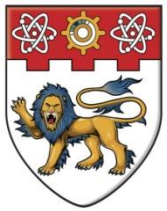


NANYANG TECHNOLOGICAL UNIVERSITY

Security Issues in SCADA Networks

by V. M. Igure, S. A. Laughter, and R. D. Williams
Computers & Security, 25(7): 498-506, 2006

presented by

Ruilong Deng
Postdoctoral Research Fellow
School of Electrical and Electronic Engineering

25 July 2014

1. Introduction

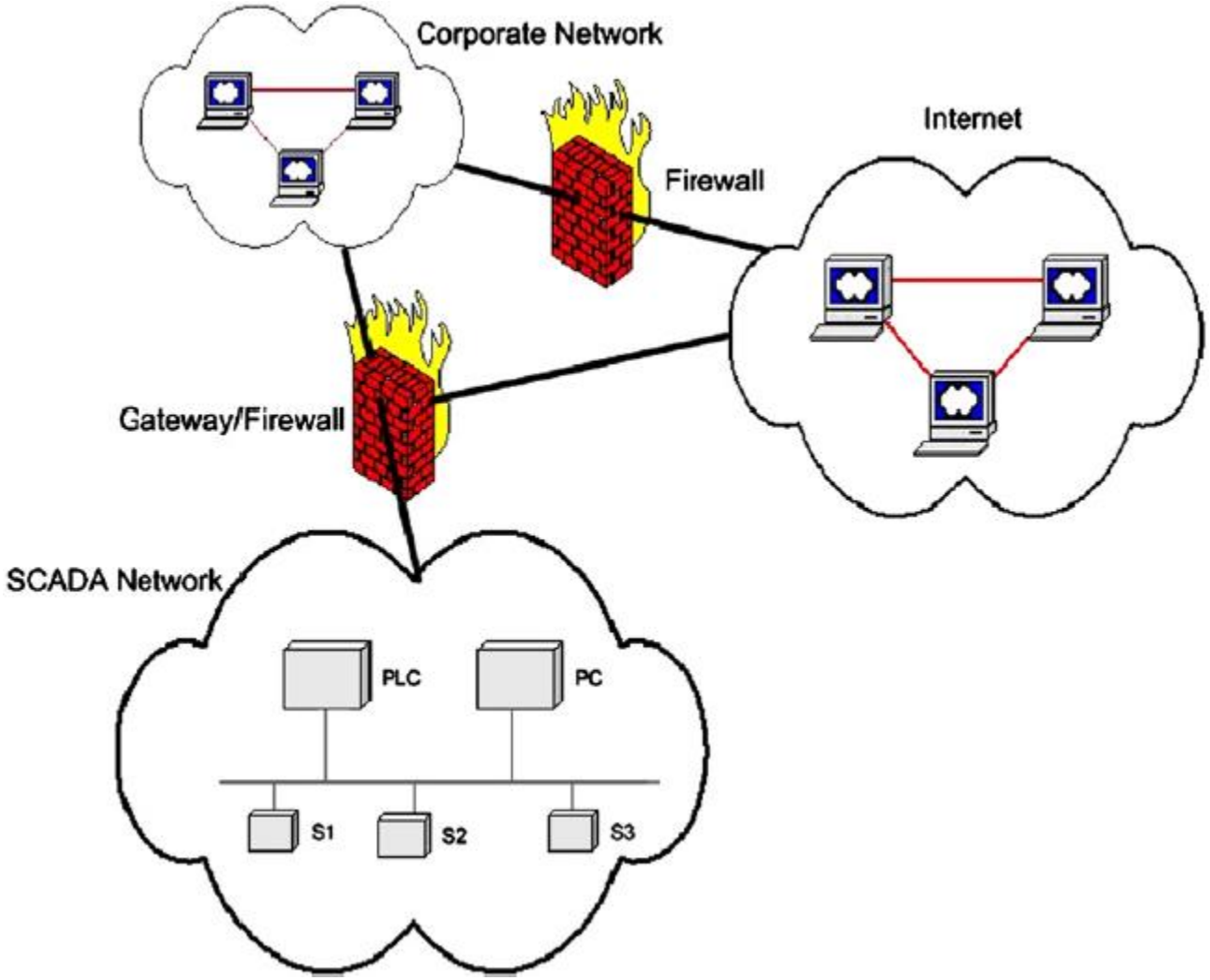
- Evolution of control networks
  - simple point-to-point networks
    - monitoring/command device
    - remote sensor/actuator
  - complex networks with field bus communication (SCADA)
    - central control unit
    - remote terminal unit (RTU)

- Why face security issues
  - increasing interconnectivity of SCADA networks
  - connect to outside corporate network/Internet via gateways

