On Building Secure SCADA Systems using Security Patterns

Eduardo B. Fernandez
Dept. of Comp. Sci. & Eng.
Florida Atlantic University
Boca Raton, FL 33431-0991
+1 (561) 297-3466
ed@cse.fau.edu

Jie Wu
Dept. of Comp. Sci. & Eng.
Florida Atlantic University
Boca Raton, FL 33431-0991
+1 (561) 297-3491
jie@cse.fau.edu

M. M. Larrondo-Petrie
Coll. of Eng. & Comp. Sci.
Florida Atlantic University
Boca Raton, FL 33431-0991
+1 (561) 297-3899
petrie@fau.edu

Yifeng Shao
Dept. of Comp. Sci. & Eng.
Florida Atlantic University
Boca Raton, FL 33431-0991
+1 (561) 297-3491
yshao1@cse.fau.edu

ABSTRACT
Critical infrastructure systems are important systems that support our daily lives. Protecting these systems is attracting attention from the research community. The key component of a critical infrastructure system is the process control system, also known as the supervisory, control, and data acquisition (SCADA) system. On the other hand, security patterns are a well established concept that are used to analyze, construct and evaluate secure systems. This paper aims to propose methods to build a secure SCADA system using security patterns. In this paper, we study the architecture of a general SCADA system and analyze the potential attacks against it. Also, we use security patterns as a tool to design a secure SCADA system that is resistant to these attacks. We believe our research work lays a new direction for future research on secure SCADA systems.

Categories and Subject Descriptors
D2 Software Engineering, D2.1 Requirements/specifications, D2.11 Software architecture D2.13 Reusable software H4 Information systems applications

General Terms
Design, Security.

Keywords
Critical infrastructure systems, process control systems, SCADA systems, security patterns, software architecture.

1. INTRODUCTION
Modern industrial facilities such as water supply systems, electric power generation plants and oil refineries often involve components that are geographically distributed. To continuously monitor and control the different sections of the plant in order to ensure its appropriate operation leads to the use of Supervisory Control and Data Acquisition (SCADA) systems. A SCADA system normally supports communication between a central control unit and multiple remote units equipped with sensors, actuators, and/or Programmable Logic Controllers (PLCs).

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.

A secure system protects itself against attacks using security countermeasures categorized into five groups: Identification and Authentication, Access Control and Authorization, Logging, Cryptography, and Intrusion Detection. Security patterns describe mechanisms that fall into (combinations of) these categories as well as the abstract models that guide the design and evaluation of these mechanisms [1, 2].

Here we consider the use of security patterns to define, in a systematic way, the defenses that we need in order to secure such a system. Our approaches are based on a secure software development methodology [3]. The methods proposed in this paper define a new direction for research on secure SCADA systems.

While many approaches to secure SCADA systems exist, e.g., [4, 5, 6, 14], none of them makes use of security patterns. The use of such patterns allows a designer to apply security throughout the lifecycle of an application (see Section 4 for a detailed discussion).

The rest of this paper is organized as follows. In Section 2, we briefly review the concepts of SCADA systems, analyze the threats and vulnerabilities of these systems, and illustrate the basic aspects of security patterns. Section 3 presents the methodology through a case study. Section 4 considers related work. We conclude this paper in Section 5.

2. PRELIMINARIES
In this section, we discuss the architecture of a SCADA system, followed by an analysis of the vulnerabilities of current SCADA systems. Also, we illustrate some concepts regarding security patterns.

2.1 SCADA Systems
Basically, a SCADA system consists of field units, a central controller, and communication networks that connect these

CSIIR'09, April 13–15, 2009, Oak Ridge, TN, USA.

components. A field unit consists of field devices and a local PLC. Field devices, such as actuators and sensors, are monitored and controlled by a local PLC. The central controller is generally geographically separated from these field units and typically has advanced computation facilities. A typical central controller may be equipped with data servers, Human-Machine Interface (HMI) stations, and other servers with advanced computation capabilities to aid the operators in managing the entire plant. Figure 1 is a class diagram for a basic SCADA architecture. The functions of the central controller include sending settings to the field units, sending commands to the field units, and receiving status information from the field units. The functions of the field units include monitoring the environment, taking actions on the environment, and sending status information and/or alarms to the central controller if necessary. The functions of the communication networks include forwarding data and commands.

