Safer | Sooner | Together

@joshcorman

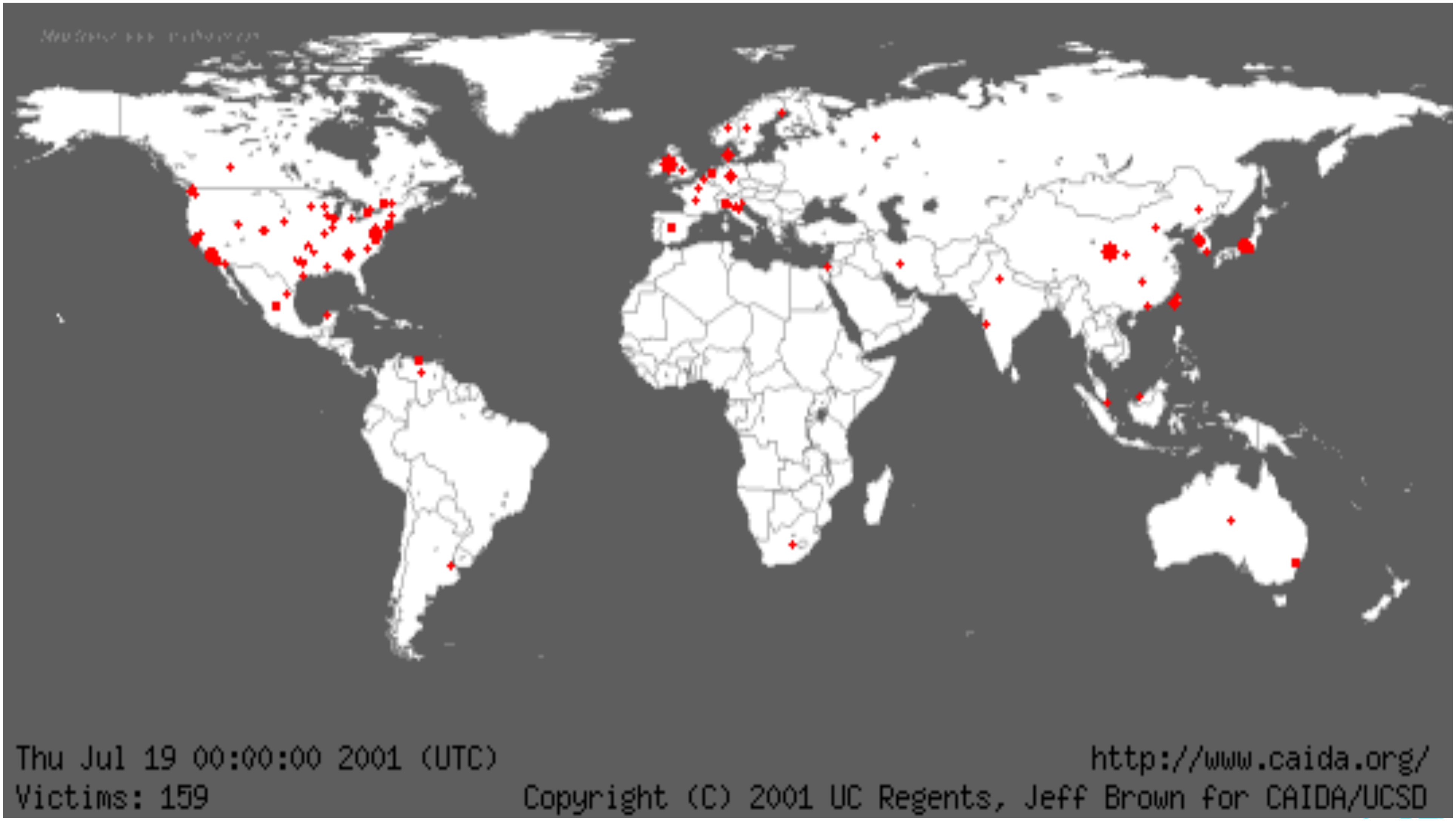
@IamTheCavalry

I am The Cavalry

BY SA

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

~ Marc Marc Andreessen 2011


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)

CVE-2014-3470	6/5/2014	CVSS Severity: 4.3 MEDIUM	← **SEIMENS** *
CVE-2014-0224	6/5/2014	CVSS Severity: 6.8 MEDIUM	← **SEIMENS** *
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	← **SEIMENS** *
CVE-2013-7373	4/29/2014	CVSS Severity: 7.5 HIGH	
CVE-2014-2734	4/24/2014	CVSS Severity: 5.8 MEDIUM	** DISPUTED **
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	
…			

As of today, internet scans by MassScan reveal 300,000 of original 600,000 remain unpatched or unpatchable

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

#RSAC
@joshcorman
@iamthecavalry

In Our Bodies

In Our Homes

In Our Cars

In Our Infrastructure

ShellShock
{bashbug}

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
What	Long-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

