Test Management Forum
26th October 2016.

"IoT Device Testing: can we provide assurance in the new wild west?"

"IoT Assurance – an Oxymoron?"

Test and Verification Solutions

Delivering Tailored Solutions for Hardware Verification and Software Testing

TVS
Test and Verification Solutions

IoT headlines – lack of consumer trust

DATA CENTRE SOFTWARE NETWORKS SECURITY TRANSFORMATION DEVOPS BUSINESS HARDWARE SCIE

Security

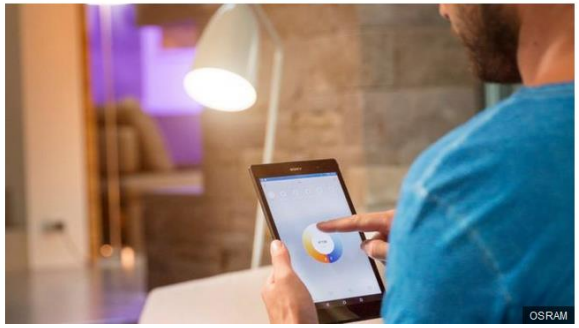
Thanks, IoT vendors: your slack attitude will get regulators moving

Networks also need to grab a mirror and look at themselves

Technology

Osram Lightify light bulbs 'vulnerable to hack'

27 July 2016 | Technology Share



No treat for you: pets miss meals after auto-feeding app PetNet glitches

A server issue has taken down PetNet's automatic feeding system for a number of users, leaving many animals without their scheduled meals

HOME SEARCH The New York Times

STYLE

Nest Thermostat Glitch Leaves Users in the Cold

Disruptions
By NICK BILTON JAN. 13, 2016

The Nest Learning Thermostat is dead to me, literally. Last week, my once-beloved "smart" thermostat suffered from a mysterious software bug that drained its battery and sent our home into a chill in the middle of the night.

Although I had set the thermostat to 70 degrees overnight, my wife and I were woken by a crying baby at 4 a.m. The thermometer in his room read 64 degrees, and the Nest was off.

Nest Smoke Alarm

- **Product -** Nest Protect smoke + CO alarm
- **Desc -** Industrial-grade smoke sensor, can be silenced from your phone, tests itself automatically and lasts for up to 10 years. It also tells you what's wrong and even alert your phone.

- **Connectivity Requirements:**
  - Wi-Fi connection
  - Free Nest account
  - Phone or tablet with iOS 8 or later, or Android 4 or later