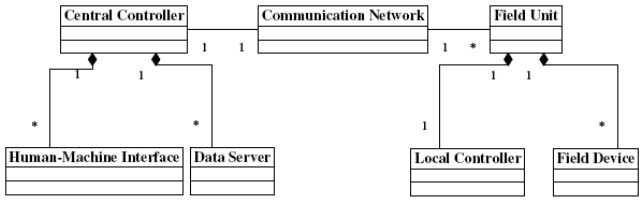


Figure 1. Class diagram for a general SCADA system

Modern SCADA systems are normally connected to the corporate networks and/or the Internet through specialized gateways, an example of which is shown in Figure 2. The gateway is used to provide protocol conversion between two different networks. The MODBUS protocol is currently one of the most popular and widely-used protocols with SCADA systems [5]. Since SCADA systems have a standard structure, we devise a specified pattern (SCADA *pattern*) to define and model them. From this point of view, Figure 1 describes the static structure of this pattern.

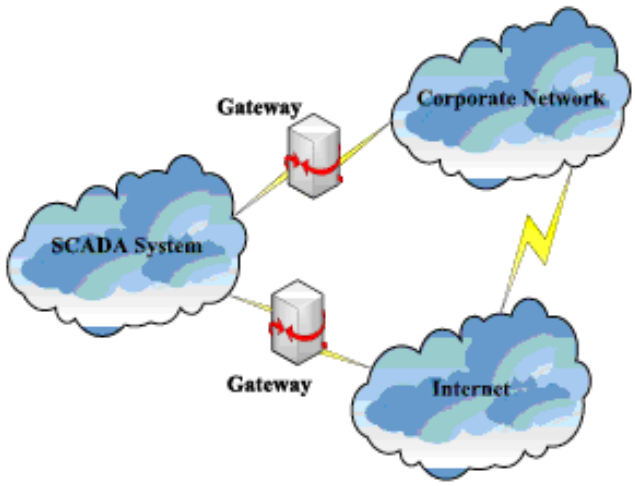


Figure 2. An example of a SCADA system connected to both the corporate network and the Internet.

2.2 Attacks against SCADA Systems

Until recently, SCADA systems were electronically isolated from all other networks and hence not likely to be accessed by outside attackers [7]. As a result, the security issues of a SCADA system focused on physical security such as physical access control. However, the fact is that the growing demands of the industry for increased connectivity between the SCADA system and the corporate network (and/or the Internet) result in an increase in security threats and vulnerabilities that are not limited to physical attacks. A recent study shows that prior to 2000, almost 70% of the reported incidents of SCADA systems were either due to accidents or to disgruntled insiders acting maliciously. Since 2001, apart from an increase in the total number of reported incidents, almost 70% of the incidents were due to attacks originating from outside attackers [8].

We can systematically enumerate the threats against a system by considering its use cases and activities, and analyzing possible ways of subverting them [9]. A simplified approach is to look at possible attacks against each unit of a system if its structure is predefined.

Here, we list some potential attacks against a general SCADA system. Recalling that in Figure 1, a general SCADA system is mainly composed of a "central controller", "communication networks" and "field units", we categorize attacks corresponding to these three components.

- Attacks against/through the central controller include those such as (i) physical attacks (T1), (ii) malicious settings of the field units (T2), (iii) wrong commands to the field units (T3), (iv) malicious alteration of the runtime parameters of the central controller (T4), and (v) denial of service attacks (T5).
- Attacks against/through the field units include those such as (i) physical attacks (T6), (ii) malicious alteration of the runtime parameters of the field units (T7), (iii) wrong commands to the field units (T8), (iv) malicious alarms to the central controller (T9), and (v) denial of service (T10).
- Attacks against/through the communication networks include (i) sniffing (T11), (ii) spoofing (T12), and (iii) denial of service (T13).

Attacks against the central controller and the network are more harmful since they may disable the whole system whereas attacks against field units only affect specific units.

