80,000 (10%)

Fall for a scam and/or share their personal info.

Increasing complexity, i.e. spear phishing or whale phishing…



Awesome Pirate graphics courtesy Canadian PSA:
http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx

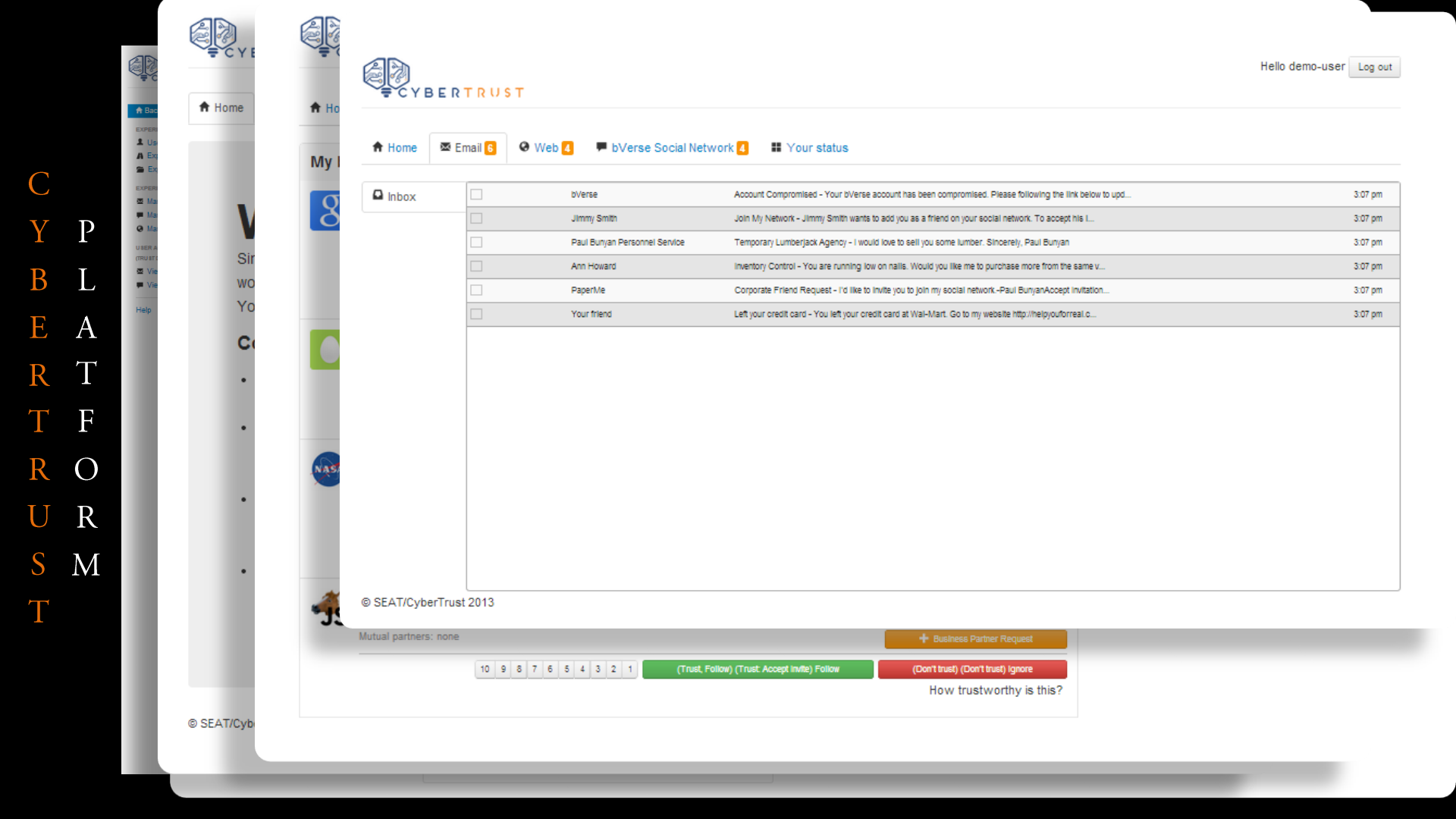
Phishing affects us all and
drains many billions of dollars annually from world economies

Clearly need more than spam filters…

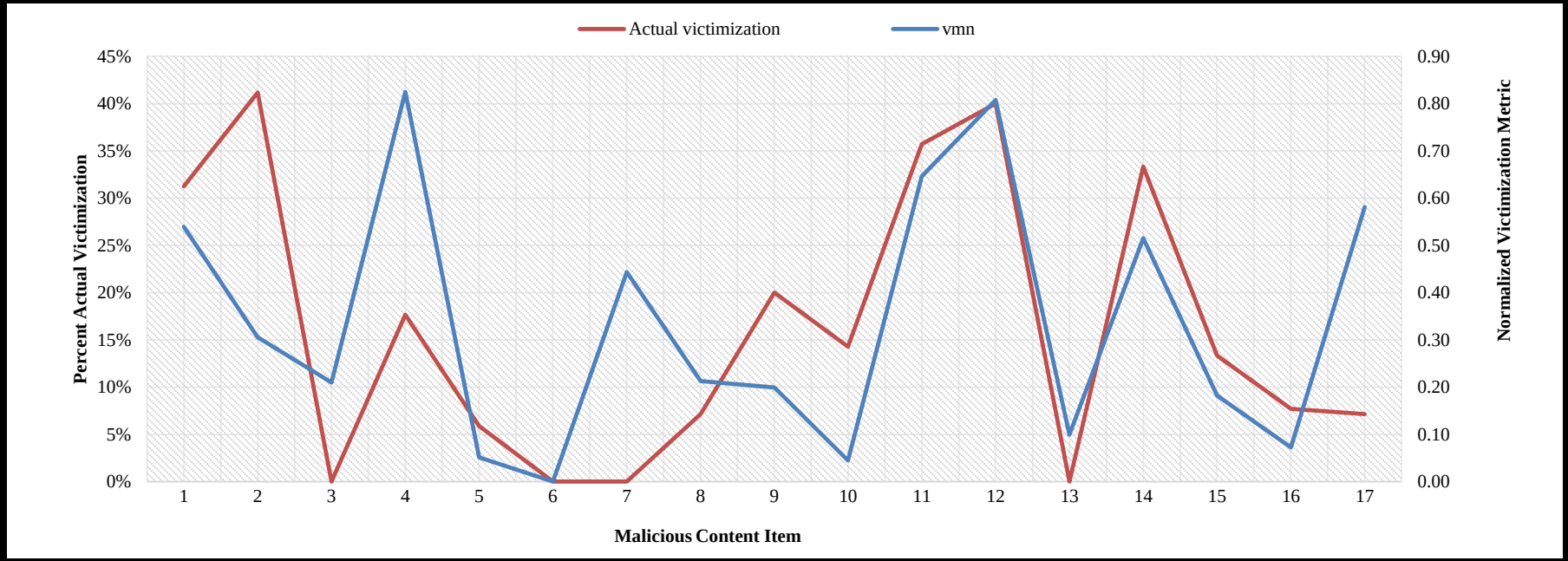
Enter the CyberPhishing
Simulation Platform

Core Idea

Identify user awareness gaps
Train them to recognize suspicious content
Prevent victimization


CYBERTRUST PLATFORM
CYBERTRUST
Hello demo-user
Log out
Home
Email 6
Web 4
bVerse Social Network 4
Your status
Inbox
bVerse
Account Compromised - Your bVerse account has been compromised. Please following the link below to upd...
3:07 pm
Jimmy Smith
Join My Network - Jimmy Smith wants to add you as a friend on your social network. To accept his i...
3:07 pm
Paul Bunyan Personnel Service
Temporary Lumberjack Agency - I would love to sell you some lumber. Sincerely, Paul Bunyan
3:07 pm
Ann Howard
Inventory Control - You are running low on nails. Would you like me to purchase more from the same v...
3:07 pm
PaperMe
Corporate Friend Request - I'd like to invite you to join my social network.-Paul BunyanAccept invitation...
3:07 pm
Your friend
Left your credit card - You left your credit card at Wal-Mart. Go to my website http://helpyourreal.c...
3:07 pm
© SEAT/CyberTrust 2013
Mutual partners: none
Business Partner Request
10 9 8 7 6 5 4 3 2 1
(Trust, Follow) (Trust: Accept invite) Follow
(Don't trust) (Don't trust) ignore
How trustworthy is this?

