SANS SCADA Security Summit 2008

Jeff Fay

1

Common SCADA Security Issues

- **Common COTS Operating Systems**
- **Systems are rarely patched**
- **Weak or default manufacturer passwords**
- **SCADA networks are almost never air-gapped**
- **Insecure Modem connections**

PATCH ADVISOR

2

Real Examples: Power Company (1)

- Unpassworded modem dial-ups found less than a dozen phone numbers away from main number
  - PcAnywhere with no password
  - SGI Irix with system default passwords
- Many administrator level accounts on main Windows server with password of "password"
- Improperly configured "captive" account on VMS nuclear power monitoring systems found (Radiation Safety Monitoring on the core)

PATCH ADVISOR

3

Real Examples: Power Company (2)

- Compromised Windows Workstation through un-patched Web server – obtained local SAM file with domain accounts
- Compromised Windows domain by escalating privileges with access gained from previous machine
- Compromised Power Grid Engineer's personal workstation with Domain Admin rights
- Pulled VNC hash from workstation registry
- Compromised Power Grid Management Unix systems through applications run locally (using VNC) from Engineer's Workstation

PATCH ADVISOR

4

Real Examples: Power Company (3)

- Open wireless allowed access to primary internal network
- The network was a large flat network with direct access to SCADA systems
- Plant Management/process control systems were running unpatched Windows-based systems
- In addition, numerous modem dialups into SCADA communications processors
- Some dialups allowed access to substation communications processors through default manufacturer passwords

PATCH ADVISOR

5

Other Environments

- Similar examples have been seen in the following:
  - Oil Refineries
  - Automated Manufacturing
    - Circuit board printing
    - Factory robotics control
    - Food Processing
  - Water Treatment Facilities
  - Transportation

PATCH ADVISOR

6