RSAC Studio

Connect to Protect

They’ll Get You On The Go

Kurt Baumgartner

GReAT - Principal Security Researcher
Kaspersky Lab

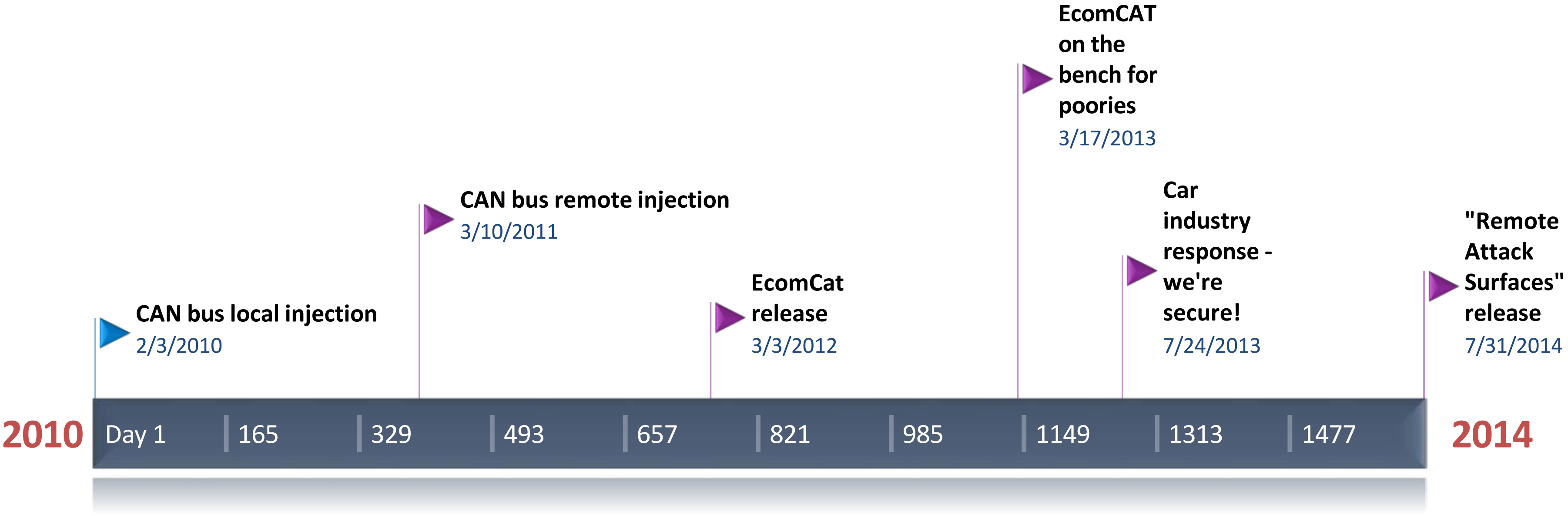
@k_sec

#RSAC

Transportation Security at 40k ft

Transportation Security at 40k ft

Automotive Research and Reactions



CAN bus local injection
2/3/2010

CAN bus remote injection
3/10/2011

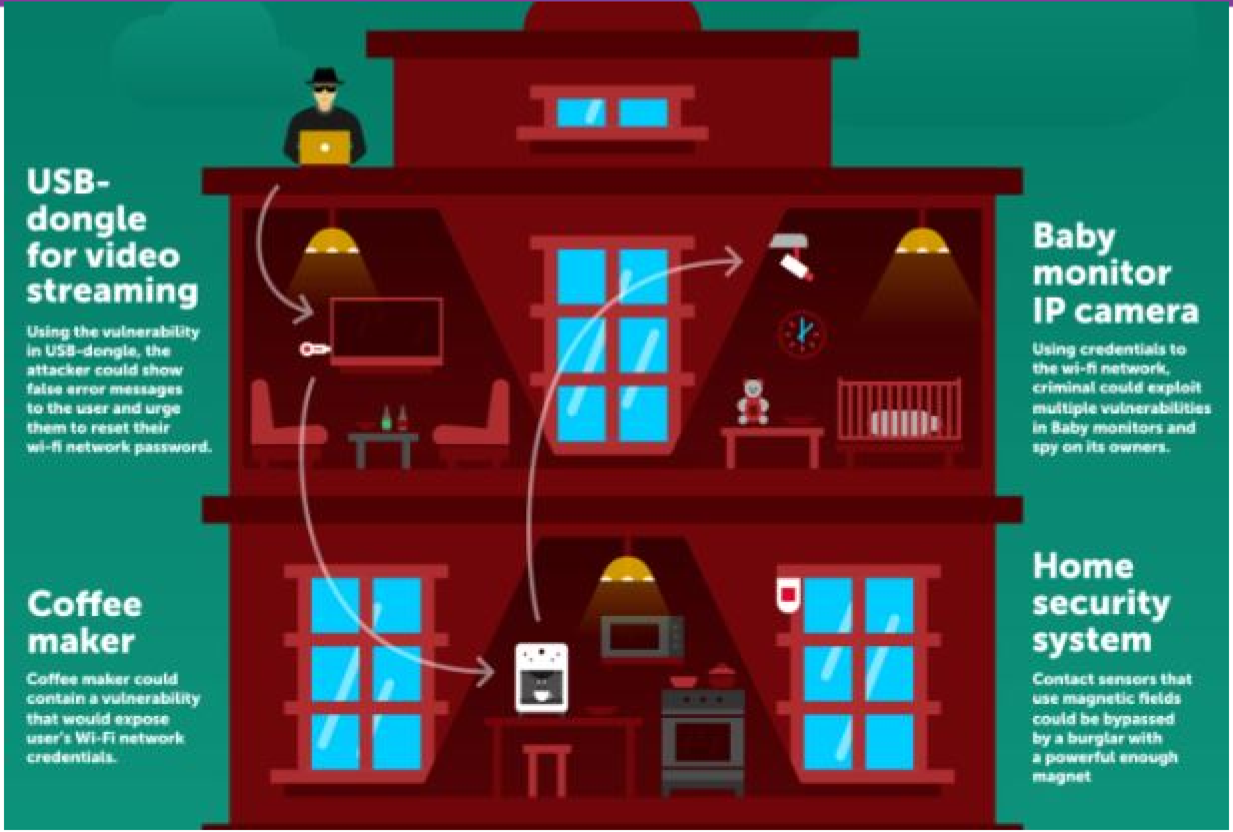
EcomCat release
3/3/2012

EcomCAT on the bench for poories
3/17/2013

Car industry response - we're secure!
7/24/2013

"Remote Attack Surfaces" release
7/31/2014

Kaspersky Lab and IoT Research



USB-dongle for video streaming

Using the vulnerability in USB-dongle, the attacker could show false error messages to the user and urge them to reset their wi-fi network password.

Baby monitor IP camera

Using credentials to the wi-fi network, criminal could exploit multiple vulnerabilities in Baby monitors and spy on its owners.

