IoT security from the consumer's perspective

Jorge Pinto

Confraria de Segurança da Informação

24th June 2015

AP2SI

Born in 2012, AP2SI is a non lucrative private association characterized by:

- Openness by associating with every individual to help in information security matters;
- Focus with the dedication to fulfill its objectives and mission;
- Non competitive: has no goal in information security services;
- Independent: not controlled by organizations.
- From concerned individuals to the society.

Mission

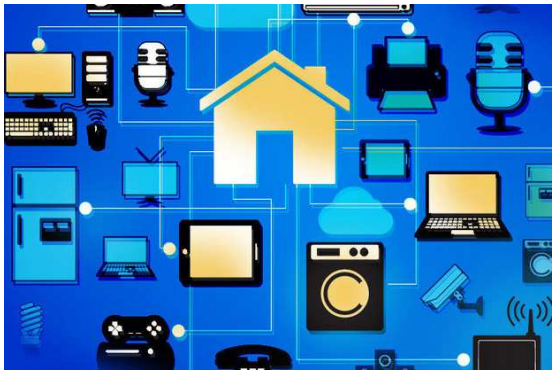
Actively contribute to the information security mindset development in Portugal:

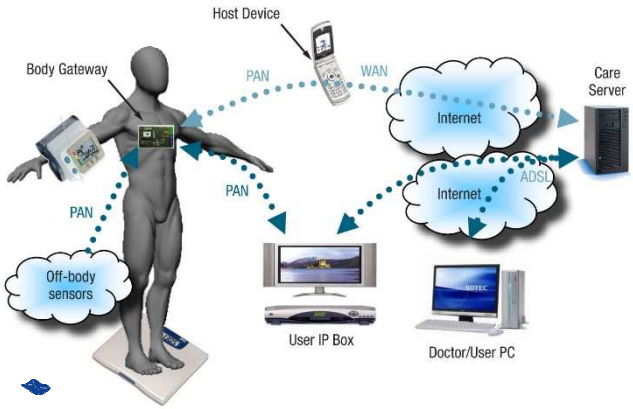
- Raising awareness to the value of information and requirements to protect it;
- Developing guidelines/best practices to enhance knowledge and help qualifying information security personnel;

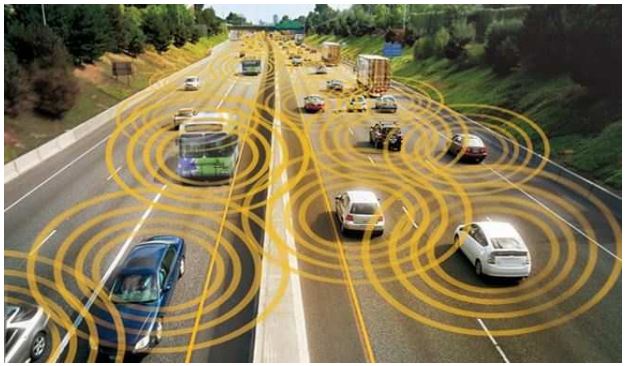
So….

What is the IoT ?

(from the consumer’s perspective)




Host Device
Body Gateway
PAN
WAN
Internet
Care Server
Internet
ADSL
PAN
PAN
Off-body sensors
User IP Box
Doctor/User PC



12:45

So….

The IoT is cool, right?

Well… yes… kind of….

Home > Security

Smart home hacking is easier than you think

Scary stories of hacking Internet of Things devices are emerging, but how realistic is the threat?

By Colin Neagle | Follow
Network World | Apr 2, 2015 4:14 AM PT

http://www.networkworld.com/article/2905053/security0/smart-home-hacking-is-easier-than-you-think.html

RELATED

How to keep your connected home safe: 7 steps you can take to boost home...

What can I do with home automation?

What is home automation and how do I get started?

on IDG Answers ↪
How can Convert OST file data into PST file formats?

http://www.theverge.com/2013/10/21/4863872/dick-cheney-pacemaker-wireless-disabled-2007

Insulin pump hack delivers fatal dosage over the air

Sugar Blues, James Bond style

27 Oct 2011 at 06:23, Dan Goodin 90

In a hack fitting of a James Bond movie, a security researcher has devised an attack that hijacks nearby insulin pumps, enabling him to surreptitiously deliver fatal doses to diabetic patients who rely on them.

The attack on wireless insulin pumps made by medical devices giant Medtronic was demonstrated Tuesday at the Hacker Halted conference in Miami. It was delivered by McAfee's Barnaby Jack, the same researcher who last year showed how to take control of two widely used models of automatic teller machines so he could to cause them to spit out a steady stream of dollar bills.

