Some thoughts on IoT

Geoff Huston

Chief Scientist, APNIC

Technology

The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it...

- Mark Weiser 1991

Technology

The age of smartphones has left humans with such a short attention spans, even a goldfish can hold a thought for longer" Leon Watson

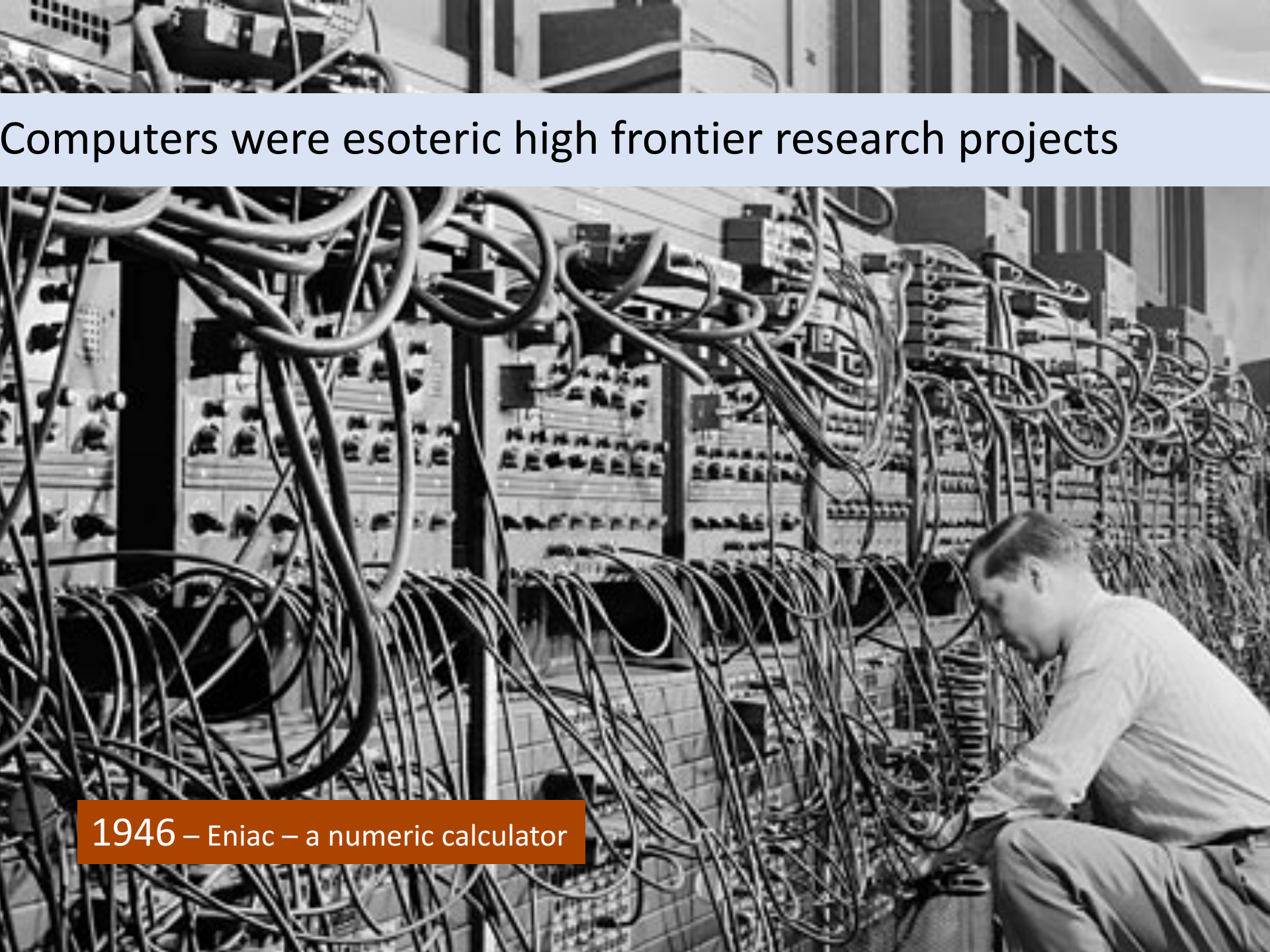
So how should we look at the Internet of Things?

Is this merely a temporary consumer fad, destined to be replaced by the next cool technology item?

Or is this an instance of a profound technology change that redefines our role in our society, and will shape our everyday life for many years to come?

