Abstract and IoT security segmentation patterns

EDUARDO B. FERNANDEZ, Florida Atlantic University
NOBUKAZU YOSHIOKA, National Institute of Informatics
HIRONORI WASHIZAKI, Waseda University

Network segmentation is the division of a network into subnets, typically for purposes of enhanced security. An institution can thus create subnetworks to access databases, servers, or any other entity that requires specific security requirements. We describe here an abstract pattern for security segmentation from which we derive a specialized pattern for segmentation of IoT networks.

Categories and Subject Descriptors: D.2.11 **[Software Engineering]** Software Architectures–Patterns;

General Terms: Design

Additional Key Words and Phrases: Security patterns, secure software, software architecture, IoT, netwok segmentation

ACM Reference Format:

E.B.Fernandez, N. Yoshioka, H. Washizaki, "Abstract and IoT security patterns for network segmentation", 2019. Procs. Asian PLoP'19, March 20-22, Tokyo, Japan. 9 pages.

1. INTRODUCTION

Network segmentation is the division of a network into subnets, typically for purposes of enhanced security. With a segmented network, the traffic of internal users can be separated from that of guests and external contacts and thus it can be better controlled. Moreover, one can further fine-tune the segmentation so that there are individual segments for web servers and databases, as well as employee devices. Segmentation is useful for compliance with regulations and it also makes it more difficult for outsiders to penetrate a network via an unsecured device, while shielding sensitive data from insiders.

Network segmentation has been used to protect networks for quite a while; now it takes special importance as a way to control the security of IoT networks, where there may be a large number of heterogeneous devices from different origins. IoT networks are proliferating and are bringing serious security problems as shown by the recent DoS attacks produced by IoT-based devices (Syed et al. 2018). We first present an abstract version of the pattern which describes the core functions of any network segmentation pattern. We then show a segmentation pattern for IoT, indicating only its differences with the abstract pattern. Segmentation may be done with purposes other than security, e.g., performance, but we emphasize here the security aspects of this pattern.

An Abstract Security Pattern (ASP) is a security pattern that describes a conceptual semantic restriction in a domain which can be a defense to a threat or a way to comply with a regulation, with no implementation aspects (Fernandez et al. 2014). An ASP describes the essential functions that must be present to handle a threat or regulation in an implementation-independent way. A concrete pattern describes a security solution within a technological context, e.g., distributed systems, XML web services, etc., which means that the pattern for IoT Segmentation is a concrete security pattern. Segmentation in fixed (non IoT) and wireless networks would be other concrete patterns between the Segmentation ASP and the IoT pattern in the Segmentation hierarchy.

Authors' addresses: Eduardo B. Fernandez (corresponding author), Dept. of Computer and Electrical Eng. and Computer Science, Florida Atlantic University, 777 Glades Rd., Boca Raton, FL33431, USA; email: fernande@fau.edu;.Nobukazu Yoshioka, GRACE Center, National Institute of Informatics, Tokyo, Japan,; email: nobukazu@nii.ac.jp. Hironori Washizaki, Waseda University, Tokyo, Japan; email: washizaki@waseda.jp.

Our audience includes system designers and administrators, and in particular those involved with IoT networks. We describe our patterns using the POSA template (Buschmann et al.).

2. SECURITY SEGMENTATION

2.1 Intent

Security segmentation protects computational entities or groups of entities by separating them into domains with restricted access.

2.2 Context

Institutions usually have a variety of databases, servers, and desktop units that handle data with different degrees of sensitivity and that need to be protected in different ways.

2.3 Problem

A large network of computational entities may include devices which are not properly secured or even be malicious. How do we protect our sensitive entities from external or internal attacks?

The forces that will affect the solution include:

- Security level. Entities may contain data with different levels of sensitivity, which must be protected from attacks.
- Attack surface. The attack surface of our information should be as small as possible.
- Heterogeneity. Typical networks include devices from many origins, which may be necessary for our applications.
- Identity. We would like to keep track of the devices which are under our control or participating in our network.
- Compliance. Some of the information in our system may have to follow regulations or industrial standards.
- Threats. Attackers may make attempts to enter a subnetwork illegally, tamper with the configuration of subnetworks, introduce a malicious entity in a network.