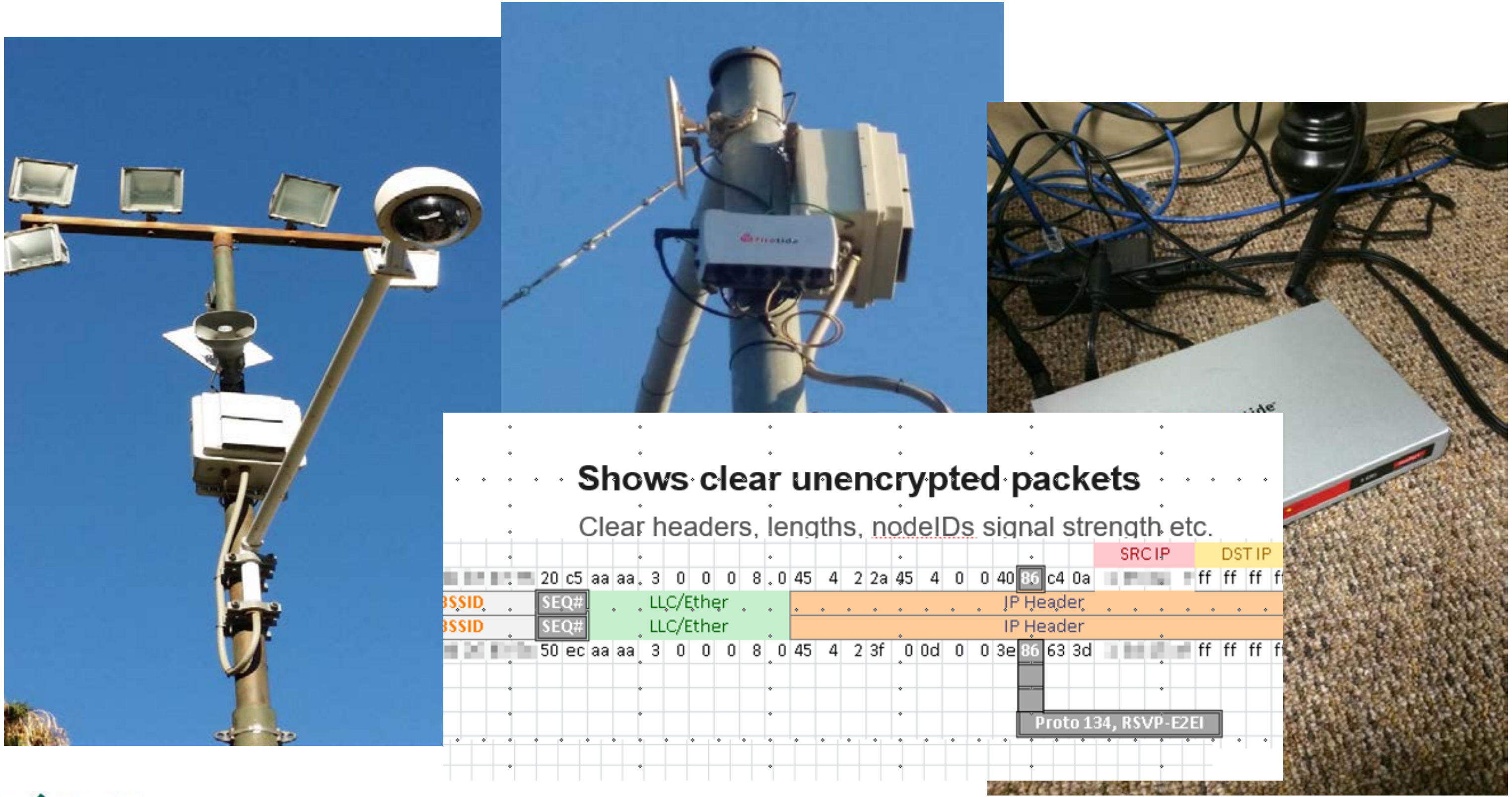
Coffee maker

Coffee maker could contain a vulnerability that would expose user's Wi-Fi network credentials.

Home security system

Contact sensors that use magnetic fields could be bypassed by a burglar with a powerful enough magnet

Kaspersky Lab and IoT Research



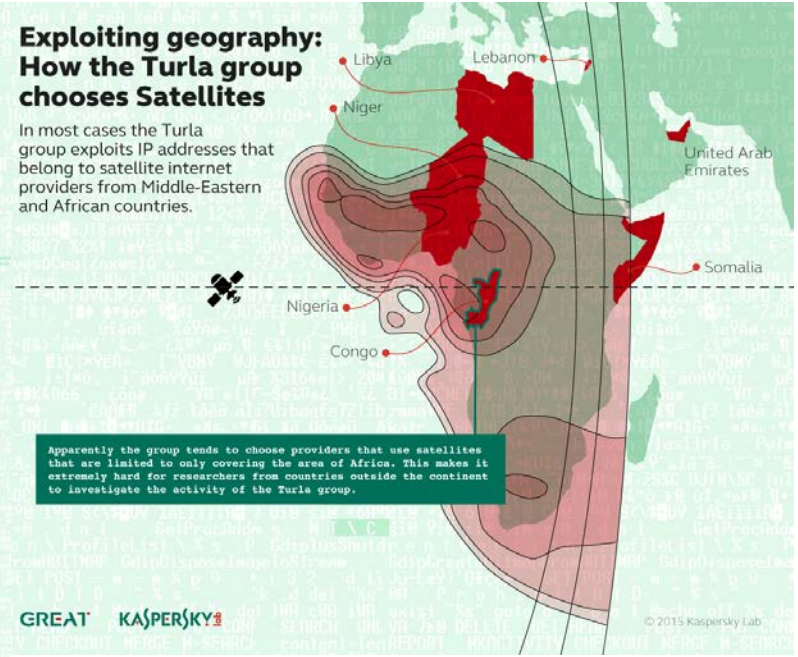
Shows clear unencrypted packets

Clear headers, lengths, nodeIDs signal strength etc.

```
                                                                           SRC IP       DST IP
[redacted] 20 c5 aa aa 3 0 0 0 8 0 45 4 2 2a 45 4 0 0 40 86 c4 0a [redacted] ff ff ff f
BSSID      SEQ#  LLC/Ether          IP Header
BSSID      SEQ#  LLC/Ether          IP Header
[redacted] 50 ec aa aa 3 0 0 0 8 0 45 4 2 3f  0 0d 0 0 3e 86 63 3d [redacted] ff ff ff f
                                                       Proto 134, RSVP-E2EI
```

Seen and Unseen

- Cybersecurity issues in transportation
  - Overt issues
  - Covert issues

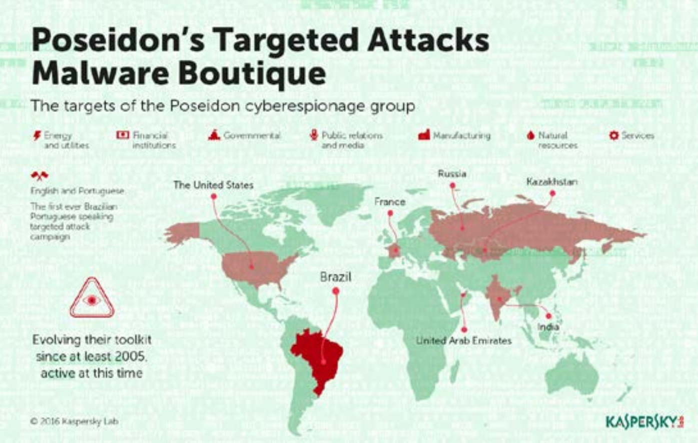


Exploiting geography: How the Turla group chooses Satellites

In most cases the Turla group exploits IP addresses that belong to satellite internet providers from Middle-Eastern and African countries.

