

Security Threat and Vulnerability Mitigation Patterns: A Case of Credit Card Theft Mitigation

Sam Supakkul¹, Tom Hill², Ebenezer Akin Oladimeji³, and Lawrence Chung¹

¹ Department of Computer Science
The University of Texas at Dallas
ssupakkul@ieee.org, chung@utdallas.edu

² Office of the EDS CTO
EDS, an HP company
tom.hill@hp.com

³ Architecture and eServices
Verizon Communications
ebenezer.oladimeji@verizon.com

Abstract

Most attacks on computer and software systems are caused by threats to known vulnerabilities. Part of the reason is that we need a lot of knowledge in developing secure systems, but it is difficult to obtain sufficient knowledge and use it correctly as security incident reports and security standards are often described informally and without context and rationale to justify and guide when each recommended security measure should be used, especially when conflicting forces exist.

This paper presents security patterns for mitigating threats and vulnerabilities that capture knowledge of security context (asset, facility, and driving forces such as security objective, cost, and usability), security problems (vulnerability associated to a facility, threat exploiting the vulnerability, and resulting undesirable outcome that negatively affects security objectives), and mitigating solutions (risk transfer, threat prevention and containment, and impact prevention and control), with selection patterns for recommending suitable mitigation techniques based on NFRs and their criticality. Such knowledge is described textual and visual using a meta-pattern that defines the textual and diagrammatical structure of pattern description. The approach has been applied to a case study in developing three patterns that could have mitigated the threats and vulnerabilities that led to the TJX incident, the largest credit theft in history.

1 Introduction

Most attacks on computer and software systems are caused by threats to known vulnerabilities. Part of the reason is that we need a lot of knowledge in developing secure systems, but it is difficult to obtain sufficient knowledge and use it correctly as security incident reports and security standards are often described informally and without context and rationale to justify and guide when each recommended security measure should be used, especially when conflicting forces exist.

Security patterns have been instrumental in capturing and reusing knowledge of architecture and design for achieving security. However, knowledge about threats, vulnerabilities, and their inter-relationships with security measures and NFRs as driving forces are not precisely captured in these patterns, making it difficult for pattern users to decide when to use each of those security patterns.

This paper presents security patterns for mitigating threats and vulnerabilities to capture knowledge about security context (asset, facility, and NFRs such as security objective, cost, and usability as driving forces), security problems (vulnerability associated to a facility, threat exploiting the vulnerability, and resulting undesirable outcome that negatively affects security objectives), and mitigating solutions (risk transfer, threat prevention and containment, and impact prevention and control), with selection patterns for recommending suitable mitigation techniques based on NFRs and their criticality. Such knowledge is described textual and visual using a meta-pattern that defines the textual and diagrammatical structure of pattern description. The approach has been applied to a case study in developing three patterns that could have mitigated the threats and vulnerabilities that led to the TJX incident, the largest credit theft in history.

The rest of this paper is structured as follows. Section 2 briefly describes the TJX credit card theft case that was the motivation for our research. Section 3 presents the meta-pattern defining the common structure of concrete threat and vulnerability mitigation patterns presented in Section 4 to 6. Section 7 discusses related work and observations. Finally, Section 8 summarizes the paper and future work.

2 The TJX Case

TJX, the holding company owning many large retail store chains such as Marshall and TJ Maxx, suffered the largest credit theft in history between 2003 and 2008 that was initially estimated to have affected 45 million credit cards, identify information of 451,000 customers, \$20 millions in fraudulent transactions, and to cost TJX \$1 billion over 5 years, excluding lawsuits [Gau07, Hil07, Hil08, Per07, US08, Can07].

This case became an infamous case study in retail and credit card industries, and in the security community. We have studied over 30 news articles, investigation reports, and court indictment on this case, but we found it difficult to get a clear understanding how the incident occurred with details about specific security related concepts, such as organizational asset and facility, exploited vulnerabilities and the realized threats beside the much talked about WEP hacking mentioned in most articles. This incident also brought an attention to the Data Security Standard issued by the Payment Card Industry, a consortium of major credit card companies [PCI05] that defines security practices to be complied by organizations, such as retailers and payment processors, that have access to payment card information. However, the standard prescribes a number of specific security measures without rationale to justify why they are needed, for which circumstances, and how one security measure may be chosen over another when conflicts arise, making it difficult for an average system or software engineer to understand how the standard could have prevented the TJX case.

