On Building Secure SCADA Systems using Security Patterns

E.B.Fernandez, J.Wu, M.M. Larrondo-Petrie, and Y. Shao
Dept. of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL, USA

Outline

- SCADA Systems
- Security Issues
- Model of a General SCADA System
- Some potential attacks
- Patterns
- Security Patterns
- Securing a SCADA system by adding security using patterns
- Examine how security measures guard against attacks
- Conclusions and Future Work

SCADA

- To continuously monitor and control the different sections of a plant in order to ensure its appropriate operation we use SCADA systems

  Supervisory
  Control
  And
  Data
  Acquisition

- SCADA systems are applied for electric power generation, water treatment, oil refining, etc.

Security issues

- SCADA systems were first designed to meet the basic requirements of process control systems where security issues were hardly a concern
- However, the growing demands for increased connectivity between a SCADA system and other network components, such as the corporate network and the Internet, expose the critical parts of a SCADA system to the public
- Therefore, security issues can no longer be ignored.

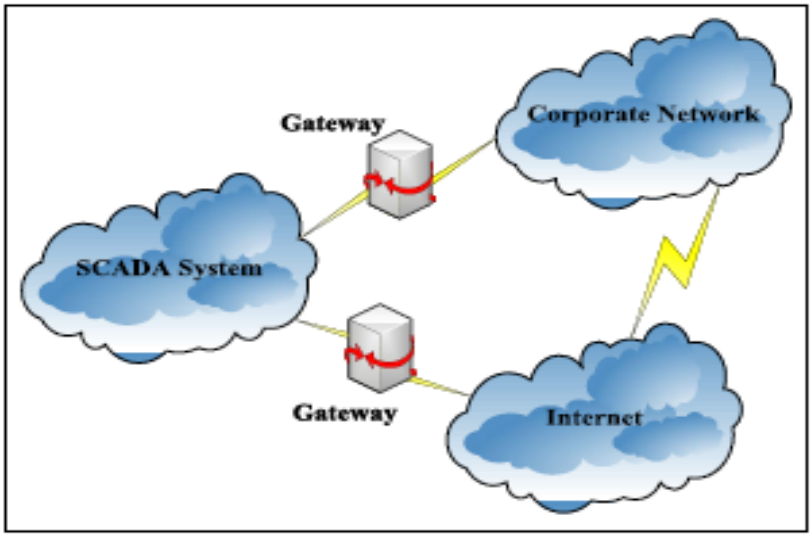


Figure 2. An example of a SCADA system connected to both the corporate network and the Internet.

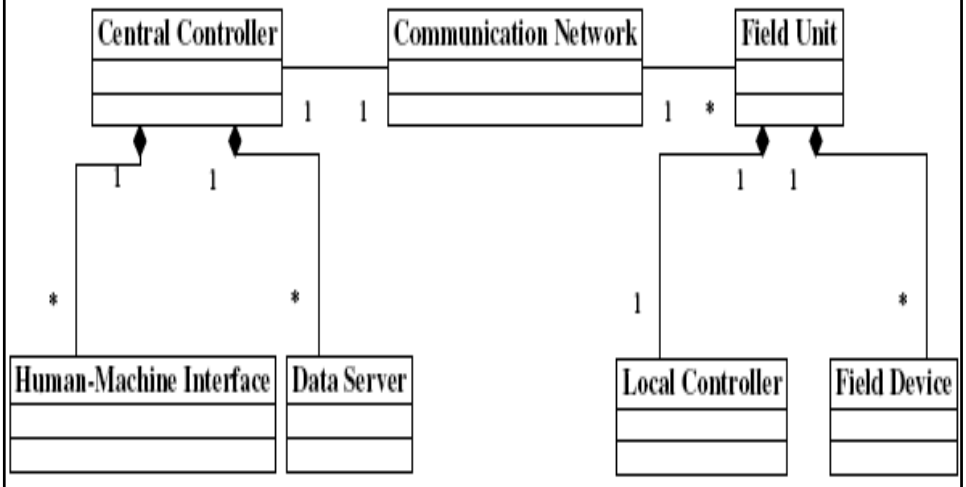


Figure 1. Class diagram for a general SCADA system.

Attacks against SCADA Systems

- We systematically enumerate the threats against a system by considering its use cases and activities and possible ways of subverting them.
- A simplified approach looks at possible attacks against each unit of a system if its structure is predefined.