2.4 Solution

Partition the network into small units with sensitive entities into separate subnetworks (Fig. 1). Segregation is typically achieved by a combination of separators (see Implementation).

2.4.1 *Structure*

Fig. 2 shows the class diagram of this pattern. The Network can be divided into several Subnetworks, which in turn can be composed of any combination of Entities and which can be connected to other Subnetworks. Class Separator describes specific separation mechanisms between subnetworks.

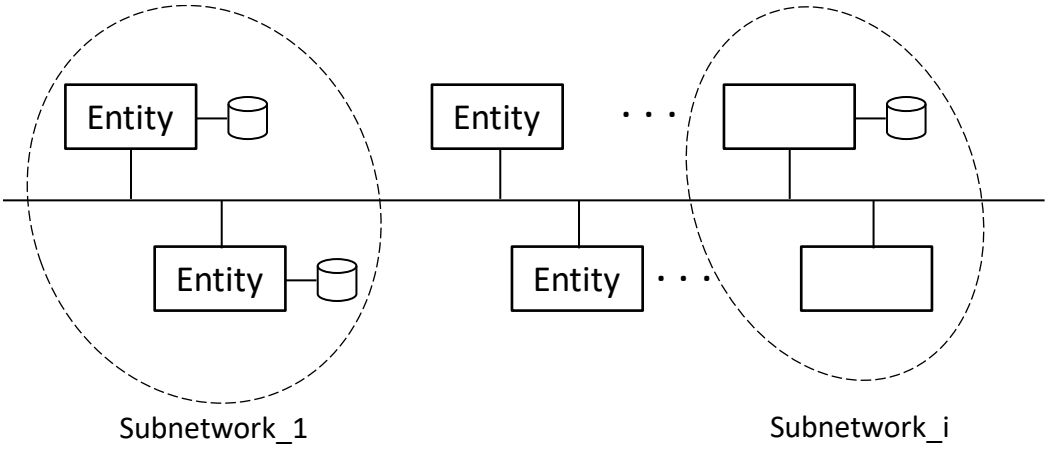

Figure 1. A segmented network

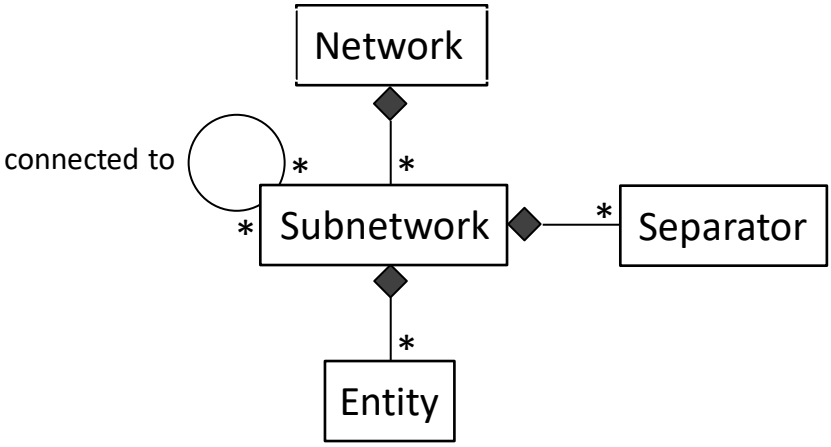

Fig. 2 Class diagram of the Segmentation pattern

2.4.2 Dynamics

Fig. 3 shows the use case “Access a subnetwork”. As shown in the figure, any protocol can be used to decide access. Other use cases include: Create/Delete a subnetwork, Define separation mechanism, Add/Remove entity to/from a subnetwork.

