

Smart Grid Security

Martyn Thomas CBE FREng
www.thomas-associates.co.uk

September 27, 2007 -- Updated 1317 GMT (2117 HKT)

Mouse click could plunge city into darkness, experts say

STORY HIGHLIGHTS

- Sources: Similar attack could
- Experts fear attacks could
- Department of Homeland Security
- DHS official: A lot of risk here

[Next Article in U.S.](#) »

READ

VIDEO

INTERACTIVE

From CNN's Jeanne Meserve

TEXT SIZE - +

WASHINGTON (CNN) -- Researchers who launched an experimental cyber attack caused a generator to self-destruct, alarming the government and electrical industry about what might happen if such an attack were carried out on a larger scale, CNN has learned.

Sources familiar with the experiment said the same attack scenario could be used against huge generators that produce the country's electric power.

Researchers at Idaho National Labs caused a generator to self-destruct

Advertisement

This is the all-new 2010 E-Class.
This is Mercedes-Benz. ILLUMINATE THE NIGHT



Mercedes-Benz

NEWS POLITICS OPINIONS BUSINESS LOCAL SPORTS ARTS & LIVING GOING OUT GUIDE JOBS CARS REAL ESTATE RENTALS CLASSIFIEDS

SEARCH: go washingtonpost.com Web : Results by Google | Search Archives

washingtonpost.com > Technology

'Smart Grid' Raises Security Concerns

By [Brian Krebs](#)
Washington Post Staff Writer
Tuesday, July 28, 2009

Electric utilities vying for \$3.9 billion in new federal "smart grid" grants will need to prove that they are taking steps to prevent cyberattacks as they move to link nearly all elements of the U.S. power grid to the public Internet.

The requirements from the Energy Department come amid mounting concern from security experts that many existing smart-grid efforts do



Electric utilities receiving "smart grid" grants must ensure cybersecurity. (By David Zalubowski - Associated Press)

TOOL BOX

Advertisement » Your Ad Here

We have answers.

Somewhere in America, Siemens has already answered the nation's toughest questions in energy, industry and healthcare.

→ See how

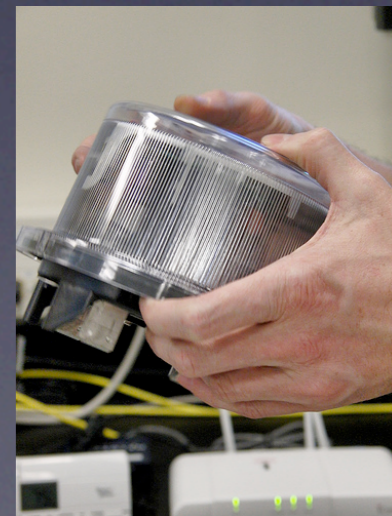
SIEMENS

IOActive claim 4 successful attacks on smart meters and the smart grid

Features and Threats

from smart metering and end-user services

- Automatic meter reading
- Real-time meter reading
- Bi-directional communications
- Load shedding/disconnection
- Software update
- *Privacy if the data is personally identifiable*
- *Home security / fraud*
- *The customer becomes vulnerable too*
- *Criminal control for harassment/blackmail*
- *Widespread disruption*



Threats from smart grid control

- isolation of power sources or local grids
- destruction of equipment
- blackouts
- blackmail



Economics of Security

lessons from other application areas

- If hacking is easy, script kiddies do it for fun
- If the target is valuable, it will attract organised crime
- If there is *serious* money to be made, very sophisticated attacks can be expected
- If widespread or critical disruption is possible, the Grid could be targeted by terrorists or foreign states

