Hacking Can Make Critical Power “Go Critical”

Edward Herbert

Co-Chairman

PSMA Energy Efficiency Committee

What is “Hacking?”

- In the fraternity of Hackers, “Hacking” is accessing a computer to view or copy data, or maybe leaving a message, without destroying data or harming the computer.
- “Cracking” is accessing a computer to cause damage.

We will call it “Hacking,” because that is the term that is familiar to the public.

“Chicken-Little” or “Rose-Colored Glasses”

- The PSMA Energy Efficiency Committee co-sponsored a workshop with EPRI on the Smart Grid in March 2013. /Ref 1.
- One of the most engaging speakers was Jonathan Pollet of Red Tiger Security. He told us about the vulnerability of SCADA in The Grid.
- Most speakers on cyber-security fall into one of two camps:
  - The “Chicken-Little” finds scary stuff everywhere. “The sky is falling.”
  - Those who make interface circuits tend to assure us that all is just fine, as long as we use their products.
  - In our workshop, EPRI called cybersecurity a “secondary concern.” /Ref 1
    That is scary.

Sensible precautions give reasonable protection.

- Keep anti-virus software up-to-date.
- Have a good firewall around operations.
- Keep security patches up-to-date.
- Train employees to be cyber-aware.
    - Do not plug phones, tablets or laptops into company computers
    - No personal programs or apps
    - Be alert for phishing, and do not respond
    - Guard login credentials

Added protection for critical organizations

- Isolated internal bus, with no connection to the Internet.
- VPN (Virtual Private Network)
- No WIFI
- No CD/DVD readers/recorders
- No USB access
- Do not allow personal laptops, tablets or phones in secured areas
- No terminals outside a secured area.
- Etc.

Take extra precautions if:

- Your organization may be a target of foreign governments
- Your activities are politically sensitive or controversial

Hacking targets

- Direct control of equipment:
  - The hacker issues commands that cause inappropriate operation of the equipment.
  - In extreme examples, equipment can be destroyed, like Stuxnet.
- Monitor corruption:
  - Monitoring signals can be corrupted, giving a false indication of failed equipment or unsafe operation, leading to shut-down.
- Indirect control:
  - Control of the loads or power sources on a power system

Opportunistic hacking

- A lot of hacking results from “sniffing” or “bots” that randomly look for vulnerabilities and exploit them.
- There are enough vulnerable computers so that if your organization has good basic cyber-security, the threat of opportunistic hacking is significantly reduced.
- THE THREAT IS *NOT* ELIMINATED.
  They may be searching for the type of equipment that your organization uses.

Who are the hackers?

- We tend to think that hackers are foreign agents who get access through the Internet.
- By some accounts, 80% of hacks are internal.
  - Different definitions, different counting methods, and different agendas, add uncertainty.
- Most agree that internal hacks are likely to be more serious.
  - Knowledge of vulnerabilities
  - Knows how to bypass security measures
  - Access --- can operate behind firewalls.

Motivations for hacking

- A hacker may steal information.
  - While a cause for concern, this may not be an operational risk.
- He/she may want to disrupt operation.
  - Unplanned shut-down.
- He/she may want to damage equipment
  - Like Stuxnet.

How does an inside hacker get employed?

- Insider hackers can be someone who has IT skills and purposefully seeks employment to gain access, like Edward Snowden.
- It can be someone inside the organization who develops a grudge.
  - Passed over for advancement
  - Relative or friend had bad experience with the company
  - Bullied (or perceived to be bullied) by supervisor or co-workers.
  - Etc., etc.,
- Consultants and other third party service providers can be a problem
  - Divided or conflicted loyalties
  - Little vested interest in your organization

Unintended cyber events

Examples:

- A gas pipeline explosion killed three and injured eight others. A communication failure locked out the central control, preventing technicians from relieving pressure in the pipeline. /Ref 3
- Unit 3 of the Browns Ferry nuclear plant shutdown after two pumps failed. The controllers for the pumps locked up due to a flood of data traffic on the plant's internal control system network. /Ref 3

Although these incidents may have been accidental, they can be instructive to those planning intentional attacks.

Vulnerable equipment.

- A connection to the Internet is an open invitation for hacking.
- A connection to an internal control bus is much better, but still it is vulnerable to hacking if the hacker can gain access to the bus or its controller.
- California's CPUC Rule 21 mandates a connection to the Internet for the control of "Smart Inverters." We thus have a government-mandated cyber-security vulnerability.
- "Smart meters" are another example of a utility-mandated cyber vulnerability. /Ref 4.