Jack's latest hack works on most recent Medtronic
insulin pumps, because they contain tiny radio transmitters that allow patients and doctors to adjust their functions. It builds on research presented earlier this year that allowed the wireless commandeering of the devices when an attacker was within a few feet of the patient, and knew the serial number of his pump. Software and a special antenna designed by Jack allows him to locate and seize control of any device within 300 feet, even when he doesn't know the serial number.

"With this device I created and the software I created, I could actually instruct the pump to perform all manner of commands," Jack told *The Register*. "I could make it dispense its entire reservoir of insulin, which is about 300 units. I just scan for any devices in the vicinity and they will respond with the serial number of the device."

Security

Related topics

Security

Most read

Airbus confirms software brought down A400M transport plane

Apple: Relax, fanbois! We never meant to read your heart rate during wild wrist action

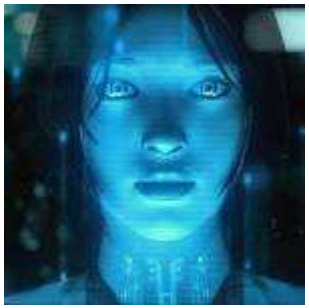
Strap-on fiddle factor: We poke ten Apple Watch apps

The rare metals debate: Only trace elements of sanity found

Fedora 22: Don't be glum about the demise of Yum – this is a welcome update

Spotlight

http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/



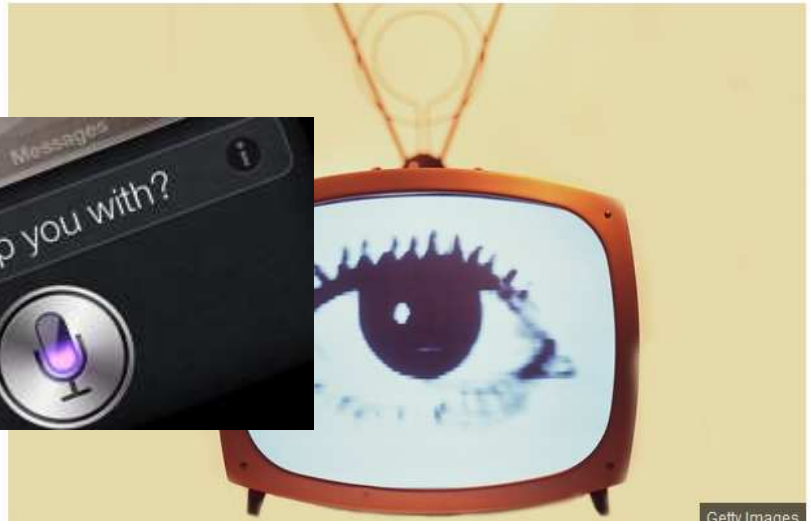
Samsung spy telly scandal erupts after firm admits its television will RECORD your "personal and sensitive" conversations

11:45, 9 FEBRUARY 2015 | BY JASPER HAMILL

New Big Brother tellies will make audio recordings and beam them back to mysterious 'third parties'

Share | Share | Tweet | +1

Subscribe



★ Rec ded In N

CHILD ABUSE

Cruel dad caught on camera dragging screaming 10-year-old along pavement by rope tied around his neck

SCHOOLS

Selfless students donate their $8,0 savings to help principal pay for cancer treatmen

CONSERVATIVE PAR

#WorkingClassT prompts giant Tw row after party b

Vlingo

http://www.mirror.co.uk/news/technology-science/technology/samsung-spy-telly-scandal-erupts-5131842

CogniToys: Internet-connected Smart Toys that Learn and Grow

We bring toys to life with speech and a personality, allowing them to interactively engage and grow with a child.

Created by

Elemental Path

2,256 backers pledged $275,000 to help bring this project to life.

https://www.kickstarter.com/projects/522717158/cognitoys-internet-connected-smart-toys-that-learn

US 20150138333A1

(19) **United States**

(12) **Patent Application Publication**

DeVaul et al.