Attacks against SCADA Systems considering attacks against/thru each unit

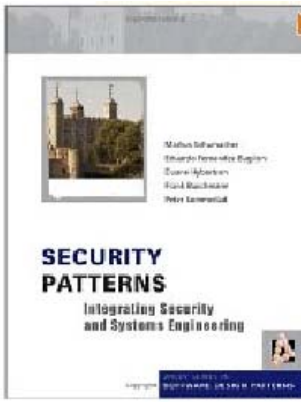
- **Central controller**, include
  - T1: physical attacks
  - T2: malicious settings of the field units
  - T3: wrong commands to the field units
  - T4: malicious alteration of the runtime parameters of the central controller
  - T5: denial of service attacks
- **Field Units**, include
  - T6: physical attacks
  - T7: malicious alteration of the runtime parameters of the field unit
  - T8: wrong commands to the field units
  - T9: malicious alarms to the central controller
  - T10: denial of service attacks
- **Communication Networks**, include
  - T11: sniffing
  - T12: spoofing
  - T13: denial of service attacks

Patterns

- Many problems occur in similar ways in different contexts or environments. Generic solutions to these problems can be expressed as patterns.
- A *pattern* is an encapsulated solution to a problem in a given context and can be used to guide the design or evaluation of systems
- Analysis, design, and architectural patterns are well established and have proved their value in helping to produce good quality software

Security patterns

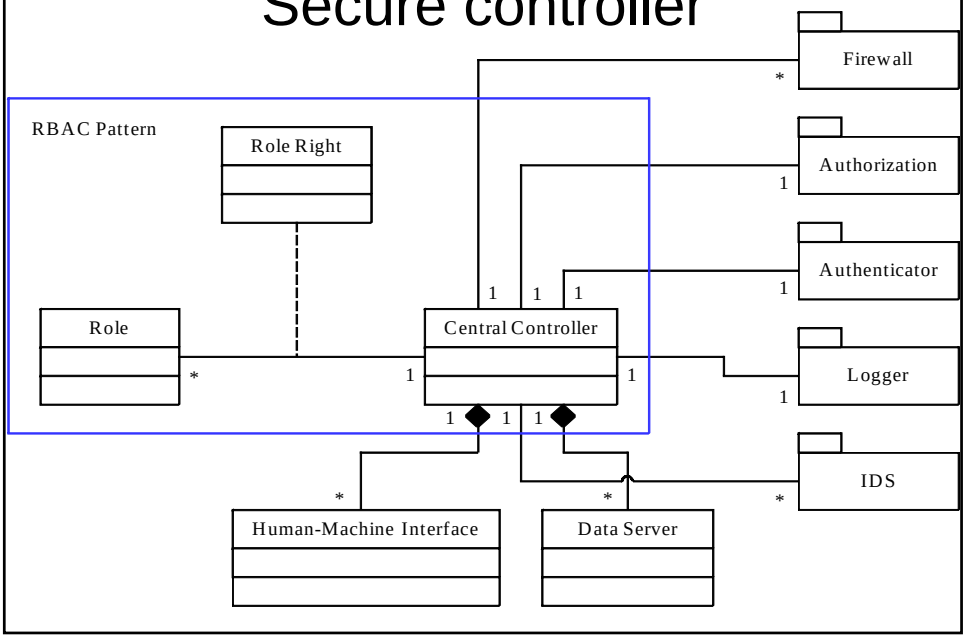
- *Security patterns* have joined analysis, design and architectural patterns and they are becoming accepted by industry
- Security patterns are useful to guide the security design of systems by providing generic solutions that can stop a variety of attacks.
- We have produced a book on security patterns and many patterns that cover all architectural levels



Securing systems

- We add instances of security patterns to the functional models
- Possible patterns include
  - authorization (Access matrix),
  - Role-Based AccessControl (RBAC),
  - Multilevel access,
  - Logger,
  - Authentication,
  - Firewalls,
  - Intrusion Detection Systems

Secure controller



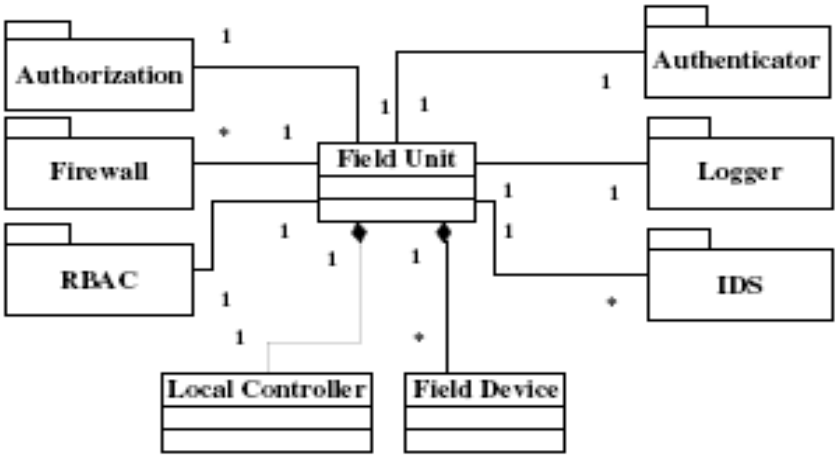


Figure 4. Secure field unit where security patterns are applied.

