Airports and their SCADA Systems

Dr Leigh Armistead, CISSP
What We May Face

For an attack to be successful it only has to cause disruption – not loss of life – to a significant number of Americans… Such a focused attack would become an immediate, and perhaps overwhelming, distraction for our national leadership…
“Weapons of Mass Disruption”

- Incidents: Continuing, Increasing, More Sophisticated
- Insurance Standards Will Increase; Insurance Will Cost More (If Available)
- Loss of Public and Customer Confidence => Potential Flood of Liability Judgments
- Demand for Safe Harbors and Risk Mitigation Measures
It gets worse with increased reliance on automated systems

- SCADA Control Systems
- Lights-Out Nodes
- Automated Switches
- Just-In-Time Deliveries, System-Based Manufacturing, etc.
- Future: Smart Houses, Intelligent Highways, Ubiquitous Information Appliances, etc.
Reduced Reaction Time

- Failure Propagation Time Decreasing Rapidly
- Fewer Circuit Breakers (Actual or Logical)
- Less Time to Muddle Through
“Information Age” depends on reliable, predictable, affordable infrastructures

- Uncertainty chills investment climate
- Unreliability raises costs, scares customers

Protection of the airports networks and systems is therefore necessary for continued expansion and daily operation
What’s so special about SCADA?

- Highly **distributed systems**
  - Control **geographically dispersed assets**, often scattered over thousands of square kilometers
- Control and monitoring data transmitted over **Long-distance communications** networks
- Most research concerning SCADA systems deals with these “standard bad examples”
  - Power grid
  - Oil and gas distribution
  - Water treatment
- The controlled assets are critical to our way of life
  - Transportation systems
  - Typically this is railroads when it should be airports
NERC Top Vulnerabilities

- Remote access to the control system without appropriate access control
- Use of inadequately secured wireless communication for control
- Insufficient application of tools to detect and report on anomalous or inappropriate activity
- Unauthorized or inappropriate applications or devices on control system networks
- Control systems command and control data not authenticated
The Key Point for Airport Systems

- Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents.

- Bottom-line:
  - They are starting to represent IT systems
  - They are being connected to the same network
  - The networks may be accessible to the public
  - Are these true in the typical airport environment?
  - SCADA systems on the same pipe? Maybe!
  - Free Wi-Fi on the same pipe? Free, anyway!
  - Separation between the two? Who knows?
Specific Airport SCADA Concerns

- What ABOUT airports? Are they vulnerable?
  - Modern airports are highly competitive cost driven operations that offer a range of public and private services
  - Many airport systems such as building control systems are SCADA controlled
    - access control and perimeter intrusion systems
    - eEnabled aircraft systems
    - radar systems
    - network-enabled baggage systems
Airport SCADA Hype

- *Expected* Threats
  - Aircraft fuel handling systems
  - Distributed airport systems such as ground approach
  - Runway signaling, radar, …

- This is based on the perceived, typical SCADA issues and concerns
Airport SCADA Reality

However…

- A widely held belief is that the SCADA systems in the airport were isolated from the main IT backbone
- Often the car parking and baggage control systems were separated from the main IT network by hardware firewalls
- These firewalls were “assumed” secure by IT staff but it was unclear who had responsibly for the managing and configuration of these firewalls
Why do these vulnerabilities exist?

- Additional services could be added to the network without all relevant IT staff being aware of the changes.
- There appeared to be no overarching group or committee that had a direct focus on cyber security measures despite the considerable size of the airport.
- Security measures were left in multiple hands and ad hoc systems were assumed isolated.
Most immediate SCADA issues

- So while there may be outside hype on enterprise Airport SCADA systems such as the radar, fuel handling, etc.
- From research conducted late last year, the main SCADA-like systems of most concern to the airport staff are as follows:
  - Automated or semi-automated baggage handling systems
  - Car parking systems (it’s the “driver” mentioned above)
Car Parking? Baggage? Seriously?

- But you can’t *get* to those car parking and baggage networks, right?
- The public network (WiFi) and the airport network were the same network but there are Firewalls between them.
- The reason that the IT infrastructure even *has* security? It has to deal with credit card transactions over the airport network, which forced these networks to become PCI compliant.”
A Network is a Network is a ..... 

- Also on this same Airport network are all of the flight arrival/departure displays ..... 
- Plus this system (ie the same network) also has of the departure displays at the gates ... 
- In addition, this common Airport network also hosts all of the tag scanners for the baggage handlers .... 

- Everything is interconnected and no one in monitoring the network holistically
How does this affect you?

- Realization that Airports face a management challenge as well as a technical challenge
- Development of “Risk Management” Approach
- Growing interest from
  - Auditors
  - Insurance Industry
  - Attorneys
- You need to look at continuing to maximize computer connectivity as an open invitation to malicious activity (at best) and cyber terrorism (at its extreme)
Risk Management Approach

- Poor Operational Coordination & Readiness

Symptoms
- No Common Training or Doctrine
- Inadequate communication across different airport departments, with no one group looking at airport security from a holistic viewpoint

- No Real Scenario-Based Combined Planning

- Policy and Standards are important too!
The SCADA Standards Labyrinth

- The good thing is that
  - There’s plenty to choose from!
- NIST (for about everyone)
  - Enhancement to 800-53
  - 800-82
- NERC (for the power industry)
  - In Hindi it means “Hell”... Coincidence?
  - Cyber protection CIP augmentations, Being enforced from July 2009
- ISO / IEC standards
Conclusions

- Because of the ubiquity of network-enabled airports connected both internally and externally, network security is paramount to ensuring international transportation safety.
- SCADA is important, but in areas that most do not.
- Each is different with particular quirks; there is no standardization in the IT infrastructures available or used at a particular location.
- Airports continue to integrate more and more functionality into the infrastructures, including Electronic Flight Bags and back-office systems.
Summary

- Cyber Security for Airport SCADA systems is a real vulnerability for needs to be part of a holistic solution to maintaining a smooth running operation.

- All systems connected to the network must be evaluated for the threats they introduce and an enterprise approach to protecting Airports must consider who has access to what, when and how often....
Questions?
Dr Leigh Armistead, CISSP

President
Peregrine Technical Solutions
114 Ballard Street
Yorktown, VA 23690-0520

larmistead@gbpts.com

(757) 581-9550