Serial Security

Michael Milvich
Cyber Security Researcher

February 3rd, 2009

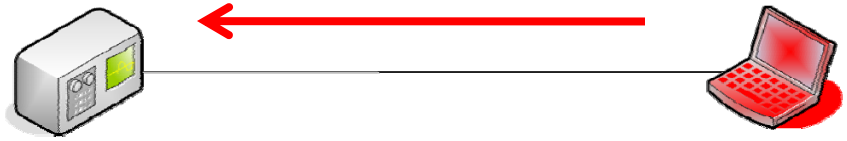
Idaho National Laboratory

Introduction

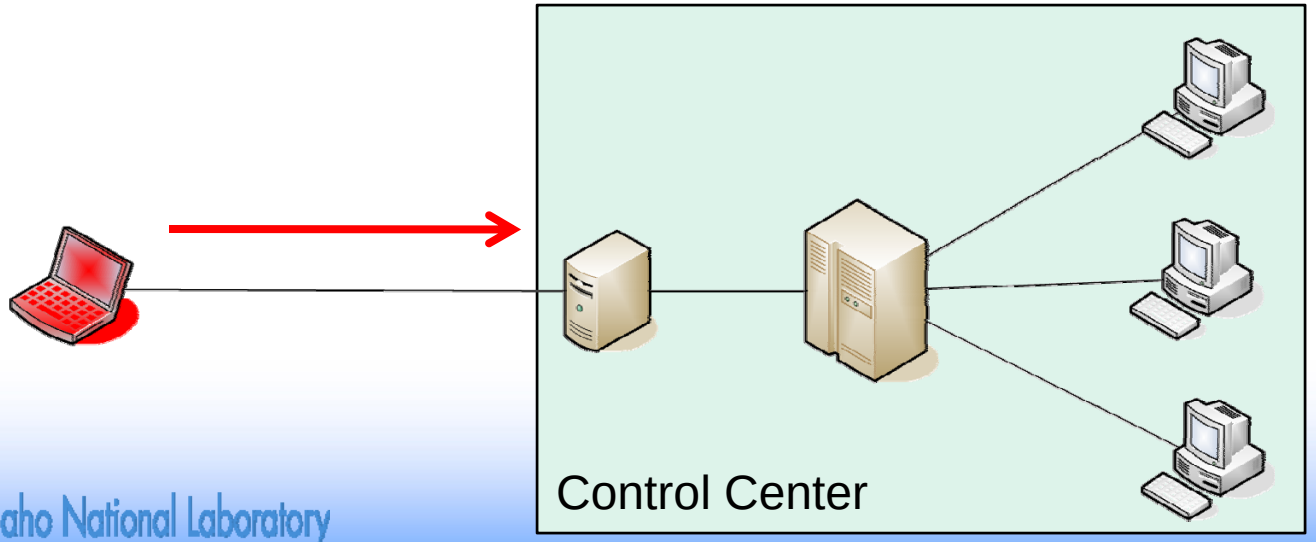
- **Cyber Security Researcher**
  - Have performed several in-house and on-site assessments
  - Have worked with serial and TCP/IP based protocols
  - Have found many exploitable vulnerabilities in SCADA systems