Example - IoT issues

HOME SEARCH The New York Times

STYLE

Nest Thermostat Glitch Leaves Users in the Cold

Disruptions
By NICK BILTON JAN. 13, 2016

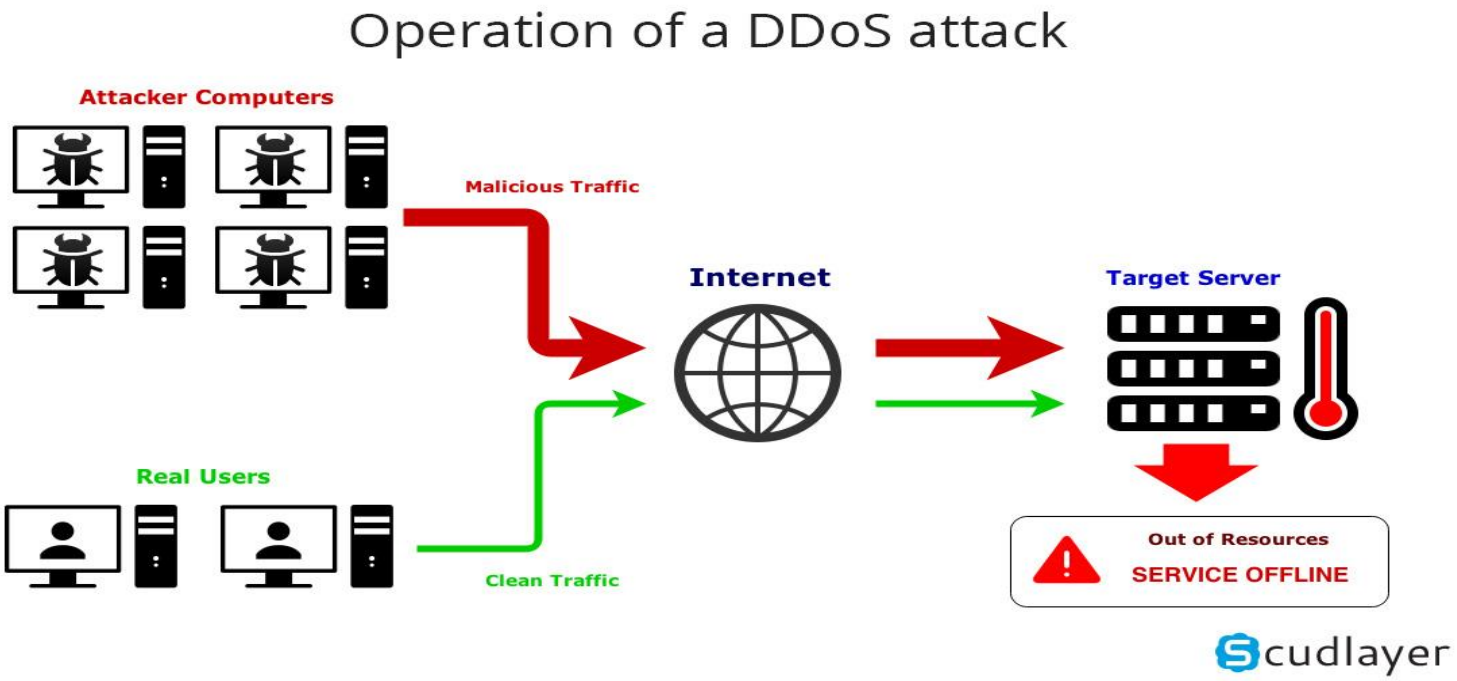
The Nest Learning Thermostat is dead to me, literally. Last week, my once-beloved "smart" thermostat suffered from a mysterious software bug that drained its battery and sent our home into a chill in the middle of the night.

Although I had set the thermostat to 70 degrees overnight, my wife and I were woken by a crying baby at 4 a.m. The thermometer in his room read 64 degrees, and the Nest was off.

- (1) Nest Protect smoke alarm fault in 2014. The alarm could be deactivated by waving at the device putting it into sleep mode.
  - Fix – users had to disable wave gesture feature, and a patch was made available via wifi.
- (2) Nest home thermostat recent fault meant the heating would deactivate and could not be turned back on.
  - Fix – a manual reset or 9 step procedure.
- (3) Nest Cam and Dropcam frequent outages on service for live home streaming – potential baby monitoring.
  - Fix – no fix yet, was a service outage on the live video streams.

What is a DDoS on DNS Services?

- DDoS = Distributed Denial of Service
- DNS = Domain Name System: translates website names into Internet Protocol (IP) addresses, and locate resources on the Internet.



Botnet DNS attack

- Hackers hijacked millions of IoT devices
- Sent vast amounts of junk traffic at DNS services operated by US company Dyn
- Popular websites inaccessible.

NETFLIX twitter airbnb

The Register®
Biting the hand that feeds IT

Two things are clear, however: the freewheeling idiots of the Internet of Things business need the fear of regulation put into them – and so do network owners and operators.

Emergent Tech ▸ Internet of Things

Today the web was broken by countless hacked devices – your 60-second summary

IoT gadgets behind tens of millions of IP addresses flooded DNS biz Dyn

21 Oct 2016 at 21:45, Chris Williams 157

Updated Today a vast army of hijacked internet-connected devices – from security cameras and video recorders to home routers – turned on their owners and broke a big chunk of the web.

Compromised machines, following orders from as-yet unknown masterminds, threw massive amounts of junk traffic at servers operated by US-based Dyn, which provides DNS services for websites large and small.

The result: big names including GitHub, Twitter, Reddit, Netflix, AirBnb and so on, were among hundreds of websites rendered inaccessible to millions of people around the world for several hours today.