Results: predictor vs actual victimization



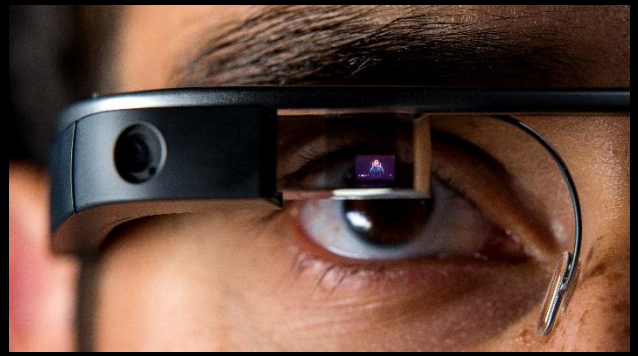
Wearables

SecuWear: An open source, multi-component hardware/software platform for exploring wearable security

Paper presented at MS2015
Project funded by NRI

Why should you care?

fitbit surge™



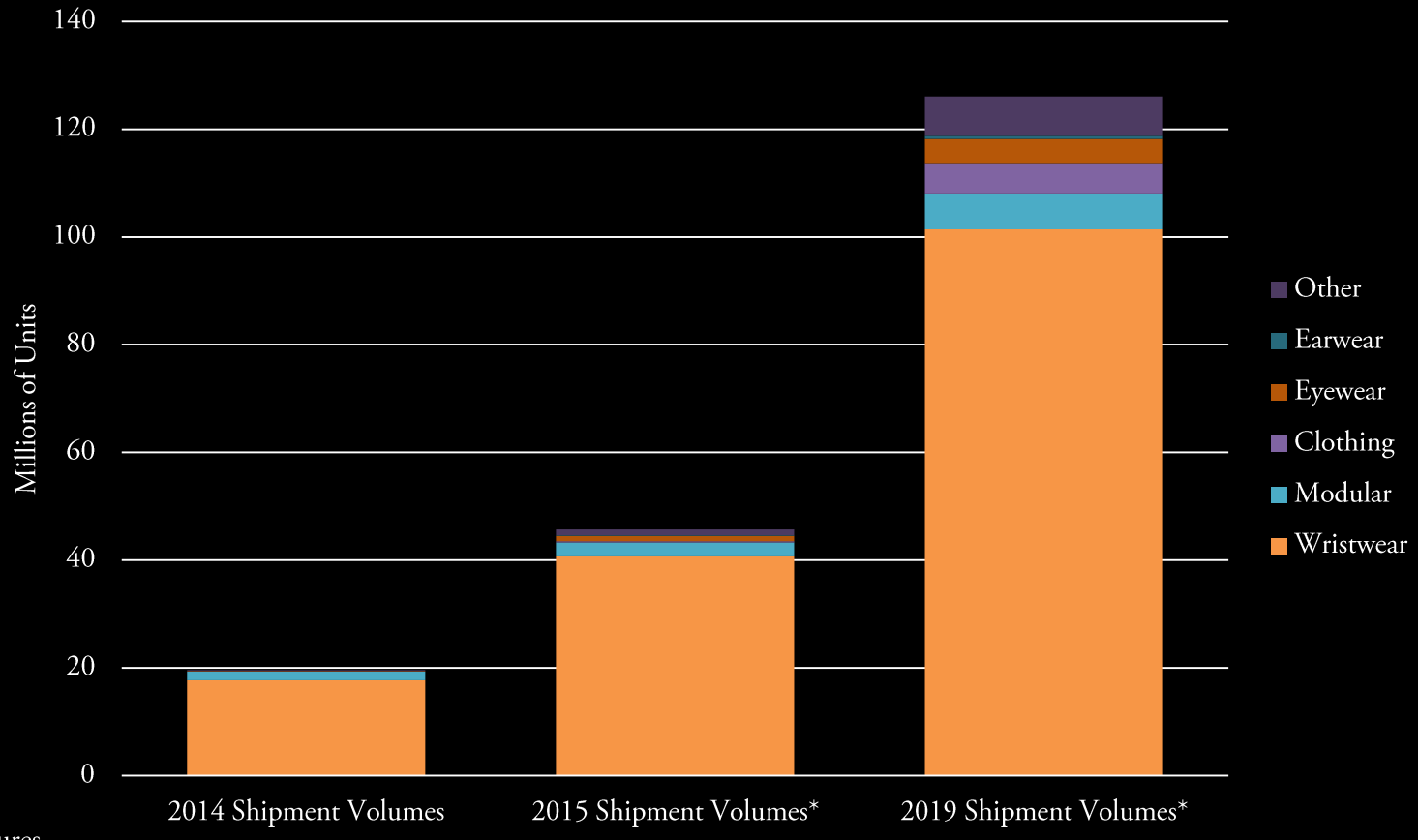
GLASS

A big (emerging) market…

NIKEFUEL

UP
by JAWBONE™

Wearable Units Shipped



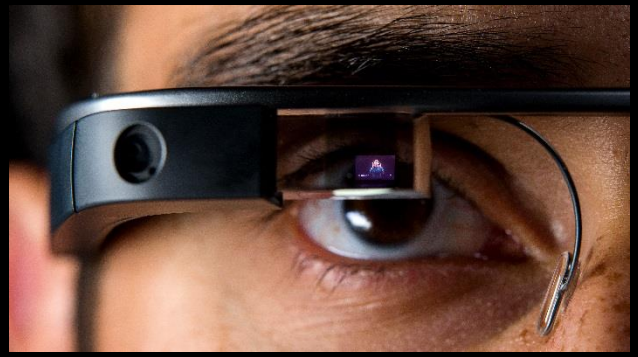
* Forecasted figures

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



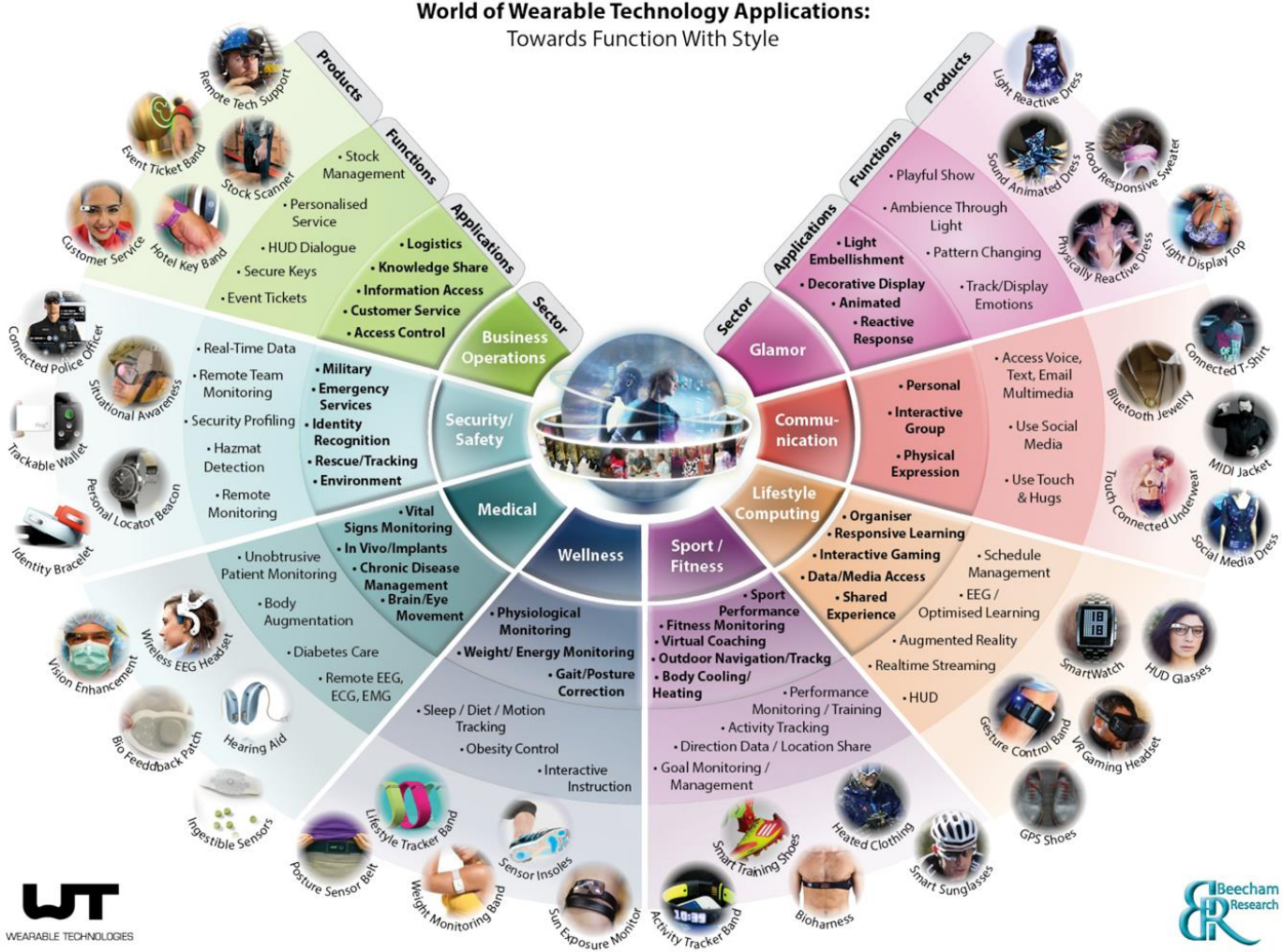
GLASS

…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

They use:

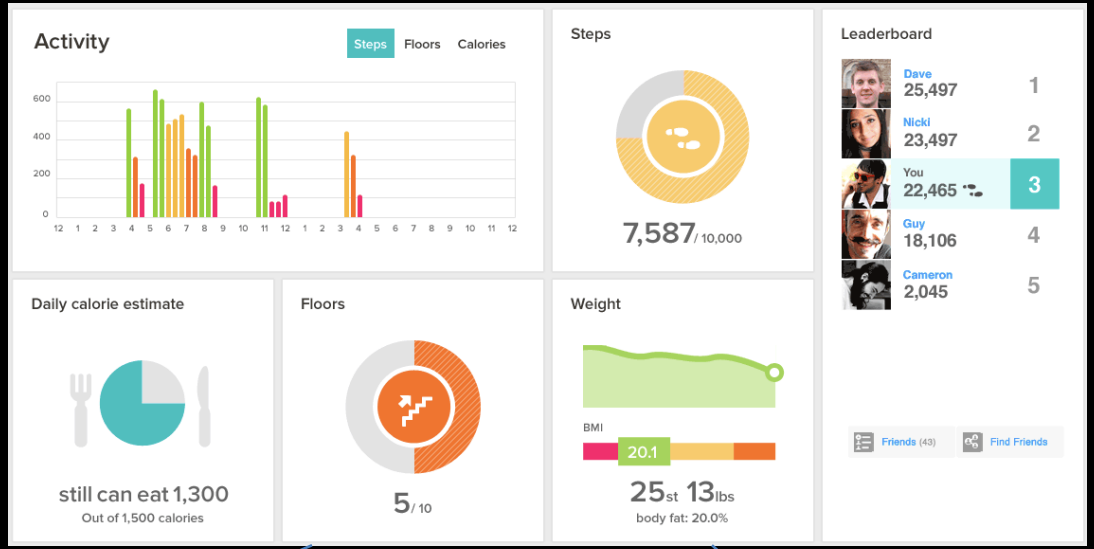
Wearables and Big Data are about better knowing the user*

*in whatever application

Mostly companies are interested in

-> Advertising and revenue generation

The possibilities:



Big data is also important for other sectors

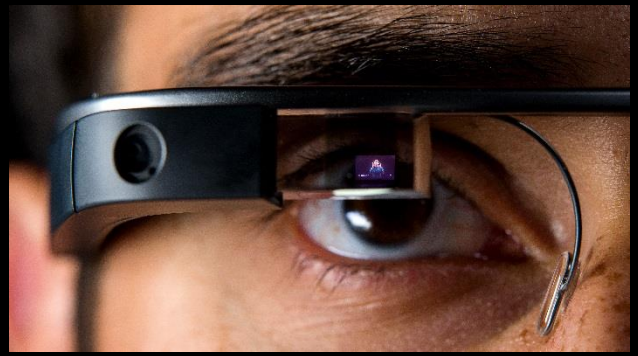
Medical -> patient well being & diagnosis