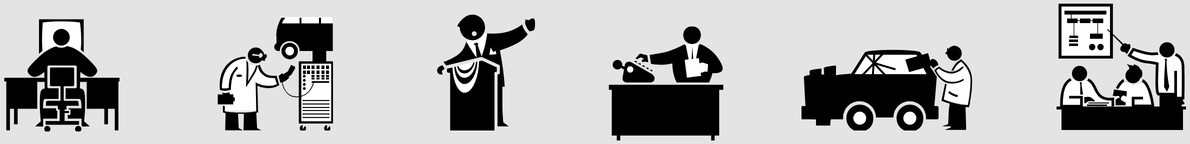
5-Star Framework

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/

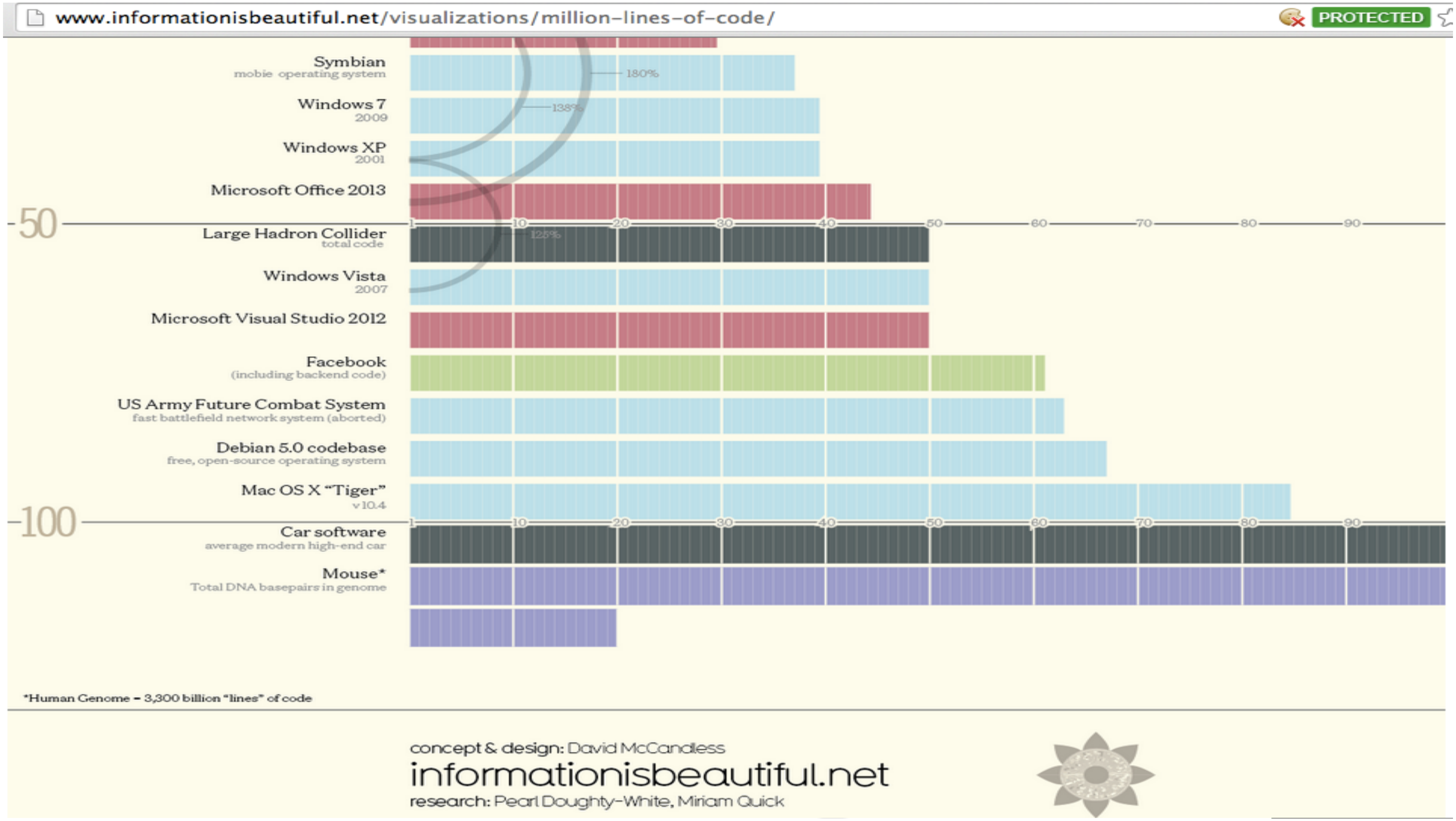
Automotive Cyber Safety

Facts, Fiction, and a 'Vehicle' for Collaboration

I am The Cavalry

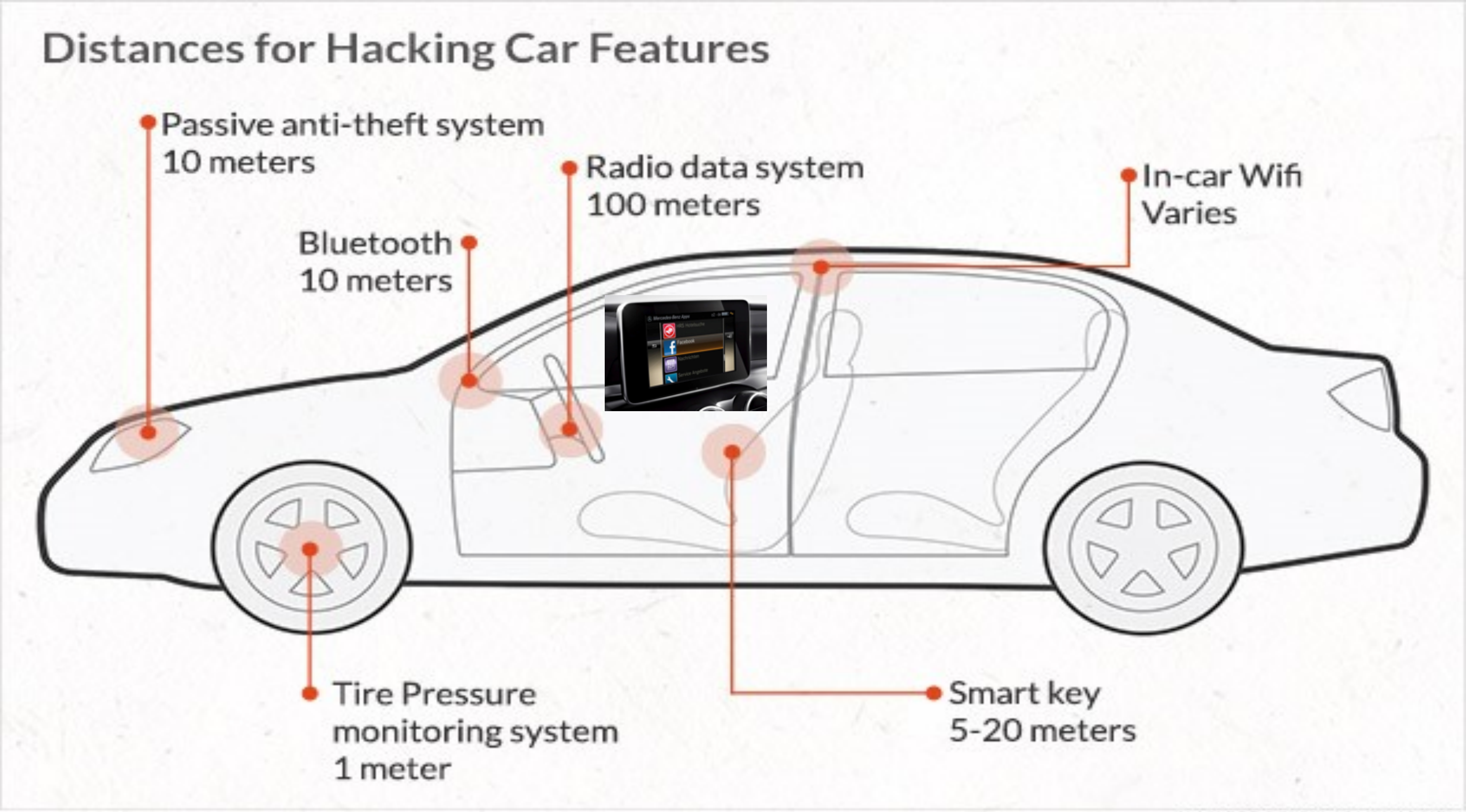
All Systems Fail*

* 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

Bluetooth
10 meters

Radio data system
100 meters

In-car Wifi
Varies

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...”

www.iamthecavalry.org
@iamthecavalry

5-Star Cyber Safety

Formal Capacities	Plain Speak
1. Safety By Design	1. Avoid Failure
2. Third Party Collaboration	2. Engage Allies To Avoid Failure
3. Evidence Capture	3. Learn From Failure
4. Security Updates	4. Respond to Failure
5. Segmentation and Isolation	5. Isolate Failure

