Chapter 24

ATTACK PATTERNS: A NEW FORENSIC AND DESIGN TOOL

Eduardo Fernandez, Juan Pelaez and Maria Larrondo-Petrie

Abstract A pattern is an encapsulated solution to a problem in a given context that can be used to guide system design and evaluation. Analysis, design and architectural patterns are established formalisms for designing high quality software. Security patterns guide the secure design of systems by providing generic solutions that prevent a variety of attacks. This paper presents an attack pattern, a new type of pattern that is specified from the point of view of an attacker. The pattern describes how an attack is performed, enumerates the security patterns that can be applied to defeat the attack, and describes how to trace the attack once it has occurred. An example involving DoS attacks on VoIP networks is used to demonstrate the value of the formalism to security designers and forensic investigators.

Keywords: Attack patterns, forensics, secure systems design, VoIP networks

1. Introduction

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 that can be used to guide system design and evaluation [10]. Analysis, design and architectural patterns are established formalisms for designing high quality software. Another type of pattern, the antipattern, focuses on design pitfalls [13]. Security patterns, on the other hand, guide the secure design of systems by providing generic solutions that prevent a variety of attacks [9, 18]. However, it is not clear to an inexperienced designer which pattern should be applied to stop a specific attack. Likewise, the patterns have limited forensic applications because they do not emphasize the *modus operandi* of attacks.

In order to design a secure system or investigate a security breach it is important to understand the possible threats to the system. We have proposed a systematic approach to threat identification involving the analysis of the use cases of a system [9]. This method identifies high-level threats such as "the customer can be an impostor," but once a system is designed, it is necessary to analyze how the various system components could be exploited in an attack.

This paper presents an attack pattern, a new type of pattern, which draws on our previous research on security patterns and threat identification. An attack pattern is specified from the point of view of an attacker. It describes how an attack is performed, enumerates the security patterns that can be applied to defeat the attack, and describes how to trace the attack once it has occurred (including specifying the types of evidence and the locations where the evidence may be found). An example involving DoS attacks on VoIP networks is used to demonstrate the value of the formalism to security designers and forensic investigators.

2. Attack Patterns

An attack pattern is presented from the point of view of an attacker. It specifies a generic way of performing an attack that takes advantage of specific vulnerabilities in a certain environment. The pattern also presents a way to counteract the development of the attack in the form of security patterns and to analyze the information collected at each stage of the attack.

This section presents a template for an attack pattern [2], which has been used for architectural patterns (design) and security patterns (defense) [18]. However, certain sections of the template have been modified to fit the new attacker's viewpoint. The sections of the attack pattern template are described below.

- **Name:** Specifies the generic name given to the attack in a standard attack repository (e.g., CERT [4] or Symantec [21]).
- **Intent:** A short description of the intended purpose of the attack.
- **Context:** A description of the general environment, including the conditions under which the attack occurs. This may include system defenses as well as system vulnerabilities.
- **Problem:** Defines the goal of the attack pattern, which (from the attacker's point of view) is the "problem" of attacking the system. An additional problem occurs when a system is protected by certain defensive mechanisms and these mechanisms have to

be overcome. The forces (a term used in pattern writing) are the factors that may be required to accomplish the attack, the vulnerabilities to be exploited, and the factors that may obstruct or delay the attack.

- **Solution:** Describes the solution to the attacker's problem: How the attack is performed and its expected results. UML class diagrams may be used to describe the system before and during the attack. Sequence diagrams could be used to display the messages exchanged during the attack. State or activity diagrams may be used to provide additional detail.
- **Known Uses:** Specific incidents that are involved in the attack. Details of previous attacks are useful in deciding how to stop the attack and where to look for evidence.
- **Consequences:** Describes the benefits and drawbacks of the attack from the attacker's viewpoint. In particular, whether the effort and cost of the attack are commensurate with the results obtained, and the possible sources of failure.
- **Countermeasures and Forensics:** This new section of the template is required for attack patterns. It describes the measures taken to stop, mitigate and trace the attack. This implies an enumeration of the security patterns that are effective against the attack. From a forensic viewpoint, this section of the template describes the information can be obtained at each stage when tracing the attack and the information that can be deduced to identify the specific attack. Also, it may indicate the additional information that should be collected to support a forensic investigation.
- **Evidence Locations:** This section may include a diagram with selected UML classes and associations relevant to a forensic investigation. UML class diagrams are useful because of their abstraction properties. The attack pattern is not a comprehensive representation of all the classes (network components) and associations involved in an attack. Rather, the pattern should represent the classes that are relevant to the investigation. When primary sources (e.g., firewalls and IDSs) do not contain enough evidence, investigators must examine secondary sources such as terminal devices (including wireless devices), servers and network storage devices.
- **Related Patterns:** This section of the template includes patterns of other attacks with different objectives that are performed in a

