Power Grid Protection

Aug 10-11, 2010

Dr. Fred Cohen
President - California Sciences Institute
CEO – Fred Cohen & Associates

Power Grid Protection

- What's the problem?
  - The consequences of failure are high
  - The mechanisms / people / process in place are not up to the task
  - The information required to understand this is not being made available to decision makers so bad decisions are being made
- What's the solution?
- Summary and conclusions

The problem

- Consequences of smart/dumb grid failures
  - Direct:
    - No / low power
    - For whom?
    - For how long?
  - Indirect:
    - No power → No water
    - No power → No phones
    - No power → No transportation
    - No power → No food
    - No power → No government
    - No power → No society

The problem

- How is “smart” better/worse than “dumb”?
- Smart better: (only a partial list)
  - More cost/energy/other efficient
  - Better control over detailed operational facets
  - More able to adopt newer technologies
    - Charging cars and similar challenges
    - Reducing energy usage more selectively
    - Remote control of home/work usage by owners
    - Better tracking of consumption by components
    - Situational adaptation of usage patterns

The problem

- How is “smart” better/worse than “dumb”?
- Smart worse: (the list is far longer…)
  - More brittle to some failure modes
    - Common mode failures that propagate (viruses)
    - EMP that wipes out control computers
    - Remote update with malicious/faulty code
  - The death of 1000 cuts more readily feasible
  - System far more complex to manage
  - Aggregated capacity of “smart” components
    - Potential for abuse when taken over in mass
    - Potential control nightmare scenarios

The problem

- Consequences ONLY of smart grid failures
  - Direct:
    - Leakage of detailed information about each device in real-time
      - Opponent can tell exactly what happens where
  - Indirect:
    - Instrument of criminal activity
      - Murder / Theft / Vandalism / Kidnapping / Assault
    - Loss of privacy
      - When who is where and behavioral patterns
      - When to call people to collect bills
    - Instrument of information warfare / etc.
      - Know when to attack what to disrupt services

The problem

- Consequences ONLY of smart grid failures
  - Direct:
    - Corruption of information in devices
      - Opponent can change what the operator sees
  - Indirect:
    - Cause operator to misoperate the grid (illusion)
      - More/less power is needed that is really needed
      - Power is needed from me (at high fees per market)
    - Change financial mechanisms (real or illusion)
      - Lower personal usage at the expense of neighbors
      - Higher usage for people I don't like
      - Higher usage for war protesters / KKK members …
    - On means off (yes means no)
      - Make controls do the opposite of normal…

The problem

- Consequences ONLY of smart grid failures
  - Direct:
    - Arbitrary combinations of usage patterns intentionally sequenced and coordinated
  - Indirect: Turning individual things on and off
    - Turn your lights on when you are having sex
    - Turn your lights off when you are in the shower
    - Turn your refrigerator on and off till it breaks
    - Turn off AC in a computer center (and heat on)
    - Turn off the exhaust, turn on the gas, wait a while, turn on things that make sparks
    - Turn off the surveillance system / rob the house

The problem

- Consequences ONLY of smart grid failures
  - Direct:
    - Arbitrary combinations of usage patterns intentionally sequenced and coordinated (cont)
  - Indirect: Turning lots of things on an off
    - Turn off all the AC on all the hot days
    - Turn off power to hospitals supporting abortion
    - Make a city into a space billboard
    - Turn lots of things on and off till they all break
    - Turn off traffic lights and alarm systems
    - Turn off power to all refrigeration systems
    - Push power consumption over rate thresholds to increase income for the month

The problem

- At least one deployment of "smart grid" has more than 1 million deployed IP addresses
  - 1 person checking for weaknesses
  - 1 person responding to detected attacks
- The solution: detect as few as you can!!!

The problem

- Lack of good information drives bad decisions
  - Disinformation from vendors and others
    - Smart grid systems are not “more secure”
    - Pen testing always succeeds against them
    - No specially effective measures are in place
    - Dysfunctional organizations (truth → fired)
  - Inadequate metrics and measurement
    - Don't see weaknesses → you aren't looking
  - Inadequate sources of information
    - Auditors / insiders / etc. paid for **limited** results
- Lack of expertise drives bad decisions
- Bad (information + expertise) → bad decisions

The problem

- Lack of good information drives bad decisions
- Lack of expertise drives bad decisions
  - Manufacturers don't have the expertise
  - Integrators don't have the expertise
  - Grid providers don't have the expertise
  - Power providers don't have the expertise
  - Regulators don't have the expertise
  - Customers don't have expertise or choice
  - They won't get people with the right expertise
    - If they do get them they won't get them again...
- Bad (information + expertise) → bad decisions

The problem

- Lack of good information drives bad decisions
- Lack of expertise drives bad decisions
- Bad (information + expertise) → bad decisions
  - Getting bad information
    - Poor/no metrics to measure the issues
      - Measurements cost – why pay for bad news?
    - Poor/no communications from those who know
      - Management structure fires those who tell
    - Inadequate overall expertise to get at facts
      - Hard to find enough qualified folks (**build**/buy)
    - Inadequate scientific basis for the field
      - Inadequate funding to do such research
  - Using information poorly