To try and answer this, lets try and put this question into some broader context of the evolution the computer and communications enterprise

Computers were esoteric high frontier research projects




Then they became a “must have” business tool
1964 IBM 360 – commercial computing

Extravagant statements of techno power

1976 CRAY-1 – “super” computing


But there was also the hobbyist market
1976 – Apple-1 “personal” computing

Consumer computers as a statement of design style

From Style to Mass Marketed Luxury Item

2007 – Apple's iPhone

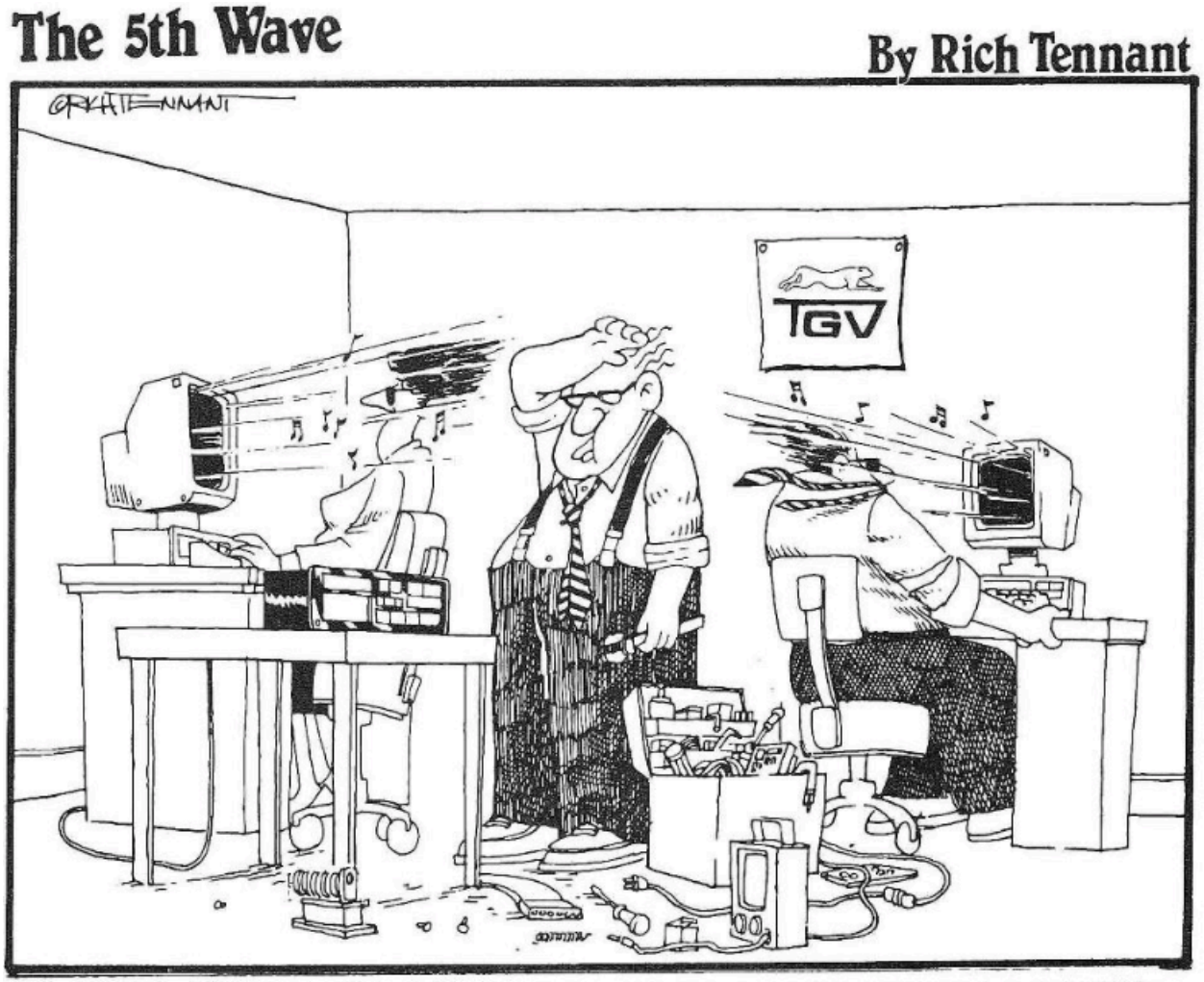

PLACED UPON THE HORIZON (CASTING SHADOWS)
MASSIVE CHANGE
The Future of Global Design
WORLD PREMIERE
October 2, 2004 to January 3, 2005