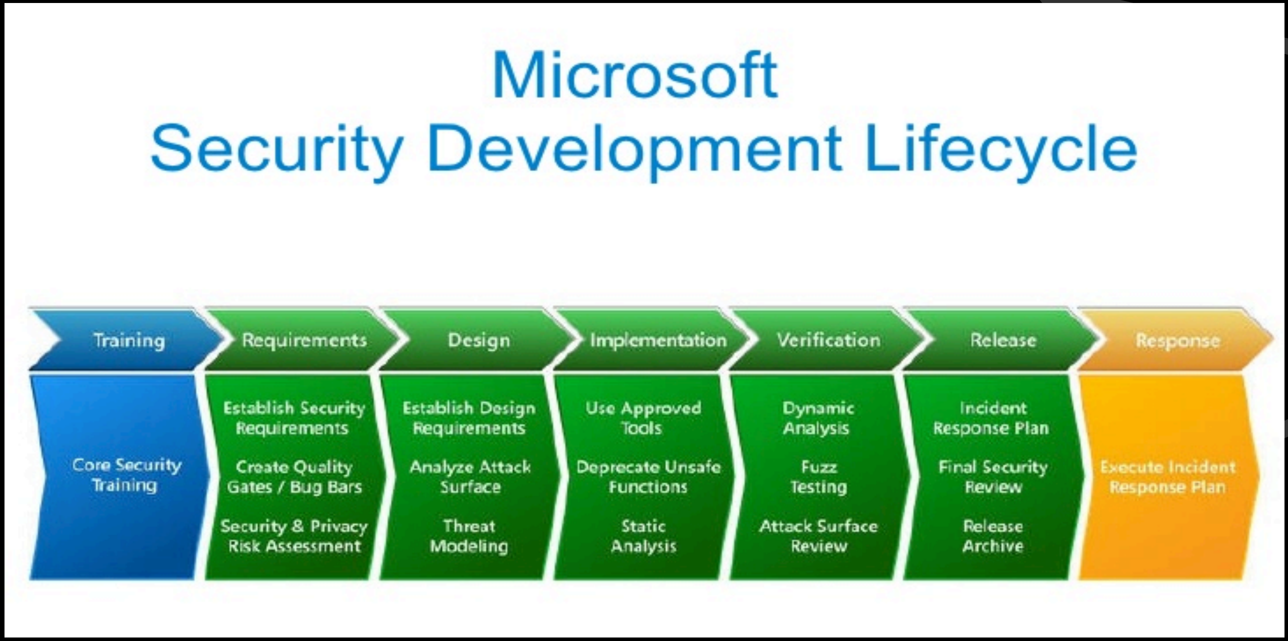
www.iamthecavalry.org
@iamthecavalry

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?

