SESSION ID: SBX4-R3

SCADA 101

Johnny Xmas
Security Researcher
Uptake
@j0hnnyxm4s

Adam Ringwood
Security Researcher
Uptake
@avidhacker
OPERATIONAL TECHNOLOGY OVERVIEW
IT versus OT

- Windows & *nix Servers
- Ethernet Networking Equipment
- Laptops & Desktops
- TCP / IP

- Electromechanical Equipment
- Real-time Operating Systems
- Simple CPUs
- SCADA & Other Comms
HMIs & PLCs

Programming Logic Controller

Modbus TCP/IP

Human Machine Interface

PLC

PLC
COMMUNICATION METHODOLOGY
Communication Methods

- Modbus/TCP Masters and/or Slaves
- PLC
- HMI
- SCADA
- Modbus over Ethernet TCP/IP
- OPC Servers/Application(s)
- Shared Memory
- Coiling Blocks
- Holding Blocks
- Modbus/TCP
- Ethernet Network
- DeviceMaster UP 2-Port
- DeviceMaster UP 1-Port
- RS-485
- RS-232
- Modbus Serial Slaves
- Modbus Serial Master
- RS-485
- Private Serial Bus
- Serial Master
- Private Serial Slaves
- Serial Connections
- Ethernet Connections
- Ethernet TCP/IP Socket Connections
- Master-to-Master Communication
- Contained In

Modbus Router Firmware
The Purdue Model Simplified

- **Level 0**: Device & IO / Physical Layer
- **Level 1**: Automation Control
- **Level 2**: Supervisory Control & Data Acquisition (SCADA)
- **Level 3**: Site Operations & Control (MES)
- **Level 4**: Business Planning (ERP)
- **Level 5**: Enterprise Integration
The Purdue Model Detailed
INDUSTRIAL PROTOCOLS
MODBUS (MODicon BUS)
Live Hacks

- Modbus Set Point Injection
- CIP Replay Attack
THANK YOU

Johnny Xmas
Security Researcher
Uptake
Johnny.Xmas@Uptake.com

Adam Ringwood
Security Researcher
Uptake
Adam.Ringwood@Uptake.com