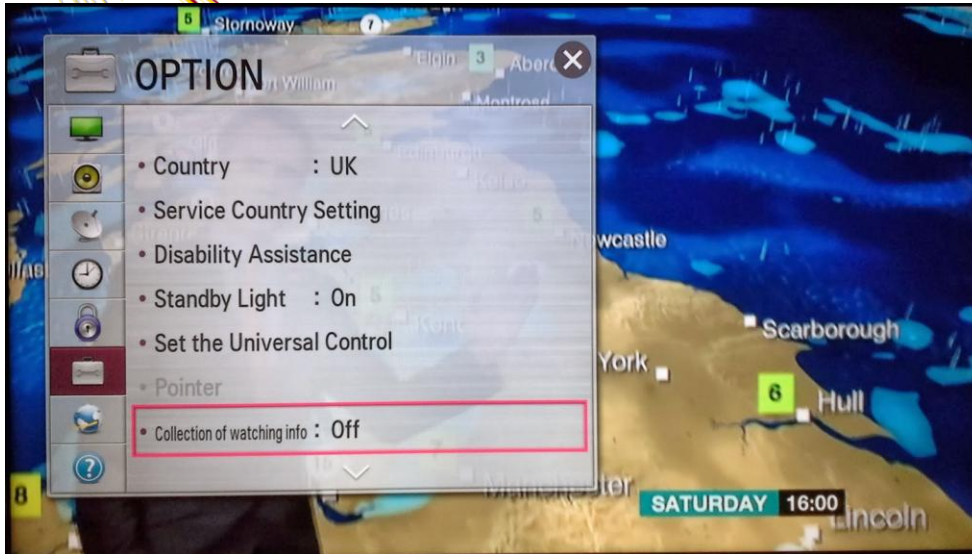


# IoT and CyberSecurity

Derek McAuley  
19<sup>th</sup> September 2014

# Not a day goes by



Content-Type: application/x-www-form-urlencoded  
&chan\_name=BBC TWO  
&device\_src\_idx=1  
&dtv\_standard\_type=2  
&broadcast\_type=2  
&device\_platform\_name=NETCAST  
4.0\_mtk5398&chan\_code=251533454-72E0D0FB0A8A4C70E4E2D829523CA235  
&external\_input\_name=Antenna  
&chan\_phy\_no=47  
&atsc\_chan\_maj\_no=2  
&atsc\_chan\_min\_no=2  
&chan\_src\_idx=1&  
dvb\_chan\_nw\_id=9018  
&dvb\_chan\_transf\_id=4170  
&dvb\_chan\_svc\_id=4287  
&watch\_dvc\_logging=0



## SECURITY

### Google leaves STUPID vuln on Nest devices

**Security? But this is the Internet of Things!**

By Richard Chirgwin, 12 Aug 2014 [Follow](#) 2,637 followers

39 [Hadoop in the cloud and Big Data analytics](#)

Google's Nest thermostat, poster-child for its Internet of Things ambitions and data collector of your home habits, gives root access to anyone with a USB drive and a quarter-minute to spare.

**RELATED STORIES**

IoT: Industry snakeoil or one-way ticket to fame and riches?  
It's WAR: Internet of Stuff firms butt heads over talking-fridge tech standards  
**Sysadmin blog**  
Hey, big spender. Are you as secure as a whitebox vendor?  
Internet of Stuff my Pockets: Investors plough 1 BEELLION dollars into IoT  
Google Nest, ARM, Samsung pull out Thread to strangle ZigBee

That's the conclusion that Yier Jin, Grant Hernandez and Daniel Buentello have come to, and told the world in their presentation to BlackHat (abstract [here](#)).

While their attack – can it be called an attack when it's so trivial? – needs physical access to the devices for "ten to 15 seconds", it's very straightforward: press and hold the power button, insert a USB drive, and Nest enters a developer mode.

In the usual you-can't-be-serious cavalier attitude of home automation vendors, Jin's demonstration attack creates a rooted device and bypasses firmware signing.