Logic bombs

- One of the most powerful tools for a hacker is the ability to set “logic bombs,” computer code that remains quiescent until some future event triggers it.
- Saudi Aramco had 30,000 computers wiped out all at once. It was an inside job. A piece of code formatted the hard drives and removed a critical piece of the boot sector. The rogue code had infected all of the computers earlier, but all were set to activate at a particular future time. /Ref 1
- Fortunately, Aramco had put firewalls in front of their operational control systems.

Refrigerator hacked to send SPAM!

- Why in the world does the refrigerator have a processor that is sophisticated enough to send SPAM?
- Extra capability is the capability to do extra damage, if hacked.
- Can that refrigerator be hacked to take control of the stove, and the rest of the appliances? Maybe.

SCADA (Supervisory Control And Data Acquisition)

- SCADA boosts efficiency by allowing central processor control.
- SCADA may allow remote control.
- SCADA exposes once-closed systems to cyber attacks.
- Night Dragon APT moved from the Internet, through Corporate IT systems and into the SCADA system.

Stuxnet and its derivatives

- Stuxnet is a highly sophisticated military programs, developed to sabotage, undermine and even physically destroy infrastructure.
- Most believe that Stuxtnet was a joint effort of the U. S. and Israeli military.
- After Stuxnet, there are its derivatives:
  DuQu, Backdoor Regin, Wiper, Flame, Gauss, Mahdi.

Is Stuxnet a threat?

- Stuxnet is very sophisticated and requires advanced expertise.
- A Stuxnet attack is very expensive and time consuming to plan.
- A Stuxnet attack requires extensive knowledge of the target’s plant and equipment

Therefore, it is often believed that most organizations would not be a target of Stuxnet or its derivatives.

NOT TRUE!: a single targeted device can bring down a system.

Many functions are on-off.

- Many operations that are controlled over a data bus have a command to turn it on and another to turn it off.
- If a device is turned off, then the data bus fails, it cannot be turned back on.

Some functions should not be controlled over a data bus.

- The pipeline would not have exploded if a mechanical pressure relief valve had been used.

Some commands set a value, which remains fixed until another command modifies it.

- A pump speed may be set for a particular RPM.
- If the data bus fails, it will remain at that speed and it cannot be changed.

Some functions should not be controlled over a data bus.

- The pumps at Browns Ferry would have remained operational if an analog control had been used.

“Safe-state” command/response

- A component controlled by a command/response over a data bus may have a state that is always “safe.”
- In the absence of verifiable data that maintains a different state, the component should revert to the safe state.
- To maintain a different operational state, the command/response must refresh the controller at frequent intervals
- The safe state need not be a static value, control can revert to an analog algorithm with multiple inputs.

Parameter adjustment

- Hacking of a command/response system can be made relatively harmless, if the command/response range is made small enough that little damage will be done.
  - Consider an analog system that is 10 % accurate, but that its efficiency can be improved significantly using the central computer and a data bus so that the accuracy is ½ %.
  - Introducing the command/response introduces a vulnerability to hacking.
  - If the authority of the command/response is limited to a 10% parametric adjustment of the 10 % analog system, the system can be degraded by hacking, but it remains operational.
  - Absent a failure or hacking, it can achieve optimal accuracy.

Parameter limits

- A control can be designed so that the command/response from a central computer over a data bus is allowed only within a range of values.
- If the value is too high, a default operation is executed regardless of the command state.
- If the value is too low, a different default operation is executed regardless of the command state.
- Within a range of values, the command/response is allowed, so the central computer can determine optimized operation.