Apparently the group tends to choose providers that use satellites that are limited to only covering the area of Africa. This makes it extremely hard for researchers from countries outside the continent to investigate the activity of the Turla group.

© 2015 Kaspersky Lab



Poseidon's Targeted Attacks Malware Boutique

The targets of the Poseidon cyberespionage group

English and Portuguese

The first ever Brazilian Portuguese speaking targeted attack campaign

Evolving their toolkit since at least 2005, active at this time

© 2016 Kaspersky Lab

IoT and Transport Orgs Operational Security

- Organizational transportation sector security incidents
  - 89% - external information security incident
  - 51% - data loss as a result of the external security incident
  - 71% - internal information security incident
  - 65% - data loss as a result of the internal security incident

Collaboration

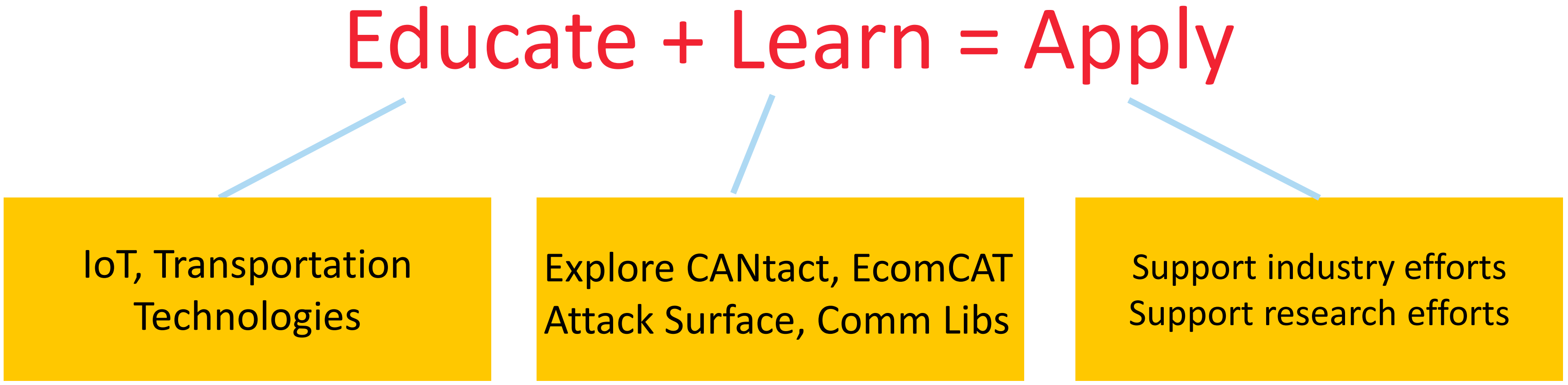
Cyber security for Smart Cities

An architecture model for public transport

Collaboration

- Major Tier 1 automotive vendor secure systems
- Shared IoT pen-test projects
- Prioritizing cyber-security in facility, system, and process design

Action



Educate + Learn = Apply

IoT, Transportation Technologies

Explore CANtact, EcomCAT Attack Surface, Comm Libs

Support industry efforts
Support research efforts

RSAC® Studio

Connect to Protect

They’ll Get You On The Go

Kurt Baumgartner

GReAT - Principal Security Researcher
Kaspersky Lab

@k_sec

RSAC Studio

Security Issues in Transportation: Need for Collaboration for Solutions

Joshua Corman

Founder

I am The Cavalry

#RSAC

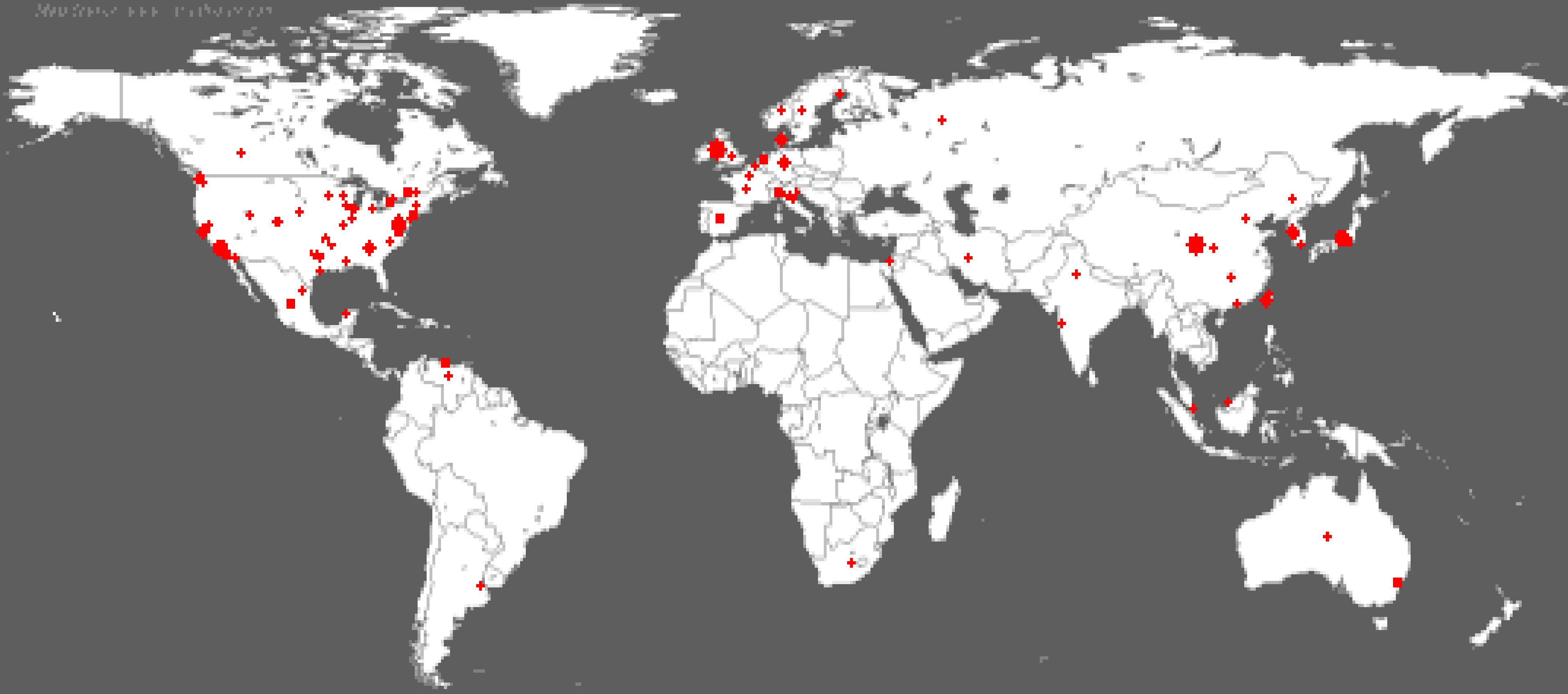
Safer | Sooner | Together

@joshcorman

@IamTheCavalry

~ Marc Andreessen 2011

@DUIVESTEIN | VISION • INSPIRATION • NAVIGATION • TRENDS
SOFTWARE IS EATING THE WORLD



Thu Jul 19 00:00:00 2001 (UTC)