2.3 Security Patterns

A pattern is a packaged solution to a recurrent problem. As indicated earlier, Figure 1 is actually a pattern for a SCADA system. Security patterns aim to join the extensive knowledge accumulated about security to provide guidelines for secure system construction and evaluation. Security patterns can be considered as a type of architectural pattern in that they usually describe global software architecture concepts. Security patterns can be considered to be a type of design pattern as well due to the fact that security can be considered as an aspect of a software unit. Also, security patterns are a type of analysis pattern in the sense that security constraints should be defined at the highest possible level of a software. A security pattern is composed of a thumbnail of the problem it solves, the context where the pattern is applicable, a brief description of how it solves the problem, the static structure of the solution (usually UML class diagrams), the dynamic structure of the solution (usually UML sequence diagrams), and guidelines for implementation of this pattern. A standard template is typically used to organize this information [2].

One way to classifying existing security patterns is to classify them according to the different software layers to which they apply. At the highest level (the application layer), existing security patterns include the Authorization Pattern [2, 10], the Role-Based Access Control (RBAC) Pattern [2, 10], the Reference Monitor Pattern [2], the Multilevel Security Pattern [2, 10] and the Attribute-Based Access Control (ABAC) Pattern [11]. Other patterns apply to firewalls and operating systems [2].

3. SECURING A SCADA SYSTEM

In this section, we propose a method to analyze, build and evaluate secure SCADA systems using security patterns. Intuitively, we use security patterns to stop and/or prevent the attacks listed in Section 2.2. As a matter of fact, the result of our solution is a security pattern itself which is called the *Secure SCADA Pattern* and which can be used as a guideline for building secure SCADA systems.

Central controller. To stop T1, we use security patterns for physical access control such as the Role-Based Access Control (RBAC) Pattern combined with the Authenticator Pattern and the Logger Pattern. To stop T2, T3, and T4, we use the Authorization Pattern together with the Authenticator Pattern and the Logger Pattern. To stop T5, we use the Firewall Pattern together with an Intrusion Detection System (IDS) pattern. Note that the implementation of the Firewall pattern can be situated at different layers of a system (e.g., the application layer and the network layer). Figure 3 depicts the class diagram for the secure central controller where necessary security patterns are applied. Also note that the users' actions are controlled at the HMI, which acts as a Concrete Reference Monitor [2] for user interactions.

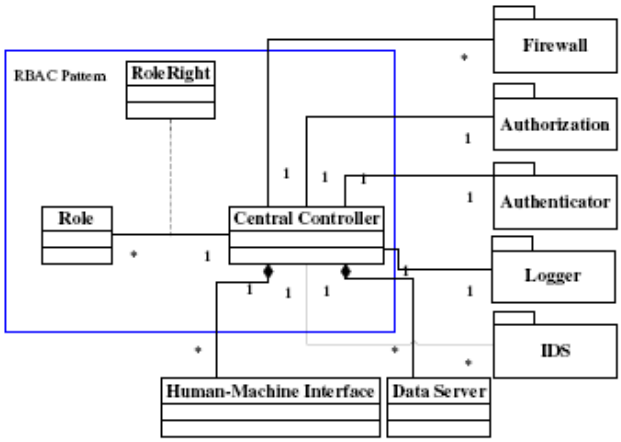


Figure 3. Secure central controller where security patterns are applied.

Field units. To stop T6, we use the RBAC pattern combined with the Authenticator Pattern and the Logger Pattern. We use the Authorization pattern together with the Authenticator pattern and the Logger pattern to stop T7, T8 and T9. By applying the Firewall pattern together with the IDS we can stop T10. Figure 4 shows the class diagram for the secure field unit where necessary security patterns are used.

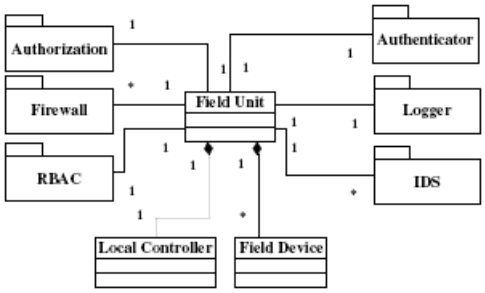


Figure 4. Secure field unit where security patterns are applied.

Communication networks. To stop T11, we use cryptography-based methods such as secure channels [12]. To stop T12, we use the Authentication pattern in the sense that every message in the system is associated with a valid signature before sending. In practice, we implement the above mechanisms using VPNs. Stopping T13 is out of the scope of this paper. Figure 5 shows the class diagram for the secure communication networks where necessary security patterns are used.

