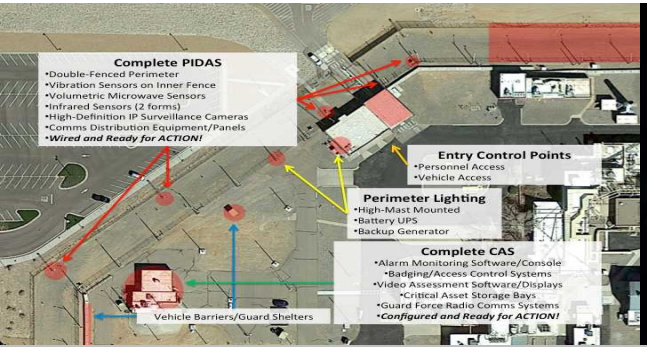
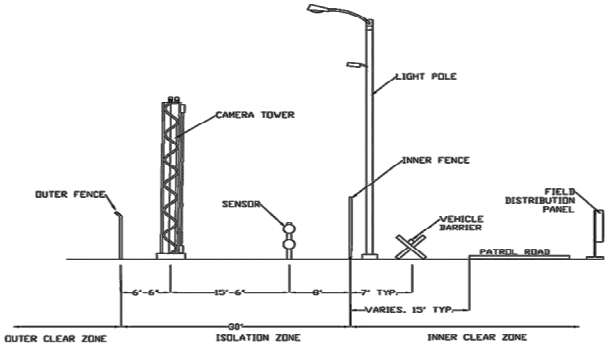
SAND2017-12084C





Potential Weaknesses in the Cyber Systems of High-Security Physical Protection Systems