similar way or attacks with similar objectives that are performed in a different way.

3. VoIP Denial-of-Service Attack

This section presents an attack pattern that describes a denial-of-service (DoS) attack against a VoIP network.

- **Intent:** The VoIP DoS attack is intended to overwhelm the client's and/or server's resources and disrupt VoIP operations by producing a flood of messages or by degrading the quality of messages, preventing subscribers from using the service effectively.
- **Context:** VoIP services should be available to subscribers trying to establish voice conversations over VoIP channels. The VoIP network should have adequate capabilities (routing, bandwidth and QoS) to meet peak communication loads. Some VoIP systems use control protocols (e.g., MGCP and Megaco/H.248) and security mechanisms (e.g., access control and firewalls) to manage the media gateways deployed across the infrastructure. More secure VoIP implementations may employ intrusion detection systems, firewalls on phones and authentication facilities.
- **Problem:** The problem from the point of view of an attacker is to conduct a DoS attack against VoIP services. The attack can be carried out by exploiting the following vulnerabilities:
  - VoIP security is in a relatively immature state; security expertise and standards are lacking. Users might inadvertently expose the system. While basic countermeasures such as IDSs and firewalls are available, administrators may not configure them correctly.
  - VoIP networks have been designed and deployed with an emphasis on functionality rather than security [23]. Advanced defenses (e.g., strong authentication mechanisms) are rarely employed.
  - VoIP is vulnerable to DoS attacks that are not an issue in the circuit-switched public telephone system.
  - With the rush to implement new VoIP systems, features and standards, implementation flaws are common. Moreover, IP-PBXs include many layers of software that may contain vulnerabilities. Programming errors (e.g., not checking the size of the parameters in a protocol request) can be exploited in several ways:

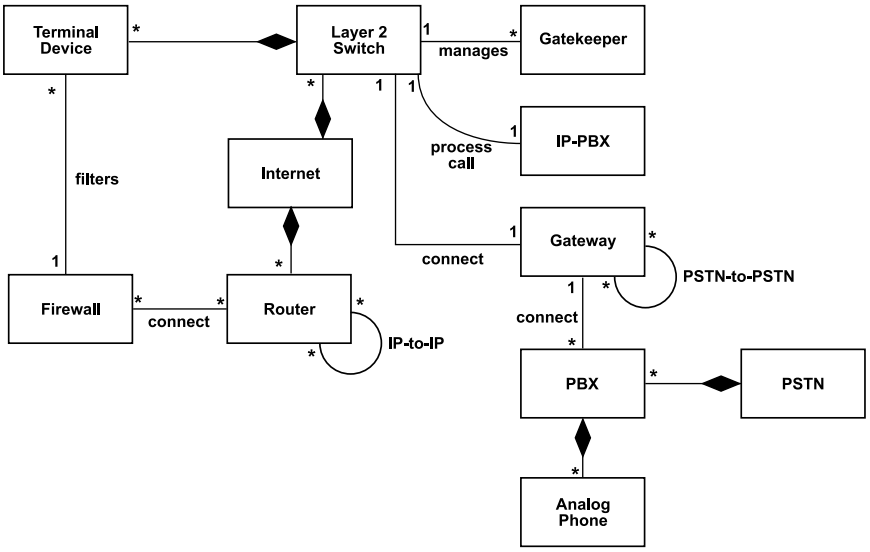

Figure 1. Class diagram for the H.323 architecture.