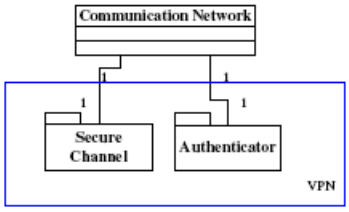


Figure 5. Secure communication networks where security patterns are applied.

Secure SCADA pattern. Note that the structure of the class diagram in Figure 3 is almost the same as that in Figure 4. This is due to the fact that the central controller and the field units are exposed to similar attacks. As a result, we produce the Secure SCADA Pattern which combines Figures 3, 4 and 5 as shown in Figure 6.

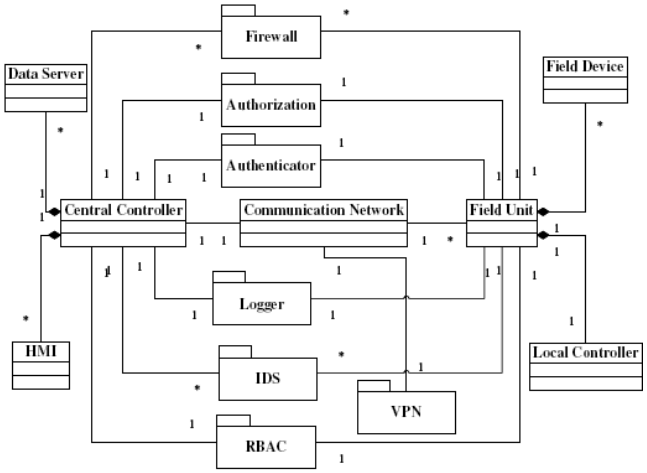


Figure 6. Class Diagram for the secure SCADA pattern

4. RELATED WORK

In this section, we describe recent works related to this paper.

SCADA systems. [13] offered an overview of technologies related to SCADA systems. Security issues regarding SCADA systems were discussed in [14, 6, 5, 15, 4]. In [14], Miller discussed the importance of the availability of process control systems within critical infrastructure systems and tried to call attention to the security aspects of these systems. In [6], Igure et al. did a survey on the research challenges of the security of modern SCADA systems. In [5], Goeke et al. examined the weakness of SCADA systems and proposed corresponding solutions. In [15], the U.S. Department of Energy proposed 21 suggestions to prevent attacks from the communication networks. In [4], Cheung et al. proposed a method to detect attacks towards SCADA systems using model-based intrusion detection. None of these studies considered the use of security patterns.

Security patterns. Security patterns were first proposed as a research paper by Yoder et al. in [16]. [2] reviewed most of the existing security patterns and provided system designers with guidelines for using security patterns to build secure systems. More information regarding the concepts of security patterns and the principles of building secure systems using security patterns were illustrated in [1, 10]. None of the proposed patterns apply specifically to SCADA systems.

5. CONCLUSION

This paper considers 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. Also, we use security patterns as a tool to design a secure SCADA system 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 in our future work by applying more existing security patterns to different layers of SCADA systems. Also, we will devise methods to adapt our secure SCADA systems to specific use. Another direction is to add constraints to the patterns to make them more precise and rigorous. Physical access control can also be integrated by using appropriate patterns [17]. In this paper, we have merely shown the idea of security patterns. We need a complete definition using an appropriate template as in [2].

ACKNOWLEDGMENTS

This research was partly funded by the Department of Defense.

REFERENCES

[1] E. B. Fernandez. Security patterns. In *Proc. of International Symposium on System and Information Security*, 2006.

[2] M. Schumacher, E. B. Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad. *Security Patterns: Integrating Security and Systems Engineering.* John Wiley & Sons, Inc., 2006.

[3] E. B. Fernandez, M. M. Larrondo-Petrie, T. Sorgente, and M. VanHilst. *Integrating security and software engineering: Advances and future vision*, Chapter 5, A methodology to develop secure systems using patterns, pages 107–126. IDEA Press, 2006.

[4] 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.

[5] D. Goeke and H. Nguyen. SCADA system security. http://islab.oregonstate.edu/koc/ ece478/05Report/Goeke-Nguyen.pdf, 2005.