The Internet is now anywhere and everywhere

Its trivial, commonplace and blends into all our activities

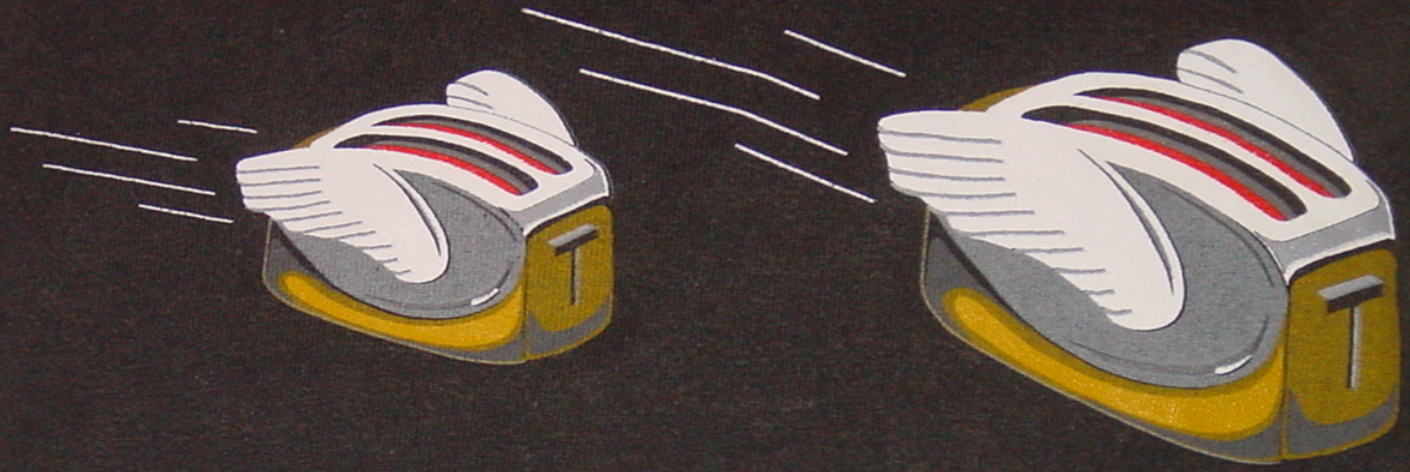

Maybe its about the demise of the “traditional” computer
As dedicated “things” are replacing it