- ∗ Remote Access: An attacker can obtain remote (possibly administrator level) access.
- ∗ Malformed Request DoS: A carefully-crafted protocol request (packet) could result in a partial or complete loss of functionality.
- ∗ Load-Based DoS: A flood of legitimate requests could overwhelm the system [5].

– As with any network-based service, enterprise VoIP must communicate with other components on a LAN and possibly over an untrusted network such as the Internet, where packets are easy to intercept.

– Because RTP carries media, which must be delivered in real-time for acceptable conversations, VoIP is vulnerable to DoS attacks that impact voice quality (e.g., jitter and delay).

– VoIP tools offer good cover traffic for DoS attacks because VoIP networks run continuous media over IP packets [22].

■ **Solution:** H.322 and SIP are the primary protocols used in VoIP systems. In this paper, we consider an attack on the H.323 protocol. A SIP attack (see, e.g., [1]) can be considered to be a variant of the H.323 attack pattern or a separate pattern.

Figure 1 shows the class diagram of the structure of an H.323 system. The Layer 2 switch provides connectivity between H.323 com-

ponents. The gateway takes a voice call from the circuit-switched public telephone network (PSTN) and places it on the IP network. The PSTN uses PBX switches and analog phones. The Internet (IP network) has routers and firewalls that filter traffic to terminal devices. The gateway queries the gatekeeper with caller/callee numbers, which the gatekeeper translates into routing numbers based on the service logic. The IP-PBX server serves as a call processing manager, setting up and routing the calls to other voice devices. Softphones are applications installed in terminal devices (e.g., PCs or wireless devices).

One method to launch a DoS attack is to flood a server with repeated requests for service. This causes severe degradation or complete unavailability of the voice service. A flooding attack can also be launched against IP phones and gateways by sending a large number of "register" or "invite" events. The target system is so busy processing packets from the attack that it is unable to process legitimate requests, which are either ignored or processed so slowly that the VoIP service is unusable. The TCP SYN flood attack (or resource starvation attack) can be used to obtain similar results. This attack floods the port with synchronization packets that are normally used to create new connections.

A distributed DoS (DDoS) attack uses multiple systems to produce a flood of packets. Typically, the attacker installs malicious software (Trojans) on compromised terminal devices known as "zombies," which are directed to send fake traffic to targeted VoIP components. Targeted DoS attacks are also possible when the attacker disrupts specific connections.

Figure 2 shows the class diagram for DoS attacks in an H.323 network, in which any VoIP component can be a target. Note that the classes "Attack Control Mechanism" and "Zombie" denote the malicious software introduced by the attacker.

Figure 3 shows the sequence of steps necessary to launch a server flood attack. An attacker (internal or remote) generates call requests using a valid user name on a VoIP system to overwhelm the IP-PBX. The attacker may disrupt a subscriber's call attempt by sending specially crafted messages to the ISP server or IP-PBX, causing the device to over allocate resources so that the caller receives a "service not available" (busy tone) message. This is an example of a targeted attack.

Out-of-sequence voice packets (e.g., media packets received before a session is accepted) or a very large phone number could open the

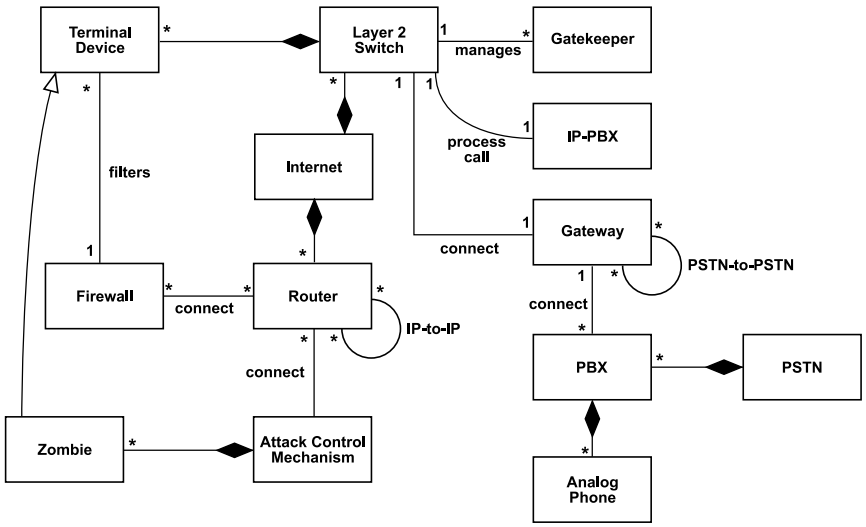

Figure 2. Class diagram for DoS attacks in a H.323 network.