Victims: 159

http://www.caida.org/

Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

Trade Offs
Costs & Benefits

BEYOND HEARTBLEED: OPENSSL IN 2014

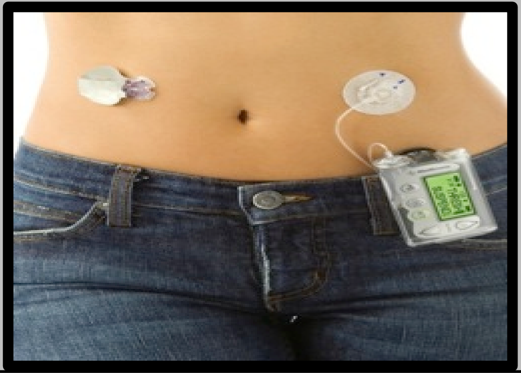
(31 IN NIST’S NVD THRU DECEMBER 2014)

CVE-2014-3470	6/5/2014	CVSS Severity: 4.3 MEDIUM
CVE-2014-0224	6/5/2014	CVSS Severity: 6.8 MEDIUM
CVE-2014-0221	6/5/2014	CVSS Severity: 4.3 MEDIUM
CVE-2014-0195	6/5/2014	CVSS Severity: 6.8 MEDIUM
CVE-2014-0198	5/6/2014	CVSS Severity: 4.3 MEDIUM
CVE-2013-7373	4/29/2014	CVSS Severity: 7.5 HIGH
CVE-2014-2734	4/24/2014	CVSS Severity: 5.8 MEDIUM
CVE-2014-0139	4/15/2014	CVSS Severity: 5.8 MEDIUM
CVE-2010-5298	4/14/2014	CVSS Severity: 4.0 MEDIUM
CVE-2014-0160	**4/7/2014**	**CVSS Severity: 5.0 MEDIUM** **← HeartBleed**
CVE-2014-0076	3/25/2014	CVSS Severity: 4.3 MEDIUM
CVE-2014-0016	3/24/2014	CVSS Severity: 4.3 MEDIUM
CVE-2014-0017	3/14/2014	CVSS Severity: 1.9 LOW
CVE-2014-2234	3/5/2014	CVSS Severity: 6.4 MEDIUM
CVE-2013-7295	1/17/2014	CVSS Severity: 4.0 MEDIUM
CVE-2013-4353	1/8/2014	CVSS Severity: 4.3 MEDIUM
CVE-2013-6450	1/1/2014	CVSS Severity: 5.8 MEDIUM

…

Heartbleed + (UnPatchable) Internet of Things == ____ ?

In Our Bodies



In Our Homes

In Our Cars

In Our Infrastructure

ShellShock

{bashbug}

A TALE OF TWO QUAKES

In the span of two months, two massive earthquakes struck in Haiti and Chile. But while the temblor in Chile registered much higher on the Richter scale, the loss of life and damage in Haiti was far more severe. Why is that? Chile—which has experienced serious earthquakes in recent decades—has a robust building code to make sure buildings are earthquake resistant; Haiti has no code to speak of. And a look at both quake's scores on the Modified Mercali Intensity Scale—which is used to measure how earthquakes affect those experiencing them—shows that while Chile's quake may have been stronger overall, Haiti had a larger population and more urban areas hit by more intense and damaging shaking.

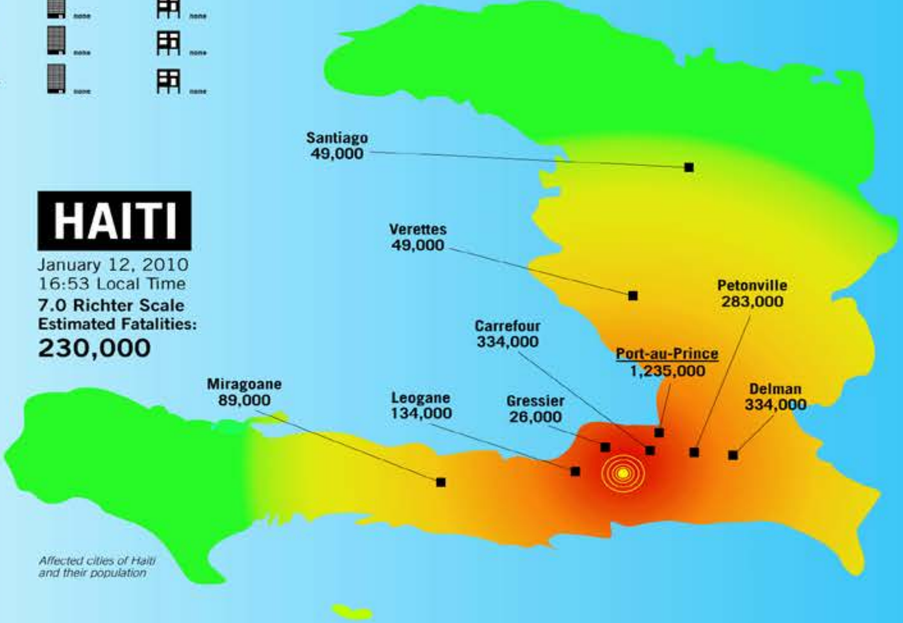
MODIFIED MERCALI INTENSITY SCALE

	Shaking	Structural Damage to Resistant Buildings	Structural Damage to Vulnerable Buildings
X	EXTREME	very heavy	very heavy
IX	VIOLENT	heavy	heavy
VIII	SEVERE	moderate/ heavy	heavy
VII	VERY STRONG	moderate	moderate/ heavy
VI	STRONG	light	moderate
V	MODERATE	very light	light
IV	LIGHT	none	none
II-III	WEAK	none	none
I	NOT FELT	none	none