www.iamthecavalry.org
@iamthecavalry

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

www.iamthecavalry.org
@iamthecavalry

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

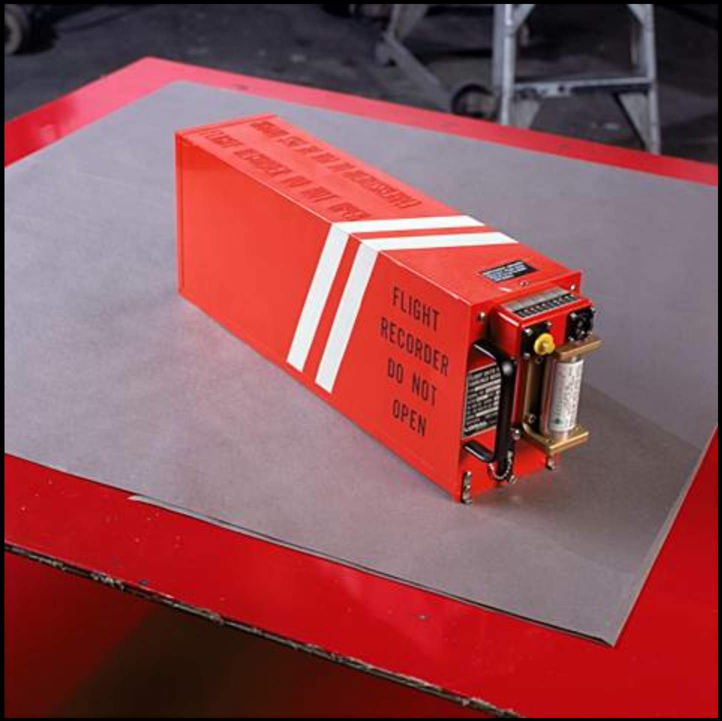
WELCOME
FRIENDS

3) Evidence Capture

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

www.iamthecavalry.org
@iamthecavalry

3) Evidence Capture

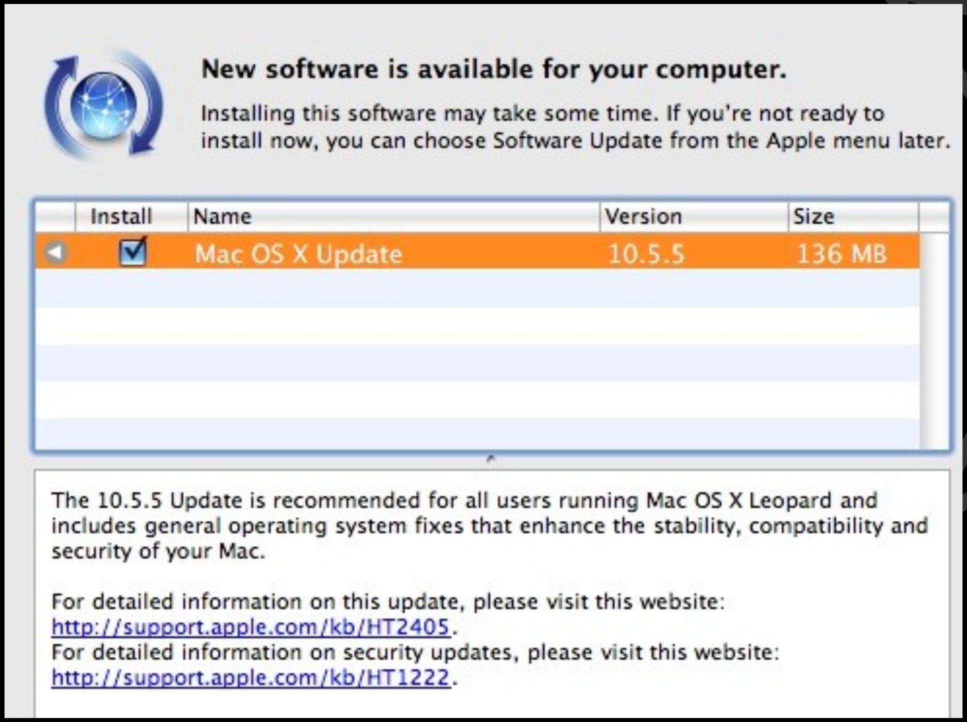


www.iamthecavalry.org
@iamthecavalry

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

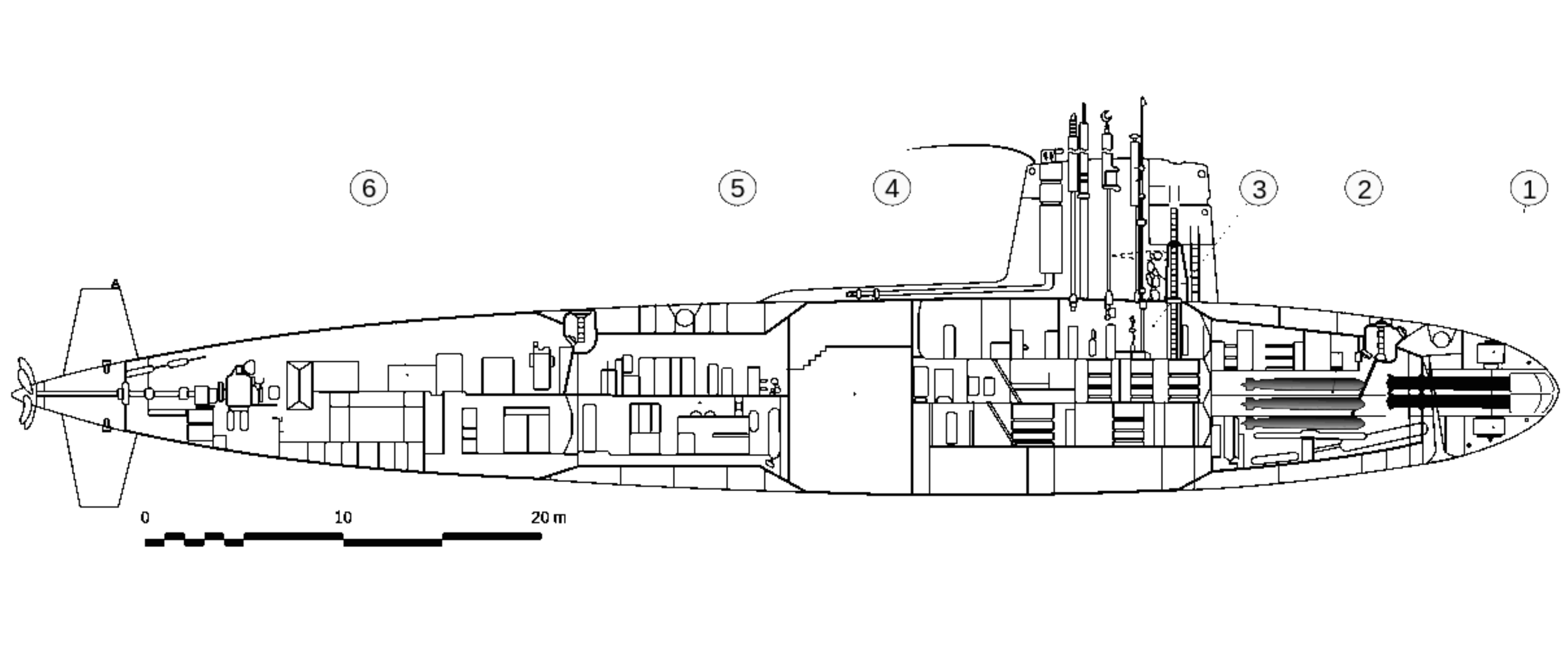
The 10.5.5 Update is recommended for all users running Mac OS X Leopard and includes general operating system fixes that enhance the stability, compatibility and security of your Mac.