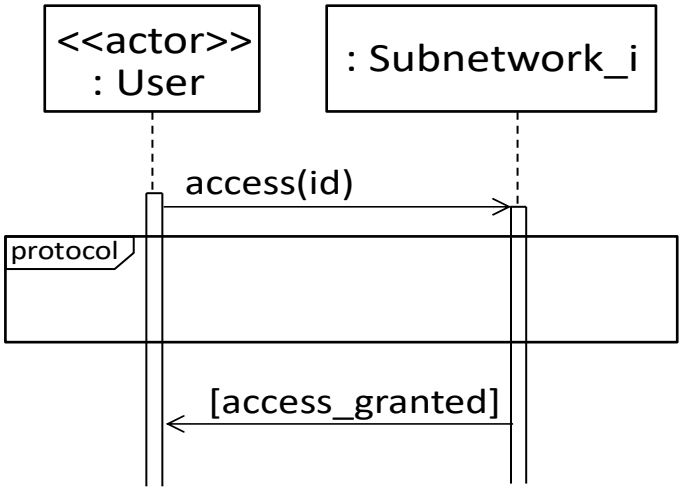

Fig. 3. Sequence diagram for use case “Access a subnetwork”. .

2.5 Implementation

There are several ways to segment networks (ACSC 2018), such as implementing demilitarized zones and gateways between networks with different security requirements (security domains) utilizing technologies at various layers such as: host-based security and firewall software to filter network traffic at the host level, network firewalls and security appliances between networks to filter network traffic. network access controls to control the devices which can access networks. A choice leads to concrete versions of this abstract pattern.

At a conceptual level we can only say:

- Separate networks based on their sensitivity or criticality to business operations. This may include using different hardware or platforms depending on different security classifications, security domains or availability/integrity requirements.

- Use the principles of least privilege and need-to-know. If a host, service or network doesn’t need to communicate with another host, service or network, it should not be allowed to. If a host, service or network only needs to talk to another host, service or network on a specific port or protocol, and nothing else, it should be restricted to this.

A data-driven segmentation approach is discussed in (Cisco). Virtual Network Segmentation is considered in (Chandramouli). Design approaches for segmented networks are shown in (Alateeq 2005) and (Peterson 2016). Cryptography can also be used to separate domains.

2.6 Known uses

- PCI-DSS (Payment Card Industry Data Security Standard) requires separating the network for Payment Card authorizations from those for Point-of-Service or customer wi-fi traffic. Network segmentation is not required but highly recommended (PCI Security Standards Council, 2016).
- ForeScout has products to achieve network segmentation through a number of physical or logical means, such as properly configured internal network firewalls, switches and routers with strong access control lists (ACLs), or other technologies such as virtual local area networks (VLANs) that restrict access to particular segments of the network (Fore Scout 2018).

- HashiCorp has products to define segmentation (HashiCorp 2018). They use what they call “intention-based model”, which builds rules on identity rather than location. For example, we can define an intention which states that the front-end service needs to communicate with the payment service. This can be considered like an extreme case where each entity can be a unit of isolation.

2.7 Consequences

This pattern brings the following advantages:

- Security levels. Separating sensitive entities from suspicious devices improves their security. We can define authorization rules specific to each type subnetwork.
- Attack surface. Since there are fewer entities, the attack surface is reduced.
- Heterogeneity. We can include in sensitive networks only devices we trust.
- Identity. We can keep track of the devices which are under our control by identifying them using an identity federation.
- Regulations. Separating servers which handle different types of data makes it easier to enforce regulations.
- Threats. Must be handled with appropriate security patterns as shown in (Fernandez 2013).

Liabilities include:

- Complexity. The design of the complete network becomes harder.
- Overhead. Accessing frequently used data may become slower because of the need to go through the subnetwork access protocol.
- Cost. The institution needs to buy or build additional software packages and possibly extra hardware to support partitioning.

2.8 Related patterns

- Security Segmentation for IoT (described below) is a concrete pattern derived from Abstract Segmentation, which defines the core functions of this pattern independently of any implementation technology. The concrete version considers the specific context for the derived pattern.
- VoIP Segmentation is a concrete segmentation pattern (E.Fernandez et al., 2007). It performs separation of the voice and data services to control cross-attacks.
- Identity Federation (Delessy et al., 2007). The Identity Federation pattern allows the formation of a dynamically created identity within an identity federation consisting of several service providers. Therefore, identity and security information about a subject can be transmitted in a transparent way for the user among service providers from different security domains.
- Microsegmentation (Shackleford 2019). It is a model for defining network isolation policies based on application profiles and workload attributes. Using micro-segmentation with dynamic policy evaluation of both network traffic between workloads and the OS and application behaviors and components within the compute elements themselves, prevents attackers from using unapproved connections to move laterally from a compromised application or system.