Connecting “things” to the Internet is nothing new



Simon Hackett’s Internet Remote Radio of 1990

Connecting “things” to the Internet is nothing new



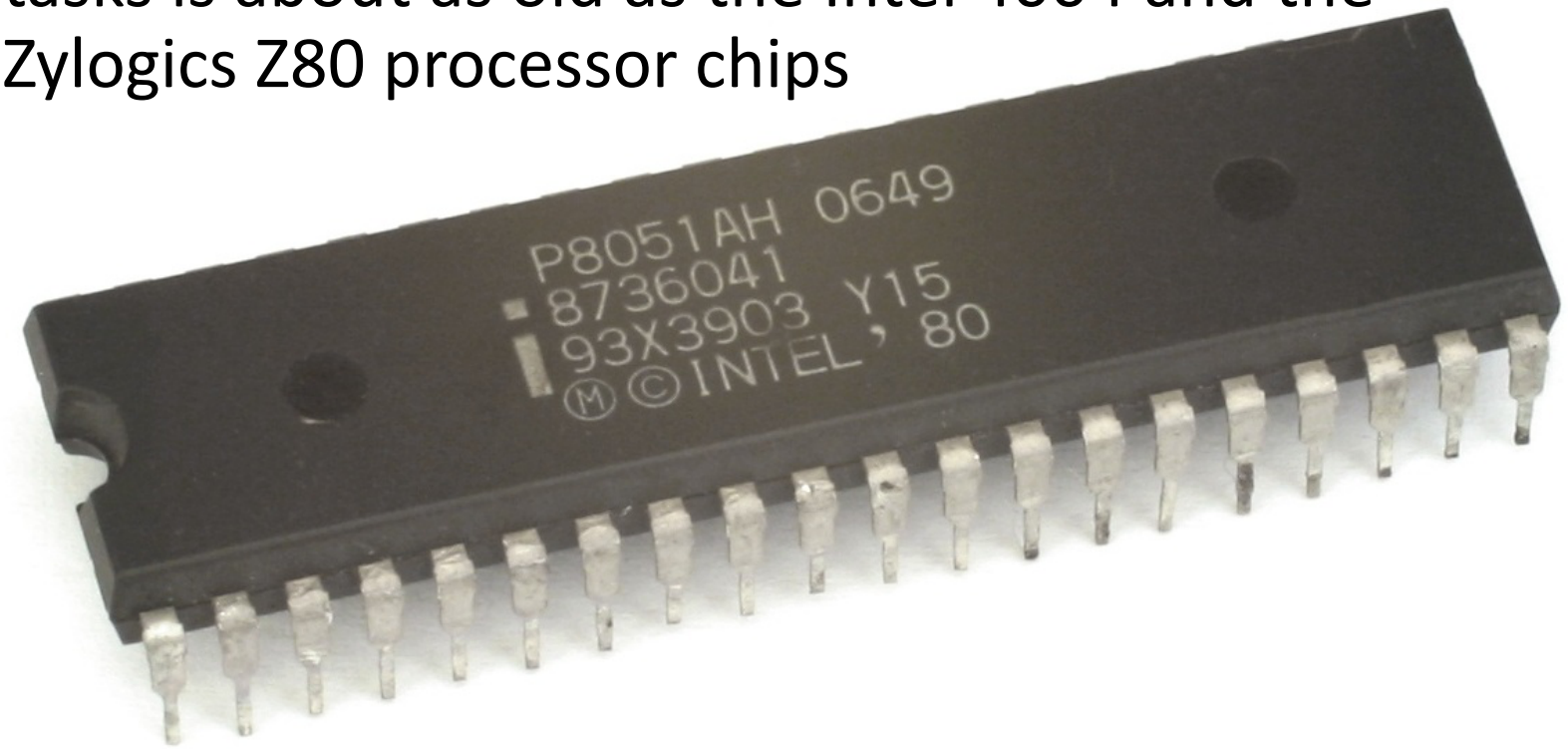
FIRST ANNIVERSARY
TOASTER NET '91

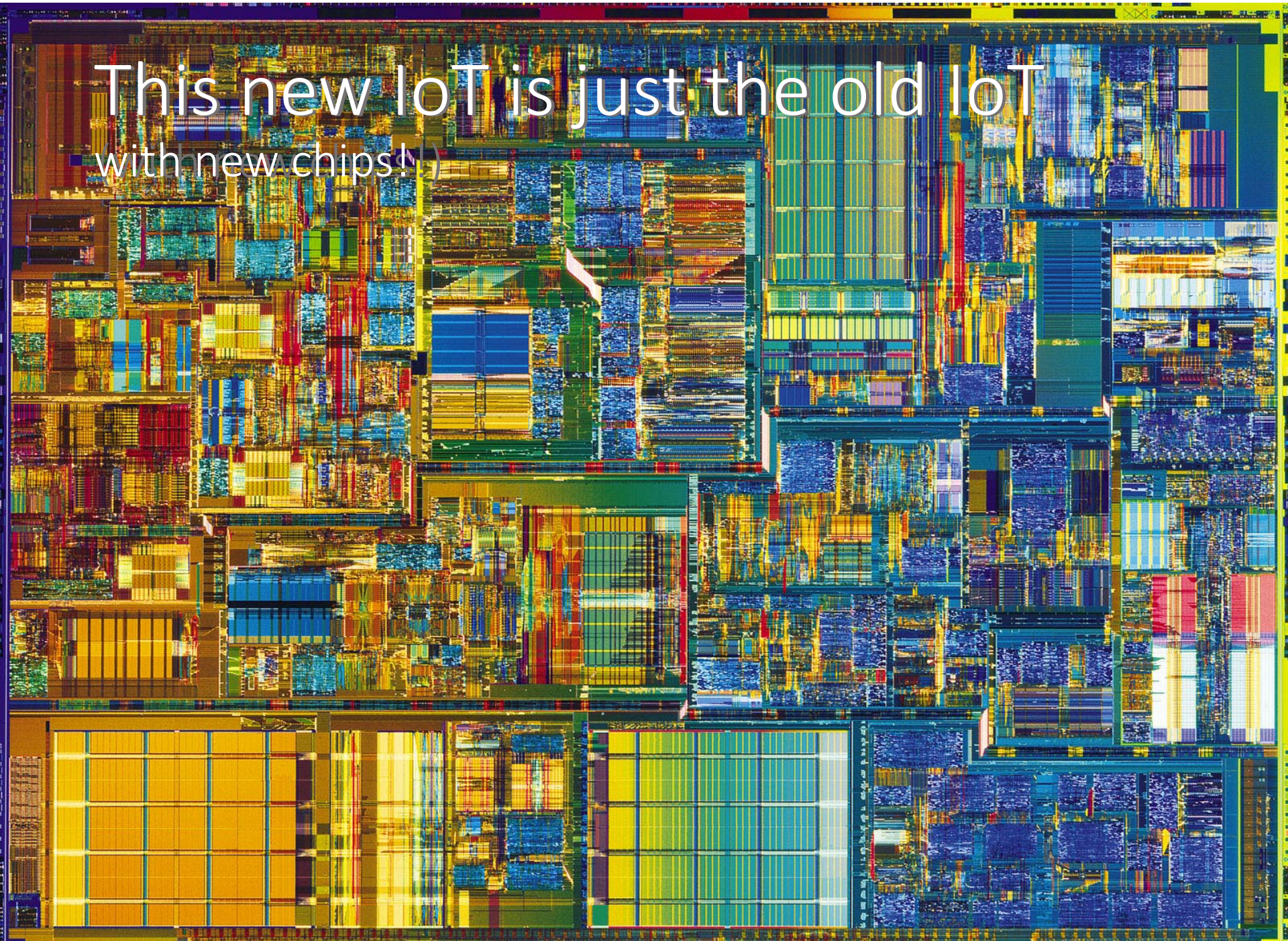
FLYING TOASTERS Artwork © 1991 BERKELEY SYSTEMS, INC.
From AFTER DARK, the Ultimate Screen Saver. Reproduced under
under license agreement by EPILOGUE Technology Corp.