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

Security Analysis of Wearable Fitness Devices (Fitbit)

Britt Cyr, Webb Horn, Daniela Miao, Michael Specter
Massachusetts Institute of Technology
achusetts, U.S.A.
, dmiao@mit.edu, specter@mit.edu

How I hacked my smart bracelet

By Roman Unuchek on March 26, 2015. 11:00 am

Hackers are coming for your smartwatch

CALE GUTHRIE WEISSMAN

APR. 13, 2015, 1:35 PM | 759

Nike+ FuelBand SE BLE Protocol Reversed

Simone Margaritelli

29 Jan 2015 in REVERSING NIKE NIKE+ FUELBAND SE FUELBAND NIKE FUELBAND HACKING BLE BLUETOOTH LOW ENERGY PROTOCOL

Anonymity is the internet's next big battleground

Jon Card

Monday 22 June 2015 07.00 EDT

about how their data is being used, with major
rs, marketers and the entire internet industry

Bluetooth: With Low Energy comes Low Security

Mike Ryan
iSEC Partners

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

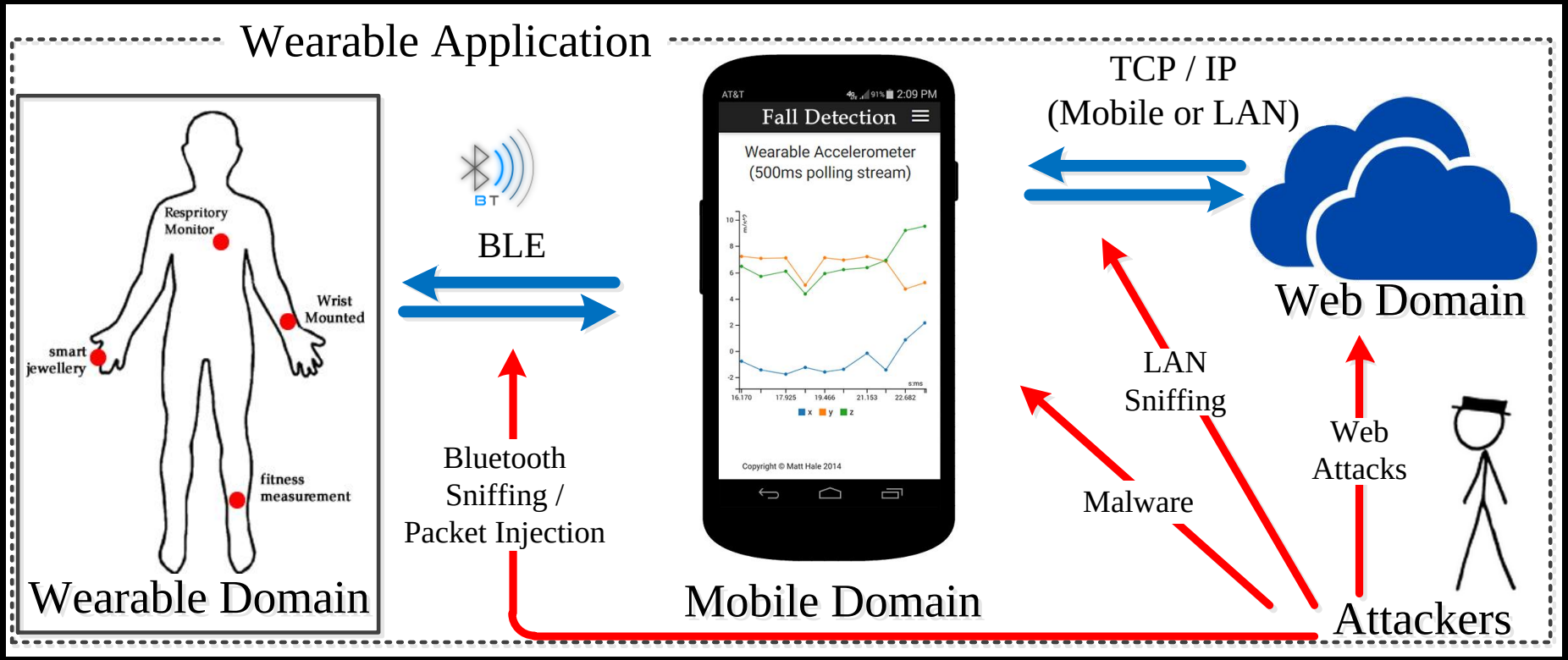
Insecure Wi-Fi or 4G
Lack of API Security (HTTPS/CORS/CSRF)