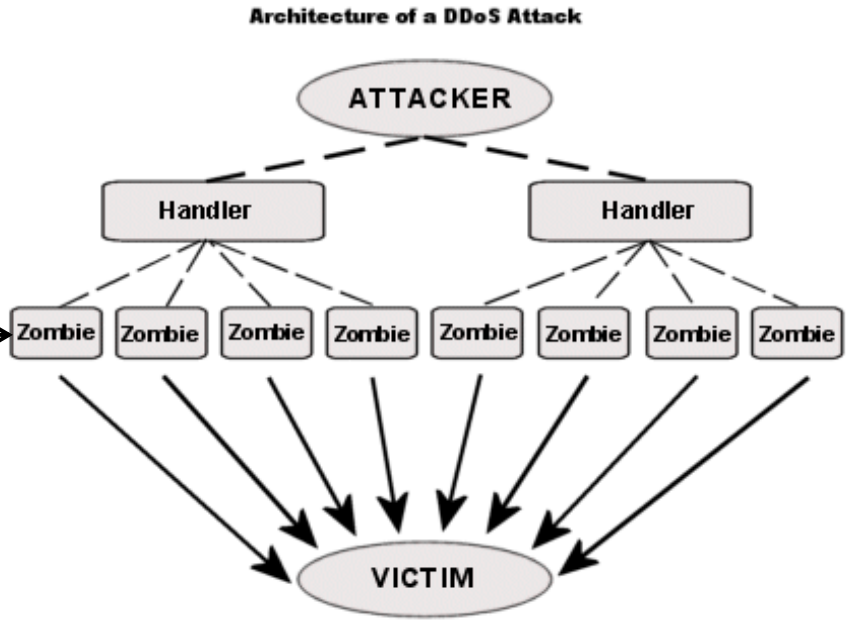
We're told gadgets behind tens of millions of IP addresses were press-ganged into shattering the internet – a lot of them running the Mirai malware, the source code to which is now public so anyone can wield it against targets.

Dyn tells us its services are coming back online after seeing out the storm and putting up new

Technical Details

- **Mirai is malware that turns computer systems running Linux into remotely controlled "botnets"**
  - It primarily targets online consumer devices such as remote cameras and home routers
- **Mirai spreads by logging into devices using their default, factory-set passwords**
  - Mirai takes over routers, CCTV cameras, digital video recorders, etc.

Zombie = IoT device running Mirai malware



Why are IoT devices so vulnerable?

Connected devices create an increased level of intrusion, generating new types and unprecedented quantities of data, raising potential quality and security issues.

Connectivity standards

onem2m	Open Interconnection Consortium	Wireless IoT forum
IETF	ZigBee Alliance	Industrial Internet Consortium
ITU	AllSeen Alliance	GSMA
IEEE	AllJoyn	Thread

Security

- Most IoT products have security measures that are 10 years out of date
- HP: 70% of the IoT devices and sensors examined were susceptible to the vulnerabilities in the OWASP IoT Top 10

Quality Assurance

- Nest home thermostat had a fault where the heating would deactivate and not be turned back on
- Petnet smart pet feeder recent incident saw a third-party server service failure, causing pet feeds to be missed.

Testing challenges – mass interoperability

- Many Communication protocols:
  - Mobile
  - Wifi
  - Bluetooth
  - Zigbee
  - Z-Wave
  - 6LowPAN
  - Thread
  - NFC
- Simulate wide range of Networking conditions:
  - RF testing
  - cell handovers
  - low signal strength
  - protocol analysis
  - moving between 2G, 3G & LTE or wifi

- Test scenarios to consider:
  - Moving between networks
  - Losing power on upgrade
  - Low bandwidth
  - Simulate signal loss (going through a tunnel)
  - Patching the device

Communication protocols - scenarios

1	Device registers to network and data connection is successfully established
2	Verify the data transferred from device to IoT platform.
3	IoT device can transfer/move between network connection types (if applicable.)
4	Device Application “stores and forwards” data to minimise the number of network connections made by the device.
5	IoT Device Application uses dynamic polling intervals.
6	Check IoT Device Application behaviour in situations when network communication requests fail
7	Check IoT Device Application reports power failure
8	Check IoT Device Application’s use of “off-peak’ communication
9	Check behaviour of IoT Device Application when resetting the Communications Module after any communication failures or error conditions
10	Upgrade testing – verify post upgrade the comms unit is functioning correctly
11	Check the IoT Communications Module does not send unsolicited messages
12	Check the IoT Communications Module sends only a AAAA DNS Query. IPV6

Security testing – OWASP TOP 10

1.) Insecure web interface
2.) Insufficient authentication/authorization
3.) Insecure network services
4.) Lack of transport encryption
5.) Privacy concerns
6.) Insecure cloud interface
7.) Insecure mobile interface
8.) Insufficient security configurability
9.) Insecure software/firmware
10.) Poor physical security

IoT - Ongoing patching & maintenance

- IoT devices require ongoing functionality & security updates
- But patching IoT devices is not easy
  - It gives another route to install malware
  - IoT devices have limited resources (CPU, memory, encryption, etc)
  - Functional issues (e.g. losing power during a patch can “brick” a device)
- Who is responsible?
  - Manufacturers? Consumers?
  - Who is going to pay for a lifetime patching warranty for their pet feeder?