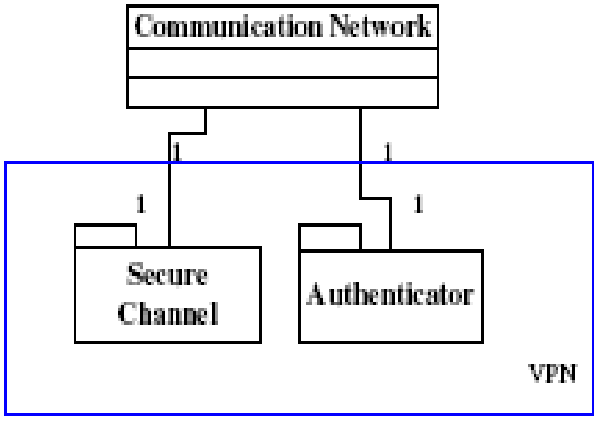


Figure 5. Secure communication networks where security patterns are applied.

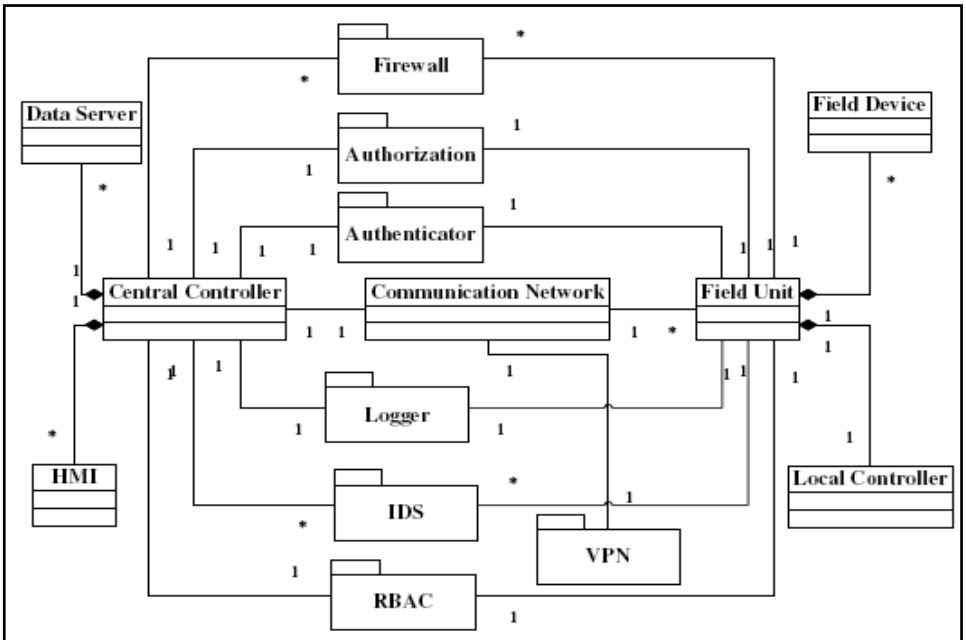


Figure 6. Class diagram for the secure SCADA pattern.

Related Work

SCADA Systems

- A. Miller. Trends in process control systems security. *IEEE Security and Privacy*, 3(5):57–60, 2005.
- V. M. Igure, S. A. Laughter, and R. D. Williams. Security issues in SCADA net-works. *Computers & Security*, 25(7):498– 506, 2006.
- D. Goeke and H. Nguyen. SCADA system security, 2005
- U.S. Department Of Energy. 21 steps to improve cyber security of SCADA networks.
- S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes. Using model-based intrusion detection for SCADA networks. In *Proc. of the SCADA Security Scientific Symposium*, Miami Beach, FL, USA, January 2007

Related Work

Security Patterns

- J. Yoder and J. Barcalow. Architectural pat-terns for enabling application security. In *Proc. of PLoP*, 1997. Also Chapter 15 in *Pattern Languages of Program Design*, vol. 4 (N. Harrison, B. Foote, and H. Rohnert, Eds.), Addison-Wesley, 2000.
- M. Schumacher, E. B. Fernandez, D. Hy-bertson, F. Buschmann, and P. Sommerlad. *Security Patterns: Integrating Security and Systems Engineering.* John Wiley & Sons, Inc., 2006.
- E. B. Fernandez. Security patterns. In *Proc. of International Symposium on System and Information Security*, 2006.
- E. B. Fernandez and R. Pan. A pattern lan-guage for security models. In *Proc. of the 8th Annual Conference on the Pattern Languages of Programs (PLoP 2001)*, Urbana, Illinois, USA, 11-15 September 2001.

Conclusions

- We considered the use of security patterns to analyze, build and evaluate a secure SCADA system
- In particular, we study the architecture of a general SCADA system and analyze the potential attacks against it
- We use security patterns as a tool to design secure SCADA systems that can control these attacks
- We believe our research work defines a new direction for future research on secure SCADA systems by indicating where security should be applied in the software lifecycle
- We will complete our methodology by applying more security patterns to different layers and types of SCADA systems
- Physical access control can also be integrated by using appropriate patterns

Acknowledgement

This research was partly funded by the Department of Defense

Questions

Secure Systems Research Group
www.cse.fau.edu/~security
to join email: ed@cse.fau.edu