3. SECURITY SEGMENTATION FOR IOT

3.1 Intent

Security segmentation for IoT partitions a network of IoT devices and supporting entities into subnetworks in order to isolate groups of IoT devices and entities with different security requirements. IoT networks have a specific context which brings different threats than other type of networks.

3.2 Context

IoT networks bring very large amounts of heterogeneous (may origins and types) devices, usually with low security and which often interact with other entities in the Internet. This results in a complex and potentially dangerous environment. IoT systems are complete cyber-physical systems (CPS) or part of a CPS and may include sensors and actuators which give them the possibility of producing catastrophic failures endangering humans or property. A common architecture controls IoT devices using clouds which in turn use fog units to reduce latency (Syed et al. 2016). A fog is defined as a collection of numerous distributed tiny clouds deployed closer to the devices at edge of the network. This environment brings new threats to the abstract model, the IoT network may include devices which are not properly secured or even be malicious.

3.3 Problem

In a large network of IoT devices, how do we protect sensitive devices or systems from attacks? The devices may have different origins, use different standards, have a variety of security models or no security, and have a large range of computational power. The typical hierarchical structuring of devices may introduce authorization conflicts.

The forces that will affect the solution include:

Security level. There may be conflicts between authorization rules coming from clouds, fog systems, and devices.

Attack surface and Compliance are the same as in Abstract Segmentation.

Heterogeneity. Typical IoT networks include devices from many origins, some of which may have poor security or no security at all.

Identity. Because of their number it may be hard to identify all devices.

Threats. IoT systems are often CPSs, which means that their threats may have safety consequences; e.g., a security attack may harm people or valuable equipment.

3.4 Solution

Partition the network into small units with well-known devices in the more sensitive partitions. Fig. 4 shows a typical case where all the devices of an institution and their fog system are partitioned out of a larger network. Segregation is typically achieved by a combination of firewalls and VLANs (Virtual Local Area Networks), and possibly SDN.

3.4.1 Structure

Fig. 5 shows the class diagram of this pattern. The Network can be divided into several subnetworks, which in turn can be composed of any combination of entities and which can be connected to other subnetworks. Class Separator describes specific separation mechanisms.

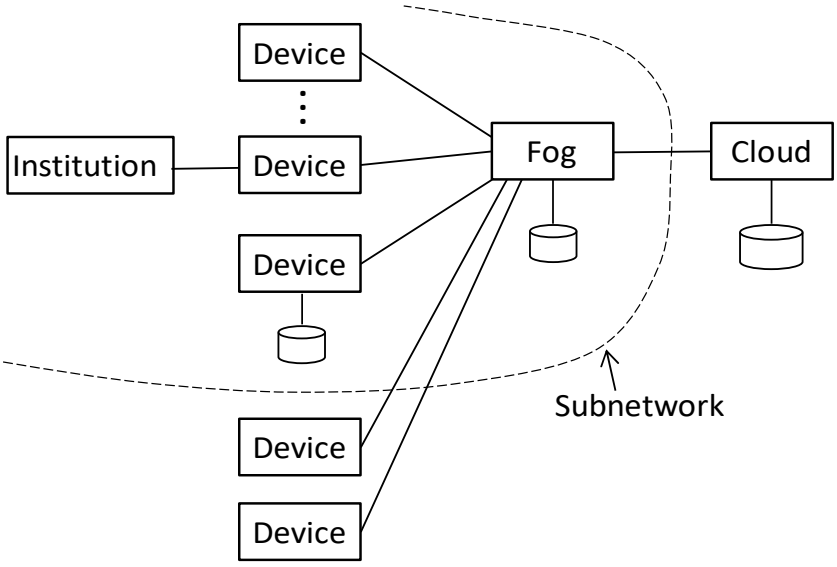

Fig. 4. A partitioned IoT network

3.5 Implementation

Each subnetwork must be disjoint from others; sharing entities could allow an unchecked way to get into a subnetwork. If larger entities need to be shared, e.g. clouds or database servers, partitioning of smaller entities like files or databases can be done by using virtual machines or virtual databases separated through the virtualization mechanism; in this case, the hypervisor would apply the access restrictions for each subnetwork. Segmentation policies must be based on business objectives and semantic affinities; they must be consistent across the whole institution.