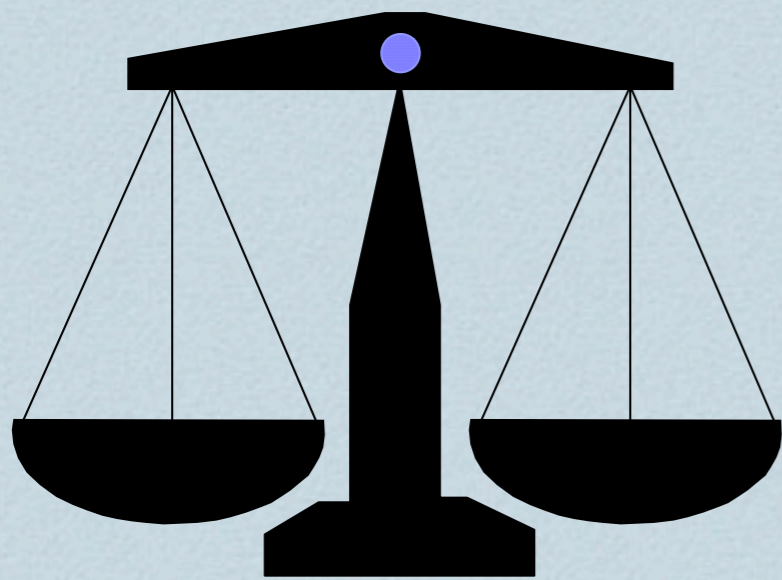
Some possible attacks

- Physical / RF interference with the meter
 - probing, disassembly, temperature changes, RFI
- Blocking the communications
 - What happens if communications cease?
- Spoofing the communications
 - Replay. Forgery. Man-in-the-middle
- Insider attacks / social engineering
- Software vulnerabilities

Software-based systems

- Inherently very complex, with *discrete* behaviour and very many states ...
- ...so *testing* provides limited assurance.

Testing software tells you that the tests work – not that the software works



Continuous behaviour means you can interpolate between test results



Discrete behaviour means that you can't (without a fully formal model).

Software errors are common

- Typical professional software development leaves one defect in every hundred lines of software.
- Programming languages like C make it easy to make mistakes and hard to find them.
- Developing high-integrity software is very difficult. *Showing* that it's secure and reliable is even harder.

Security Engineering

- Threat analysis: develop a threat model
- Vulnerability analysis: use HAZOP and FMECA
- Determine the *assumptions* you can make about the environment and the *properties* you require from the system and its components
- Express assumptions and properties explicitly, using mathematically formal specification languages
- Validate *assumptions* by testing
- Develop the systems using formal methods and use *analysis* to show that the system has the required properties
- Use testing as a confidence check that the analysis was sound.
 - any failure at this stage should be seen as a significant problem, as it shows that the design is faulty *and* that earlier analysis was faulty.

Mathematically formal methods are essential

- to document required properties
- to document assumptions
- to specify the system to be designed
- to develop the system so that it can be analysed
- to analyse the system to show that it has the required properties

There is no other way to provide adequate evidence of security

Testing is essential

- to help elucidate requirements (prototyping)
- to validate assumptions about the environment
- to validate assumptions about the behaviour of informal components - including humans
- as a (poor) double-check that analyses are sound

But the confidence level is likely to be low - and may be inadequate

Cryptography is no panacea

“Whoever thinks that his problem can be solved using cryptography, doesn’t understand his problem and doesn’t understand cryptography.”