This, they write, "allows us to backdoor the Nest software in any way we choose ... Loading a custom kernel into the system also shows how we have obtained total control of the device".

And since Nest uses Internet connections to talk to The Chocolate Factory, the same connection can be reprogrammed to report when the owner is home and when they're away, and data like Wifi credentials are available to the attackers.

There's also a real potential for a dodgy operator to buy bulk Nests, interfere with them, and resell them to unsuspecting punters.

It seems to *The Register* a good idea for people to block Nest at their firewall. ©

[Hadoop in the cloud and Big Data analytics](#)

# A new threat?

## Short Paper: Extrapolation and Prediction of User Behaviour from Wireless Home Automation Communication

Oxford, August 2014

Frederik Möllers\*, Sebastian Seitz, Andreas Hellmann<sup>†</sup> and Christoph Sorge\*  
\*Saarland University

\*{frederik.moellers|christoph.sorge}@uni-saarland.de, <sup>†</sup>kontakt@anhellmann.de

North Sea, August 1914

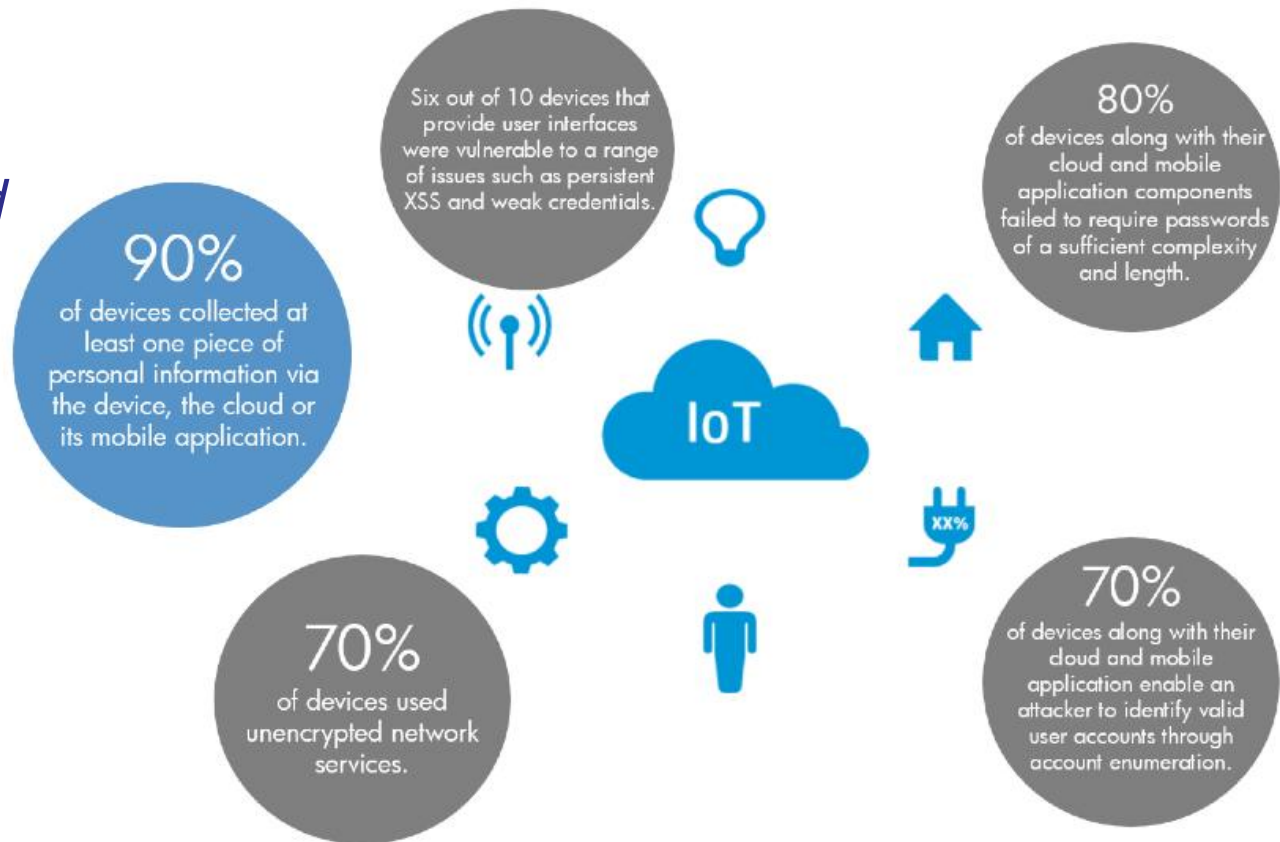


“I always knew there was some sort of crisis going on in the West Wing after hours when I saw the arrival of pizzas,”

CNN’s Wolf Blitzer 1990

# State of play

*"80% of devices raised privacy concerns"*



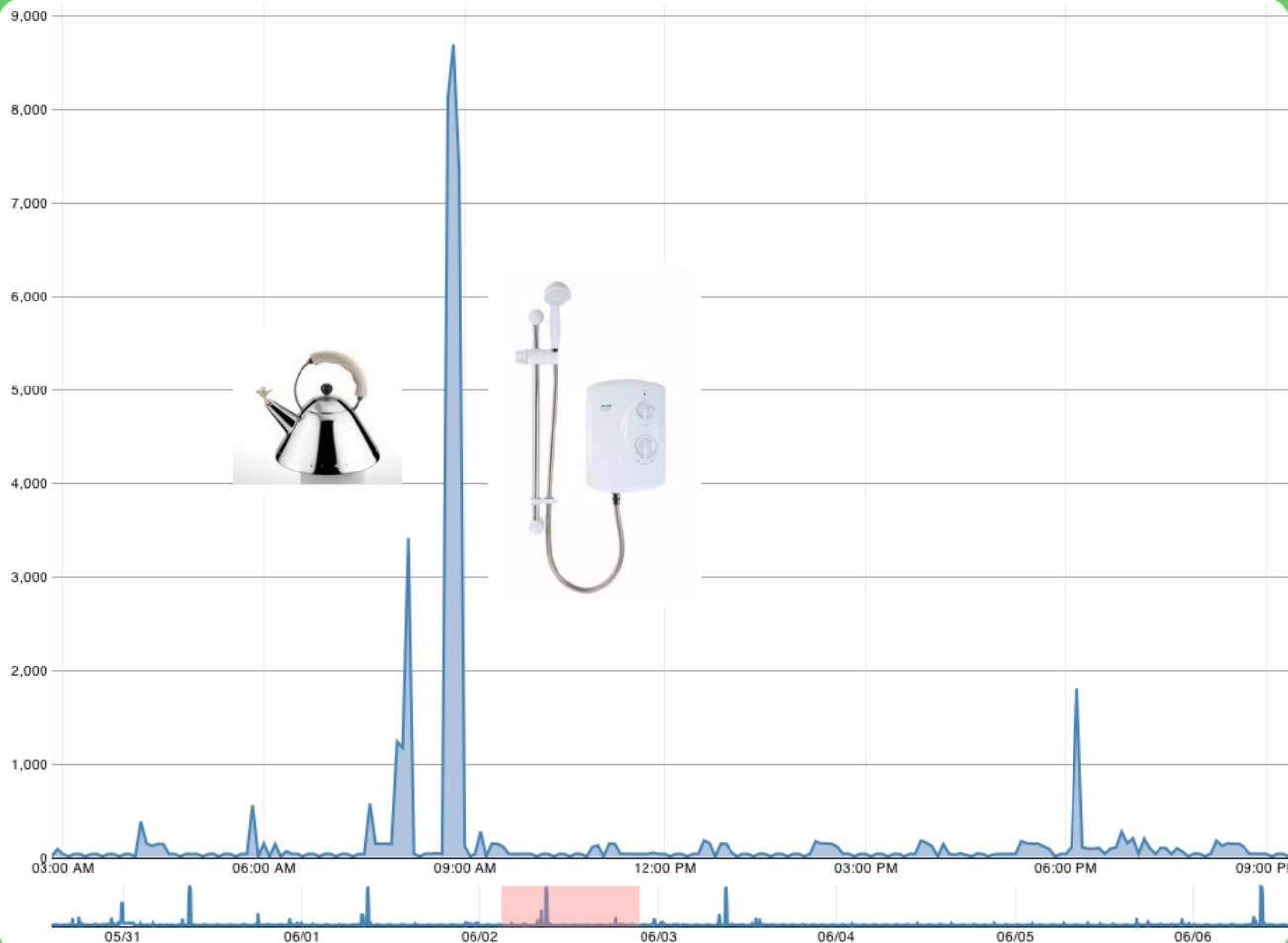
HP "Internet of Things Security Study", July 2014