John F. Clem

IAEA-CN-254-298

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

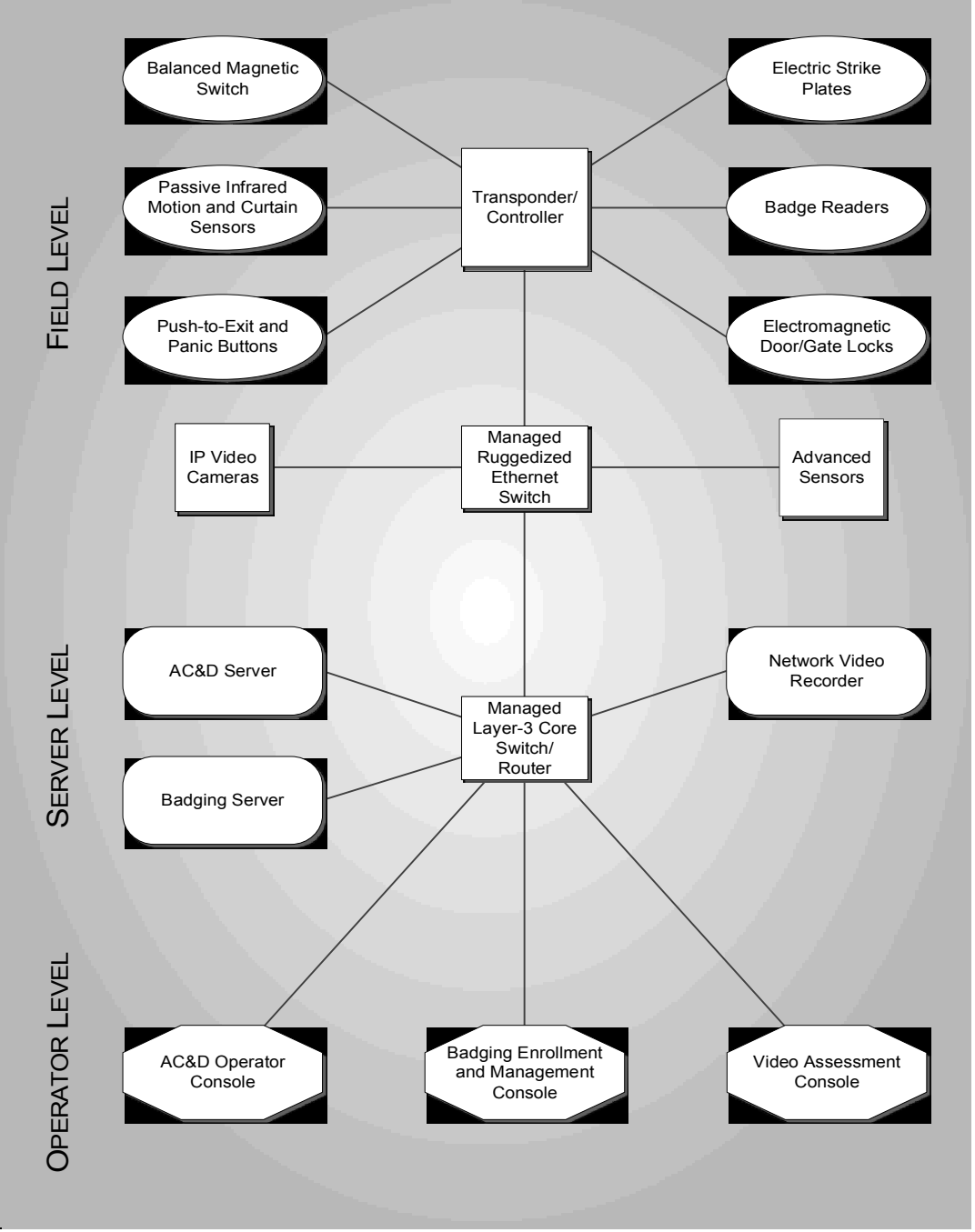
Briefing Agenda

- Problem Overview and Research Questions
- Research Facilities Supporting our R&D
- Important Results

Typical Physical Protection System

Stakeholder Questions

- **Is it possible for an adversary to find and exploit cyber vulnerabilities in a modern, high-security PPS?**
  - **Could an adversary conduct cyber exploitation to increase the chances of a successful physical attack?**
  - **Would operators be aware if their system was compromised?**
- Which subsystems and components are vulnerable?
- How does the threat of cyber exploitation change the set of attack scenarios against which the PPS is engineered to protect?



What cyber systems support a modern Physical Protection System (PPS)?

Physical protection system (PPS) hardware and networks can be abstracted into layers.

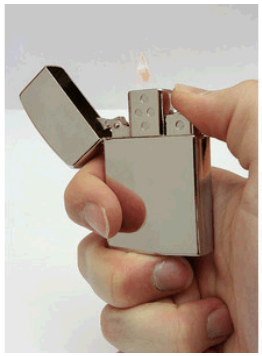
This image represents a notional system.

Cybersecurity Threats

- Modern PPS are dependent on commodity hardware and software. Time has proven that such systems used in enterprise IT and Industrial Control System environments are at risk from poor cyber hygiene:
  - Failure to apply patches promptly
  - Weak configurations
  - Insufficient protection of physical IT assets
- Undue confidence in network security
  - Logical separation techniques are potentially vulnerable
  - Detection of network intrusion is dependent on humans
- Implantation of unauthorized technology that circumvents controls

Threat Technology

- Isolation is a myth.
  - Exhibit (A) Stuxnet – sneaker net attack; target done in by a USB drive with malicious code
  - Exhibit (B) – the Pwn Plug R3, $1,160
  - Exhibit (C) – the Pwn Pad, $895