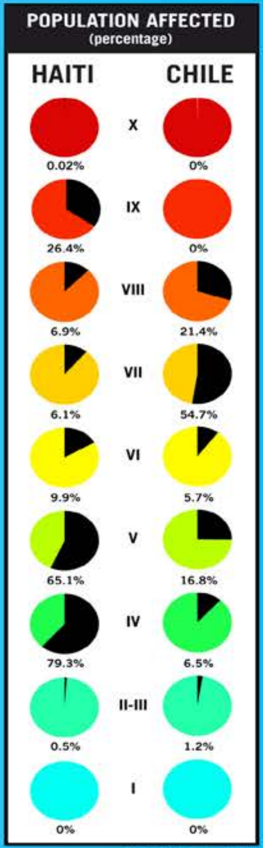
HAITI

January 12, 2010
16:53 Local Time

7.0 Richter Scale
Estimated Fatalities:
230,000



Affected cities of Haiti and their population

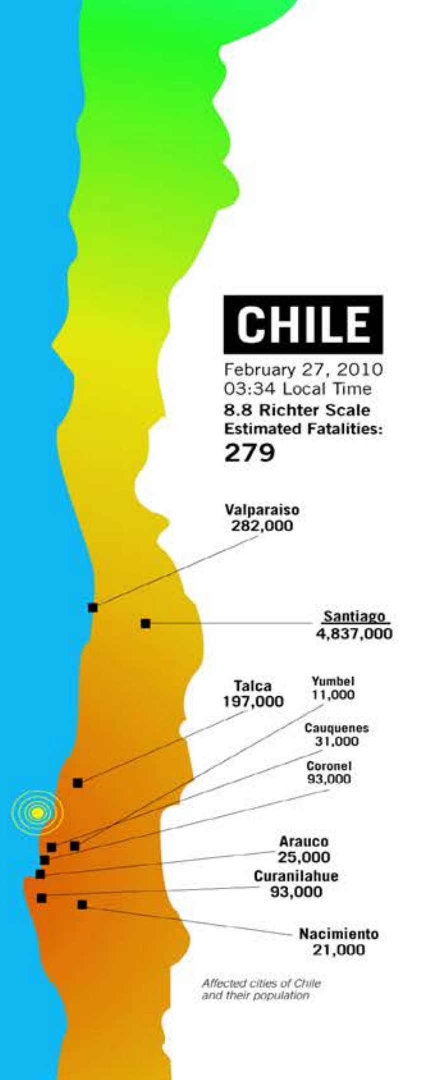


SOURCE U.S. Geological Survey
A collaboration between GOOD and karlssonwilker

CHILE

February 27, 2010
03:34 Local Time

8.8 Richter Scale
Estimated Fatalities:
279



Affected cities of Chile and their population

CASE
THR: 3
DPT: 4865'
HDG: 166
TRM: 0.3
Maxx3
150 165 180 195 210 225
P: -13
192
R: -1
TRM: 3.5
ROV
DPT: 4833
ALT: 78
OCEANEERING
07/12/1

I Am The Cavalry

The Cavalry isn’t coming… It falls to us

Problem Statement

Our society is adopting connected technology *faster than we are able to secure it*.

Mission Statement

To ensure connected technologies with the potential to impact public safety and human life are *worthy of our trust*.

Medical

Automotive

Connected Home

Public Infrastructure

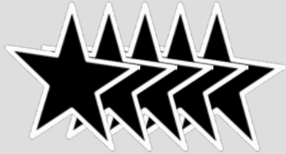
Why Trust, public safety, human life
How Education, outreach, research
Who Infosec research community
Who Global, grass roots initiative
WhatLong-term vision for cyber safety

Collecting existing research, researchers, and resources
Connecting researchers with each other, industry, media, policy, and legal
Collaborating across a broad range of backgrounds, interests, and skillsets
Catalyzing positive action sooner than it would have happened on its own

5-Star Framework

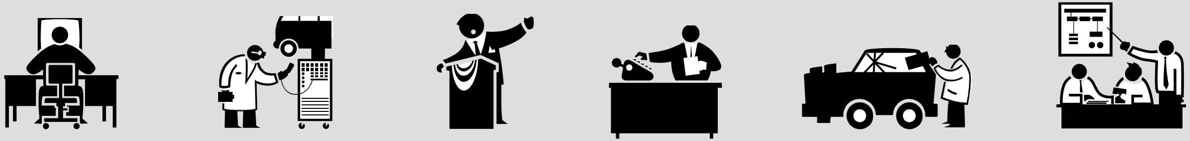
Addressing Automotive Cyber Systems

5-Star Capabilities



- ★ **Safety by Design** – Anticipate failure and plan mitigation
- ★ **Third-Party Collaboration** – Engage willing allies
- ★ **Evidence Capture** – Observe and learn from failure
- ★ **Security Updates** – Respond quickly to issues discovered
- ★ **Segmentation & Isolation** – Prevent cascading failure