[6] V. M. Igure, S. A. Laughter, and R. D. Williams. Security issues in SCADA networks. *Journal of the Computers & Security*, 25(7):498–506, 2006.

[7] A. Risley, J. Roberts, and P. Ladow. Electronic security of real-time protection and SCADA communications. In *Proc. of the 5th Annual Western Power Delivery Automation Conference*, 1-3 April 2003.

[8] E. Byres and J. Lowe. The myths and facts behind cyber security risks for industrial control systems. In *Proc. of VDE Congress*, Berlin, Germany, 2004.

[9] E. B. Fernandez, M. VanHilst, M. M. L. Petrie, and S. Huang. Defining security requirements through misuse actions. *Advanced Software Engineering: Expanding the Frontiers of Software Technology*, 219:123–137, 2006.

[10] E. B. Fernandez and R. Pan. A pattern language 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.

[11] T. Priebe, E. B. Fernandez, J. I. Mehlau, and G. Pernul. A pattern system for access control. In *Proc. of the 18th. Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, 2004.

[12] A. Braga, C. Rubira, and R. Dahab. *Pattern Languages of Program Design 4*, chapter 16, Tropyc: A pattern language for cryptographic object-oriented software. Addison Wesley Publishing Company, 1999. Also in *Proc. of PLoP*, 1998.

[13] S. A. Boyer. *Supervisory Control and Data Acquisition*. ISA – The Instrumentation, Systems and Automation, 1999.

[14] A. Miller. Trends in process control systems security. *IEEE Security and Privacy*, 3(5):57–60, 2005.

[15] U.S. Department Of Energy. 21 steps to improve cyber security of SCADA networks. http://www.oe.netl.doe.gov/docs/

[16] J. Yoder and J. Barcalow. Architectural patterns 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.

[17] E. B. Fernandez, J. Ballesteros, A. C. Desouza-Doucet, and M. M. Larrondo-Petrie. Security patterns for physical access control systems. In *Proc. of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, Redondo Beach, California, USA, pp. 259-274, 8-11 July 2007.

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.

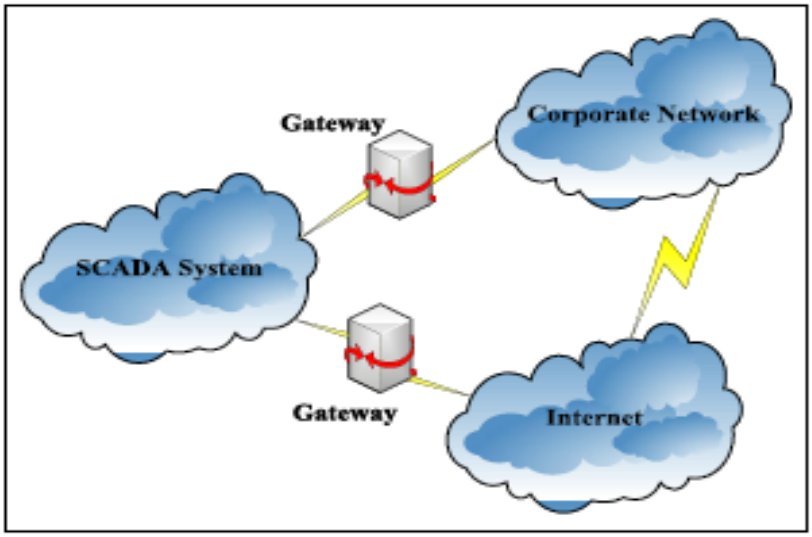


Figure 2. An example of a SCADA system connected to both the corporate network and the Internet.