(10) **Pub. No.: US 2015/0138333 A1**

(43) **Pub. Date: May 21, 2015**

(54) **AGENT INTERFACES FOR INTERACTIVE ELECTRONICS THAT SUPPORT SOCIAL CUES**

(75) Inventors: **Richard Wayne DeVaul**, Mountain View, CA (US); **Daniel Aminzade**, Mountain View, CA (US)

(73) Assignee: **Google Inc.**, Mountain View, CA (US)

(21) Appl. No.: **13/407,159**

(22) Filed: **Feb. 28, 2012**

Publication Classification

(51) **Int. Cl.**

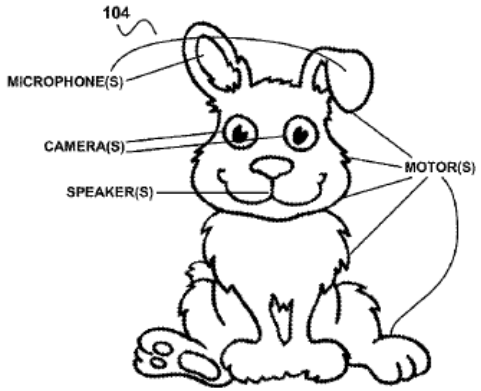
A63H 33/00	(2006.01)
G06F 3/01	(2006.01)
G06F 3/16	(2006.01)
H04N 5/225	(2006.01)
G06K 9/00	(2006.01)
H04R 1/32	(2006.01)

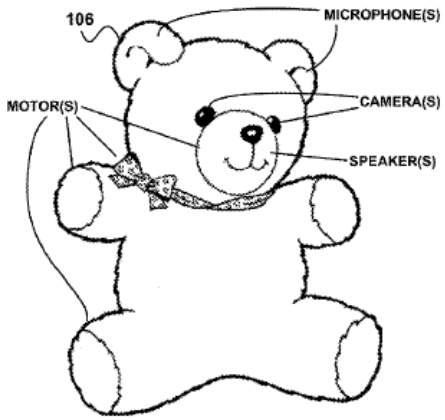
(52) **U.S. Cl.**

CPC ***G06F 3/013*** (2013.01); ***H04R 1/32*** (2013.01); ***H04N 5/2257*** (2013.01); ***G06F 3/16*** (2013.01); ***G06K 9/00288*** (2013.01)

