Smart Vulnerabilities:

Some cybersecurity issues of Smart Buildings, not-so-Smart Cars, Smart Metering and the Smart Grid.

A seminar for the Aberystwyth University Computer Science Department

Martyn Thomas CBE FREng

16/1/2014

ROYAL ACADEMY OF ENGINEERING

Cyber Security

a “Tier One” threat

A Strong Britain in an Age of Uncertainty: The National Security Strategy

National Security Strategy: Priority Risks

HM Government

Tier One: The National Security Council considered the following groups of risks to be those of highest priority for UK national security looking ahead, taking account of both likelihood and impact.

- International terrorism affecting the UK or its interests, including a chemical, biological, radiological or nuclear attack by terrorists; and/or a significant increase in the levels of terrorism relating to Northern Ireland.
- Hostile attacks upon UK cyber space by other states and large scale cyber crime.
- A major accident or natural hazard which requires a national response, such as severe coastal flooding affecting three or more regions of the UK, or an influenza pandemic.
- An international military crisis between states, drawing in the UK, and its allies as well as other states and non-state actors.

ROYAL ACADEMY OF ENGINEERING

Smart Buildings
offer significant benefits
and new vulnerabilities

- Access passes / Attendance monitoring/ follow-me printing
- Calendar / Room booking / HVAC control
- CCTV / Wifi / Remote and central monitoring and control
- Dynamic displays / emergency messages / fire alarms … …

- Denial of access / unauthorised access / data compromise
- Disruption / wasted energy / damage
- Intrusion / loss of control
- Safety

ROYAL ACADEMY OF ENGINEERING

Smart Cars

2005 Toyota Camry L4 uncommanded acceleration claims

- see Michael Barr's expert report in the Bookout v Toyota lawsuit. http://www.safetyresearch.net/Library/BarrSlides_FINAL_SCRUBBED.pdf

- Barr inspected the electronic throttle control system code. He stated that he found buffer overflow, invalid pointer dereferencing, stack overflow, undetected task death, unsafe casting, race conditions and >80,000 violations of MISRA-C coding standards.

Recall the C130J flight software analysis.

In Nov 2013, Honda recalled 344,000 Odyssey vans for a software bug that could cause sudden braking.

'Every new car' connected to web by 2014 http://www.bbc.co.uk/news/technology-21411335