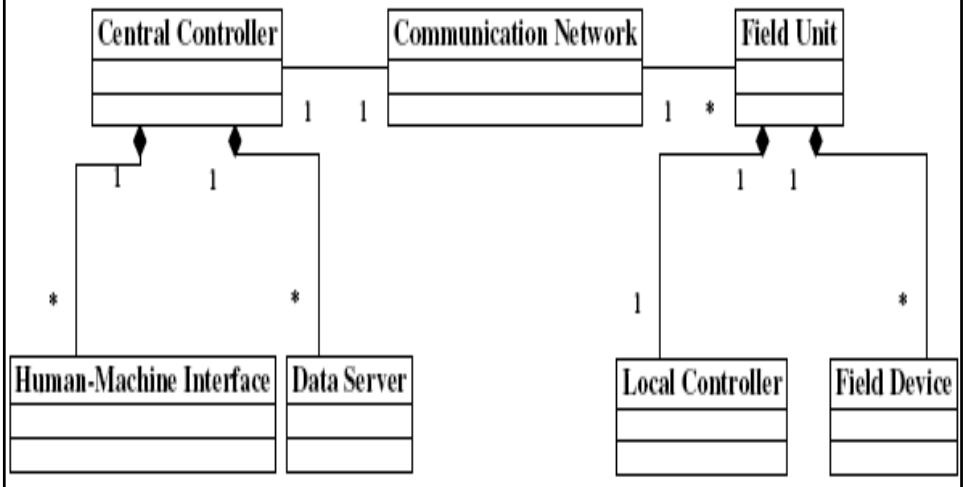


Figure 1. Class diagram for a general SCADA system.

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

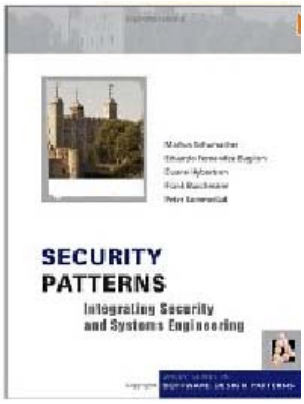
- **Central controller**, include
  - T1: physical attacks
  - T2: malicious settings of the field units
  - T3: wrong commands to the field units
  - T4: malicious alteration of the runtime parameters of the central controller
  - T5: denial of service attacks
- **Field Units**, include
  - T6: physical 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

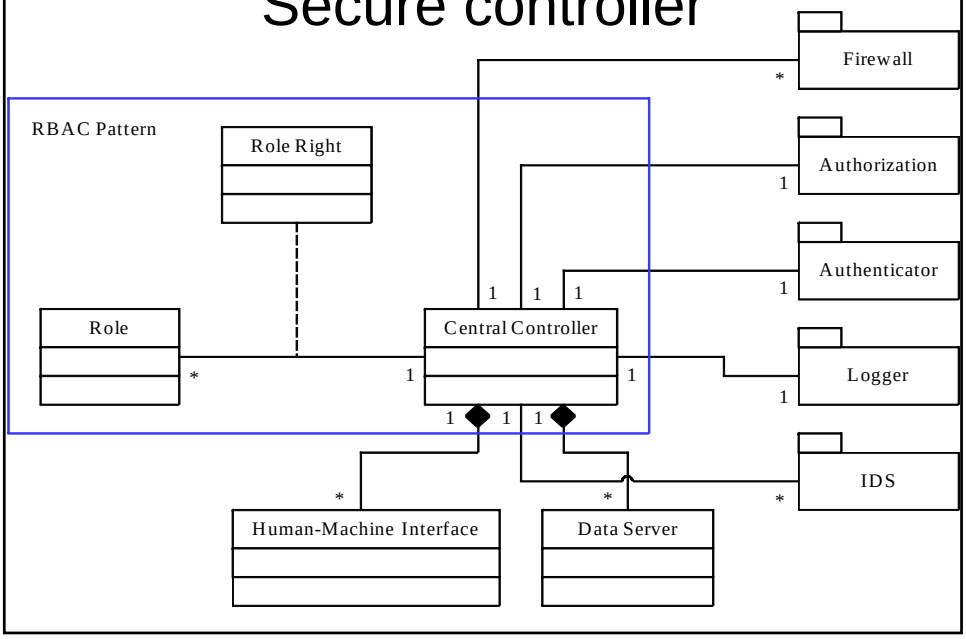
- *Security patterns* have joined analysis, design and architectural patterns and they are becoming accepted by industry
- Security patterns are useful to guide the security design of systems by providing generic solutions that can stop a variety of attacks.
- We have produced a book on security patterns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