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



My Contribution: SecuWear

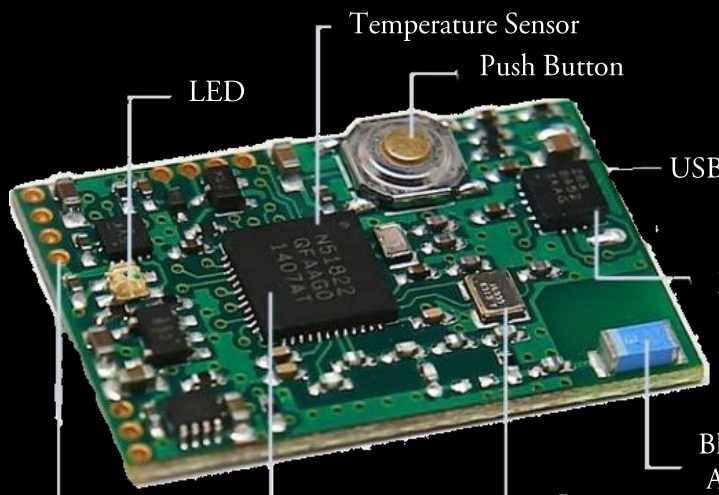
Basic Idea: Empower researchers to study wearable security issues

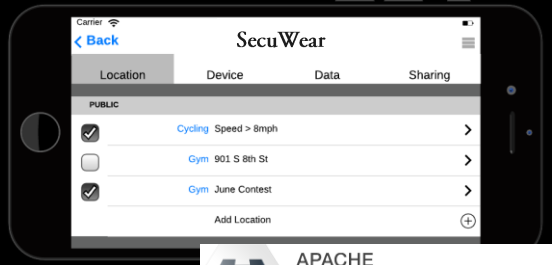
Sponsored by NRI grant: **Identifying, assessing, and mitigating wearable security issues in the internet of things**

SecuWear: Made with open source

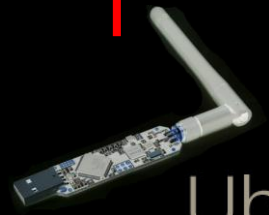
mbientlab

MetaWear



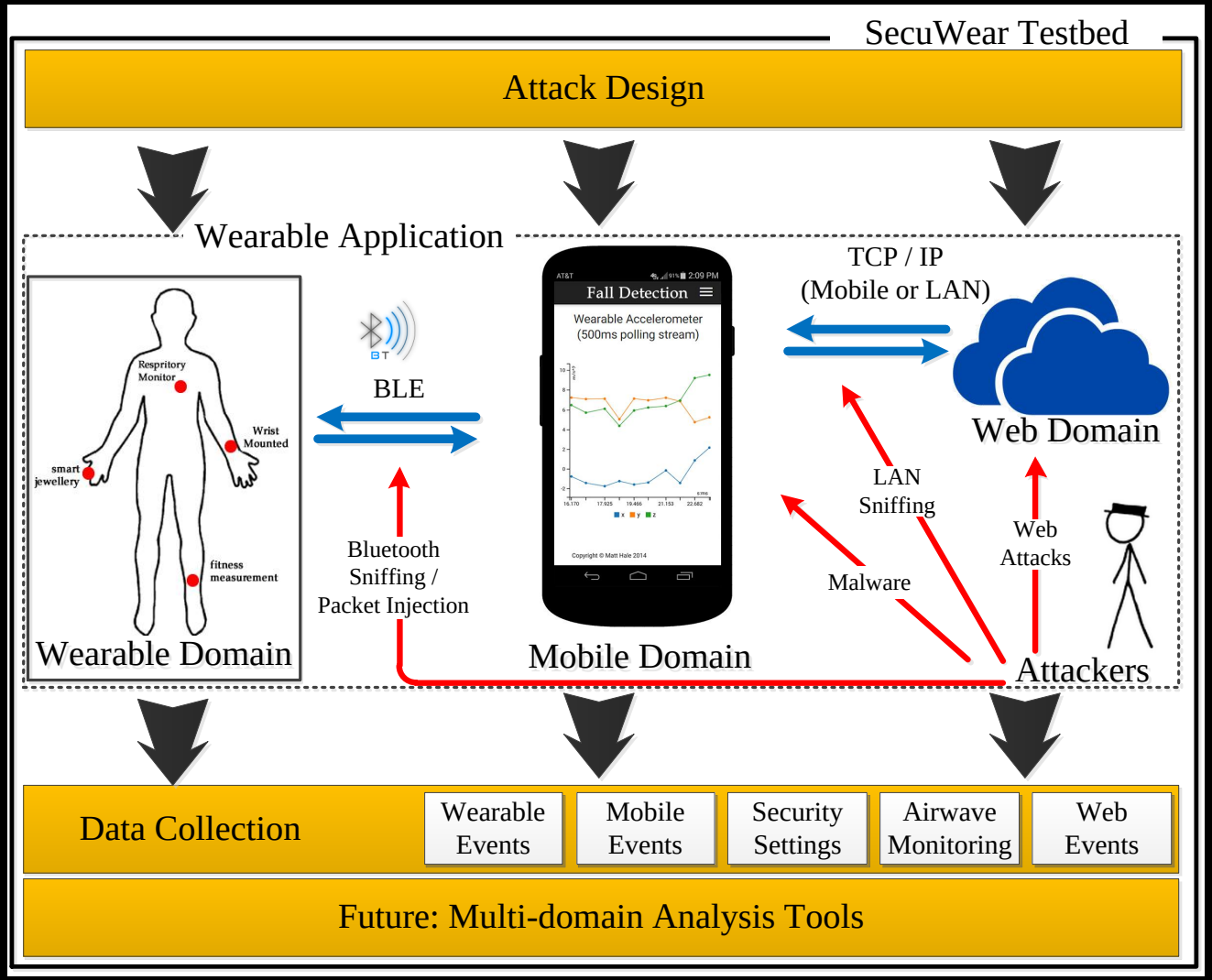


APACHE CORDOVA™



Ubertooth One

Designing and Exploring Attack Vectors



Some classes I teach that you may be interested in the future

Secure Web Development: (graduate class) IASC8470
Secure Mobile Development: (graduate class) IASC8080
Information Security Policy: IASC3600
Undergrad capstone: IASC 4580

Interested in Joining My lab?

http://faculty.ist.unomaha.edu/mhale/

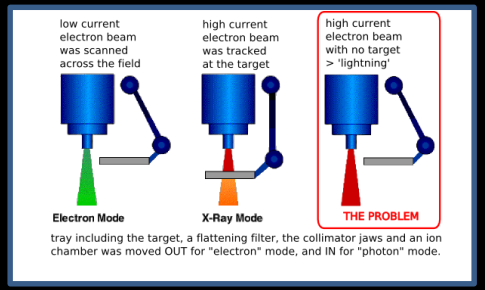
Today's Meat and potatoes: Test-driven Development

Some Material from Bernd Bruegge and Allen Dutoit Object-Oriented SE: Using UML, Patterns, and Java (because their slides are hilarious)

Famous Problems

- F-16 : crossing equator using autopilot
  - Result: plane flipped over
  - Reason?
    - Reuse of autopilot software

- The Therac-25 accidents (1985-1987), one of the most serious non-military computer-related failure in terms of human life (at least five died)
  - Reason: Bad event handling in the GUI
- NASA Mars Climate Orbiter destroyed due to incorrect orbit insertion (September 23, 1999)
  - Reason: Unit conversion problem.