John Romkey’s Internet Toaster – Let them eat Toast!

The “old” IoT

The use of microprocessors to undertake simple tasks is about as old as the Intel 4004 and the Zylogics Z80 processor chips




This new IoT is just the old IoT
with new chips!

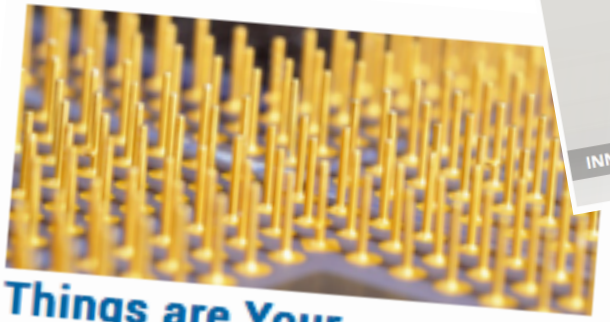
The New IoT is just the Same Old IoT

And we are already living in a processing-dense world:

- A modern car has around 150 – 200 microprocessor-controlled systems, from the windscreen wipers, to the entry system, to engine control and all things in between
- Many / most consumer appliances have all turned to microprocessor control
- Industrial processes, logistics and inventory control, environmental monitoring all use various forms of embedded processing

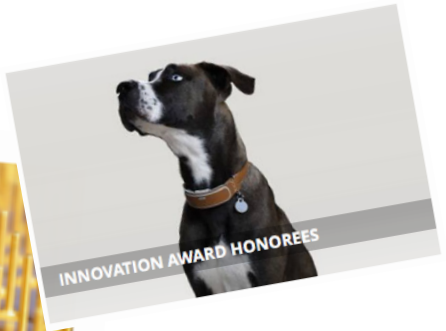
So if this has been going on for years, why is IoT a hot topic today?

The Hype



Things are Your Foundation

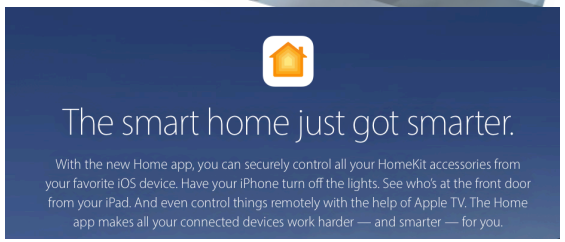
The Internet of Things (IoT) is the heart of the digital business. You need this marriage of operational and information echnology to create a business



Android Auto

The right information for the road ahead

For the third year in a row, the Internet of Things has dominated CES. More than 900 companies out of 3,800 at the show said they had Internet of Things products. Andrew Begin at Mirum observed that the IoT has "caught fire in a big way" and Perry Simpson at Direct Marketing predicted that the IoT will solidify "from marketing dream to full on marketing channel."



The smart home just got smarter.

With the new Home app, you can securely control all your HomeKit accessories from your favorite iOS device. Have your iPhone turn off the lights. See who's at the front door from your iPad. And even control things remotely with the help of Apple TV. The Home app makes all your connected devices work harder — and smarter — for you.

Lego Boost, on display at CES 2017, allows kids to build their own robot.

IoT is …?

- It is a generic term that encompasses a huge variety of application that have little in common other than a propensity to operate in an unmanaged environment
- Its hard to talk about the IoT in anything other than highly generic terms

Why **now**?

Why **now**?

- Low power, high capability silicon now dominates chip fabrication plants
  - Saturation of the smart device market
  - Full stream silicon production volumes requires some form of consumption model

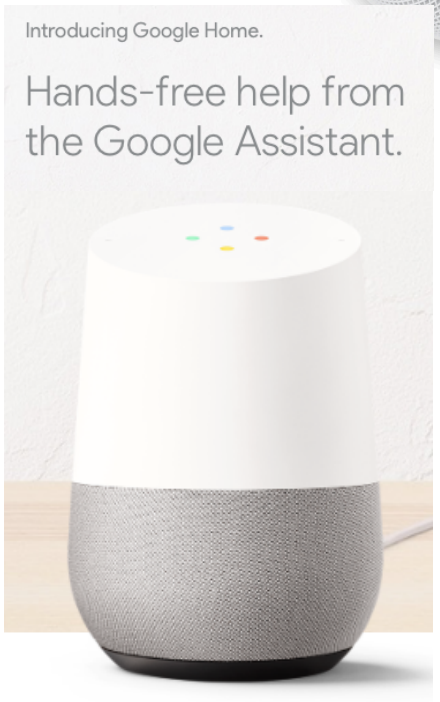
Why **now**?