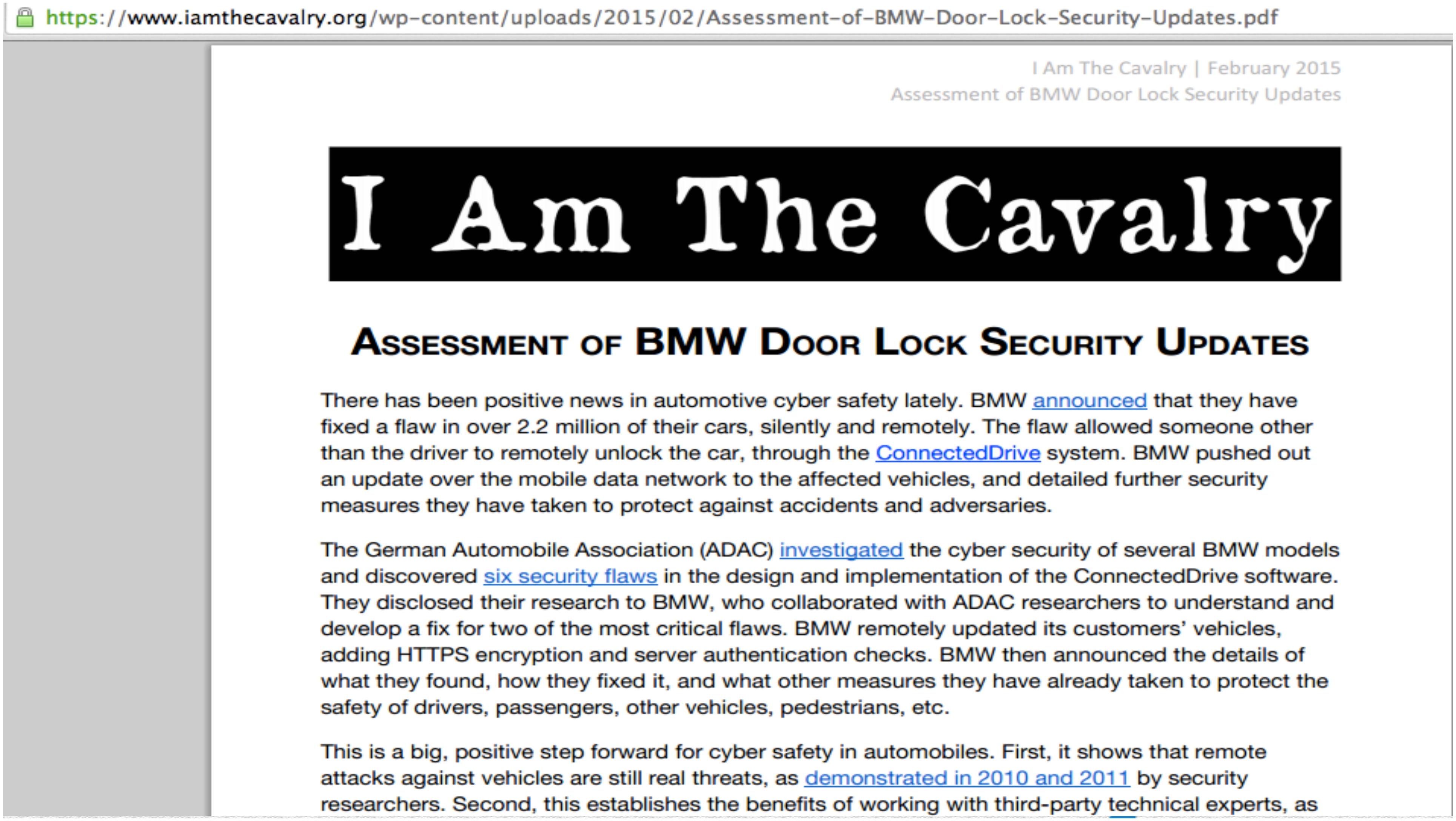
For detailed information on this update, please visit this website:
http://support.apple.com/kb/HT2405.
For detailed information on security updates, please visit this website:
http://support.apple.com/kb/HT1222.

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





https://www.iamthecavalry.org/wp-content/uploads/2015/02/Assessment-of-BMW-Door-Lock-Security-Updates.pdf

I Am The Cavalry | February 2015
Assessment of BMW Door Lock Security Updates

I Am The Cavalry

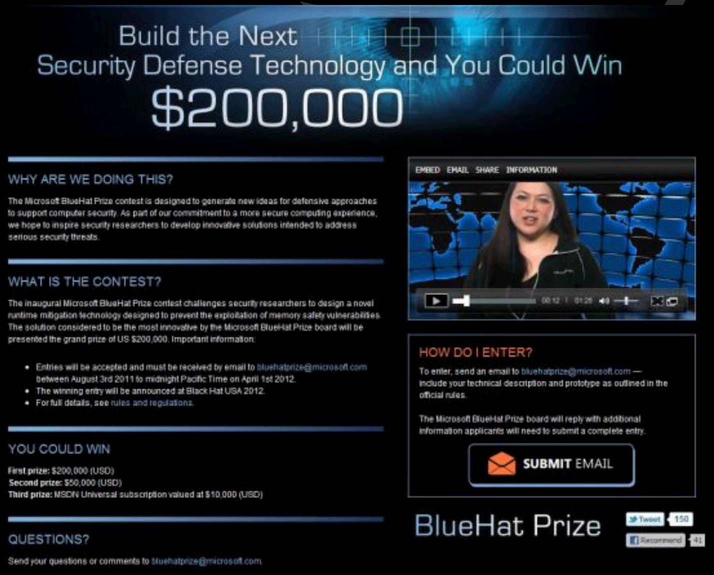
Assessment of BMW Door Lock Security Updates

There has been positive news in automotive cyber safety lately. BMW announced that they have fixed a flaw in over 2.2 million of their cars, silently and remotely. The flaw allowed someone other than the driver to remotely unlock the car, through the ConnectedDrive system. BMW pushed out an update over the mobile data network to the affected vehicles, and detailed further security measures they have taken to protect against accidents and adversaries.

