Cybersecurity for Critical Industrial Systems

Nasser S. Abouzakhar

10th Nov, 2015
Content

- Introduction
- Security Threats
- Security Process
- Recent Projects

Introduction
Introduction: Identifying Critical Systems

US Nuclear Regulatory Commission (NRC), 2010
A forecast of the share of Internet economy in the GDP in 2016

http://www.statista.com

Cyberattack causes physical damage for the second time ever

Amid all the noise the Sony hack generated over the holidays, a far more troubling cyber attack was largely lost in the chaos. Unless you follow security news closely, you likely missed it.

I'm referring to the revelation, in a German report released just before Christmas (PDF), that hackers had struck an unmanned steel mill in Germany. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive" — though unspecified — damage.
Net Losses: Estimating the European Cost of Cybercrime

Source: McAfee 2014 Report
Apollo 11 - 1969

Source: http://www.computerweekly.com/
Internet Live Statistics

- Twitter Usage Statistics
- Internet Live Statistics

A Twitter bot predicted the Paris shootings 2 days before it happened

- despite the shootings happening on November 13th, 2015

http://skeptics.stackexchange.com/
Security Threats

- Application Backdoors to manipulate database
- Compromised PLC could manipulate sensor values or disrupt chemical operation
- Weak Firewall Rules
- Insecure Wireless Link

Unauthorised remote access to SCADA system and data e.g. identify active processes or send false commands

ICS Network
DMZ

- Remote Station: A Technical equipment that contains a PLC and RTU.
- RTU receives and translates signals from the sensors.
- PLC generates control signals e.g. a PLC monitors temp and turns on a heater if a gauge exceeds a certain temp as part of an industrial process.
- Ability to read, modify and fabricate industrial protocol messages e.g. production disturbances
Security Threats, cont.

• Through **reconnaissance**, attackers gain understanding of the control process
  – Communication protocols refer to devices by numbers
  – Unique numbers of sensors, pumps, etc. **stored in a DB**
Security Threats, cont.

Security Threats, cont.
Security Process
Cybersecurity Organisational Standards

- ISO/IEC 27032: The international Standard focusing explicitly on cyber security.
- BSI Standards on IT and Cyber Security
  - BS ISO/IEC 27032:2012, Guidelines for cybersecurity
  - BS ISO/IEC 27037:2012, Guidelines for identification, collection, acquisition, and preservation of digital evidence
- UK Government standards on IT and Cyber Security
  - Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks (BIS/14/696)
- GPG13 (Good Practice Guides)

Security Process

- Assets Identification
- System Monitoring
- Risk Assessment
- Defences Implementation
- Penetration Testing
Penetration Testing

- A process of evaluating industrial systems and networks by validating their security settings, functions and capabilities
- To ensure services utilisation and minimise exploitations
- To improve the quality of the systems operability

Penetration Testing Life Cycle

- **Reconnaissance**
  - Network enumeration
  - Nodes & Services identification
  - Passive scanning

- **Vulnerability Scanning**
  - Scan targets
  - Information retrieval
  - Vulnerabilities identification

- **Exploitation**
  - Validate vulnerabilities
  - Compromise systems
  - Launch attacks

- **Reporting**
  - Document findings
  - Prioritise vulnerabilities
  - Propose recommendations
  - Maintain access
Recent Projects

3 Phase Power Grid for City and Neighbourhood Sub-systems

Source: Gani Nashi, 2015
PLC Controlled Paint Mixer


Intrusion Detection Evaluation

Jiyan Mahmud, 2014
Webcam Remote Access

Anomalous Text Detection