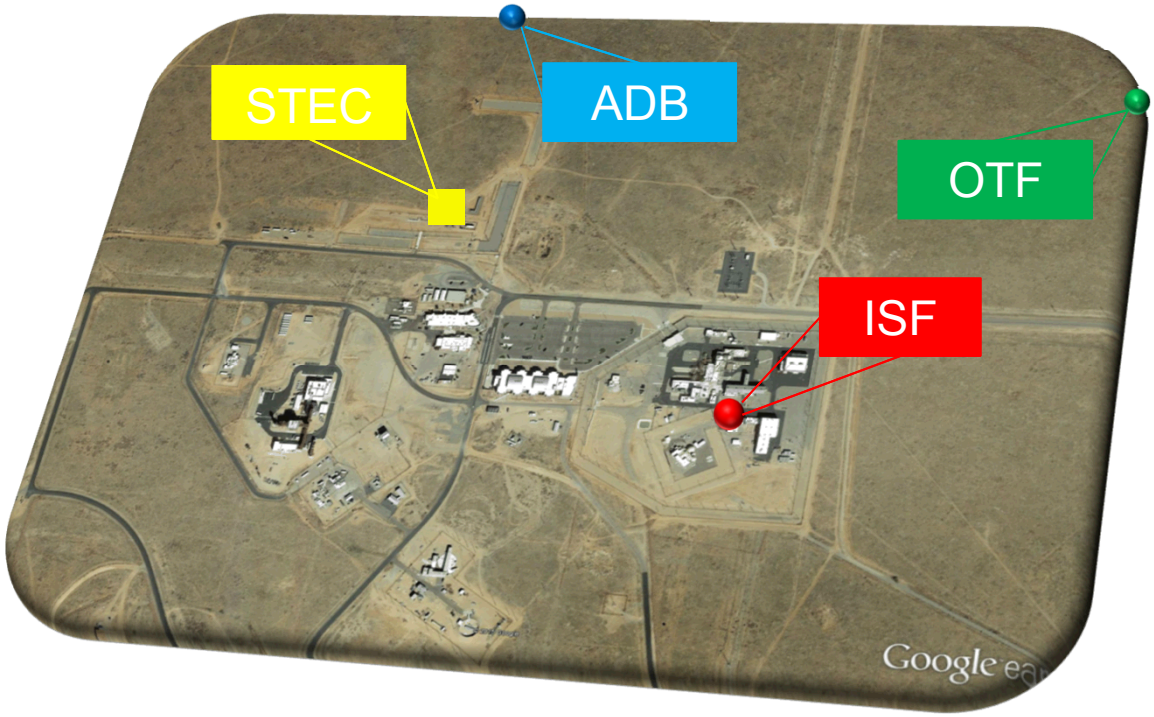


Low-cost, commercially available, innovative disrupters available to <u>anyone</u>.

Nuclear Security Technology Complex (NSTC)

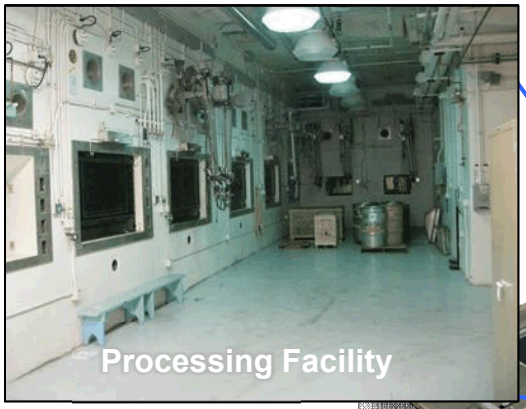
The NSTC delivers next generation solutions to critical national security issues by providing testing, evaluation, and demonstration capabilities for security technologies. The facility is comprised of:

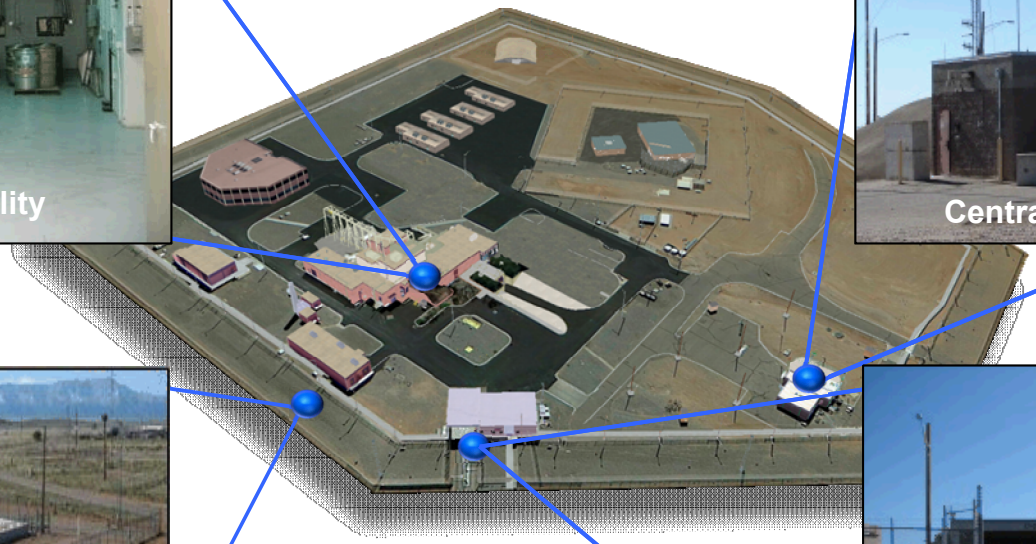
- *Integrated Security Facility (ISF)*
- *Sensor Test and Evaluation Center (STEC)*
- *Outdoor Test Facility (OTF)*
- *Access Delay Bunker/Igloo Complex*



Integrated Security Facility

The Integrated Security Facility (ISF) in Tech Area V (TA-V) provides a unique venue for physical protection, nuclear materials management, and nuclear safety training, demonstration, and equipment testing/evaluation to domestic and international partners.