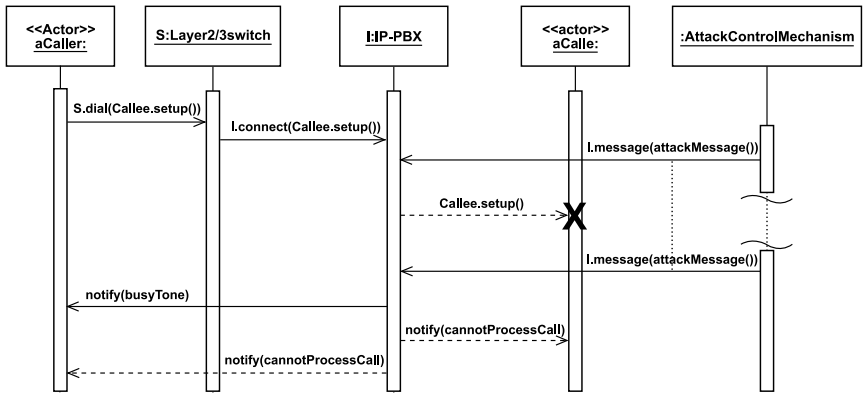

Figure 3. Sequence diagram for a DoS attack in a H.323 network.

way to application layer attacks (a.k.a. attacks against network services). Buffer overflow attacks can paralyze a VoIP number using repeated calling. For example, an attacker could intermittently send garbage (e.g., the header and the payload are filled with random bytes that corrupt the callee's jitter buffer voice packets) to the callee's phone in between those of the caller's voice packets. This causes the callee's phone to so busy trying to process the increased packet flow that the jitter (delay variation) causes the conversation to be incomprehensible [1].

- **Consequences:** The consequences of a successful attack include:
  - A DoS attack renders key voice resources (e.g., media gateways) inoperable.
  - Flooding a firewall prevents it from properly managing ports for legitimate calls.
  - QoS is degraded by jitter and delay, causing the VoIP network to become totally unusable.
  - Zombies in the targeted network launch DoS attacks on other networks.

  Attacks may fail for several reasons:
  - Attacks can be defined in theory, but are difficult to carry out in practice. The main reasons are lack of knowledge, testing opportunities and entry points for attackers.
  - Countermeasures may be able to defeat the attack or mitigate its effects.
- **Countermeasures and Forensics:** The attack can be defeated or mitigated by the following countermeasures:
  - A DoS attack is mitigated by disabling and removing unnecessary network services, reinforcing the operating system, and using host-based intrusion detection systems (see [6] for an IDS pattern). This makes it harder for attackers to introduce Trojan horses to compromise terminal devices.
  - IDSs and firewalls ensure that packets with very large sequence numbers and garbage packets are discarded (see [18] for a firewall pattern).
  - Stateful firewalls (see [18] for a pattern) with deep packet inspection technology can be used to analyze voice packet headers and contents to ensure that they are safe.

- The authenticated call feature (see [8] for a pattern), which performs device and user authentication prior to permitting access to VoIP services, can be used to protect against targeted attacks.

Several network forensic mechanisms may be employed:

- Terminal device logs not only provide call details (e.g., start and end times of calls), but also reveal the presence of Trojans.
- Router logs and firewall logs provide information on how the attacker entered the network and how the exploits were performed.
- Certain attacks selectively send events to the ISP or IP-PBX; these attacks can be traced by examining logs on these devices.
- Network forensic analysis techniques such as IP traceback and packet marking can be used for attack attribution. During a DoS attack, the target system receives enough traceback packets to reconstruct the attack path [19]. Locating attackers with the IP traceback technology is also a potential security mechanism to counter DoS attacks. Effective traceback requires the cooperation of all network operators along the attack path.
- Comparing traffic patterns against predefined thresholds (as is done by some IDSs) is an effective method for detecting DDoS attacks. It also helps detect malicious traffic (e.g., observing congestion in a router's buffer) before it enters or leaves a network.
- Event logging enables network administrators to collect important information (e.g., date, time and result of each action) during the setup and execution of an attack. For example, logs may identify the type of DDoS attack used against a target.
- Positioning honeypots and other network forensic appliances on selected VoIP components can help in the event of a successful attack.
- In a VoIP network, the attack pattern technique may be complemented with a network forensics analysis tool to offer a better view (interpretation) of the collected voice packets.