The problem

- Lack of good information drives bad decisions
- Lack of expertise drives bad decisions
- Bad (information + expertise) → bad decisions
  - Getting bad information
  - Using information poorly
    - Decision processes are not well defined to deal with information security-related risks
      - Standard risk management is ineffective
      - Business decisions favor short-term ignorance
      - Feedback is backwards for decision-makers
    - Inadequate measurements don't lead to better measurement – they lead to reduced liability
      - Highly motivated to not get bad news

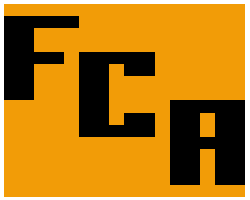
Power Grid Protection

- What's the problem?
- What's the solution?
  - Bring more/better expertise to bear
  - Get better information
  - Make better decisions
- Summary and conclusions

The solution(s)

- Lots of folks tout solutions
  - Often solve the wrong problem
    - I have a hammer – you must have nails
  - Often purchased when management gets scared and lets the CISO do whatever
    - An earthquake damaged the computer center – we better upgrade our network firewalls
- Causality gets confused

  - If I offer you a solution, you may say it's because I provide it (I have hammers too)



  - You have it backwards...
    - I build hammers when I see nails...

The solution(s)

- Build human capital for smart grids
  - Education → knowledge

Graduate education in critical infrastructure protection (MS, Ph.D. in National Security)

- Ph.D.s in digital forensics (incl. control systems)

  - Training → skills
    - Lots of training programs and undergraduate education available - improvements needed

A Human Capital Crisis in Cybersecurity

Technical Proficiency Matters

A White Paper of the
CSIS Commission on Cybersecurity for the 44th Presidency

The solution(s)

- Lack of expertise drives bad decisions →
  - Get more/better expertise
  - Consulting from real experts
    - Get experienced folks with right background
    - Pay them well and listen to their advice
    - Exclude the large firms – this is not in their experience base – you need specialists
  - Build/buy decision
    - Today, only build can work at scale
    - Build through training and education
    - These take time – slow it down
    - See previous slides

The solution(s)

- Manufacturers / integrators lack expertise
  - The solutions are not large-scale ready yet
- Providers don't have the expertise
  - Start with smaller scale deployments
  - Build expertise over time and grow
- Regulators don't have the expertise
  - Hire good experts and listen to them
- Customers don't have expertise or choice
  - Government should regulate monopolies
  - Media should inform the public

The solution(s)

- Bad information drives bad decisions →
  - Poor/no metrics to measure the issues
    - Improve measurements till you understand what all information and state is and means
  - Measurements cost – why pay for bad news?
    - Only regulation will force these issues
  - Poor/no communications with experts
    - Your CEOs are not here – are they?
    - Till they hear it they won't change...
    - Necessary – not sufficient
  - Management structure fires those who tell
    - Get new job – tell – get you and them fired

Get the folks who need to be fired to hire FCA We tell what has to be told and they get fired...

The solution(s)

- Bad information drives bad decisions →
  - Inadequate overall expertise to get at facts
    - Education and research are required
  - Hard to find enough qualified folks (build/buy)
    - Not enough resources to allow for buy
    - Education and training are required (build)
  - Inadequate scientific basis for the field
    - Only research will do it – and we need Ph.D.s

Inadequate funding to do such research

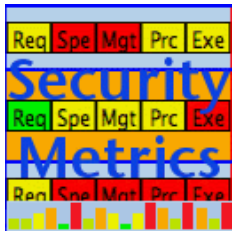
- Fund the seed corn of the information age

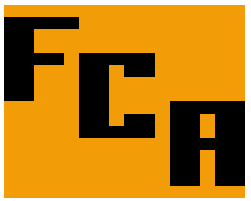
Oh yeah... Some more corrections

- There is expertise – but you have to pay for it

The solution(s)

- Bad (information + expertise) → bad decisions
  - Better decision making is hard to get
    - This presentation should help in the information and expertise parts, but decision-making...
  - We are working on it...
    - Decision support tools can help organize things
    - Checklists can help avoid missing the obvious
    - A sound process would help many situations
      - Do the background work to get good facts
      - Put the facts into a proper analytical structure for the decisions to be made
      - Do the analysis in a clear manner
      - Present the results so as to properly portray the situation and response alternatives





Summary and conclusions

- We have some serious information protection challenges for smart grids
  - But we aren't going to abandon them because we need the benefits they bring
- We lack the knowledge, skills, expertise, training, and experience to do it well
  - We need to gain it, and that takes time
  - We need to slow down deployment and speed up research, development, education, and training
  - We need to improve the decision-making that put us in this situation

As an aside... how it really works

- Some dis/misinformation
  - No forensics/IDS/IPS/etc. for control systems
  - It's too slow / not right for us / etc.
    - Of course we can do it so it works right for you
    - But you have to pay for it – and it takes time
    - Which is why you don't have it right now
- How security markets really work
  - ~~Proactive: invest in advance of it going bad~~
    - ~~Bet things will go bad – thoughtfully~~
  - Reactive: respond after it goes bad
    - Buy in desperation – from whoever is there
    - You have the money to do it then...

Thank You

http://calsci.org/ - calsci at calsci.org
http://all.net/ - fc at all.net