Terminology

- Failure: Any deviation of the observed behavior from the specified behavior
- Erroneous state (error): The system is in a state such that further processing by the system can lead to a failure
- Fault: The mechanical or algorithmic cause of an error (“bug”)
- Validation/testing: Activity of checking for deviations between the observed behavior of a system and its specification.

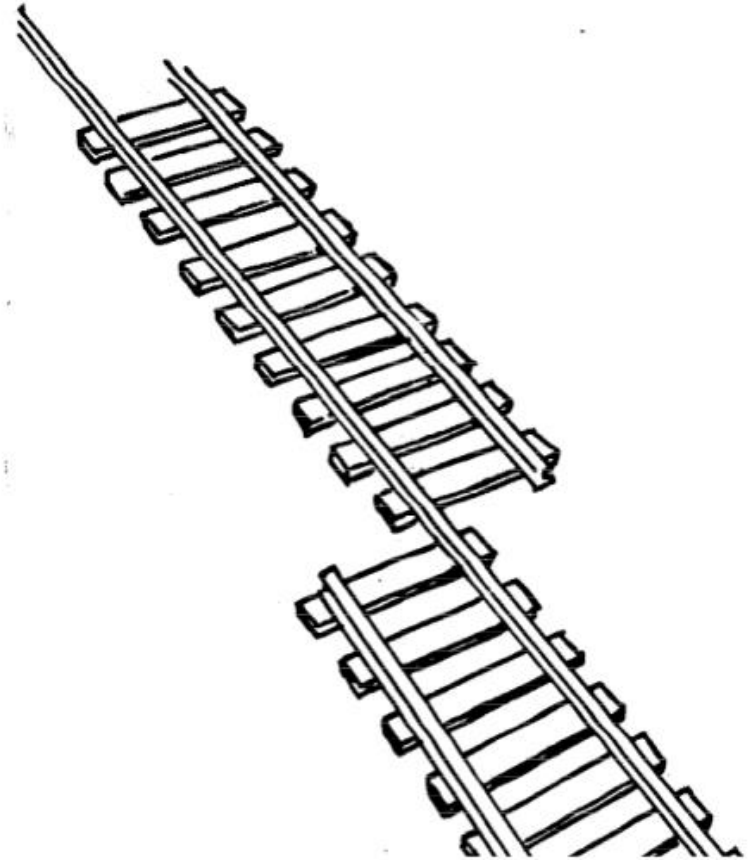
What is this?

A failure?

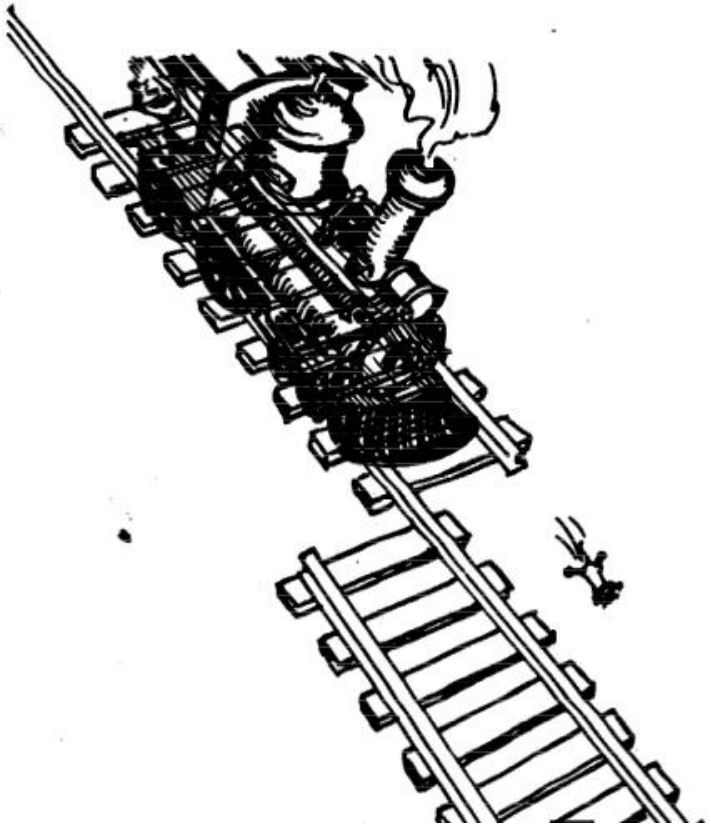
An error?

A fault?

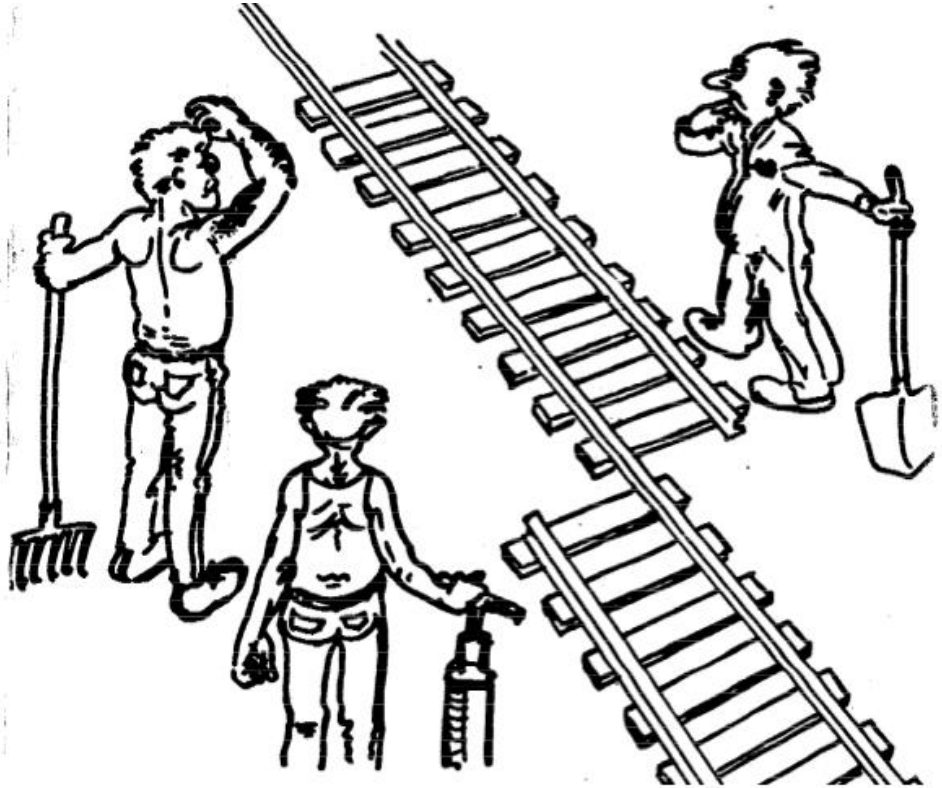
We need to describe specified and desired behavior first!