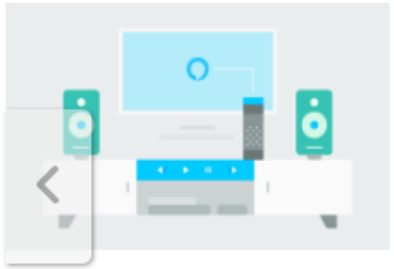
- Low power, high capability silicon now dominates chip fabrication plants
  - Saturation of the smart device market
  - Full stream silicon production volumes requires some form of consumption model

- Radio Technology: RFID, Bluetooth, WiFi, LTE
  - Improvements in AD convertors is providing range and bandwidth to radio systems
  - Protocol development provides ”seamless” connectivity
  - i.e. Passports and Clothing Tags, wireless earbuds, Home controllers and similar

Why **now**?

- Low power, high capability silicon now dominates chip fabrication plants
  - Saturation of the smart device market
  - Full stream silicon production volumes requires some form of consumption model
- Radio Technology: RFID, Bluetooth, WiFi, LTE
  - Improvements in AD convertors is providing range and bandwidth to radio systems
  - Protocol development provides ”seamless” connectivity
  - i.e. Passports and Clothing Tags, Apple earbuds, Home controllers and similar
- Actors seeking new markets
  - 5G for SIMs and wide area mobility
  - Smart phone platform providers seeking to enter the car, home and work environments
  - Industrial and process automation seeking to expand market reach





New in Alexa Smart Home: Entertainment Capabilities

New Device Controls for TVs, AV Receivers and IR Hubs

Why **now**?

- Because we have saturated our traditional markets for technology and the production capacity is being redirected to new opportunities

  - PC sales volumes are plummeting
  - Smartphone sales are now peaking
  - The computer technology industry is seeking to use its existing capability to provide new product to high volume markets
  - Which means looking at low margin very high volume opportunities by adding ”smart” network centric interfaces and controllers to existing devices and functions

The opportunities

- “smart” lighting - e.g. Philips
- “smart” home appliances and networks - e.g. Miele
- “smart” power management
- ”smart” labels for retail
- “smart” traffic control
- “smart” image analysis
- “smart” video surveillance

Almost anything else that uses the word “smart”

The Variety of ~~Life~~ IoT

It's a set of discrete applications that have highly divergent requirements:

- Radius of connectivity varies from mm to kilometers
- Bandwidth varies from bits to gigabits per second
- Data volumes vary from bytes to petabytes
- Connectivity models may be push or pull
- Connectivity may be ad-hoc relays to dedicated wired
- Transactions may be unicast, multicast or anycast in nature
- Applications include sensing and reporting, command and control, adaptation and interfacing

There is little that these environments have in common, except maybe a common underlying gene pool!

The Tyranny of Economics

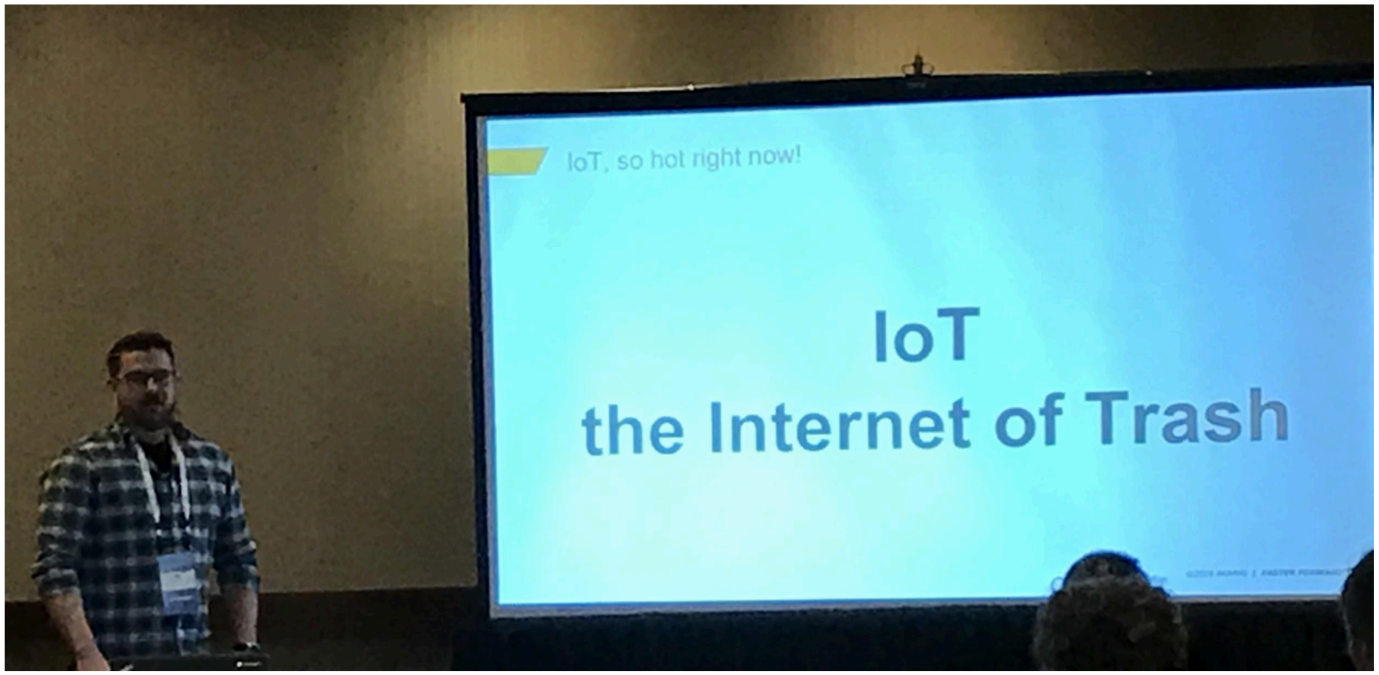
"Things" are meant to be largely autonomous and operate with human intervention and do not command human attention