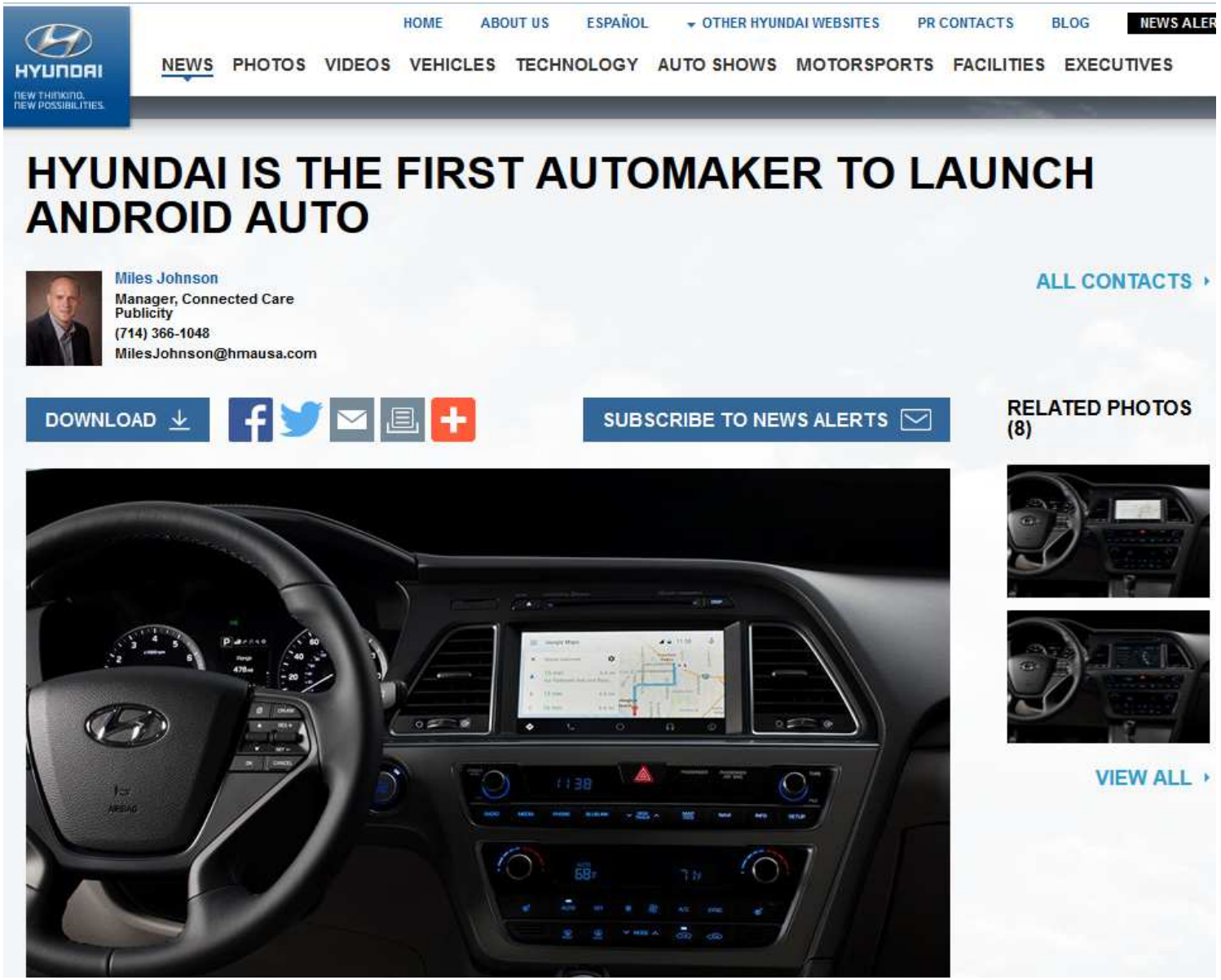
(57) **ABSTRACT**

An anthropomorphic device, perhaps in the form factor of a doll or toy, may be configured to control one or more media devices. Upon reception or a detection of a social cue, such as movement and/or a spoken word or phrase, the anthropomorphic device may aim its gaze at the source of the social cue. In response to receiving a voice command, the anthropomorphic device may interpret the voice command and map it to a media device command. Then, the anthropomorphic device may transmit the media device command to a media device, instructing the media device to change state.





http://pdfaiw.uspto.gov/.aiw?PageNum=0&docid=20150138333&IDKey=1EF5AB92E988



http://www.hyundainews.com/us/en/media/pressreleases/43387/hyundai-is-the-first-automaker-to-launch-android-auto

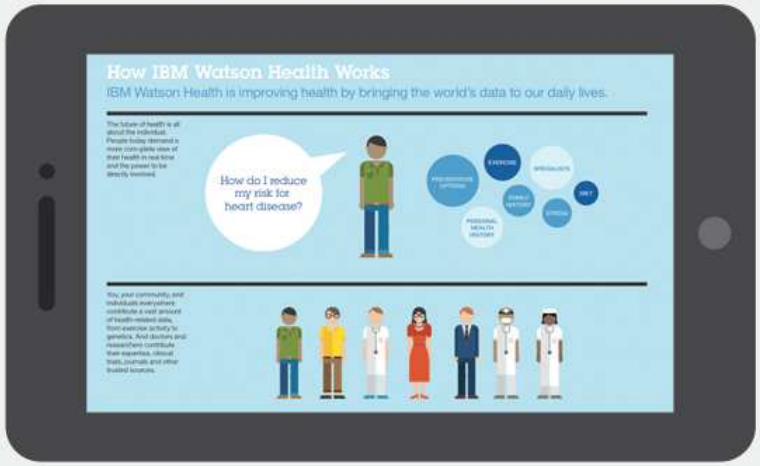
IBM Watson Health

Overview | Health Cloud | Partnerships | Solutions | About | IBM.com

Fueling a New Generation of Health Insights

People today want more information to inform the decisions they make about their health. Many different factors that affect one's health: nutrition, lifestyle, medical history - and today, much of this information can be captured in data. Personal fitness trackers, wearable health monitors, and other connected devices are generating more and more data every day. But without a glimpse into all the information out there, individuals only receive a fragmented view of the whole picture.

For the first time, IBM Watson Health is creating a more complete and personalized picture of health, powered by cognitive computing. Now individuals are empowered to understand more about their health, while doctors, researchers, and insurers can make better, faster, and more cost-effective decisions.



http://www.ibm.com/smarterplanet/us/en/ibmwatson/health/

BIOTECHNOLOGY

Electronic Tattoos for Baby and You

MAR 11, 2014 02:55 PM ET // BY GLENN ZORPETTE, IEEE SPECTRUM

Athletes, soldiers, and just about everybody else in the future will have embedded electronic tattoos.