To help better understand the incident, we developed a diagram as shown in Figure 1 to depict the scenario of how the incident occurred and how three attacks were carried out to successfully steal a large number of credit card information (with some simplification). We then diagrammatically represented more detailed security contextual concepts (asset, facility, security objective), security problems (vulnerabilities, threats, and undesirable outcome), and mitigating solutions as recommended by the PCI DSS along with their consequences toward other NFRs. We felt that acquiring such knowledge about threats and vulnerabilities, and understanding about mitigation alternatives and how to choose them are not simple and straight forward. It seemed difficult for average system and software engineers to quickly acquire sufficiently knowledge for each new security incident in order to prevent future attacks. Capturing knowledge in a well defined structure as patterns should be helpful for understanding known threats and vulnerabilities, and how to prevent them. This was the motivation for us to develop the patterns presented in this paper.

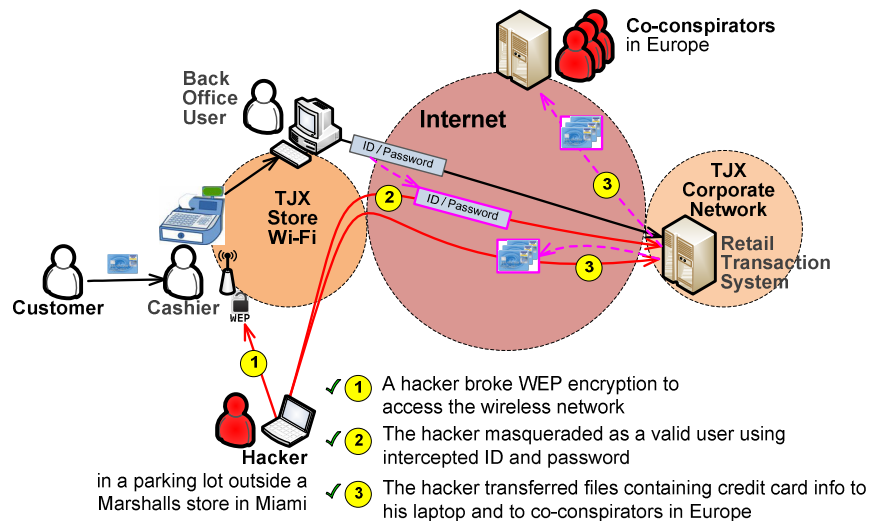


Figure 1. The Attack Scenario and Three Realized Security Threats in the TJX Incident

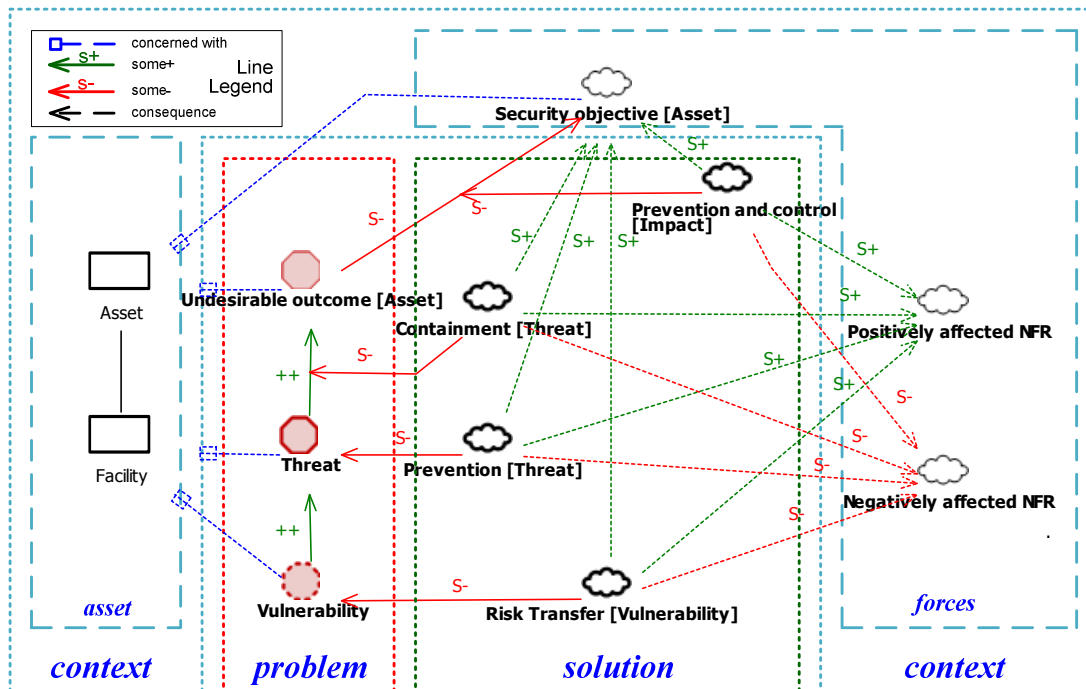


Figure 2. A Visual Meta-Pattern for Security Threat and Vulnerability Mitigation Patterns

