

The not so smart grid

“A clever cat in a hat is the subtlest manifestation of cyber threats”

Nicht ger fingerpoken!

- Electricity networks are highly regulated and standardized , as simple errors or omissions could result in catastrophic failure of equipment or loss of life.
- Devices and appliances that are attached to these networks are built to specified standards, tolerances, limits, overrides and failsafes

Separated = safe

- Previously an esoteric error detected in a controller on these closed networks unless it presented an immediate operational threat did not require amelioration i.e it was not a threat.
- This is because the control system was not entropic, did not have uncontrolled connections and was performing within acceptable limits and consequently there was no likelihood of the operating conditions changing.



Not all business drivers are a good idea

- SCADA networks already have had sustained cyber attacks with devastating consequences
- attacks have had to have crossed certain security barriers presented by the infrastructure provider in the form of firewalls, IDS and other network countermeasures
- In a smart metered reality the meters are the infrastructure and these provide routes to and from the operational cores of the infrastructure provider

Grid + p0wn = darkness

- The smart meters potentially add a series of compounding extreme risks into power networks that up until now have largely been unaffected by network effects such as DDoS and flash worms
- We have an Internet that largely is now a hostile place in which to operate. Viruses, worms and malicious codes are part of the landscape and are often spread via network means to infect more victims.



Same stuff different shovel

- Defective network stacks embedded in devices and operating systems have been a long known and utilized avenue for exploit and vulnerability.
- Many of these smart meters are designed as low power devices and as such do not have significant computational power.
- Firmwares of many of these devices do not have the capacity to perform CRC or standard integrity checks on the firmware upgrade being sent to the device. This exploit has been proven in concept on one of the processor platforms used in smart meters (Goodspeed 2007)



Dumb and dumber

- Malfeasant firmwares could be the installation of firmware that falsely reports a lower rate of energy supply from the company or the converse of this for someone supplying power back into the grid
- Many of the current range of smart enabled meters and devices rely on wireless based protocol such as Zigbee of 802.15.4. Designers seem to constantly forget that any wireless signal can be brute forced into a denial of service by the use of a stronger signal base in the same frequency band it is basic physics.

Why?reless

- (Ocenasek 2009) the author identifies security issues with Zigbee and breaks them into three topical areas management problems, insufficient integrity protection and key management problems.
- Many of these problems are inherent or similar to ones in WiFi or 802.11b it will not take many experienced attackers to rapidly assimilate knowledge and produce tools capable of breaking many of these identified issues.



Remedy?

- Remedy is not simple but it is also not impossible to achieve a reasonable level of assurance and safety within the network even by adding these particular devices.
- This not only means conventional systems testing but also extensive testing for deployment in a situation where it may come under sustained network attack.
- It is apparent that at least some of the existing systems and chips themselves are vulnerable to exploit or attack. So this has major impacts on how these chips should be used and the circuits and boards into which they are designed.

Less rhetoric more rationality

- Currently there is some hyperbole in some of the discourse on both sides of the argument.
- One of the problems is that unlike many of the issues faced by the Internet at present it does not largely touch or control large parts of the infrastructures we need to sustain our modern society.
- What parts are touching have been proven to be significant cause for concern in particular SCADA.

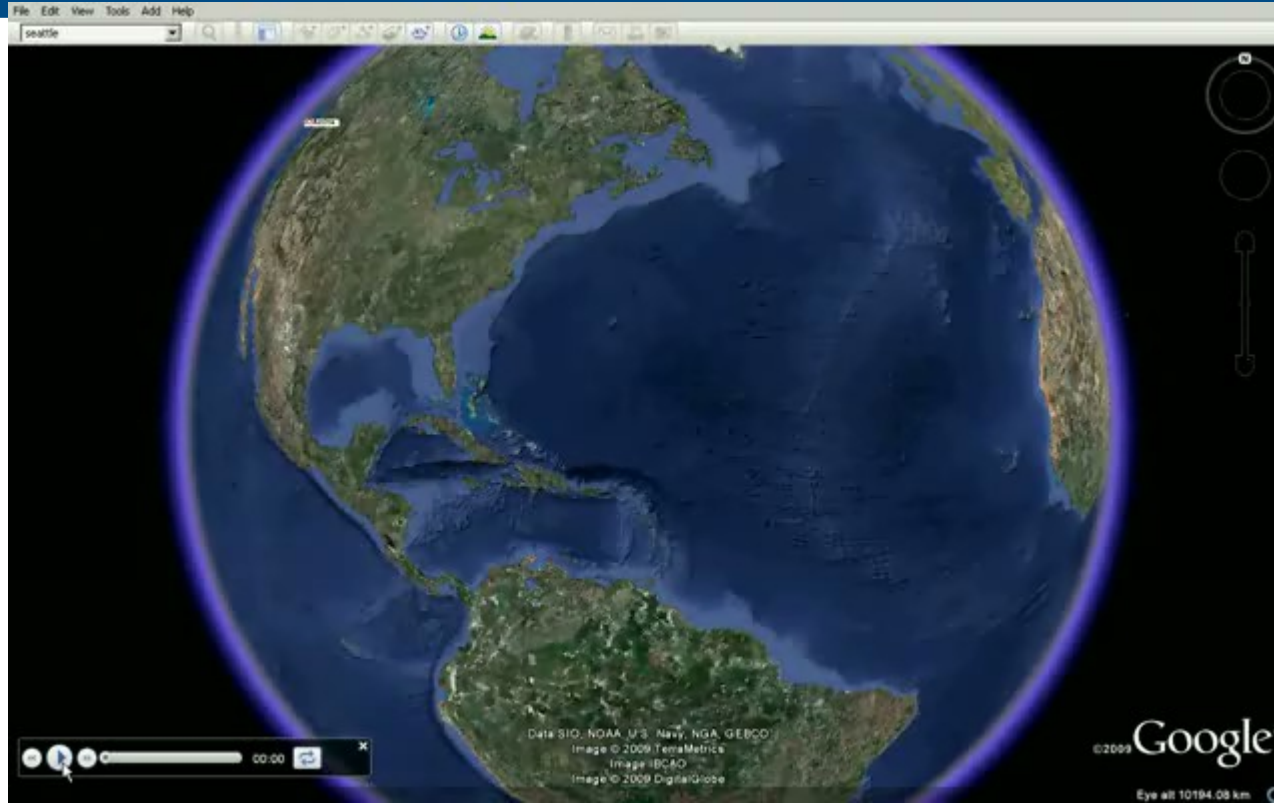


Conclusion

- If I analogise for a moment if smart meters were drugs and these drugs had a known potential flaw that killed people effectively in large numbers when they came into contact with salt water would we allow its production let alone sale?
- Yet currently smart meters/grid (drugs) have known potential flaw that can kill large numbers of them when they become connected to a network (water) that contains malware (salt).

A demo

- Simulation of 22,000 node smart-meter worm propagation using GPS points gathered from geo-coded home addresses purchased from a bulk mailing list. The simulation takes into account radio range



ECU