ROYAL ACADEMY OF ENGINEERING

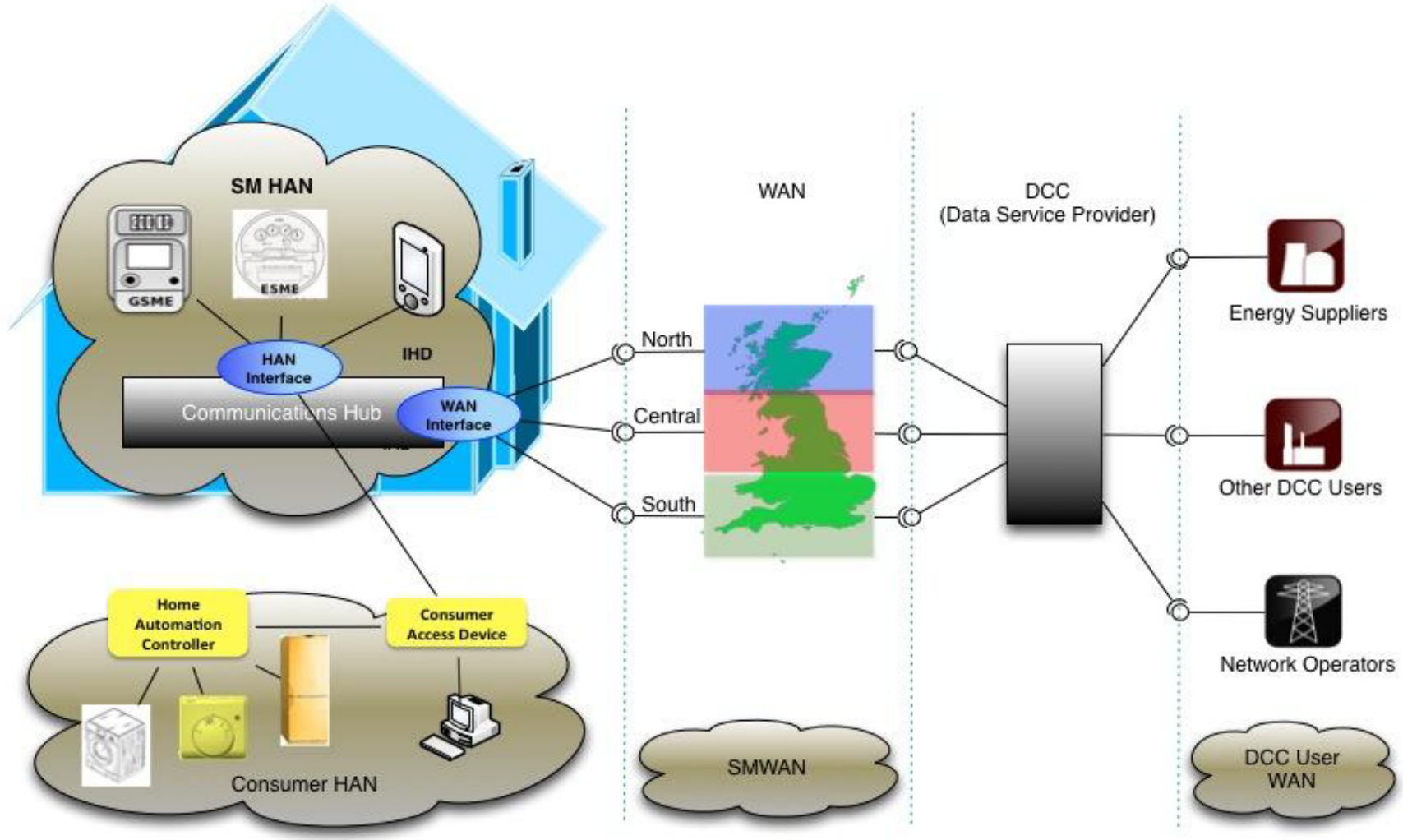
Smart Meters and the Smart Grid

- 43 million Smart Meters to be installed across the UK
- Electricity and Gas (which lack power)
- Provide remote meter reading, fraud control, IHD, ToD tariffs, FITs, device control, power quality monitoring
- Smart Grid must balance the Distribution Networks to accommodate EVs, distributed generation, heat pumps etc without major network renewal
- Transmission Grid must be balanced using demand control to allow greater use of renewable generation

ROYAL ACADEMY OF ENGINEERING

Smart Meter Security

end to end security. “No trusted components”



ROYAL ACADEMY OF ENGINEERING

Vulnerabilities

- Meters contain clocks and billing data
- If these are changed, bills can be manipulated
- Meters contain an “off switch”
- Misuse could cause distress, harm, or (if it could be misused widely) substantial disruption
- Meter firmware will be able to be updated
- Corruption or malicious interference could affect the meters, infrastructure, IHD and devices on the HAN
- The Gas meter can only handle low-grade encryption

ROYAL ACADEMY OF ENGINEERING

Smart Meter Implementation Programme Security

DECC have taken security seriously, with guidance from CESG and an expert group

The resulting Security Architecture is complex. Version 2.08 has 91 pages of text, diagrams and message choreographies

Nevertheless, it is an *informal* document.

- There is no unambiguous statement of the security requirements, commands, data, …
- There is no way to show with high confidence that the architecture provides adequate security

This is normal for commercial products.

Is it good enough for smart meters?

ROYAL ACADEMY OF ENGINEERING

Who controls the Off Switch?

Anyone who has the authority to send the relevant messages through the DCC

Anyone who can mount a successful **cyber attack** on the network

- Hostile states?
- Terrorists?
- Organised criminals?
- Hacktivists?
- Vandals?
- Insiders?
- COTS component suppliers?

ROYAL ACADEMY OF ENGINEERING

How will security be assured?

By human review of the specifications

By testing the system

By focused “penetration testing”

But testing can only show that faults **do** exist — it can *never* show that there are no faults or vulnerabilities

For high confidence, you need mathematically formal analysis as well – which must start with ***formal specifications***

ROYAL ACADEMY OF ENGINEERING

Cyber Security is a through-life discipline

Planning -> Control -> Monitoring -> Response

- From *design* through to *decommissioning*
- Control system lifetimes may be 20 years +
- Control systems don’t run standard Antivirus
- Security monitoring is difficult (and uncommon)
- How to respond to incidents?
- Insider threats are real
- Lifetime security needs discipline and excellent configuration control through years of maintenance and upgrades

ROYAL ACADEMY OF ENGINEERING

Systems Engineering for Security

High integrity will be required, *with high assurance*

- Greater integration between systems requires clear, rigorous specifications and assured subsystem properties

- Control of the supply chain – can COTS be trusted?

- Integrity and resilience *cannot* be assured by testing alone

ROYAL ACADEMY OF ENGINEERING

M2M and the IoT

- As Bruce Schneier wrote this week on Wired, the IoT is a transition similar to the move to PCs in the 1980s
- The demand is for low costs and facilities, not security and good engineering
- Most security strategies don't transfer
- The threat is greater because everything is internet accessible
- It will be very costly to patch or upgrade
- There are already Linux worms moving from PCs to routers to cameras…

ROYAL ACADEMY OF ENGINEERING

Cyber Security

a “Tier One” threat

A Strong Britain in an Age of Uncertainty: The National Security Strategy

National Security Strategy: Priority Risks

HM Government

Tier One: The National Security Council considered the following groups of risks to be those of highest priority for UK national security looking ahead, taking account of both likelihood and impact.

- International terrorism affecting the UK or its interests, including a chemical, biological, radiological or nuclear attack by terrorists; and/or a significant increase in the levels of terrorism relating to Northern Ireland.
- Hostile attacks upon UK cyber space by other states and large scale cyber crime.
- A major accident or natural hazard which requires a national response, such as severe coastal flooding affecting three or more regions of the UK, or an influenza pandemic.
- An international military crisis between states, drawing in the UK, and its allies as well as other states and non-state actors.

ROYAL ACADEMY OF ENGINEERING

Conclusions and *Questions*

- More automation *inevitably* means more vulnerabilities unless critical system properties can be assured.
- The current approaches to Smart System security do not (and cannot) provide adequate assurance. *What to do?*
- Cost pressures lead to the use of COTS components that become common points of vulnerability and failure.
- COTS components could import vulnerabilities into critical infrastructure. *Might these have been deliberately introduced? Who knows about them?*
- *Strategically, should our cybersecurity budget go into developing hardened replacements for common COTS?*
- *Would a liability law be helpful?*

ROYAL ACADEMY OF ENGINEERING