# Privacy and smart meters

## Detailed data

These graphs show detailed data for your chosen hub/sensor. The **upper larger graph** gives a detailed view of energy use in a particular time window; the **lower smaller graph** gives a less detailed view of *all* energy use since the hub/sensor was commissioned. Drag the pink shaded area in the lower smaller graph to shift the time window, or click and drag elsewhere within the lower graph to create a new time window. [View stacked data](#) [View live data](#)

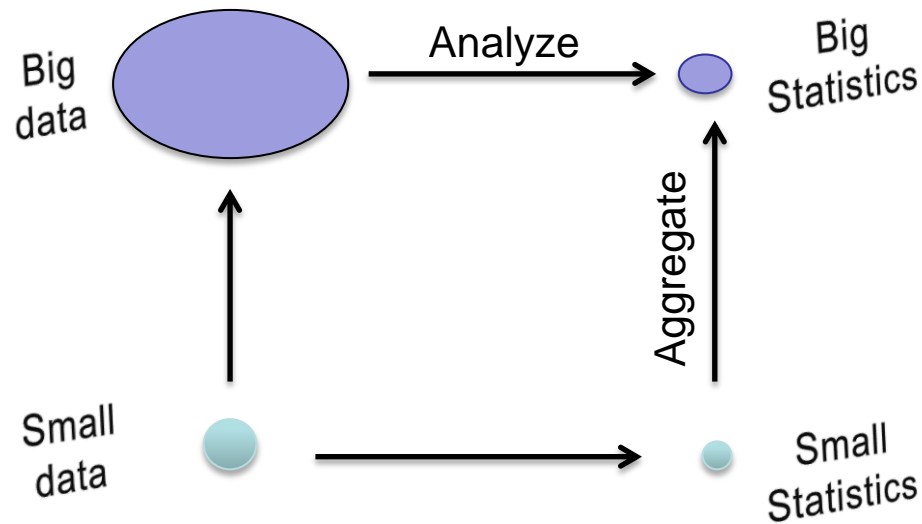
[Back to the energy monitor network](#)



Rollout  
across UK  
by 2020

# Cyber-security in the "small"

- Do you need all your data in one place at one time?
  - may be costly
  - may be difficult
  - may be a risk...



# In the large

Synchronized attacks  
Systematic compromise



## BUSINESS REPORTER

DISTRIBUTED WITH *The Daily Telegraph* | *The Sunday Telegraph*

Management Columnists Investment Technology Sustainability Print Edition

### Turning off the power: Smart grids and smart cyber attacks

21 February 2014 • By [Dave Baxter](#)

With smart systems comes the risk of smart cyber-attacks. **Dave Baxter reports.**



Britain risks “anarchy and chaos” if it fails to defend its smart systems from cyber attacks, according to a security specialist.