Access Delay Bunker

Access Delay Test and Demonstration Area

- Remote facility for extensive testing of
  - Barriers
  - Passive and activated dispensable materials
  - Delay methodologies
- As an active lab space, this facility offers
  - Realistic environment for component and system tests
  - Opportunities for training and demonstration
  - Flexible capability for Sandia to develop expertise in all facets of access delay technologies from basic research to implementation

Attack Discovery and Exploitation

- Which PPS subsystems and components are vulnerable?
- Scratching the surface, our research targeted the access control and alarm communications and display (AC&D) systems
- Demonstrated three types of attacks against the PPS
  - From the Outside – exploited remote PPS infrastructure to target the access control system
  - Using Insider Access – implanted attacker technology to target the PPS network and access control system
  - Hacking the PPS Supply Chain – targeted the AC&D software

No system configuration changes were made to make the PPS vulnerable.

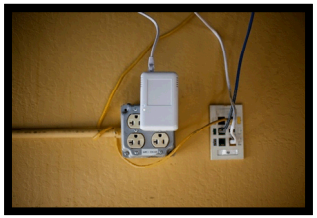
1st Attack: hacking the access control system from a remote bunker

1st Attack: hacking the access control system from a remote bunker

- Used inexpensive hardware and freely available software tools to attack the PPS:
  - Obtained blank access control cards used at target site (our testbed)
  - Compromised remote bunker PPS network point of presence (MITM)
  - Very quickly implanted rogue wireless access point (WAP)
  - Moved to “safe” distance 1km away
  - Connected to WAP/PPS network and hacked access control server
  - Enrolled “bad guy” in access control data base
  - Gave “bad guy” unfettered and undetected access to every building/room

Clever adversaries might use low-cost, commercially available technology to compromise communications and network infrastructure!

2nd Attack: implantation of attacker technology



- Implanted low-cost, commercial components with opportunistic insider access at the Central Alarm Station:
  - Two power-line ethernet comms adapters available at electronics retailers
  - One Pwn Plug: off-the-shelf security “inspection” tool
  - Quickly plugged the devices to electrical sockets in areas of low/no foot traffic
  - Quickly connected the Pwn Plug to one EoP device, and also to the nearest cellular comms tower
  - Drove to Starbucks, had a coffee and connected to the Pwn Plug, then hacked a different PPS access control server – same result ☺

Capable adversaries might use low-cost, commercially available technology to leverage cellular communications and building electrical infrastructure for nefarious purposes, while hiding their tech from system defenders!

3rd Attack: hacking the PPS supply chain

- This research attack combines a data breach, software exploitation, and social engineering:
  - Obtain a copy of the AC&D software used by the facility;
  - Reverse engineer portions of the software to identify critical functions;
  - Modify the software with malicious changes;
  - Clone the vendor's software update FTP site;
  - Upload the modified AC&D software to the attacker's FTP site;
  - Perform a spear-phishing email attack against facility personnel;
  - Confirm the email attack was successful (i.e., the facility downloaded the attacker's AC&D update); then
  - Launch a physical attack crossing the PIDAS with confidence AC&D sensor events were not transmitted to CAS operator workstations.

Each phase of this attack requires different skills and knowledge: software reverse engineering; the art of phishing; standing up a spoofed FTP site.

Caveats

- The demonstrated attacks do not guarantee that operational systems deployed in the real world are susceptible to the same attacks
- The final attack did not incorporate video surveillance systems or potential presence of guard patrols that a real-world attacker would be expected to encounter when crossing a secured boundary such as a PIDAS

Analysis & Conclusions

- Consequential cyber attacks were demonstrated against the testbed PPS
- The PPS testbed environment was judged by SNL SMEs to be representative of modern PPS found throughout the world
- Other SNL experts judged the cyber vulnerabilities discovered and exploited to be representative of those found in similar ICT environments
- The method and techniques used by SNL researchers to discover and then exploit cyber weaknesses in the PPS testbed were reflective of processes used by both cybersecurity red teams and real-world cyber attackers