- **Evidence Locations:** Based on Figure 2, secondary sources of forensic information in VoIP networks include terminal devices (softphones, hardphones and wireless VoIP phones), gatekeepers, gateways and IP-PBXs.

- **Related Patterns:** Security patterns for defending against these and related attacks are presented in [1, 8, 17]. Some general security patterns such as firewalls [18], IDSs [6] and authentication [18] can be used to control attacks. An attack pattern can be developed to describe similar attacks on SIP networks.

4. Discussion

Attack patterns can guide forensic investigators in the search for evidence. They also serve as a structured method for obtaining and representing relevant network forensic information. Investigators often find it difficult to determine which data should be collected. Data collection often involves identifying all the components involved in the investigation, deciding which are most likely to be of interest, finding the location of the components, and collecting data from each component [12].

Attack patterns are useful when attackers break into VoIP network segments that are not monitored by security devices. Therefore, investigators should look for evidence in secondary data sources such as terminal devices. Attack patterns also enable investigators to ensure that they have considered all possible contexts and evidence sources by referring to the appropriate attack templates.

Much of the value of the attack pattern formalism comes from the fact that an attack, which is described dynamically in a sequence diagram, makes direct reference to the system components, which are described by a class diagram. The sequence diagram uses objects from classes in the class diagram; thus, messages can be related to the components where they are sent (classes represent the system components). The parameters of the messages are data that can be found in the corresponding components. In other words, the combination of sequence and class diagrams provide guidance to forensic investigators on what evidence can be found after an attack and where to look for the evidence.

Other approaches for describing attacks and their effects include fault trees and attack trees [14]. A fault tree uses combinations of AND and OR nodes to specify the conditions under which a system will fail. An attack tree specializes the notion of a fault tree by specifying the conditions for an attack to succeed. Probabilities of occurrence may be assigned to conditions or events in a fault tree or attack tree. However, these probabilities are difficult to estimate and require detailed system

descriptions, which renders the approach impractical for generic analyses and for systems that have not yet been constructed. Consequently, attack trees are mostly used to determine the risk of attacks and the associated costs.

Another tool is an attack net, which is a Petri net whose places represent attack steps and transitions represent events that activate steps [15]. Attack nets have been used in a web-based system to collect expert knowledge about attacks [20]. An attack net can represent the dynamics of an attack very effectively, but it does not take system components into account, which limits its forensic applications. The Analyst's Notebook, a product based on attack nets, is useful for tracing the propagation of attacks in computer networks [3]. However, it works at the hardware component level and cannot abstract similar types of components, which leads to a proliferation of units that must be considered.

Hoglund and McGraw [11] also use the term "attack pattern." Their attack pattern is simply a description of a step in a generic attack, e.g., string format overflow in `syslog()`. Moreover, they do not provide a systematic discussion of patterns and do not consider any forensic aspects. Moore and colleagues [16] also use the term; their attack pattern describes the goal of an attack, attack steps, preconditions and postconditions. In fact, their attack pattern is essentially one step in our attack pattern. Anwar and co-workers [1] use the term "design patterns," which are really security patterns, but they do not consider system components and forensic aspects.

5. Conclusions

An attack pattern provides a systematic description of the attack objectives and attack steps along with strategies for defending against and tracing the attack. The attack pattern template presented in this paper is intended to document and organize generic attack patterns. The example involving DoS attacks on VoIP networks demonstrates the value of the formalism to security designers and forensic investigators. We are currently constructing a catalog of attack patterns for VoIP networks, including wireless implementations. We are also using the formalism as the basis for an integrated methodology for building secure systems.