Connections and Ongoing Collaborations



Security Researchers

Automotive Engineers

Policy Makers

Insurance Analysts

Accident Investigators

Standards Organizations

https://www.iamthecavalry.org/auto/5star/

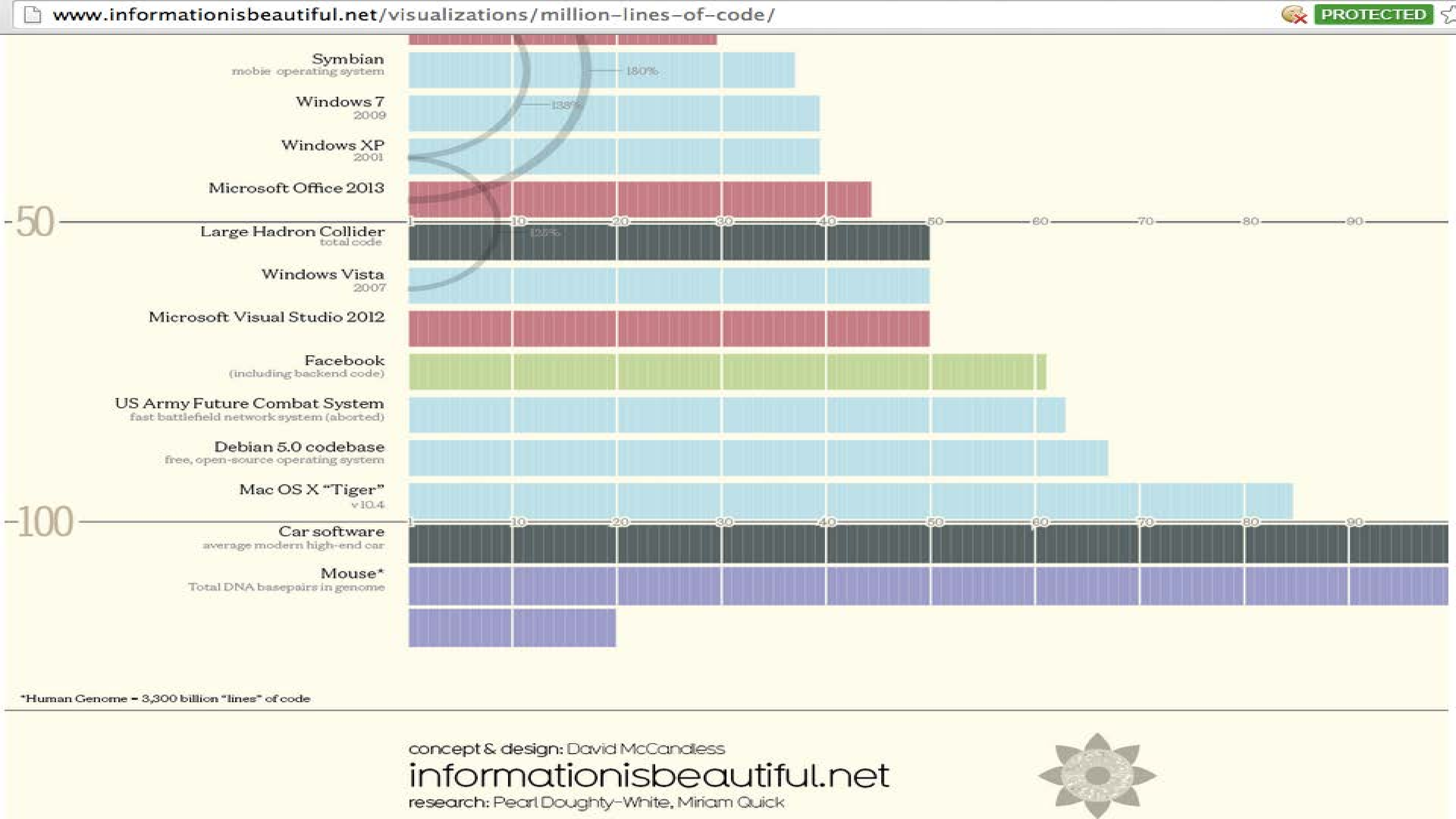
Automotive Cyber Safety

Facts, Fiction, and a ‘Vehicle’ for Collaboration

I am The Cavalry

All Systems Fail*

* Yes; all



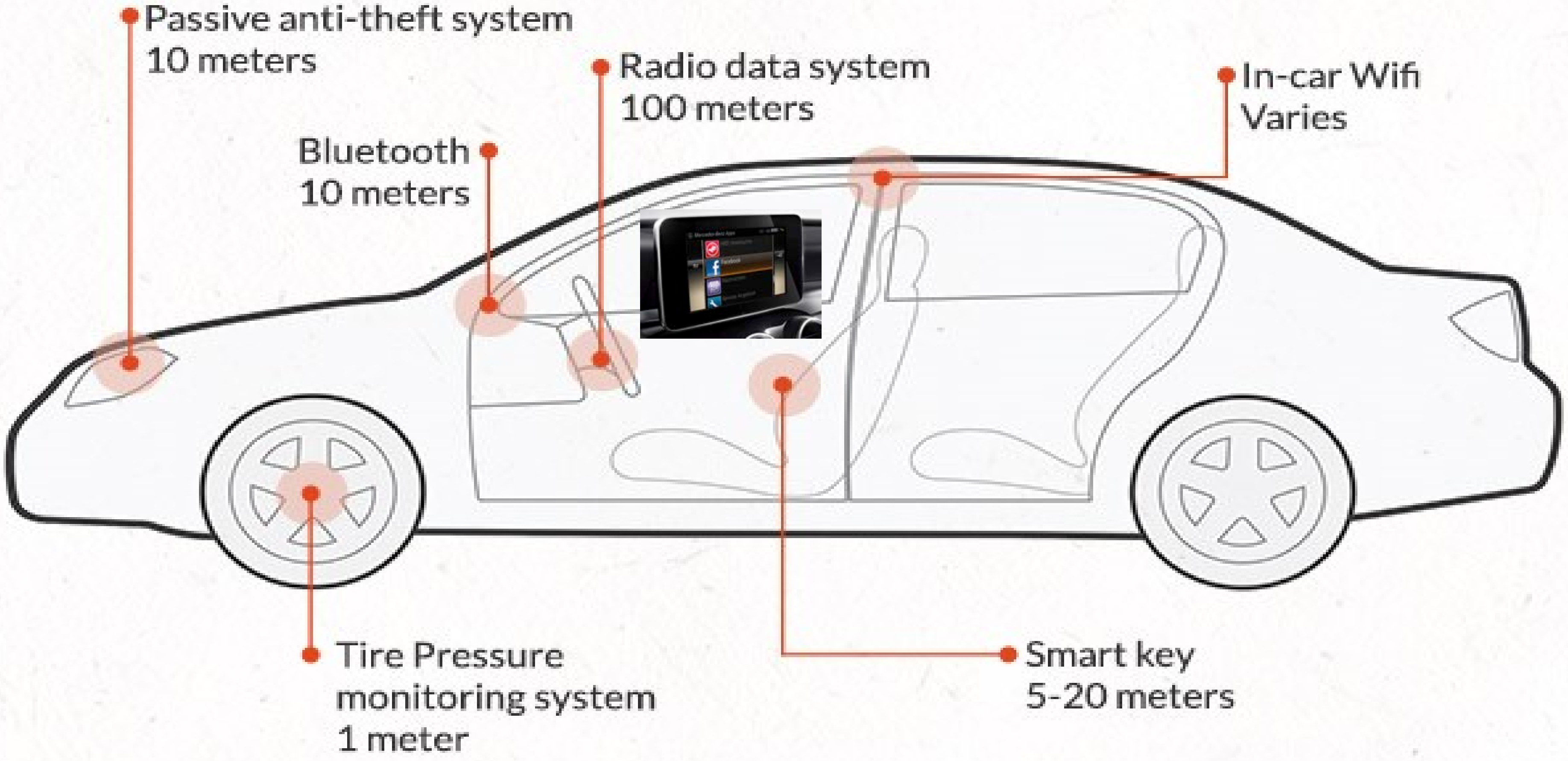
*Human Genome = 3,300 billion "lines" of code

concept & design: David McCandless

informationisbeautiful.net

research: Pearl Doughty-White, Miriam Quick

Distances for Hacking Car Features



Passive anti-theft system
10 meters

Radio data system
100 meters

In-car Wifi
Varies

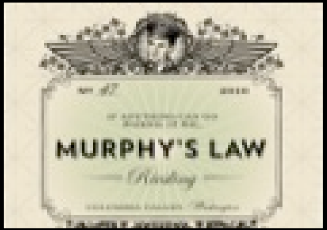
Bluetooth
10 meters

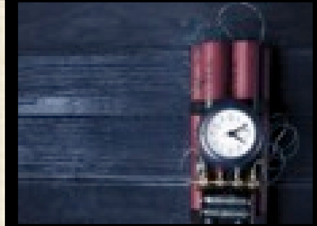
Tire Pressure
monitoring system
1 meter

Smart key
5-20 meters

ILLUSTRATION: CNNMONEY

“But they *wouldn’t* hurt you!”





“I’d prefer that they *couldn’t* hurt me…”

5-Star Cyber Safety

Formal Capacities

1. **Safety By Design**
2. **Third Party Collaboration**
3. **Evidence Capture**
4. **Security Updates**
5. **Segmentation and Isolation**