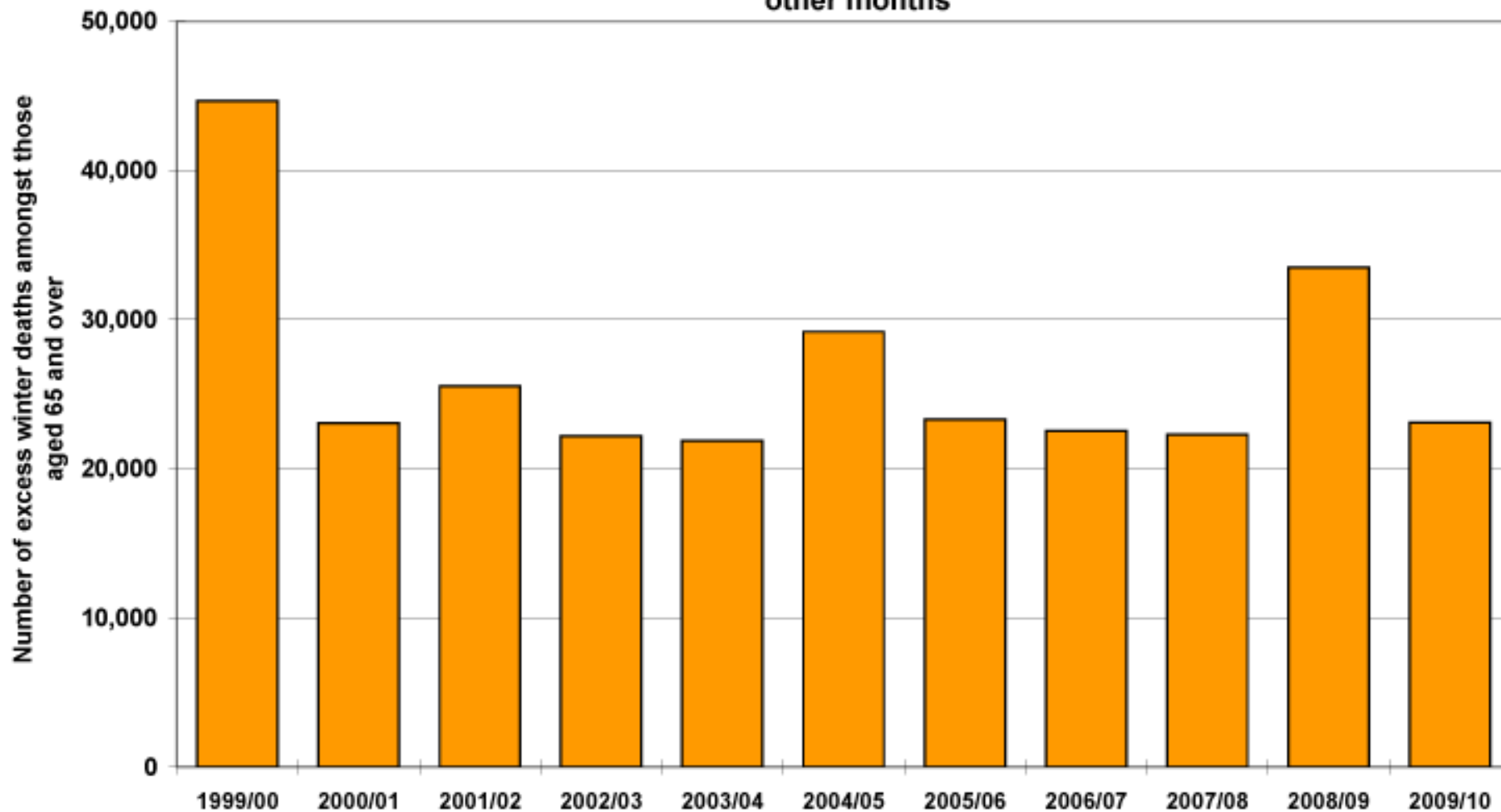
Chris McIntosh, CEO at ViaSat UK, says that without high-grade defences to protect them, devices such as smart meters remain prone to hacking from remote locations. To combat fraud or abuse, energy companies could use smart meters to remotely shut off customers from the energy grid. But this function could also be put to more malicious use by hackers.