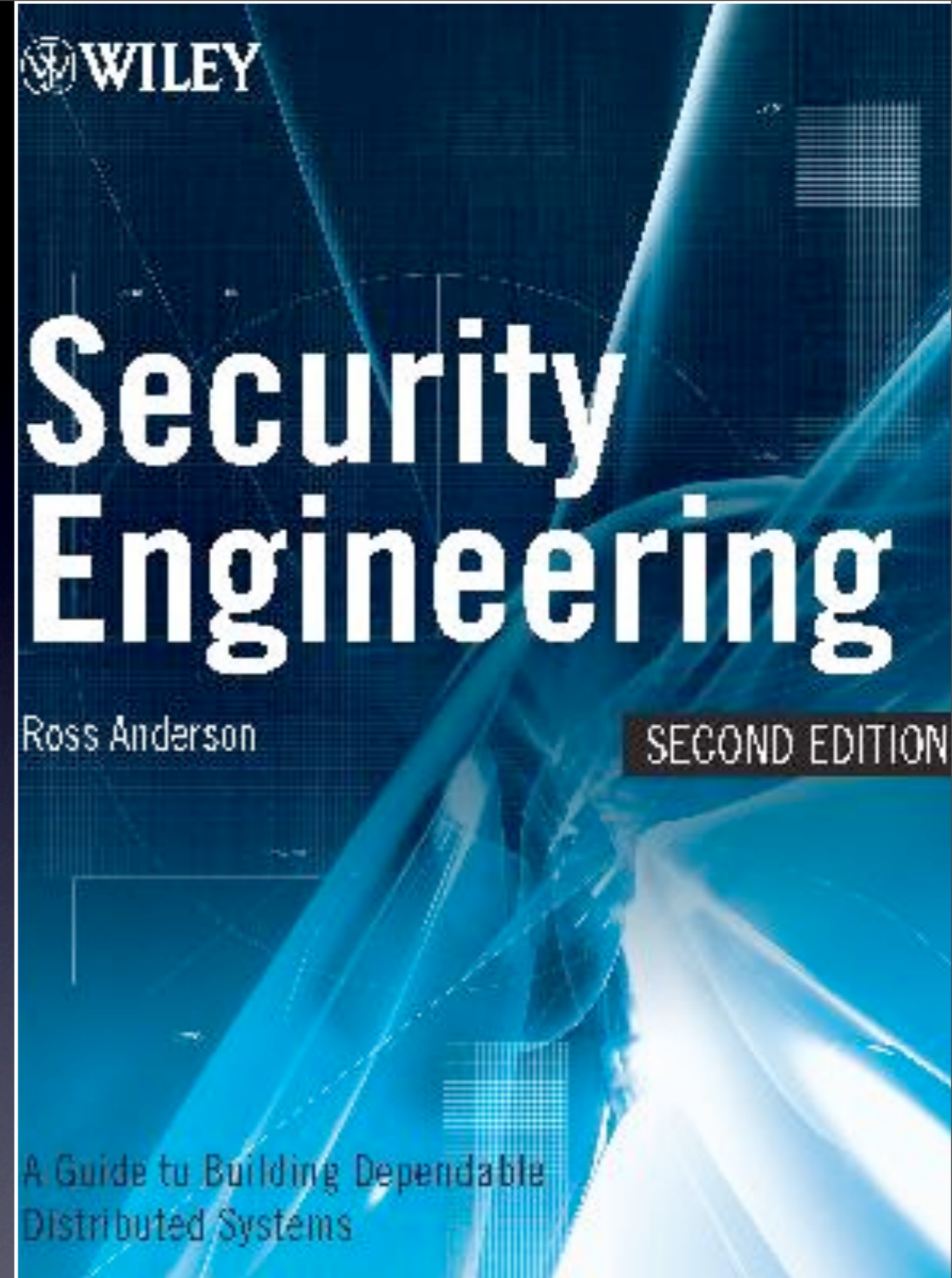
- attributed by Butler Lampson and Roger Needham to each other

quoted in *Security Engineering*, Chapter 18.

The definitive guide
is Ross Anderson's
Security Engineering

The first edition is available for
free download from:

[http://www.cl.cam.ac.uk/~rja14/
book.html](http://www.cl.cam.ac.uk/~rja14/book.html)



Conclusions

- Security is a concern for the smart grid
- Security has to be designed in architecturally. It is very hard or impossible to make an insecure architecture secure later.
- Threat analysis and vulnerability analysis are key
- Security engineering is a specialism: use experienced professionals.
- Formal methods are essential for high assurance.