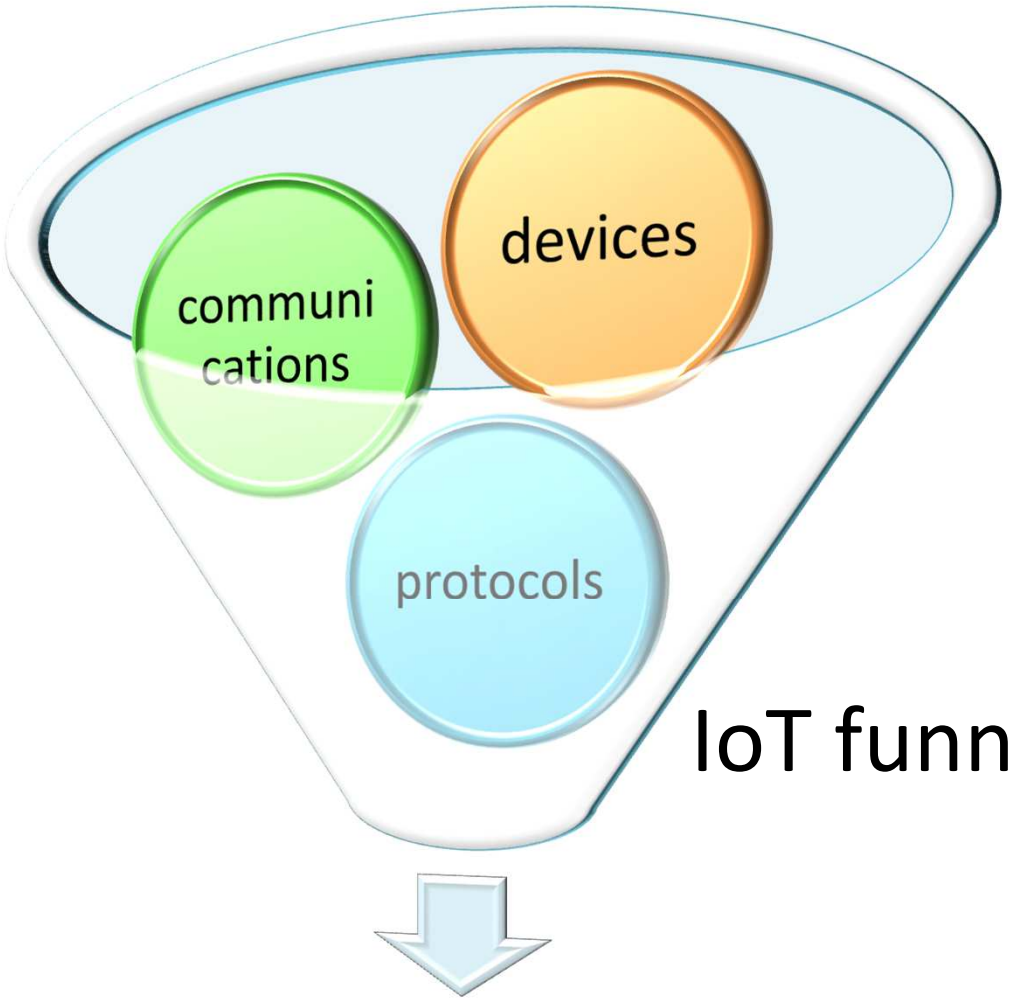
FRANKY DE MEYER/GETTY IMAGES

RELATED links

Skin Tattoo Takes Body Temperature

A baby born five to 10 years from now in a developed country may get a tattoo not long after her first feeding. It would be an integrated circuit, a discreet and flexible affair, smaller than a postage stamp and probably placed on the chest. It would monitor such biometric parameters as electrocardiogram (EKG), physical activity, nutritional status, sleep duration, breathing rate, body

http://news.discovery.com/tech/biotechnology/electronic-tattoos-for-baby-and-you-140311.htm