McIntosh warns that with an interconnected smart grid system, an attack could quickly spread across an entire network of devices,

playing havoc with power stations and other critical infrastructure.

# Vulnerable populations

Each year around 20,000 more people aged 65 or over die in winter months than in other months

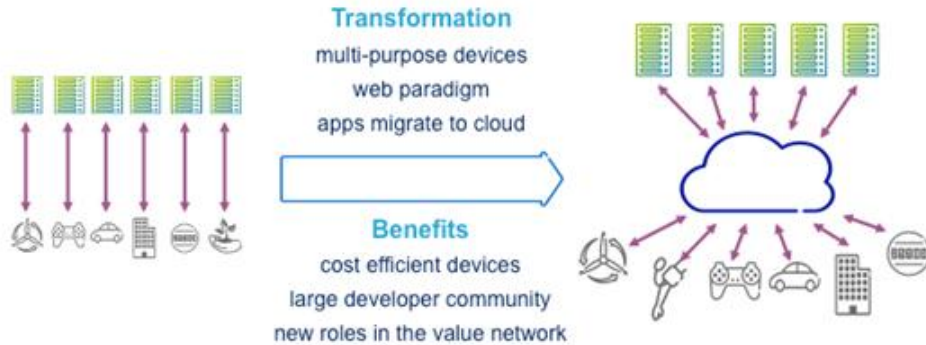


Source: ONS mortality data; England & Wales; updated Dec 2010





# Little fluffy clouds



“apps migrate to cloud”

- Massive attack surface
  - No auditability
  - No consumer perspective
  - Lack of any rational compartmentalization
- ... no thought to overall IoT security architecture.

## ARM rails against 'internet of silos' with new UK forum

Wants chips with everything

By Patrick Goss July 26th 2012

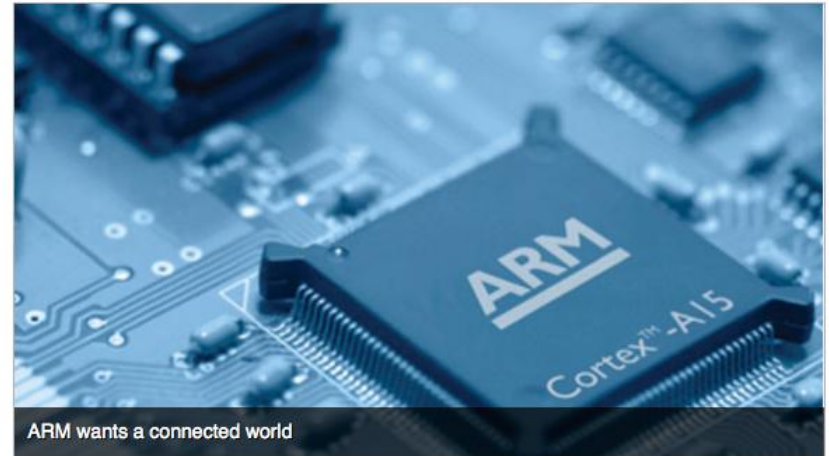
COMMENTS

f SHARE

TWEET

g+ SHARE

EMAIL





It's an integrated computer network, and I will not have it aboard this ship.