2. SCADA Network Architecture

- SCADA network
  - interconnection for field devices on plant floor
    - PC/PLC (programmable logic controller)
    - remote sensor/actuator
  - field bus protocol-based network
    - mater-slave/client-server communication
    - peer-to-peer communication
- Corporate network/Internet
  - IP-based network
- Gateway
  - interface between field bus protocol/IP-based networks

2. SCADA Network Architecture (cont'd)



3. Security Threats & Vulnerabilities

- Why face security issues
  - connectivity between plant floor and corporate network
    - simple, isolated control network → complex inter-network
  - increased interconnectivity of SCADA networks
    - multiple access points → physical isolation does not guarantee security
    - phone line/intranet → connection from local to outside network
- Attacker aim to compromise SCADA security
  - integrity
  - confidentiality
  - authentication
  - availability
  - privacy of data

3. Security Threats (cont'd)

- Security threats and vulnerabilities
  - sniff communication traffic
    - gain unauthenticated access to confidential information
  - tamper with data transmitted/stored
    - compromise data integrity
    - change control signal: cause device malfunction
    - change set point: device fail at very low threshold or alarm not go off when it should
    - change operator display value: when alarm actually go off, human operator is unware of it
  - DoS (denial-of-service) attack
    - block/reroute communication traffic
  - plant malicious code
    - obtain greater network access/cause other damage

4. SCADA Security Research Challenges

- Overview
  - improve access control
  - improve security inside SCADA network/develop efficient security-monitoring tool
    - detect intrusion and/or other suspicious activities
  - improve security management
- Constraint
  - limitation of field bus network
    - slow communication rate (3125 Kbps)
    - small message packet (a few octets)
    - real-time operating requirement

4.1 Access Control

- Challenge
  - difficulty in defining perimeter to SCADA network
    - gateways are not the only means of connection to outside
    - other unexpected links: phone line/intranet
    - apart from technical access control, clearly define security policy
  - gateway authentication
    - provide protocol compatibility between local and outside networks
    - assign login account to authorized user
    - password-based authentication
    - smart card-based authentication
    - ... ...

4.2 Firewalls and IDSs

- Challenge
  - block unauthorized access
    - recognize/allow specific traffic
    - control/monitor activity of authorized access (permission)
  - 3-zone architecture for firewalls
    - SCADA or process control network, demilitarized zone (buffer), corporate network
  - micro-firewalls
    - embedded within each field device
    - many field devices do not have enough computational capability
  - few commercial firewalls/IDSs (intrusion detection systems) capable of monitoring SCADA protocol traffic
    - structure of SCADA protocol
    - vulnerability assessment of SCADA protocol

4.3 Protocol Vulnerability Assessment

- Challenge
  - two categories of SCADA protocol vulnerabilities
    - inherent in protocol specification itself
    - result of improper implementation of protocol
    - the latter is easier
  - taxonomy of SCADA protocol vulnerabilities
    - require database of vulnerabilities
    - no public database of SCADA protocol vulnerabilities

4.4 Cryptography and Key Management

- Challenge
  - SCADA protocols do not support complex cryptography implementation
    - limited computational capability of field device
    - low rate data transmission on SCADA network
    - real-time response requirement on device
  - WSNs (wireless sensor networks) have similar operating constraints
  - techniques to implement cryptography in WSNs could possibly be applied to SCADA network

4.5 Device and OS Security

- Challenge
  - security of end devices on SCADA network
    - embedded computing device (printer, router)
    - real-time operating system (RTOS)
    - other real-time control software
    - more susceptible to DoS attack
  - vulnerability assessment of end device and their embedded operating system
  - not practical to provide physical protection to every node
    - OS equipped with tamper-resistant feature
    - existing ones can be prohibitively expensive for SCADA network
    - low-cost alternative with almost same level of security
    - network survive from compromise of a few devices

4.6 Security Management

- Challenge
  - security policy tailored to specific company
    - not possible to develop common security policy meet all companies goal/requirement/need/objective
  - provide guideline for critical administration issues
    - data security policy
    - communication security policy
    - audit security policy
    - physical security policy
  - continuous process
    - constantly monitor SCADA network for security vulnerabilities
    - regularly update/secure with latest patches on SCADA network software/hardware
    - regular maintenance on system

5. Conclusion

- Security issues in SCADA networks
  - introduction
  - SCADA network architecture
  - security threats and vulnerabilities
  - SCADA security research challenges
    - access control
    - firewalls and intrusion detection systems
    - protocol vulnerability assessment
    - cryptography and key management
    - device and OS security
    - security management

Any comments to share with us? ☺