For hacking a critical power system

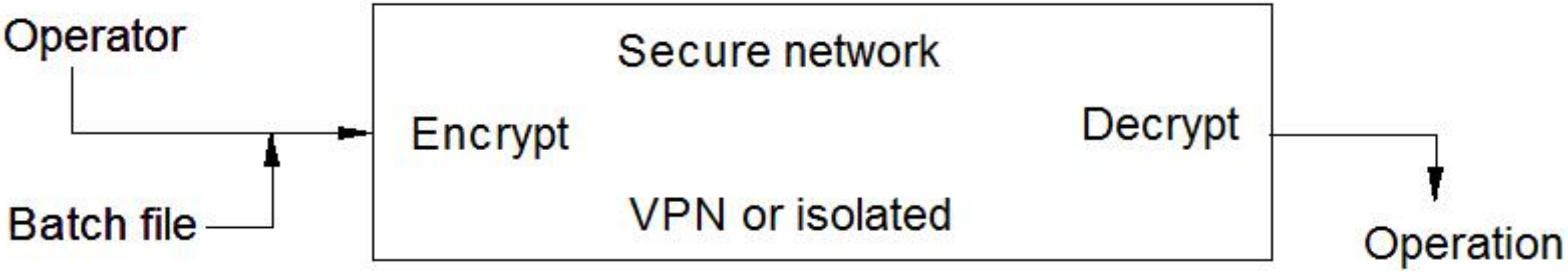
- It may not be a component of the power system that is the target.
- A rogue load or external power source could do extensive damage to the critical power system to which it is connected if the control of the load or external power source is hijacked.

IP credentials and encryption keys.

- The IP credentials and encryption keys of a controller on a data bus are necessary for a command to be received and acted upon.
- A “worst case” cyber-security concern would be a controller that was hacked to put it into a destructive state, then its IP credential and/or encryption keys are modified so that it is accessible only to the hacker, or to no one at all. /Ref 4.

Encryption does not prevent hacking

Example: An operator sees an overdue bill, and flags an account to be disconnected. The signal is encrypted, sent over a secure network, decrypted, and acted upon.



- A rogue operator can disconnect a customer despite encryption.
- A hacker can write a batch file to disconnect 10,000 customers at a future date (logic bomb), despite encryption.
- Anything that corrupts the network *prevents* the operation, which can be a form of hacking.

Very scary News:

800,000 Microinverters Remotely Retrofitted on Oahu—in One Day IEEE Spectrum, February 5, 2015

In a single day, Enphase and the Hawaiian Electric Company remotely reprogrammed some 800,000 microinverters attached to individual photovoltaic panels on Oahu.

Fortunately, it was a legitimate upgrade.

Failure modes and effects analysis (FMEA)

- The FMEA probably is familiar to designers of critical systems.
- For a critical system that relies on command/response over a data bus, every possible state of every controller should be analyzed in view of possible hacking, including disabled communications.

Possible cyber-security scenarios:

1. Business as usual. Slow progress will be made, with budget constraints, as awareness increases.
2. Pressure from insurers: Some organizations and suppliers of equipment may find that they cannot get insurance without major security upgrades. /Ref 5
3. Equipment vendors whose equipment is too easily hacked may face warranty claims, liability for damages, and possibly recalls.
4. Major security breach: If there is a well-publicized major security breach (think 9/11 scale), there will be a panic reaction to cyber-security threats, with unimaginable mandates and consequences.

References

1. "Are You Smart Enough for the Smart Grid?" PSMA-EPRI workshop,
2. "Nuclear Power Plant Security," Nuclear Energy Institute, September 2014
3. "Cyber Incident Blamed for Nuclear Power Plant Shutdown," Brian Krebs, Washingtonpost.com, June 5, 2008.
4. "Who controls the off switch?" Ross Anderson, Shailendra Fuloria, Computer Laboratory, Cambridge University, UK
5. "Energy firm cyber-defence is 'too weak', insurers say" Mark Ward, BBC News Technology, February 26, 2014
6. "800,000 Microinverters Remotely Retrofitted on Oahu—in One Day" Peter Fairley, IEEE Spectrum, February 5, 2015

Additional references

- Puerto Rico smart meters believed to have been hacked – and such hacks likely to spread, Metering.com, April 11, 2012
- Smart Grid Threat Landscape and Good Practice Guide, Louis Marinos, European Union Agency for Network
and Information Security
- Security Concerns Behind Slowdown in Itron Rollout? Greentechgrid, Jeff St. John February 9, 2009.
- Smart Meter Slowdown Blues: Itron Cuts Workforce, Greentechgrid, Jeff St. John, September 13, 2013.
- Electricity Grid in U.S. Penetrated By Spies, The Wall Street Journal, Siobhan Gorman, April 8, 2009
- Smart refrigerators and TVs hacked to send out spam, according to a new report, NBC News, Julianne Pepitone, Jan. 18, 2014.
- "Stopping Hardware Trojans in Their Tracks ," IEEE Spectrum, Subhasish Mitra, H.-S. Philip Wong & Simon Wong, 20 Jan 2015.