# DSM acceptability

1. Appliances automatically turning off when left on standby



2. Shower turning off after a set period of time, manual override possible



3. Setting washing machine to wash clothes before a certain time



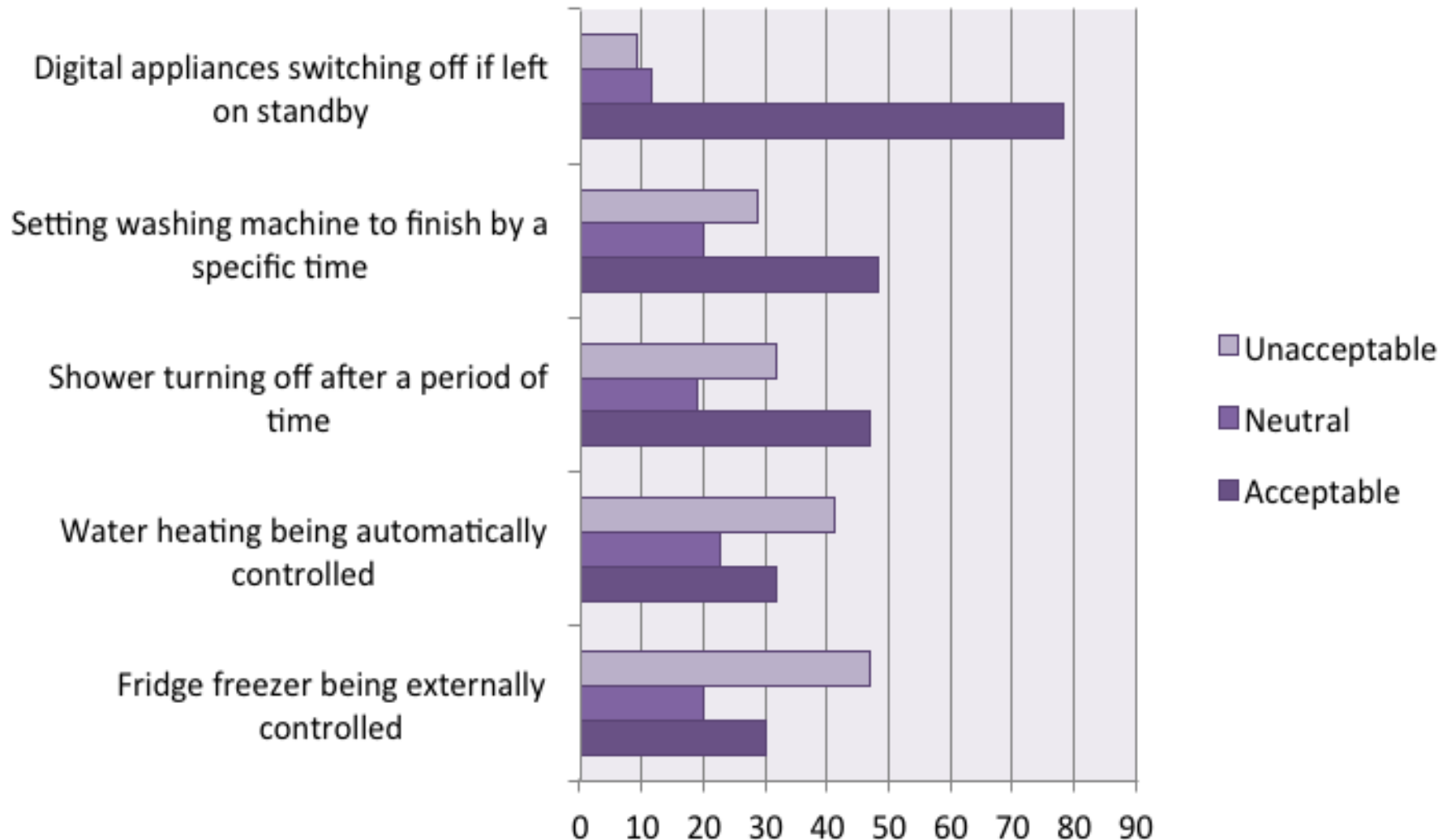
4. Allowing fridge-freezers to be switched off for short periods