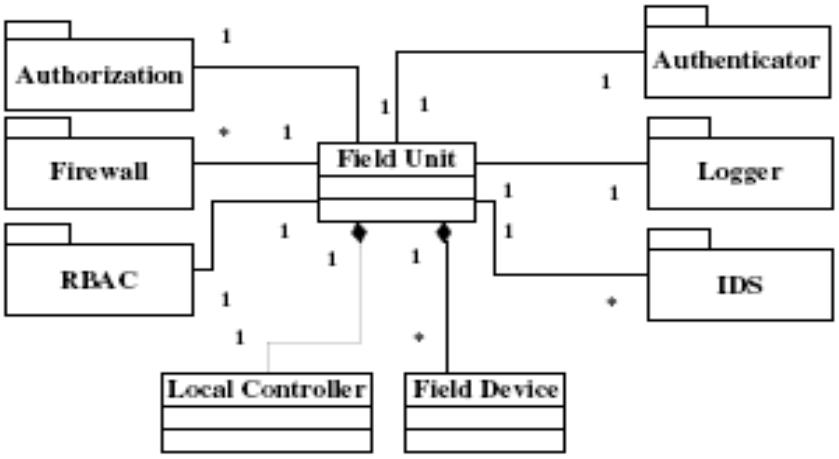


Figure 4. Secure field unit where security patterns are applied.

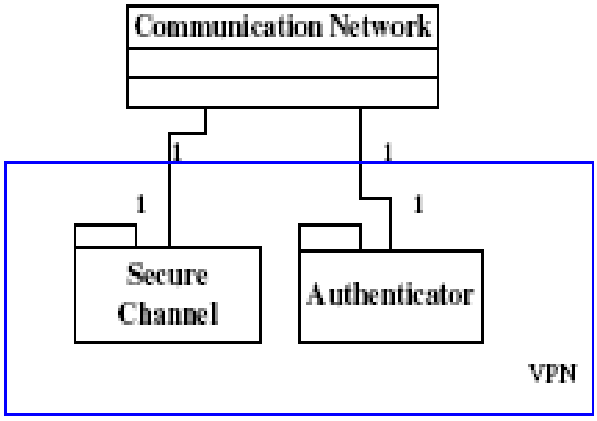


Figure 5. Secure communication networks where security patterns are applied.

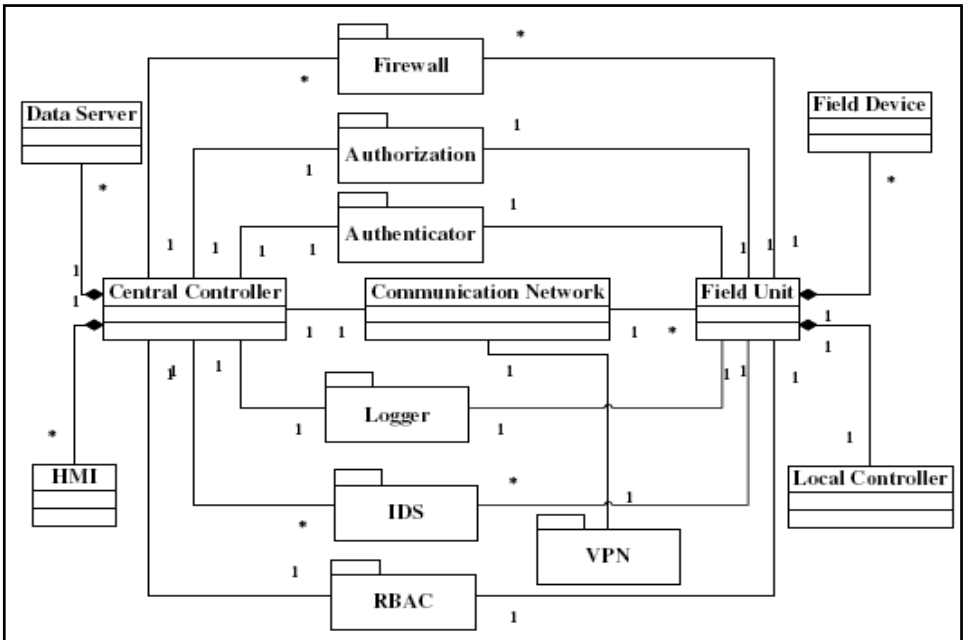


Figure 6. Class diagram for the secure SCADA pattern.

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