IoT funnel

code

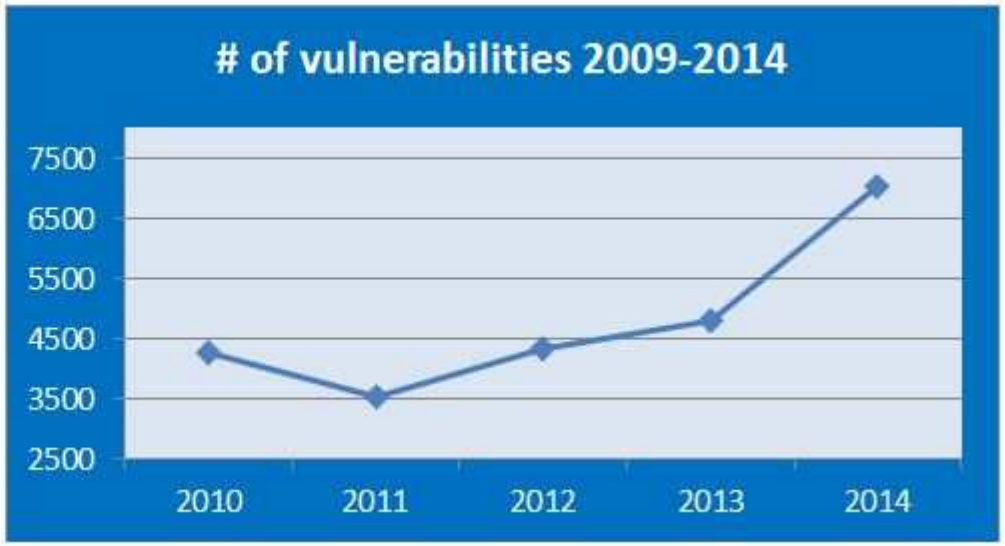
…and…

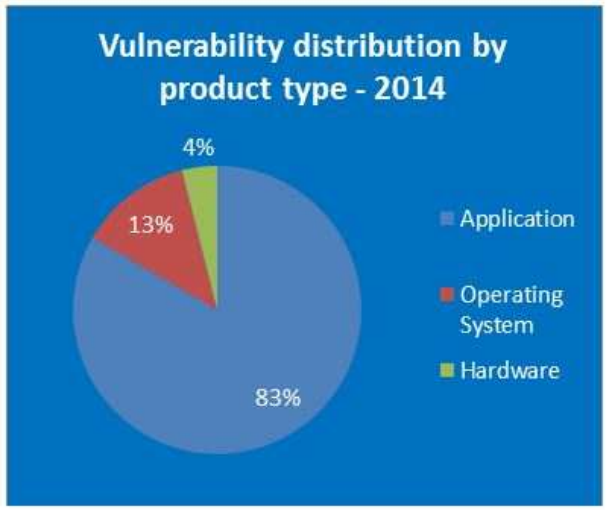
we know that everyone can code

…but, can they code securely?

An average of 19 vulnerabilities per day were reported in 2014, according to the data from the National Vulnerability Database (NVD) - http://nvd.nist.gov/