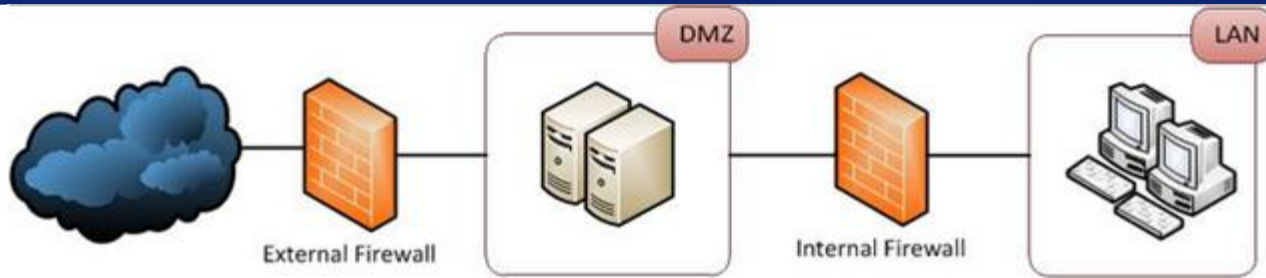
5. Having optimum time to heat water determined by network operator



# DSM Acceptance



# More old ideas...

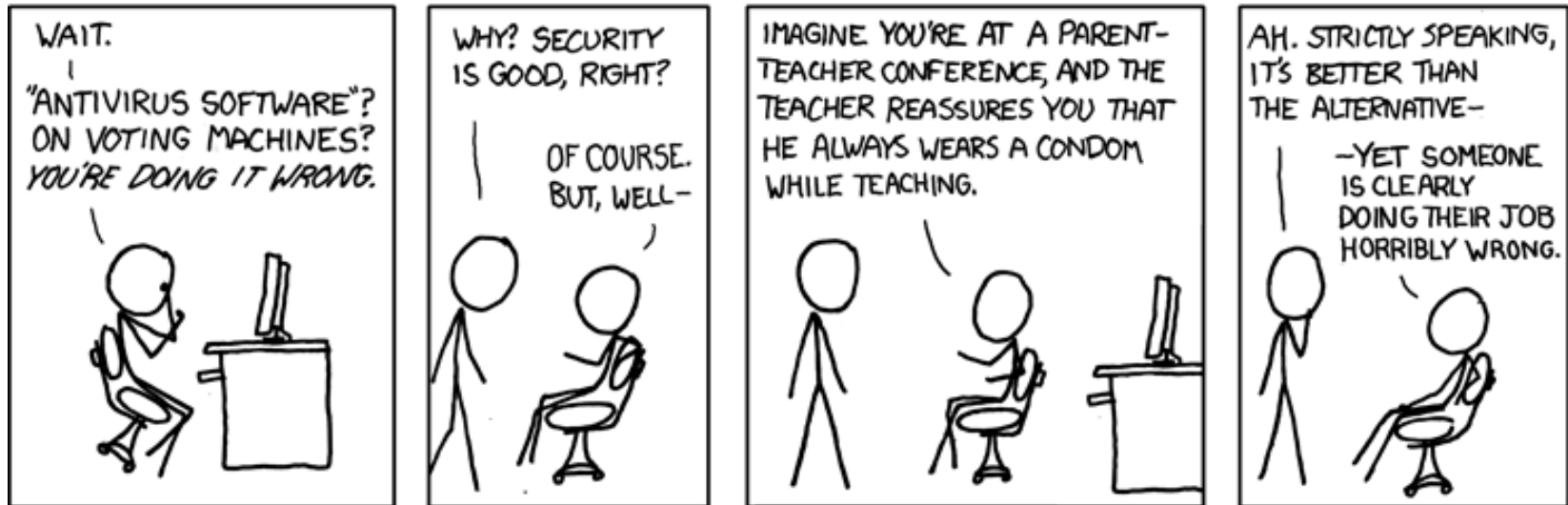


What is shared or accessible outside the home is limited, logged and on a need to know basis

Sensitive data is used within the home and shared with personal devices only using secure channels



PREMIER ELECTION SOLUTIONS (FORMERLY DIEBOLD)  
HAS BLAMED OHIO VOTING MACHINE ERRORS ON PROBLEMS  
WITH THE MACHINES' MCAFEE ANTIVIRUS SOFTWARE.



Questions?

[derek.mcauley@nottingham.ac.uk](mailto:derek.mcauley@nottingham.ac.uk)