- Which means that that are not necessarily highly valued devices
- Nor are they continuously human monitored or managed devices
- These are low cost devices
- Which implies that there are not necessarily high quality devices
- Quite the opposite, in fact
- Which means that we simply have to consider…

Security

Seen at NANOG 69…

The S in IoT is for Security.



Security

Interesting quote ...

“At last count I have about 43 devices on my LAN, with less than a third running an OS that I can actually interact with. The rest are embedded systems that get updated (hah!) by the vendors at their whim. Easily two-thirds would 'phone home' to somewhere at various times. About 7 have external access without explicitly setting port-forwarding.

Of course, my router monitors and reports on all outbound traffic - but do I actively look at it? I should. But I don’t. And of course everything we value on our LAN we protect and encrypt end-to-end and at-rest as the LAN is actually occupied by foreign devices with unknown network capability... sure we encrypt absolutely everything...”

An Internet of insanely Stupid Things

We keep on seeing the same stupidity again and again:

- Devices with the telnet port open
- Devices with open DNS resolvers on the WAN side
- Devices with open NTP / SNMP / chargen etc
- Devices with the same preset root password
- Devices using vulnerable libraries that are susceptible to root kit exploitation

An Internet of insanely Stupid Things

We keep on seeing the same stupidity again and again:

- Devices with the telnet port open

Mirai Mirai on the Wall, who's the least secure of them all?

Mirai propagates by bruteforcing telnet servers with a list of 62 horribly insecure default passwords, starting with the infamous admin:admin. Although Mirai could technically infect any box upon successful login, it uses a busybox specific command which causes the infection to fail if busybox is not present. Once inside a box, the malware will attempt to kill and block

https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

insanely An Internet of Stupid Things

We keep on seeing the same stupidity again and again:

- Devices with the telnet port open

Mirai Mirai on the Wall, who's the least s… f them all?

And this simple technique was used to mount a 1 Tbps attack!

Mirai pro… …ecure default … Although Mirai could technically infect any … it uses a busybox specific command which causes the infection to fail if busybox is not present. Once inside a box, the malware will attempt to kill and block

https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

The Internet of Stupid Things

- How do you perform field upgrades of otherwise neglected and unmanaged devices
- What's the economics of incenting field upgrades from the manufacturer?
- Who is responsible for broken "things"?

Who do you call when you're a victim?

- Your ISP?
- Your insurer?
- The police?
- The government?

And what can they do anyway?

Who do you call when you're the attacker?

- The retailer of the shonky equipment?
- The importer?
- The manufacturer?
- The software author?
- The police?
- The government?

A non-terminating blame game

- The problem is that while it is sometimes possible to identify the individual who orchestrated an attack, the underlying issue of the shoddy, poorly maintained, insecure and toxic equipment that populates the Internet simply has no culpability!
- Nobody is clearly “responsible” for creating this common mess

The Internet of Stupid Things

Is this stupidity even avoidable?

- The bleak picture is maybe not!
- In a price sensitive market where system robustness and quality is largely intangible where is the motive to maintain high quality code?
- How can a consumer tell the difference in the quality of the software, in term of its robustness and security of operation?

high clock speed industry + commodity components + low margin = market failure for IoT Security

Privacy

Samsung SMART TV
TV has never been this Smart

Privacy

Not in front of the telly: Warning over 'listening' TV - BBC News

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel | Mo

NEWS

Home | Video | World | Asia | UK | Business | Tech | Science | Magazine | Entertainmen

Technology

Not in front of the telly: Warning over 'listening' TV

9 February 2015 | Technology

Share

Samsung said personal information could be scooped up by the Smart TV

Samsung is warning customers about discussing personal information in front of their smart television set.

The warning applies to TV viewers who control their Samsung Smart TV using its voice activation feature.

When the feature is active, such TV sets "listen" to what is said and may share what they hear with Samsung or third parties, it said.