IoT networks share recommendations with other concrete networks and include (Arctic Wolf Blog 2018):

- Create a unique SSID for the network, leading to an isolated VLAN that connects to the internet separately from the internal network. A dedicated circuit for the guest network may also be installed.
- Require passwords be entered through a captive portal. This not only prevents network overuse, but also enables logging of every visitor and the enhanced access controls – including session termination – that comes with it.
- Monitor all traffic on the guest network. It may be segmented and have its own circuit, but you don't want it to become a blind spot in your IoT defenses. Managed detection and response (MDR) via a security information and event monitoring (SIEM) solution can ensure you keep tabs on network activity and spot anomalies quickly.

An specific implementation recommendation for IoT networks is the need to uniquely identify each IoT device and further separate devices by their security mechanisms. For example, some devices may not be able to support authorization for lack of the corresponding mechanism; in this case we can wrap the device and add authorization as part of the wrapper.

3.6 Known uses

- Arctic Wolf has solutions for IoT segmentation (Arctic Wolf Blog, 2018).

- Tempered Networks have segmentation products (Tempered Networks 2018). Their latest release includes support for transparent multi-factor end-user authentication and authorization enabling the simple creation of zero trust workgroup networks.

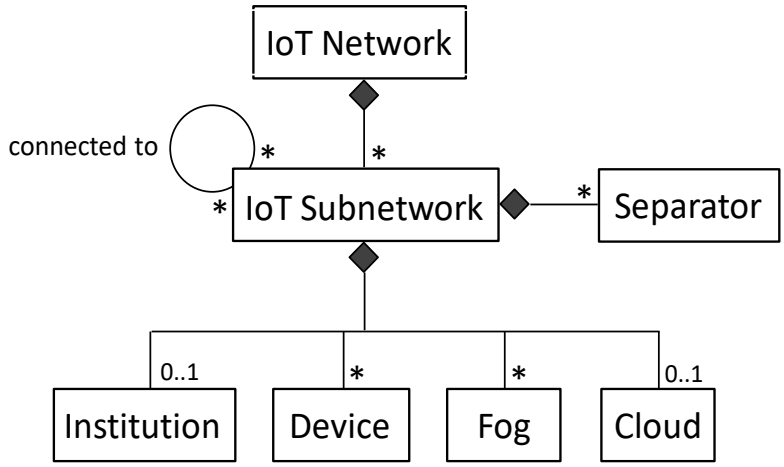

Fig. 5. Class model of the IoT Segmentation pattern

3.7 Consequences

This pattern has the following advantages:

Security level. It is possible to define policies for authorizations rules such that they do not conflict, such as overriding or inclusion.

Attack surface and compliance can be handled similarly to the way done in Abstract Segmentation

Heterogeneity. Abstraction allows handling any type of device, all of which are handled in similar ways. For example , sensor nodes can be described by patterns (Sahu,

Threats. Because of their physical actions, IoT devices need to be carefully protected and monitored. Segmentation makes this job easier. Failing to use segmentation allowed the destruction of steel furnace in Germany (Pau2014).

Its liabilities are similar to the abstract pattern although because of the possible high number of devices, it may be hard to identify all devices.

3.8 Related patterns

In addition to the ones in the abstract Segmentation pattern some security patterns have been defined for IoT devices (Reinfurt et al. 2017). This paper presents six patterns including Well-Known Communication Partner, Outbound-Only Connection, Permission Control, Personal Zone Hub, Whitelist, and Blacklist.

Fog Computing pattern (Syed et al., 2016). It is a virtualized platform that stands between cloud computing systems and Internet devices, providing to these computation, storage, and networking services and allowing a cloud to control and communicate with these devices and to the devices to perform some functions in the fog or the cloud.

The Wrapper Façade (Schmidt et al.) encapsulates the functions and data provided by existing non-object-oriented APIs withing more concise, robust, portable, and cohesive object-oriented class interfaces. Wrapper Facades can be used to encapsulate those IoT devices which do not have appropriate security mechanisms.