Acknowledgements

This research was supported by a grant from the U.S. Department of Defense administered by Pragmatics, Inc., McLean, Virginia.

References

[1] Z. Anwar, W. Yurcik, R. Johnson, M. Hafiz and R. Campbell, Multiple design patterns for VoIP security, *Proceedings of the Twenty-Fifth IEEE Conference on Performance, Computing and Communications*, 2006.

[2] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad and M. Stal, *Pattern-Oriented Software Architecture: A System of Patterns, Volume 1*, Wiley, Chichester, United Kingdom, 1996.

[3] E. Casey, Investigating sophisticated security breaches, *Communications of the ACM*, vol. 43(2), 48–54, 2006.

[4] CERT Coordination Center, Carnegie Mellon University, Pittsburgh, Pennsylvania (www.cert.org).

[5] M. Collier, The value of VoIP security (www.cconvergence.com /showArticle.jhtml?articleID=22103933), 2004.

[6] E. Fernandez and A. Kumar, A security pattern for rule-based intrusion detection, *Proceedings of the Nordic Conference on Pattern Languages of Programs*, 2005.

[7] E. Fernandez, M. Larrondo-Petrie, T. Sorgente and M. VanHilst, A methodology to develop secure systems using patterns, in *Integrating Security and Software Engineering: Advances and Future Vision*, H. Mouratidis and P. Giorgini (Eds.), IGI Publishing, Hershey, Pennsylvania, pp. 107–126, 2006.

[8] E. Fernandez and J. Pelaez, Security patterns for voice over IP networks, *Proceedings of the International Multiconference on Computing in the Global Information Technology*, p. 33, 2007.

[9] E. Fernandez, M. VanHilst, M. Larrondo-Petrie and S. Huang, Defining security requirements through misuse actions, in *Advanced Software Engineering: Expanding the Frontiers of Software Technology*, S. Ochoa and G. Roman (Eds.), Springer, New York, 123–137, 2006.

[10] E. Gamma, R. Helm, R. Johnson and J. Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software*, Addison-Wesley/Pearson, Boston, Massachusetts, 1994.

[11] G. Hoglund and G. McGraw, *Exploiting Software: How to Break Code*, Addison-Wesley/Pearson, Boston, Massachusetts, 2004.

[12] K. Kent, S. Chevalier, T. Grance and H. Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.

[13] P. Laplante and C. Neill, *AntiPatterns: Identification, Refactoring and Management*, CRC Press, Boca Raton, Florida, 2006.

[14] N. Leveson, M. Heimdahl, H. Hildreth and J. Reese, Requirements specification for process-control systems, *IEEE Transactions on Software Engineering*, vol. 20(9), pp. 684–707, 1994.

[15] J. McDermott, Attack net penetration testing, *Proceedings of the New Security Paradigms Workshop*, pp. 15–22, 2000.

[16] A. Moore, R. Ellison and R. Linger, Attack modeling for information security and survability, Technical Note CMU/SEI-2001-TN-001, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, 2001.

[17] J. Pelaez, Security in VoIP networks, Master's Thesis, Department of Computer Science and Engineering, Florida Atlantic University, Boca Raton, Florida, 2004.

[18] M. Schumacher, E. Fernandez, D. Hybertson, F. Buschmann and P. Sommerlad, *Security Patterns: Integrating Security and Systems Engineering*, Wiley, Chichester, United Kingdom, 2006.

[19] K. Shanmugasundaram, N. Memon, A. Savant and H. Bronnimann, ForNet: A distributed forensics network, *Proceedings of the Second International Workshop on Mathematical Methods, Models and Architectures for Computer Network Security*, pp. 1–16, 2003.

[20] J. Steffan and M. Schumacher, Collaborative attack modeling, *Proceedings of the ACM Symposium on Applied Computing*, pp. 253–259, 2002.

[21] Symantec, Antivirus Research Center (www.symantec.com).

[22] TMCnet.com, CRN finds security risk in VoIP applications (www.tmcnet.com/usubmit/2006/01/27/1320122.htm), January 27 2006.

[23] C. Wieser, J. Roning and A. Takanen, Security analysis and experiments for VoIP RTP media streams, *Proceedings of the Eighth International Symposium on Systems and Information Security*, 2006.