Direction of Attacks

- **Attacking remote device**



- **Attacking control center from a remote device**

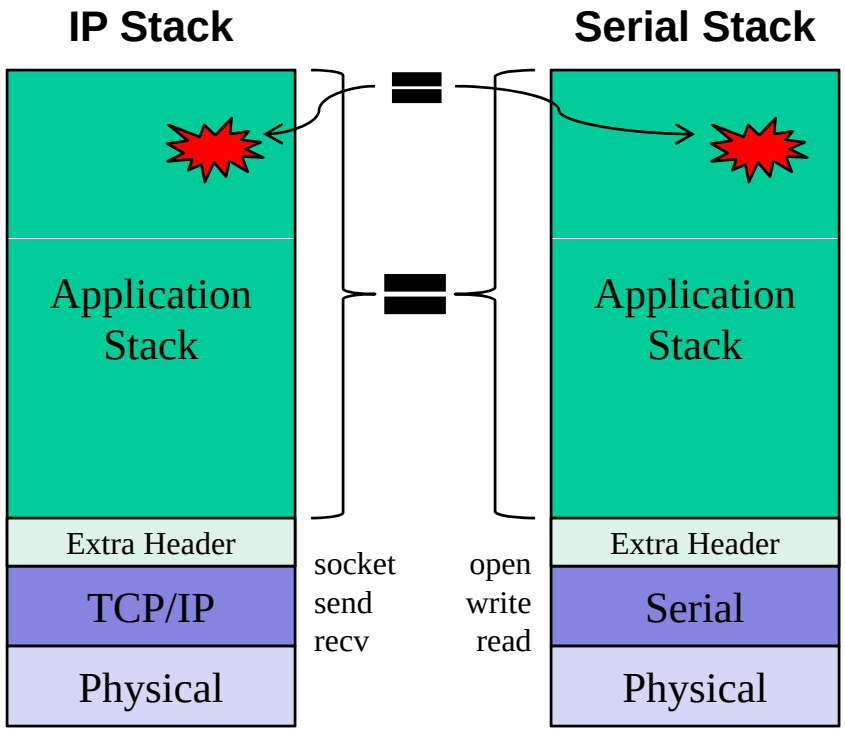


Remote Devices

- **Access Control**
  - Most remote devices have poor authentication
    - Still using default passwords
    - Password disabled
    - Vendors have installed backdoor (maintenance) accounts
  - Protocols without authentication
- **Exploitable Vulnerabilities**
  - Can be used to compromise the remote device

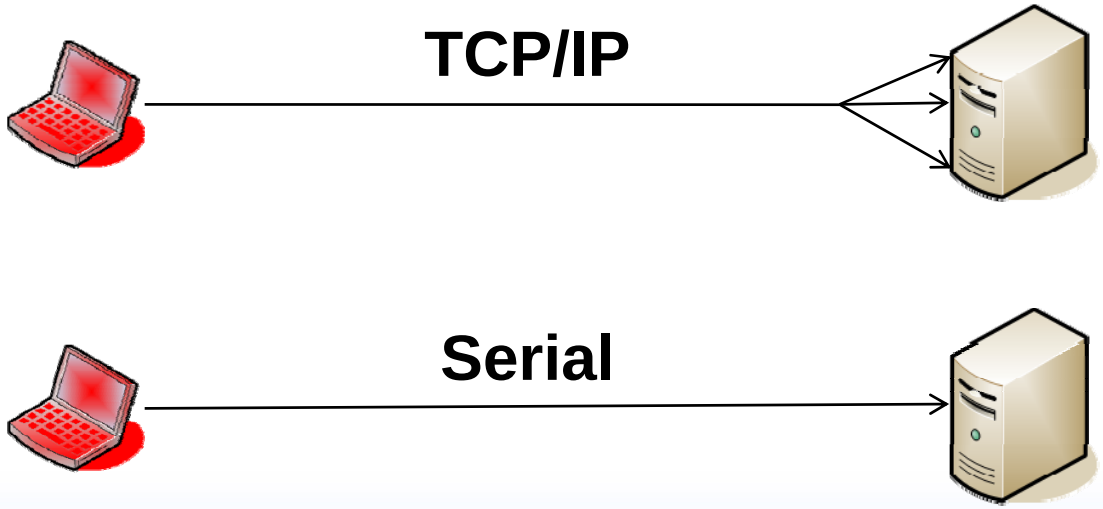
Are Serial Comms Exploitable?

- **Have assessed multiple protocols over IP and Serial for vulnerabilities**
  - Majority of the code is reused
  - Send becomes write, recv becomes read
  - Sometimes there is an additional header over the TCP/IP or Serial layer
  - Vulnerabilities found in the application stack running over IP are almost always also found in the serial version
  - Have used the same exploit to compromise a TCP/IP link and a serial link
  - Very useful to “hack back” into the control center



Exposure – Attack Surface

- **Service Exposure**
  - IP runs multiple services, increasing attack surface
  - Serial runs one service, decreasing attack surface



Exposure – Gaining Access

- **War Dialing**
  - Still have unsecured remote devices
- **Wireless**
- **Physical Access**
  - How secure are the remote substations?
- **Hack the Telco**
  - No such thing as a point to point line anymore
  - Social Engineering

Conclusion

- **Yes, serial communications are vulnerable**
- **Can be used to “hack back” into a control center**
- **Exposure of serial lines is less than TCP/IP but should not be ignored**