Year	# of vulnerabilities
2010	4,258
2011	3,532
2012	4,347
2013	4,794
2014	7,038

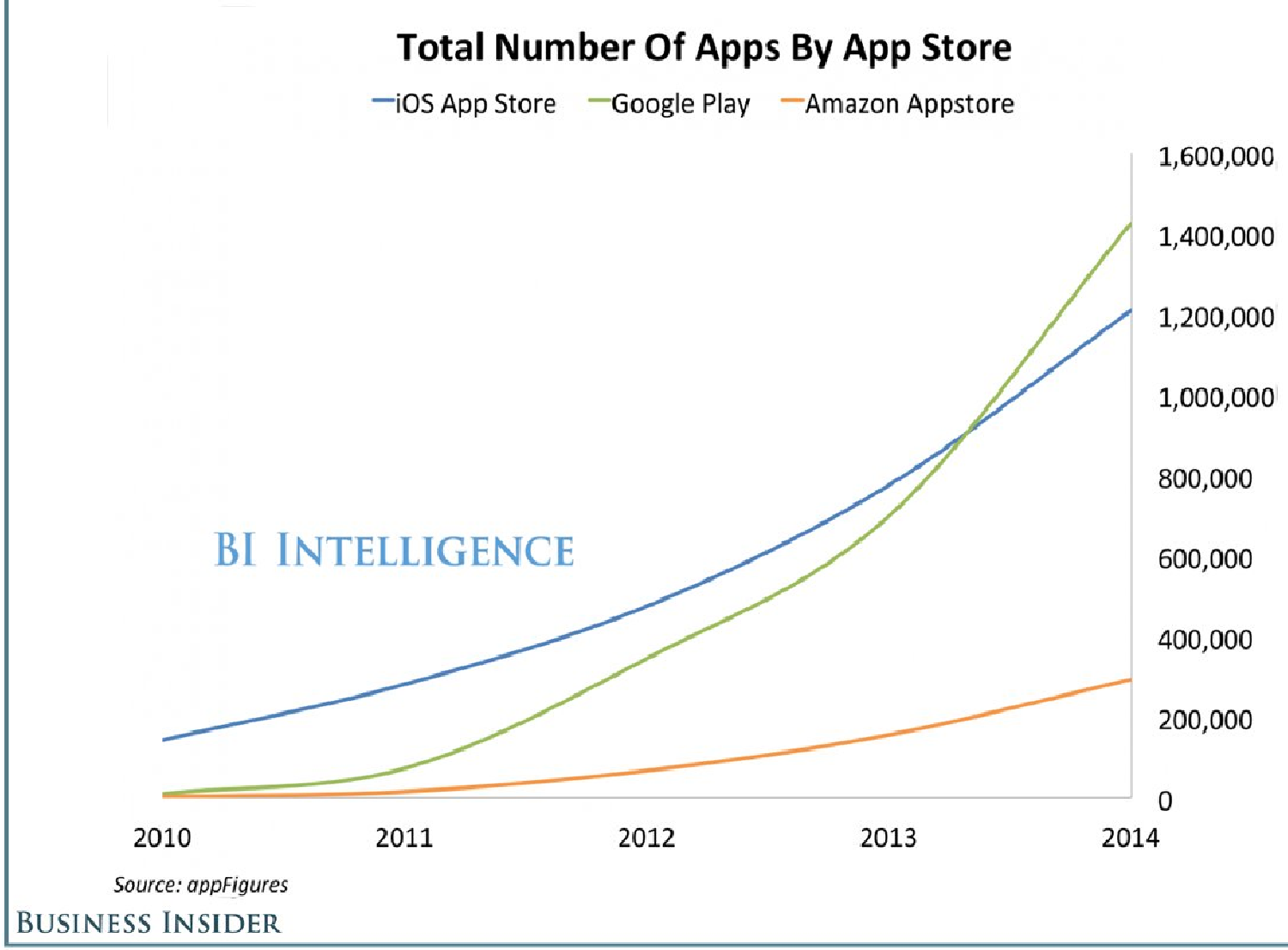




Application	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Microsoft Internet Explorer	242	220	22	0
Google Chrome	124	86	38	0
Mozilla Firefox	117	57	57	3
Adobe Flash Player	76	65	11	0
Oracle Java	104	50	46	8
Mozilla Thunderbird	66	36	29	1
Mozilla Firefox ESR	61	35	25	1
Adobe Air	45	38	7	0
Apple TV	86	29	49	8
Adobe Reader	44	37	7	0
Adobe Acrobat	43	35	8	0
Mozilla SeaMonkey	63	28	34	1

http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/

Tech Chart of the Day



http://uk.businessinsider.com/google-play-vs-apple-app-store-2015-2?r=US

…so…

what can we do?

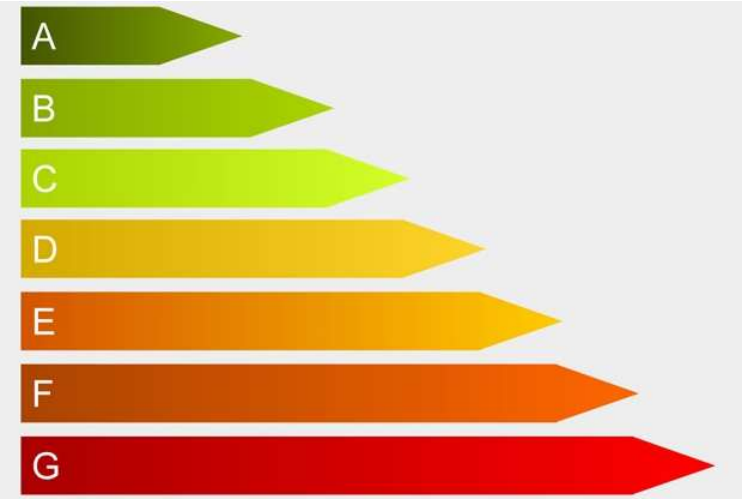
to raise consumer awareness
and improve security using market rules