NMI - IoTSF

- September 2015 NMI launched the Internet of Things Security Foundation (IoTSF), a non-profit organisation established to drive security excellence.
- Collaborative, vendor-neutral and international initiative; the IoTSF is a dedicated expert resource to drive security excellence by sharing knowledge, best practice and advice.
- 5 working groups:
  - **1: Self-Certification Scheme**
  - **2: Connected Consumer Products**
  - **3: Patching Constrained Devices**
  - **4: Framework for Vulnerability Disclosure**
  - **5: IoT Security Landscape**

Standards bodies – building TRUST

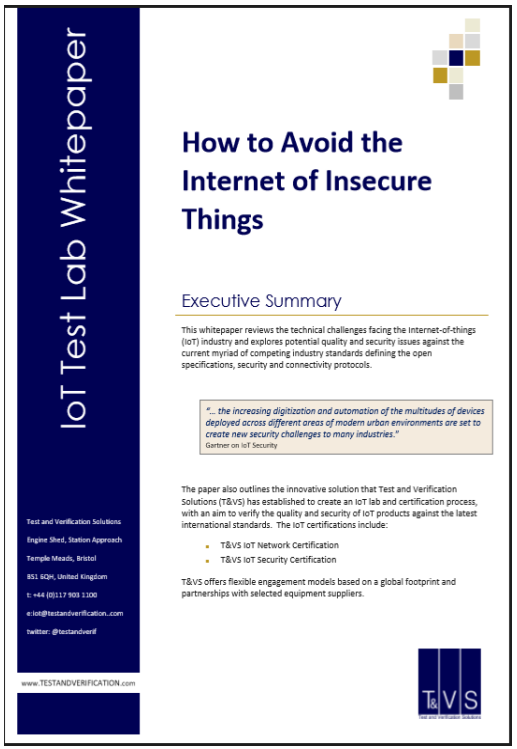
- **The BSI (British Standards Institute) attempts to build TRUST with consumers**
  - Can we build standards that guarantee some level of confidence
- **Do we need different levels of confidence?**
  - Autonomous car vs. smoke detector vs. pet feeder
  - In safety systems we start with a hazard analysis
    - From that we can set an integrity level
    - And that implies different levels of development practises
- **The NMI prefers levels of sign off**
  - Self- certification
  - External certification
  - Independent certification
  - Full certification against industry standards

IoT Kitemark Model

	IoT Network connectivity – (1)	IoT End 2 end security – (2)
Purpose	ensure IoT solutions verified against a wide range of networking connection / connectivity protocols	ensure IoT solutions verified against a wide range of security conditions and scenarios
Standards	• GSMA IoT connection efficiency guidelines • onem2m connection standards	• GSMA IoT security standards • Onem2m security standards • OWASP Internet of Things Top 10 • Online Trust Alliance's IoT Trust Framework
Example scenarios	1.) minimize the number of network connections. 2.) cope with variances in network data speed and latency considering 3.) communication requests fail. 4.) Communication retry mechanisms implemented verified.	1.) Authentication / authorisation eg interfaces disallows weak passwords. 2.) Encryption model eg HTTPS. 3.) Cloud interface has account lockout 4.) Software / firmware. Eg Ensure all devices operate with a minimal number of network ports active.

Summary

- Increased regulation
- Focus on QA & security
- IoT ongoing maintenance
- IoT Kitemark model
- Rebuild consumer trust



Unless these issues are addressed the only winners in the IoT wild west will be the hackers.

Discussion - the Test Management Forum
on 26th October 2016.

Thank you

"IoT Device Testing: can we provide assurance in the new wild west?"

Test and Verification Solutions

Delivering Tailored Solutions for Hardware Verification and Software Testing

TVS
Test and Verification Solutions