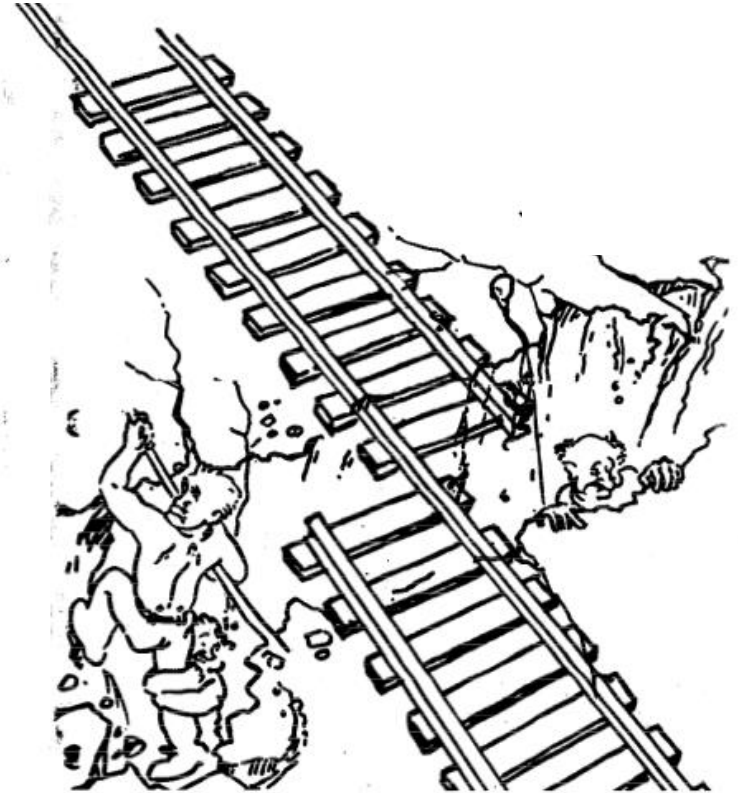
Erroneous State ("Error")



Algorithmic Fault



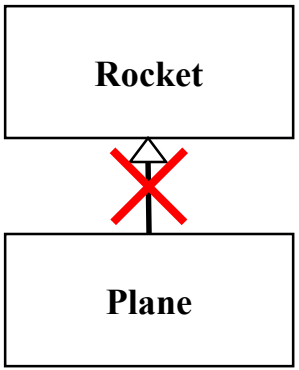
Mechanical Fault



F-16 Bug

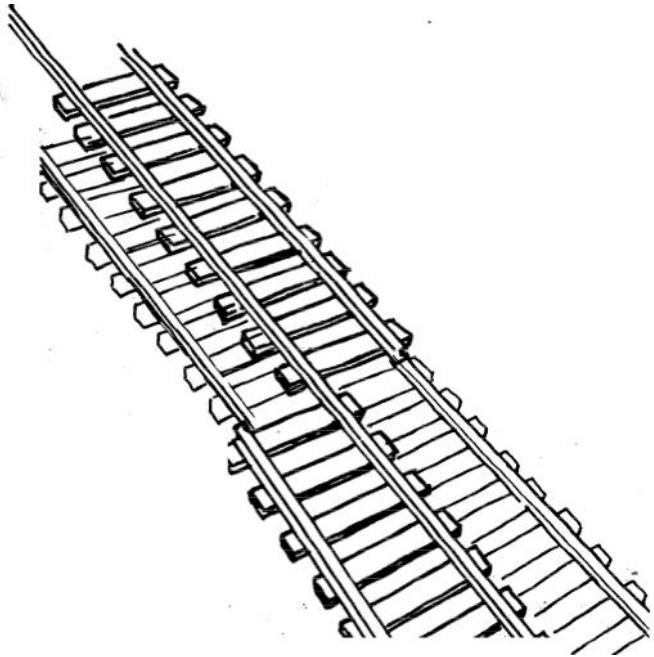


- What is the failure?
- What is the error?
- What is the fault?
  - Bad use of implementation inheritance
  - A Plane is **not** a rocket.

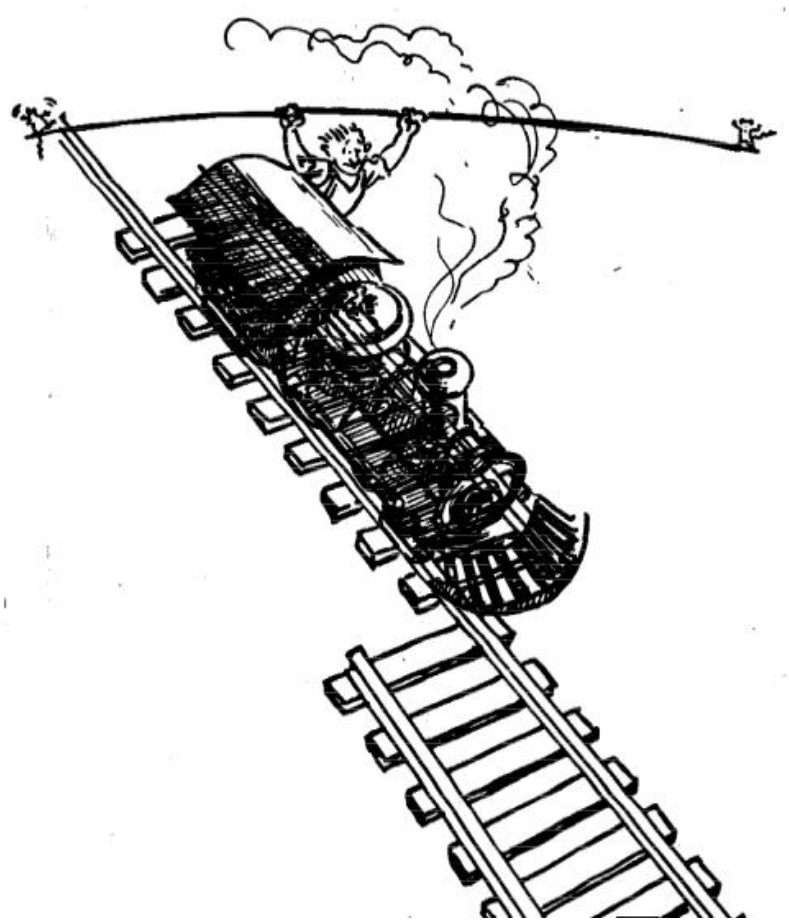


How do we deal with Errors, Failures and Faults?