3 A Meta-Pattern for Threat and Vulnerability Mitigation

All threat and vulnerability mitigation (TVM) patterns presented in this paper are described using Alexander's "three-part rule", expressing "a relation between a certain context, a problem, and solution" [Ale77] with respect to security and the mitigation of associated threats and vulnerabilities. This section describes the meta-pattern that describes the pattern of all patterns [Mes95]. Not only the TVM patterns are described using the same textual pattern, they are also described using the same visual pattern as depicted in Figure 2 where the outer area (left, top, and right), represents the context, including asset (primary asset, facility) and forces (security objective and other NFRs), for the security problems (undesirable outcome, threats, vulnerabilities) and their corresponding mitigation alternatives (impact prevention and control, threat prevent and containment, vulnerability risk transfer) that may have positive and/or negative consequences toward the forces that need to be taken into account.

Synopsis

The synopsis section textually and diagrammatically summarizes the pattern, describing relations between contextual elements, security problems, and mitigating solutions, using a textual and a diagrammatical patterns. The synopsis provides a compact, understandable, consistent, and predictable summary across multiple TVM patterns, although some minor deviations may be useful. Figure 2 depicts the diagrammatical (meta-) pattern, which can be described using the following textual (meta-) pattern/template, with the meta-concepts in bold:

The **TVM pattern** is concerned with a **security objective** of an **asset** that may be compromised via a **facility**, by a **threat** that exploits an associated **vulnerability**, that could lead to an **undesirable outcome** that may negatively affects the security objective.

The **vulnerability** could be mitigated by **risk transfer** measures that change the facility to that with a more acceptable vulnerability. Alternatively, the threat may be prevented by **threat prevention** measures, and/or contained by **threat containment** measures. In the case that those mitigation techniques were unsuccessful, the

undesirable outcome may be prevented or controlled by **impact prevention and control** measures to limit the impacts on the **security objective**. These mitigating solutions have positive and/or negative consequences upon **other NFRs**.

As an example, a concrete TVM pattern for wireless WEP attack could be described as follows, with the meta-concepts substituted by concrete concepts in bold with the respective meta-concept in parenthesis:

The **Wireless WEP attack threat and vulnerability mitigation** (pattern) is concerned with **confidentiality of credit card information** (security objective) that may be compromised via a **wireless network** (facility), by **encryption key cracking** (threat) that exploits **WEP 24-bit encryption** (vulnerability), that could lead to **stolen credit card information** (undesirable outcome) that may negatively affects the **confidentiality of the credit card information** (security objective).

The **WEP 24-bit encryption** (vulnerability) could be mitigated by **using a wireless network that uses WPA or WPA2 encryption** (risk transfer measure) that changes the facility to that with a more acceptable vulnerability. Alternatively, the **WEP encryption cracking** (threat) may be prevented by **strengthen WEP that uses at least 104-bit, frequently rotating the WEP key, using with WPA or VPN, or controlling access based on MAC addresses** (preventive measures), and/or contained by **isolating the compromised sub-net** (quarantine measure). In the case that those mitigation techniques were unsuccessful, **stolen credit card information** (undesirable outcome) may be prevented or controlled by **not storing card sensitive authentication data** (impact prevention and control) to limit the impacts on the **confidentiality of credit card information** (security objective). These mitigation solutions have positive and/or negative consequences upon **Cost, Usability, Recurring Administrability** (NFRs).

The rest of this section describes the sectional (meta-) pattern describing the elements of the concrete patterns in more detail.

Context

Asset

One or more primary assets, which may be information, operation, physical entities, or human, that are of high value that need to be protected, for example, credit card information or an e-commerce web site.

Facility

One or more secondary assets that are used in the course of business that when compromised could lead an undesirable outcome against the primary asset, for example, network and server that have direct or indirect access to credit card information.

Security Objective 

A security concern in relation to an asset, providing the context for security problems and solutions, which could be different for different domains or organizations. For example, US government considers security as confidentiality, integrity, and availability [FIS02], while the payment card industry considers only the confidentiality, even recommending confidential measures that sacrifice availability for the sake of confidentiality [PCI05].

Affected NFRs 

NFRs such as security, usability, and cost may be positively or negatively affected by different mitigation alternatives. These NFRs are the driving forces for selecting mitigation techniques. For example, instead of using retina scan for maximum access confidentiality, most e-commerce web sites opt for less but

acceptably secure ID and password authentication, yielding to other more critical NFRs for e-commerce such as customer privacy and cost. On the other hand, these NFRs are considered less important for highly sensitive assets such as a nuclear facility or a major data center.