The German Automobile Association (ADAC) investigated the cyber security of several BMW models and discovered six security flaws in the design and implementation of the ConnectedDrive software. They disclosed their research to BMW, who collaborated with ADAC researchers to understand and develop a fix for two of the most critical flaws. BMW remotely updated its customers' vehicles, adding HTTPS encryption and server authentication checks. BMW then announced the details of what they found, how they fixed it, and what other measures they have already taken to protect the safety of drivers, passengers, other vehicles, pedestrians, etc.

This is a big, positive step forward for cyber safety in automobiles. First, it shows that remote attacks against vehicles are still real threats, as demonstrated in 2010 and 2011 by security researchers. Second, this establishes the benefits of working with third-party technical experts, as

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.

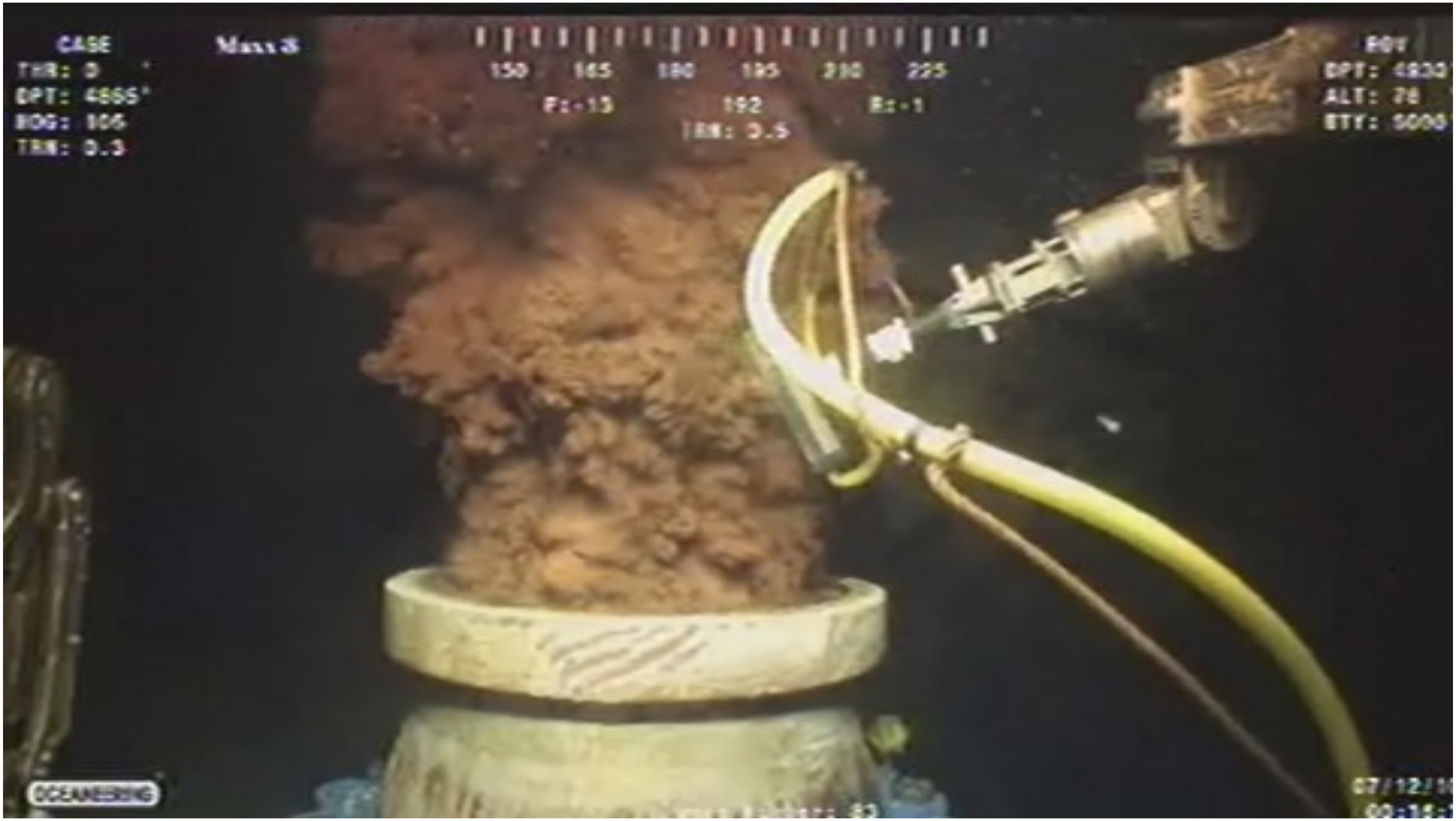
The Microsoft BlueHat Prize board will reply with additional information applicants will need to submit a complete entry.