Privacy campaigners said the technology smacked of the telescreens, in George Orwell's 1984, which spied on citizens.

Samsung SMART TV
TV has never been this Smart

Privacy


CloudPets
Home
How It Works
Getting Started
Support
Buy Now
Jack will love this!
Miss You Kiddo! Be home soon!
Send & Receive Messages You Can Hug™ From Anywhere In The World
1 CloudPets Friends can record and send messages using the CloudPets App from anywhere in the world.
2 A parent or loved one at home gets the message on their CloudPets App and then approves it and delivers it wirelessly to the CloudPet.
3 When the CloudPet has a message, its heart blinks. When your child squeezes its paw, the message plays.
4 Your child can record a message by squeezing the CloudPet's paw. The message goes wirelessly to the nearby device. From there, it can be delivered to a CloudPets Friend anywhere in the world!

Privacy

CloudPets

Home | How It Works | Getting Started | Support | Buy Now

NETWORKWORLD FROM IDG

INSIDER Sign In | Register

Home > Security

Smart teddy bears involved in a contentious data breach

The toy maker experienced a serious data breach, say security researchers, but the company denies that any voice recordings were stolen

By Michael Kan | Follow
U.S. Correspondent, IDG News Service | FEB 27, 2017 6:08 PM PT

Credit: CloudPets

If you own a stuffed animal from CloudPets, then you better change your password to the product. The toys -- which can receive and send voice messages from children and parents -- have been involved in a data breach dealing with more

RELATED


Hacker wiping unprotected MongoDB installs and holding data for ransom


10 biggest hacks of user data in 2016


Witcher dev, XBOX 360 ISO & PSP ISO forums hacked: Over 4.4 million accounts...


VIDEO
Bruce Schneier and the call for "public service technologists"

CIO PERSPECTIVES
March 15, 2017

4 Your child can record a message by squeezing the CloudPet's paw. The message goes wirelessly to the nearby device. From there, it can be delivered to a CloudPets Friend anywhere in the world!

How bad can it get?

- Only five web service providers are big enough to withstand commonplace attacks.
  - And none can withstand a concentrated Tb attack
- The Internet is now so toxic that noone should be exposing their equipment to the net
  - NATs are never going to go
  - Which means that IPv6 is probably doomed
- And lets not kid ourselves that somehow driverless cars will be immune from attack!
- And its just getting worse

It's a tough problem…

A rather bleak prognosis from the Economist in April this year – don't look for technology to improve this rather disturbing situation!

They suggest looking at economics and markets to try and address this problem…

But markets may not help either…

"The market can't fix this because neither the buyer nor the seller cares.

The owners of the webcams and DVRs used in the denial-of-service attacks don't care. Their devices were cheap to buy, they still work, and they don't know any of the victims of the attacks.

The sellers of those devices don't care: They're now selling newer and better models, and the original buyers only cared about price and features.

There is no market solution, because the insecurity is what economists call an externality: It's an effect of the purchasing decision that affects other people. Think of it kind of like invisible pollution."

https://www.schneier.com/blog/archives/2017/02/security_and_th.html

Is this another of those massive challenges of our time?

We just don’t have the tools to figure out how to stop this environment being fatally overrun by these devices:

- We can’t improve their quality
- We can’t keep building ever larger DOS barriers
- We can’t regulate behaviours of the equipment, their makers or distributors

Some things we can't tell yet

- Will we standardize the IoT space or will it continue to be a diverse set of mutually incompatible devices?
- Will the market consolidate to be dominated by a small number of providers and their pseudo-open proprietary architectures?
- When will the IoT embrace IPv6, if ever?
- Will the IoT market ever discriminate on quality and robustness?
- How do we manage the risk of coercion of these devices?

Some things we can't tell yet

- Will we standardize the IoT space or will it continue to be a diverse set of mutually incompatible devices?
- Will the market consolidate and be dominated by a small number of proprietary pseudo-open proprietures?
- Will the IoT embrace IPv6, if ever?
- Will the IoT market ever discriminate on quality and robustness?
- How do we manage the risk of coercion of these devices?

But we can guess!

Some things we can't tell yet

- Will we standardize the IoT space No! continue to be a diverse set of mutually incompatible devices?
- Will the market consolidate to be dominated by a small number of providers and their Unlikely! proprietary architectures?
- When will the IoT embrace IPv6, if Unlikely!
- Will the IoT market ever discriminate Unlikely! robustness?
- How do we manage the risk of coer We can't! devices?

There are some things we can count on…

- The volumes are already huge, and they're growing
  - "Things" already outnumber everything else on the Internet
- Comprehensive security is unachievable
- Privacy is now an historical concept
- Digital pollution is pervasive

We now have an Internet that is a largely chaotic and definitely toxically hostile environment

Why will this get any better?

It wont.

Thanks!