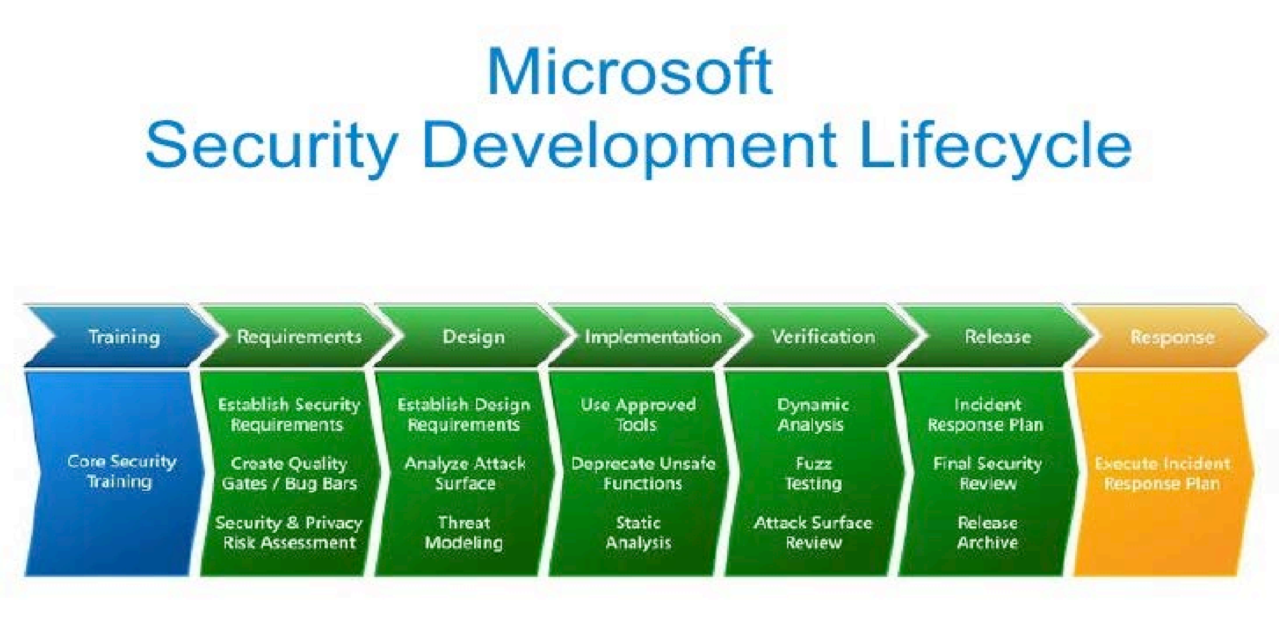
Plain Speak

1. Avoid Failure
2. Engage Allies To Avoid Failure
3. Learn From Failure
4. Respond to Failure
5. Isolate Failure

1) Safety By Design

Do you have a published attestation of your Secure Software Development Lifecycle, summarizing your design, development, and adversarial resilience testing programs for your products and your supply chain?

1) Safety By Design



Microsoft
Security Development Lifecycle

Training	Requirements	Design	Implementation	Verification	Release	Response
Core Security Training	Establish Security Requirements Create Quality Gates / Bug Bars Security & Privacy Risk Assessment	Establish Design Requirements Analyze Attack Surface Threat Modeling	Use Approved Tools Deprecate Unsafe Functions Static Analysis	Dynamic Analysis Fuzz Testing Attack Surface Review	Incident Response Plan Final Security Review Release Archive	Execute Incident Response Plan

2) Third Party Collaboration

Do you have a published Coordinated Disclosure policy inviting the assistance of third-party researchers acting in good faith?

2) Third Party Collaboration

BEWARE
OF
DOG

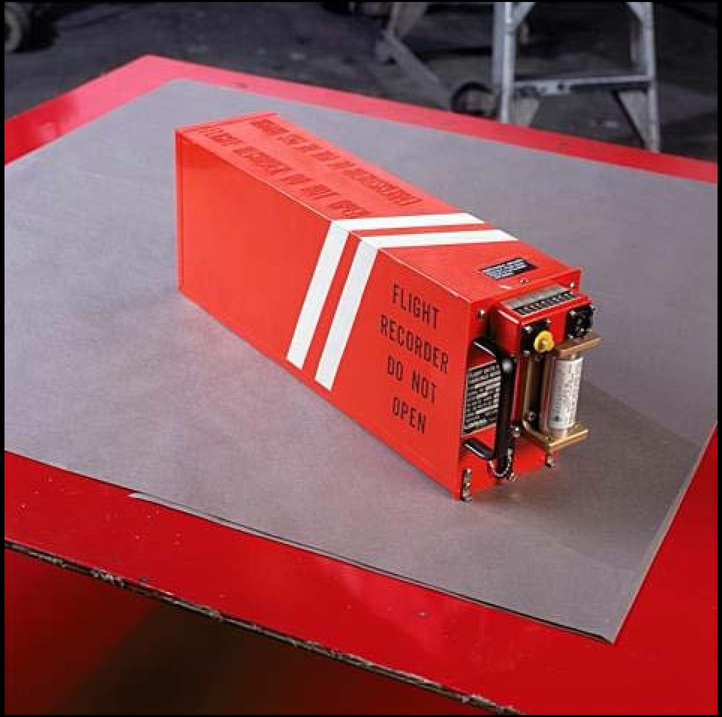
Vs

WELCOME
FRIENDS

3) Evidence Capture

Do your vehicle systems provide tamper evident, forensically-sound logging and evidence capture to facilitate safety investigations?

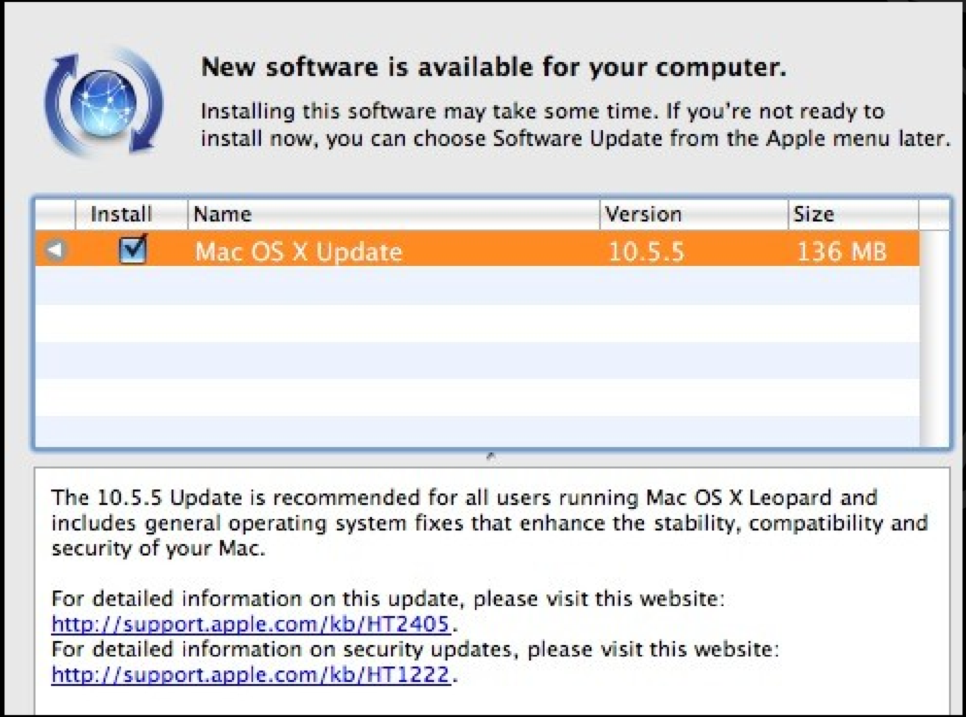
3) Evidence Capture



4) Security Updates

Can your vehicles be securely updated in a prompt and agile manner?

4) Security Updates



New software is available for your computer.

Installing this software may take some time. If you're not ready to install now, you can choose Software Update from the Apple menu later.

Install	Name	Version	Size
☑	Mac OS X Update	10.5.5	136 MB

The 10.5.5 Update is recommended for all users running Mac OS X Leopard and includes general operating system fixes that enhance the stability, compatibility and security of your Mac.