www.iamthecavalry.org
@iamthecavalry

Past versus Future

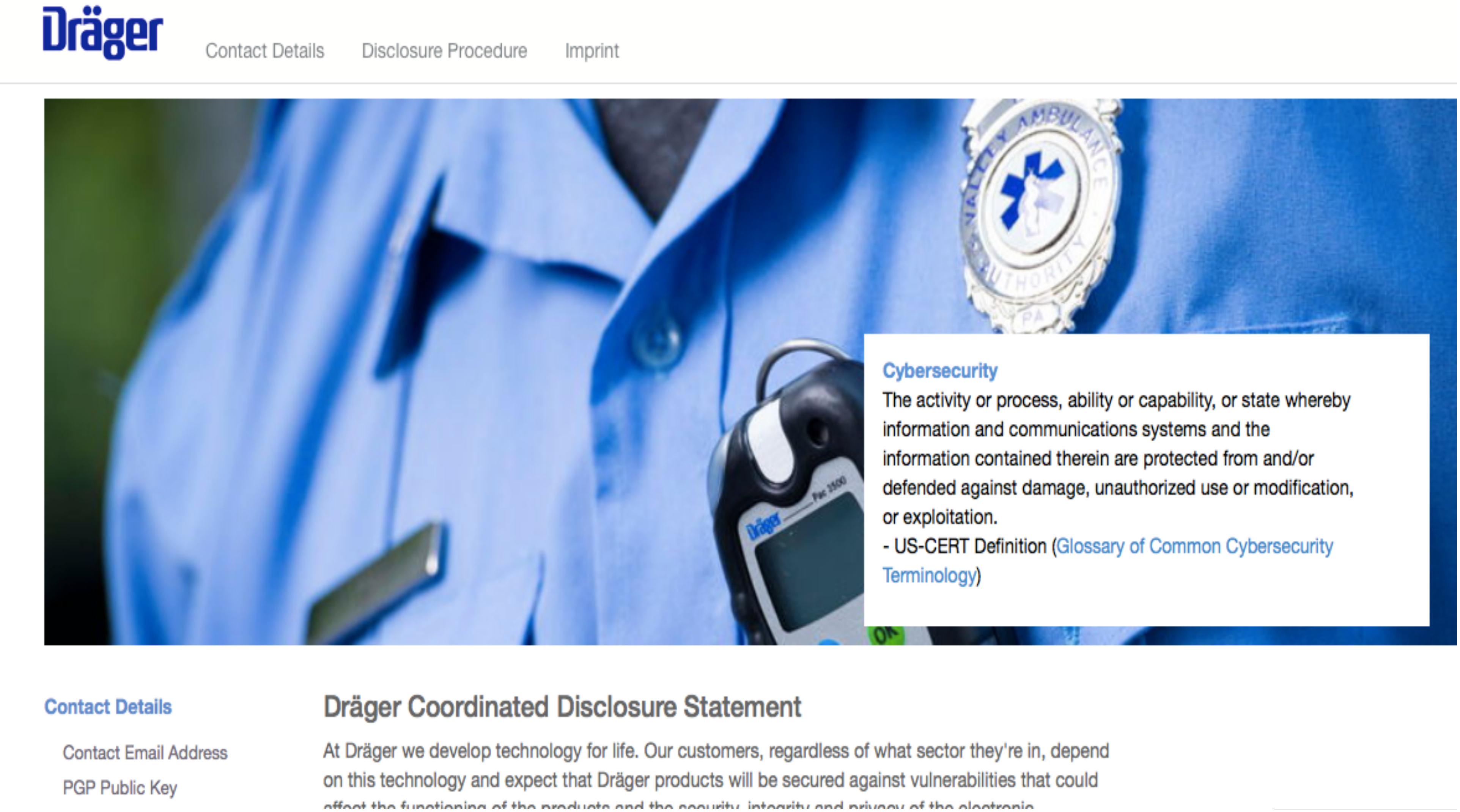
Bolt-On Vs Built-In

www.iamthecavalry.org
@iamthecavalry


CASE
Maxx 3
THR: 0
DPT: 4865'
HDG: 106
TRN: 0.3
150 165 180 195 210 225
P: -15
192
R: -1
TRN: 0.5
ROV
DPT: 4830'
ALT: 78
BTY: 5000'
OCEANEERING
07/12/10
00:15:

UNITED

TESLA



Cybersecurity

The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

- US-CERT Definition (Glossary of Common Cybersecurity Terminology)

Contact Details

- Contact Email Address
- PGP Public Key

Dräger Coordinated Disclosure Statement

At Dräger we develop technology for life. Our customers, regardless of what sector they're in, depend on this technology and expect that Dräger products will be secured against vulnerabilities that could affect the functioning of the products and the security, integrity and privacy of the electronic

?

www.iamthecavalry.org
@iamthecavalry

$
cc BY SA

Safer | Sooner | Together

@joshcorman

@IamTheCavalry

I am The Cavalry