ACKNOWLEDGEMENTS

The work of Eduardo Fernandez was possible due to a travel grant from the National Institute of Informatics of Japan. Our shepherd, Sumit Kalra, provided valuable comments that significantly improved this pattern.

REFERENCES

ACSC (Australian Cyber Security Center), "Network segmentation and segregation", July 2018. https://acsc.gov.au/publications/protect/Network_Segmentation_Segregation.pdf (last accessed Dec. 12, 2018)

Ibrahim N. Alateeq, 2005, "Design Secure Network Segmentation Approach", https://www.sans.org/reading-room/whitepapers/hsoffice/design-secure-network-segmentation-approach-1645 (last accessed Dec. 12, 2018)

Arctic Wolf Blog, "Network segmentation: A key measure for IoT security", 2018, https://arcticwolf.com/blog/network-segmentation-a-key-measure-for-iot-security/

Ramaswamy Chandramouli, "Analysis of Network Segmentation Techniques in Cloud Data Centers", https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=918440

Cisco Corp., "A framework to protect data through segmentation", https://www.cisco.com/c/en/us/about/security-center/framework-segmentation.html (last accessed Dec. 12, 2018)

N. Delessy, E.B.Fernandez, and M.M. Larrondo-Petrie, "A pattern language for identity management", Procs. of the 2nd IEEE Int. Multiconference on Computing in the Global Information Technology (ICCGI 2007), March 4-9, Guadeloupe, French Caribbean.

E.B.Fernandez, J.C. Pelaez, and M.M. Larrondo-Petrie, "Security patterns for voice over IP networks", Procs. of the 2nd IEEE Int. Multiconference on Computing in the Global Information Technology (ICCGI 2007), , March 4-9, Guadeloupe, French Caribbean.

Eduardo B.Fernandez, Nobukazu Yoshioka, Hironori Washizaki, and Joseph Yoder, "Abstract security patterns for requirements specification and analysis of secure systems'', Procs. of the 17th Ibero-American Conf. on Soft. Eng.(CIbSE 2014), Pucon, Chile, April 2014

E.B.Fernandez, "Security patterns in practice: Building secure architectures using software patterns", Wiley Series on Software Design Patterns, 2013.

ForeScout, Solution Brief, https://www.forescout.com/wp-content/uploads/2018/08/fs-sb-network-segmentation.pdf

HashiCorp, "Network segmentation in modern environments", 2018, https://www.hashicorp.com/blog/network-segmentation-in-modern-environments

D. Pauli, "Hackers pop German steel mill, wreck furnace", The Register, UK, http://www.theregister.co.uk/2014/12/22/hackers_pop_german_steel_mill_wreck_furnace/

PCI Security Standards Council, "Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation", December 2016.

J.C.Pelaez, Chapter 4 of "Security for VoIP networks", M.S. Thesis, Florida Atlantic University, 2007.

B. Peterson, 2016, "Secure Network Design: Micro Segmentation", https://www.sans.org/reading-room/whitepapers/bestprac/secure-network-design-micro-segmentation-36775 (last accessed Dec. 12, 2018

L. Reinfurt et al., "Internet of Things security patterns", PLoP'17, Vancouver, CA, Oct. 2017

D. Shackleford, "Evolving Micro-Segmentation for Preventive Security: Adaptive Protection in a DevOps World", January 2019, https://www.sans.org/reading-room/whitepapers/awareness/evolving-micro-segmentation-preventive-security-adaptive-protection-devops-world-38760

D. Schmidt, M. Stal, H.Rohnert, F. Buschmann, "Pattern-Oriented Software Architecture, Vol. 2, Patterns for Concurrent and Networked Objects", Wiley Series in Software Design Patterns, 2000.

M. H. Syed, E.B.Fernandez, M.Ilyas, "A pattern for fog computing", Procs. of Pattern Languages of Programming (VikingPLoP 2016), 7th-10th April 2016, Leerdam, Netherlands, ACM New York, NY, USA doi>10.1145/3022636.3022649

M.H. Syed and E.B. Fernandez, "A misuse Pattern for DDoS in the IoT", EuroPLoP'17, Irsee, Germany, July 2018

Tempered Networks, 2018, https://www.temperednetworks.com/news/press/new-iot-edge-to-multi-cloud-solutionm-makes-wan-segmentation-simple