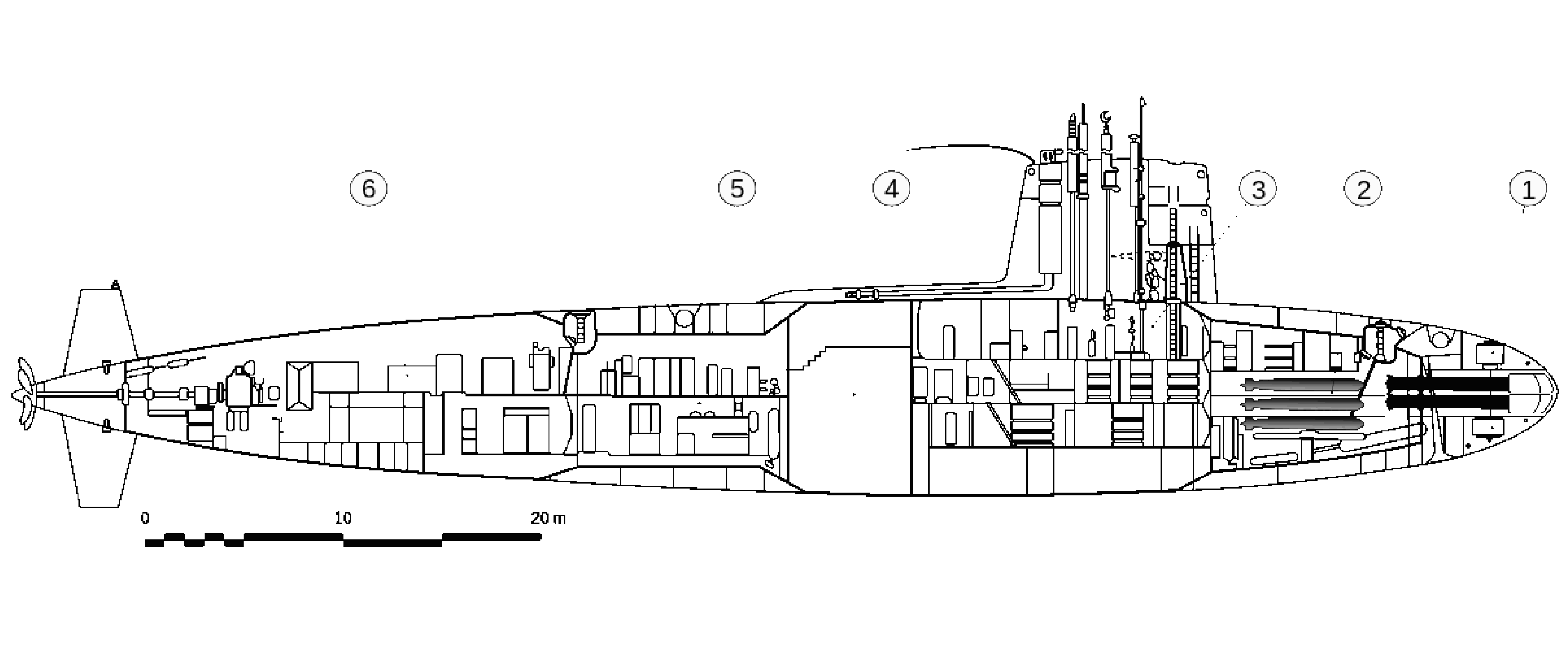
For detailed information on this update, please visit this website:
http://support.apple.com/kb/HT2405.
For detailed information on security updates, please visit this website:
http://support.apple.com/kb/HT1222.

www.iamthecavalry.org
@iamthecavalry

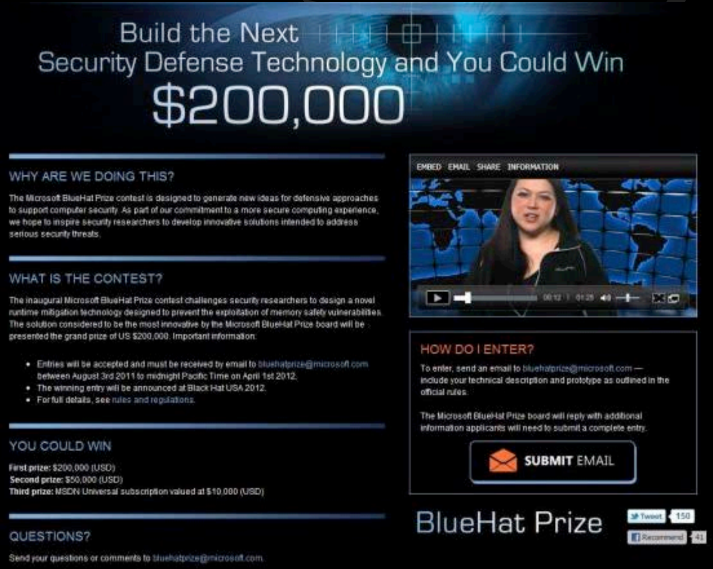
5) Segmentation and Isolation

Do you have a published attestation of the physical and logical isolation measures you have implemented to separate critical systems from non-critical systems?

5) Segmentation and Isolation



Microsoft (Then & Now)



Build the Next
Security Defense Technology and You Could Win
$200,000

WHY ARE WE DOING THIS?

The Microsoft BlueHat Prize contest is designed to generate new ideas for defensive approaches to support computer security. As part of our commitment to a more secure computing experience, we hope to inspire security researchers to develop innovative solutions intended to address serious security threats.

WHAT IS THE CONTEST?

The inaugural Microsoft BlueHat Prize contest challenges security researchers to design a novel runtime mitigation technology designed to prevent the exploitation of memory safety vulnerabilities. The solution considered to be the most innovative by the Microsoft BlueHat Prize board will be presented the grand prize of US $200,000. Important information:

- Entries will be accepted and must be received by email to bluehatprize@microsoft.com between August 3rd 2011 to midnight Pacific Time on April 1st 2012.
- The winning entry will be announced at Black Hat USA 2012.
- For full details, see rules and regulations.

YOU COULD WIN

First prize: $200,000 (USD)
Second prize: $50,000 (USD)
Third prize: MSDN Universal subscription valued at $10,000 (USD)

QUESTIONS?

Send your questions or comments to bluehatprize@microsoft.com.

HOW DO I ENTER?

To enter, send an email to bluehatprize@microsoft.com — include your technical description and prototype as outlined in the official rules.

The Microsoft BlueHat Prize board will reply with additional information applicants will need to submit a complete entry.

TESLA

Past versus Future

Bolt-On Vs Built-In

5-Star Cyber Safety

Formal Capacities

1. **Safety By Design**
2. **Third Party Collaboration**
3. **Evidence Capture**
4. **Security Updates**
5. **Segmentation and Isolation**

Plain Speak

1. Avoid Failure
2. Engage Allies To Avoid Failure
3. Learn From Failure
4. Respond to Failure
5. Isolate Failure

$
BY SA

Safer | Sooner | Together

@joshcorman

@IamTheCavalry

RSAC Studio

Connect to Protect

Security Issues in Transportation: Need for Collaboration for Solutions

Joshua Corman

Chief Technology Officer
Sonatype

#RSAC