One way is to promote self assessments

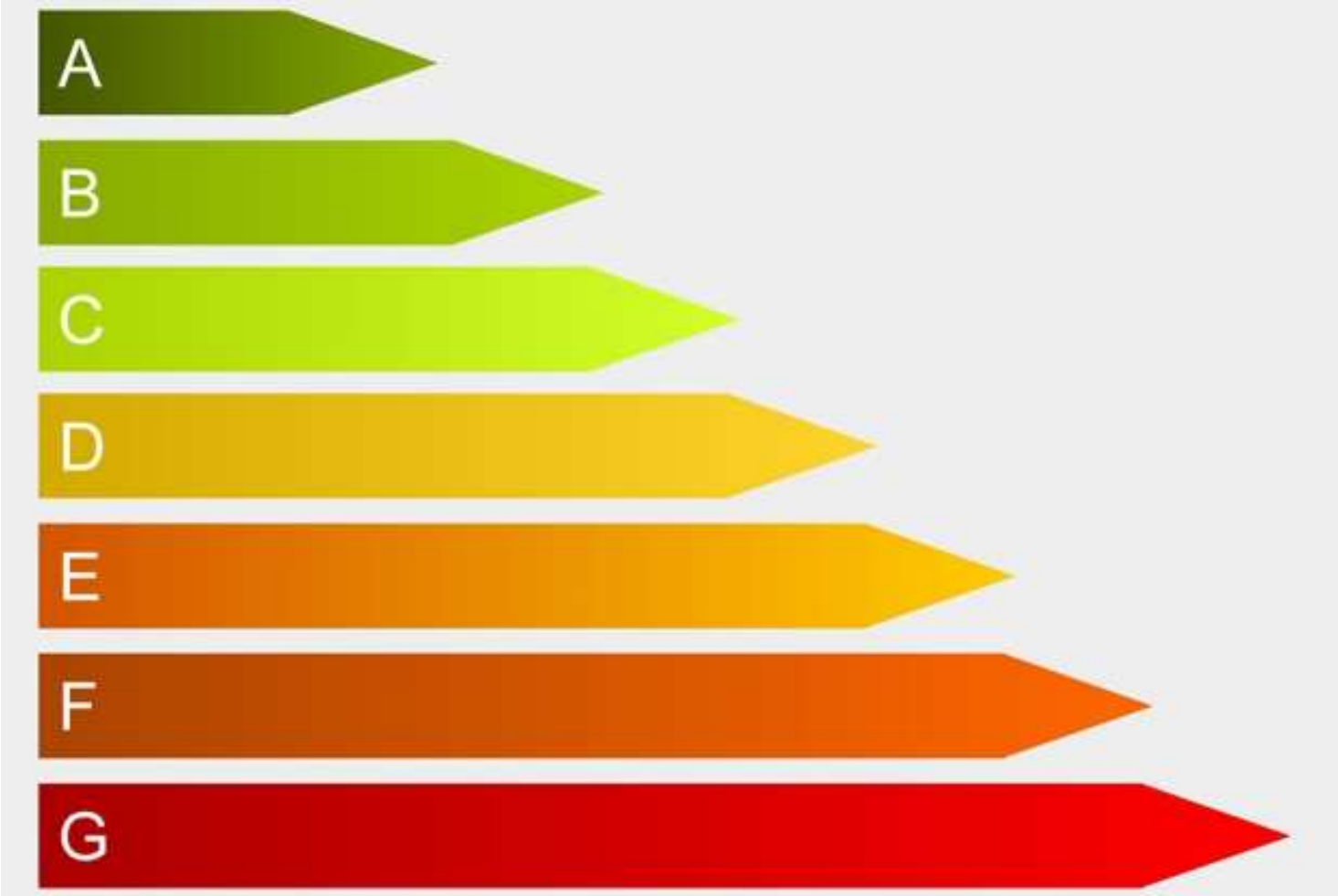
Another is to legislate

<u>Better yet – use both</u>

Energy efficiency



Euro NCAP



Full testing
Existing Controls

No testing
No controls

Not Exaustive
Access Controls
Local vs remote (maintenance / comms, etc.)
Code Testing
ToU transparency
User Agreements Transparency
Score
Cloud
Privacy
Supply chain
Encryption
Resilience
Tampering

This presentation was inspired by:

Building Code for Medical Device Software Security by Tom Haigh e Carl Landwehr
http://cybersecurity.ieee.org/images/files/images/pdf/building-code-for-medica-device-software-security.pdf

I Am The Cavalry

Five Star Automotive Cyber Safety Framework
https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf

Digital Carjackers Show Off New Attacks
by Forbes
1 year ago • 1,450,614 views
A couple of **hackers** show off a series of nasty new attacks on **cars**—with Forbes' Andy Greenberg behind the wheel. "Stomping on ...
HD

https://www.youtube.com/watch?v=oqe6S6m73Zw

Thank you for your time

Questions?

Find us on:

https://ap2si.org

https://facebook.com/ap2si

Find me on:

jorge.pinto@ap2si.org

https://www.linkedin.com/in/jorgepinto