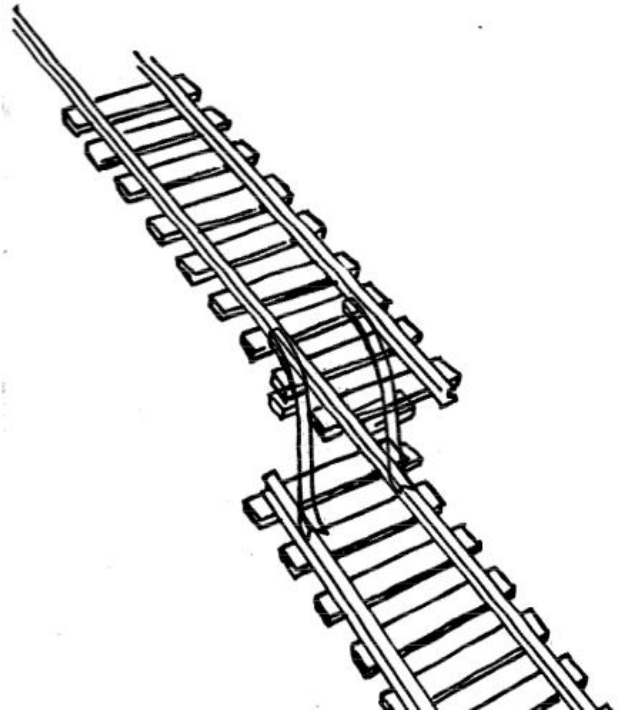
Modular Redundancy



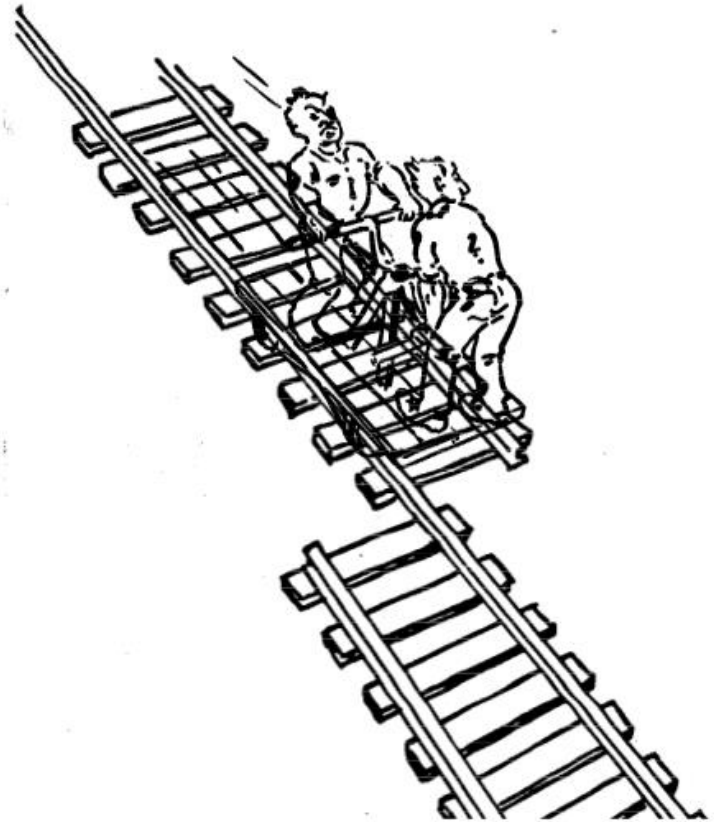
Declaring the Bug as a Feature



Patching



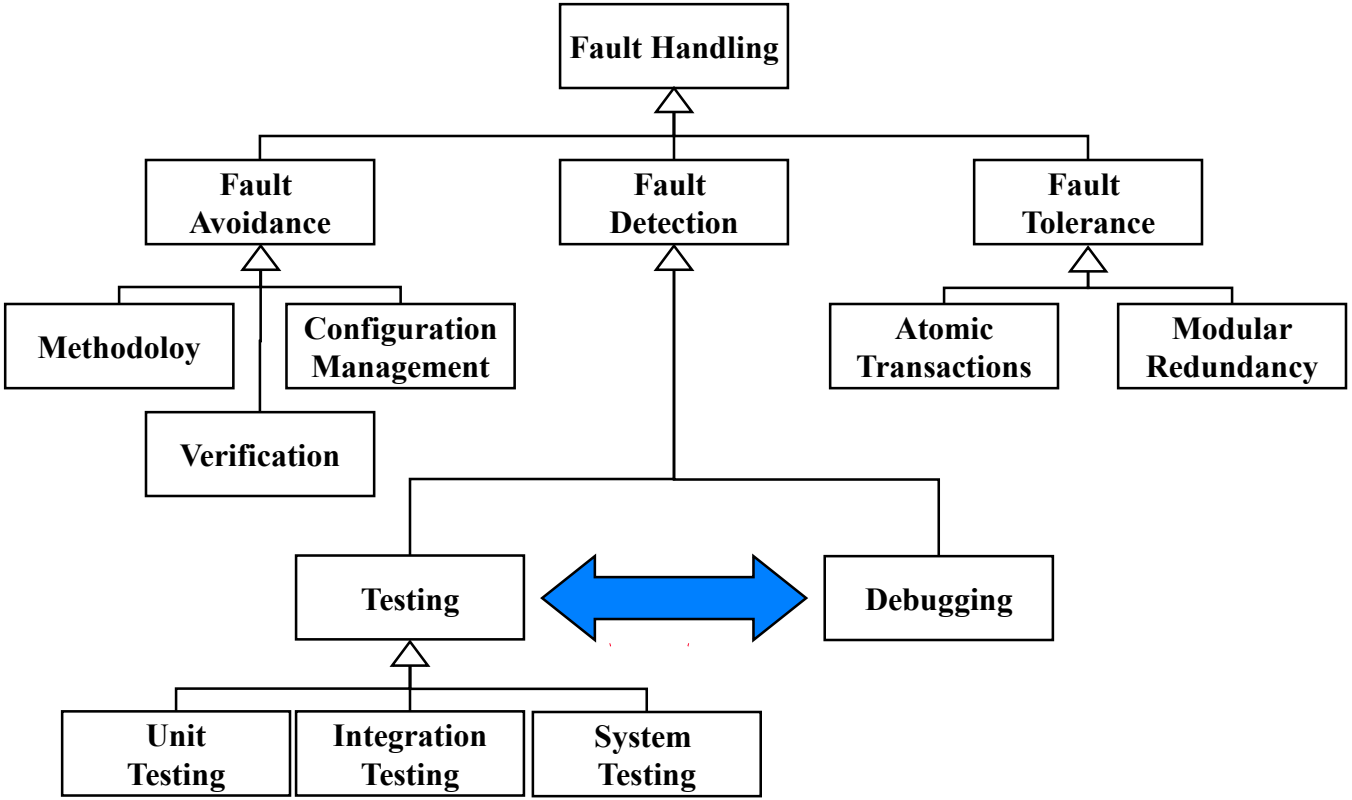
Testing



Another View on How to Deal with Faults

- Fault avoidance
  - Use methodology to reduce complexity
  - Use configuration management to prevent inconsistency
  - Apply verification to prevent algorithmic faults
  - Use Reviews
- Fault detection
  - Testing: Activity to provoke failures in a planned way
  - Debugging: Find and remove the cause (Faults) of an observed failure
  - Monitoring: Deliver information about state => Used during debugging
- Fault tolerance
  - Exception handling
  - Modular redundancy.

Taxonomy for Fault Handling Techniques

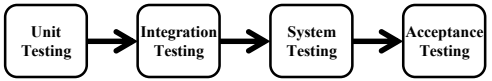


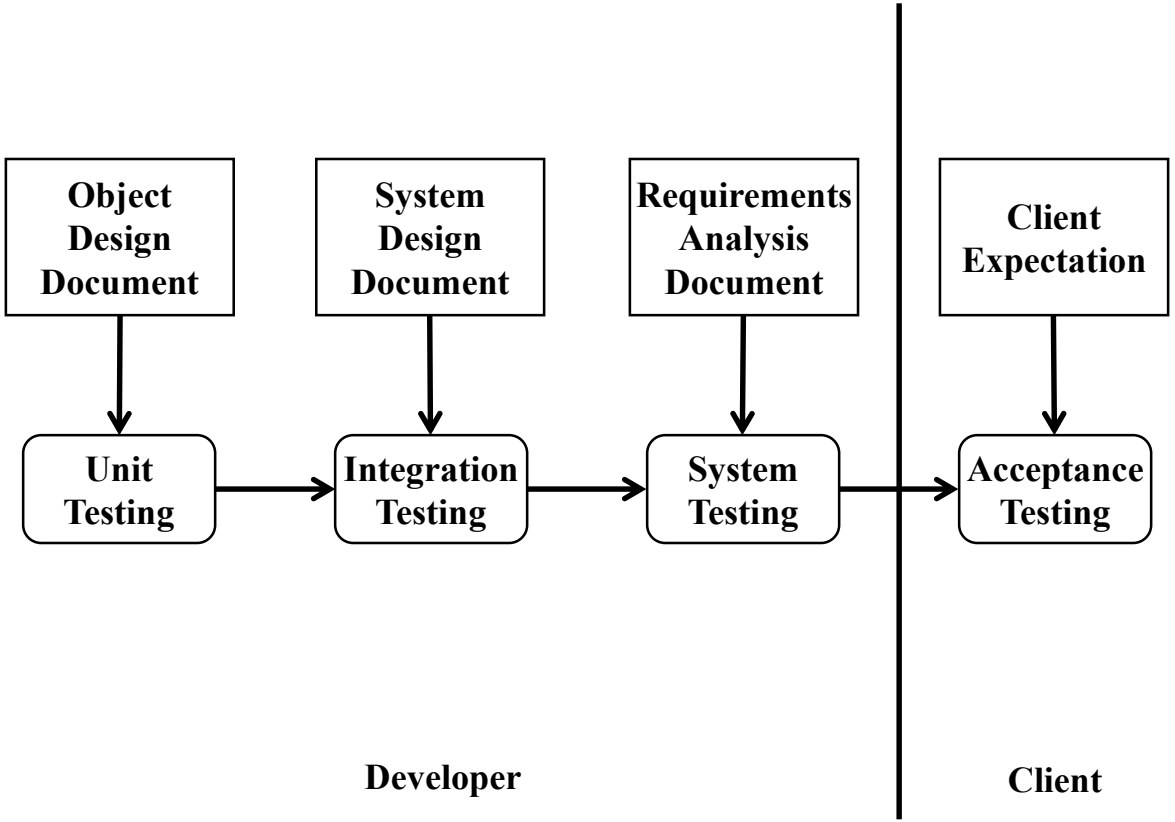
Observations

- It is impossible to completely test any nontrivial module or system
  - Practical limitations: Complete testing is prohibitive in time and cost
  - Theoretical limitations: e.g. Halting problem
- “Testing can only show the presence of bugs, not their absence” (Dijkstra).
- Testing is not for free

=> Define your goals and priorities

Testing Activities





Types of Testing

Acceptance Test – A measure that ensures that a feature meets functional demands. Usually acceptance tests are tied to user stories or use cases.

Unit test – A smaller test that ensures isolated chunks of functionality (known as units) are functional and operating as expected.

Integration tests – Between unit tests and acceptance tests. Focuses on ensuring that different units function together (said to be integrable).

UNIT Testing

Can be done manually or programmatically – MUCH easier to do the latter – since your components may change and manually testing each time is onerous

Basically you boil down exactly what a feature or component should be doing and you logically state these criteria. Each time you modify the feature/component you run the unit tests to see if they pass. When they all pass you move on to integration tests.

Integration Testing

Can be done manually or programmatically – MUCH easier to do the latter – since your components may change and manually testing each time is onerous

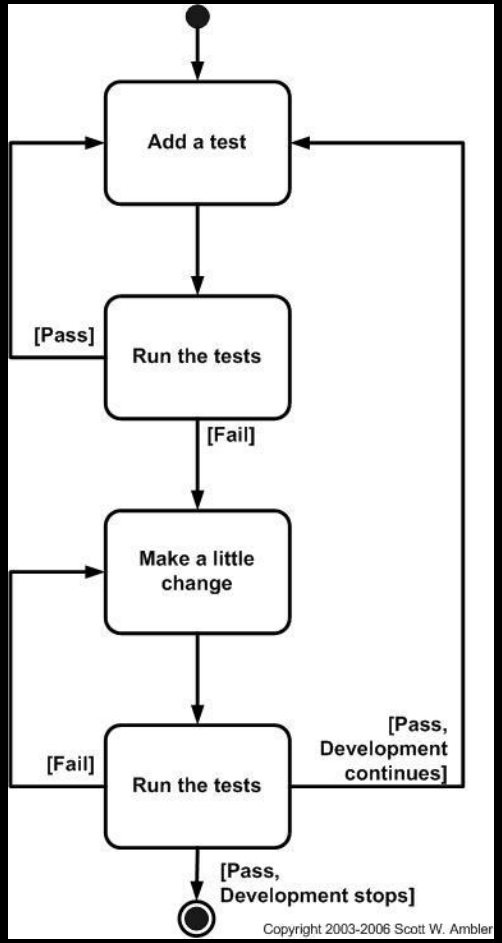
Here you define how different components need to interact and state those constraints logically. When all of the integration tests work – it means you move on to acceptance tests and make sure the collected components satisfy the original goals in the user story or use cases.

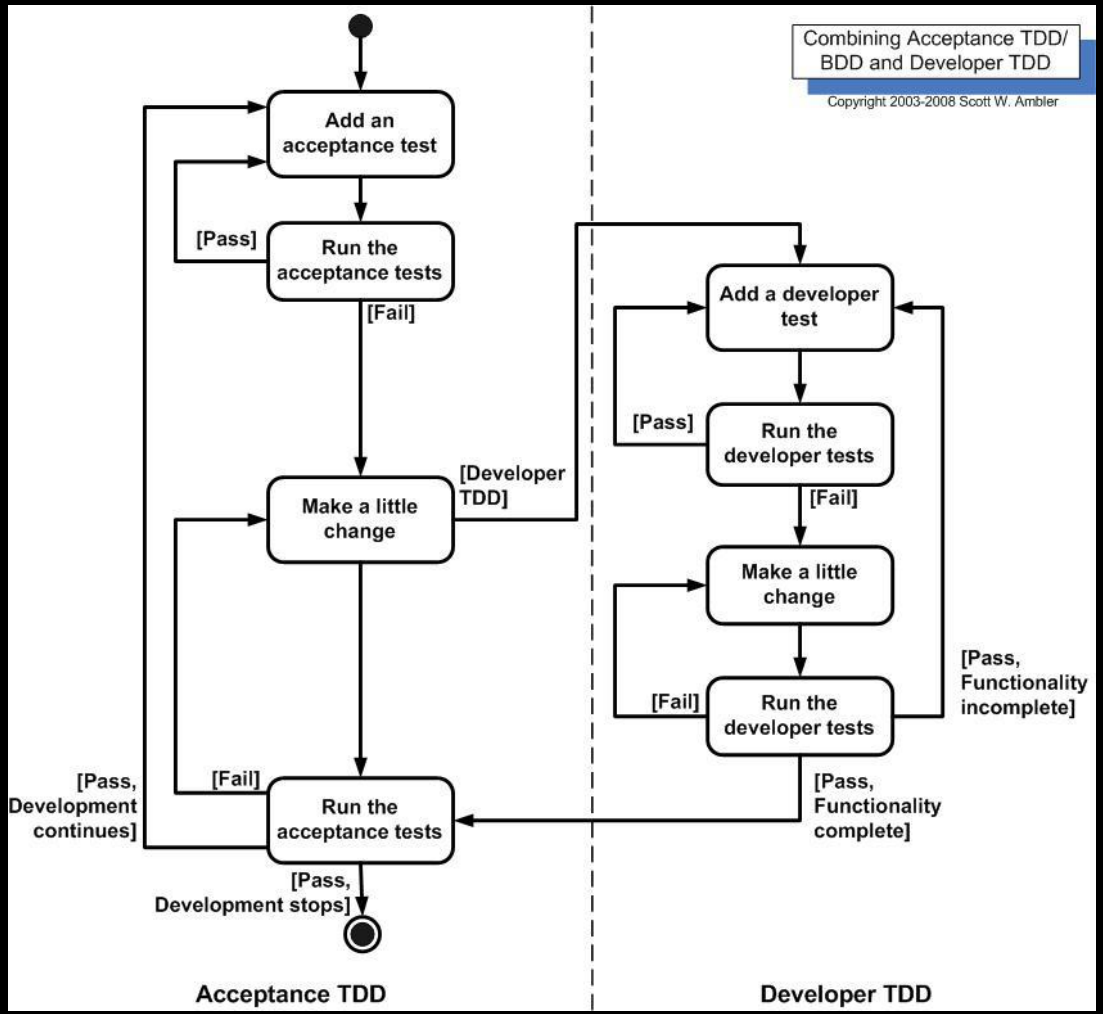
Acceptance Testing

Can be done manually or programmatically – often the former, but can repeat easier with the latter.

You basically define the set of all acceptance tests related to your user stories and use cases and – when you demonstrate the app passes all of the tests you are done!

Test Driven Development Core Philosophy




Combining Acceptance TDD/ BDD and Developer TDD
Copyright 2003-2008 Scott W. Ambler
Add an acceptance test
[Pass]
Run the acceptance tests
[Fail]
Make a little change
[Developer TDD]
[Pass, Development continues]
[Fail]
Run the acceptance tests
[Pass, Development stops]
Add a developer test
[Pass]
Run the developer tests
[Fail]
Make a little change
[Fail]
Run the developer tests
[Pass, Functionality incomplete]
[Pass, Functionality complete]
Acceptance TDD
Developer TDD

QUnit DEMO (Javascript)
http://benalman.com/talks/unit-testing-qunit.html

Questions?

Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics

mlhale@unomaha.edu

Twitter: @mlhale_