Security Problems

Undesirable Outcome

An undesirable situation in the context of an asset that negatively impacts a security objective, for example, stolen credit card information is an undesirable outcome for TJX and the payment card industry.

Threat

An operation or technique that may be used by hostile agents to exploit a vulnerability to achieve an undesirable outcome, for example, the hacker in the TJX case broke wireless network WEP encryption key by exploiting the easy-to-crack WEP encryption on his way to stealing credit card information.

Vulnerability

A weakness of an asset or facility that can be exploited by a threat to achieve an undesirable outcome.

Mitigating Solutions

Impact Prevention and Control

A mitigation technique that prevents a realized undesirable outcome from inflicting a negative impact on a security objective. For example, PCI recommends that card authentication data (e.g. card verification code) be not stored to prevent credit card information to be useful if stolen.

Positive Consequences

One or more positive impact contributed by a mitigation technique toward the security objective or other NFRs. For example, not storing card authentication data is highly helpful toward security. Positive contributions are depicted on the mitigation diagram with green dashed directed lines with a label to indicate the contribution, where "++" represents "Make" for sufficiently positive to consider that the NFR is achieved by this contribution, "+" represents "Help" for somewhat positive and helpful toward achieving the NFR, while "S+" represents an undetermined positive contribution.

Negative Consequences

One or more negative impact contributed by a mitigation technique toward security objective or other NFRs. For example, not storing card authentication data is detrimental for availability making it impossible to store and process a payment at a later time, and it also hurts usability as the customer has to wait for a payment clearance. Negative contributions are depicted on the mitigation diagram with red dashed directed lines with a label to indicate the contribution, where "--" represents "Break" for highly negative against achieving an NFR, "-" represents "Hurt" for somewhat negative and hurtful toward denying the NFR, while "S-" represents an undetermined negative contribution.

Threat Containment

A mitigation technique that isolates a realized threat or reduces the possibility for a realized threat to cause an undesirable outcome. For example, if a wireless network is known to have been hacked, the organization may immediately isolate and disconnect the sub-network from the rest of company's network so that the hacker could not steal credit card information that may reside in the corporate network.

Positive Consequences

A positive impact contributed by the mitigation technique toward the security objective or other NFRs.

Negative Consequences

A negative impact contributed by the mitigation technique toward the security objective or other NFRs.

Threat Prevention

A mitigation measure that helps prevent the threat from being realized.

Positive Consequences

A positive impact contributed by the mitigation technique toward the security objective or other NFRs.

Negative Consequences

A negative impact contributed by the mitigation technique toward the security objective or other NFRs.

Vulnerability Risk Transfer

A mitigation technique that changes the facility so that the risk associated with the old facility is transferred to a lower risk of the new facility. For example, the high risk associated with wireless WEP encryption could be transferred to a lower risk of a more secure wireless WPA encryption. The notion of risk transfer is adapted from a risk management technique discussed in [Boe89].

Positive Consequences

A positive impact contributed by the mitigation technique toward the security objective or other NFRs.

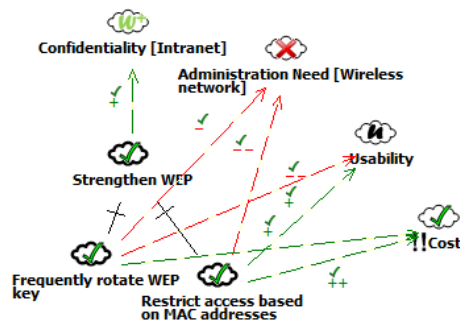
Negative Consequences

A negative impact contributed by the mitigation technique toward the security objective or other NFRs.

Selection Sub-Patterns

Each threat and vulnerability mitigation pattern may contain a number of mitigation techniques, each may have different effectiveness in countering the security problems, and may have different positive and negative consequences toward NFRs. Selecting appropriate mitigation techniques is not simple, especially when the security objective and other NFRs are conflicting. Therefore, each pattern may also contain selection sub-patterns to recommend appropriate mitigation techniques for a given set of NFRs and corresponding criticality that can be used as a starting point by the pattern users.

For example, Strengthen WEP is recommended for mitigating WEP breaking related threat and vulnerability when cost of mitigation is considered to be very critical, while confidentiality and usability are also considered but are given less weight. The selection pattern can be depicted with an excerpt from the main pattern as follows:



The selection pattern captures the rationale for the recommendation based on the positive and negative consequences and criticality of the NFRs. The selection of the mitigation techniques is indicated by the check mark labeled on the thick-border cloud icons representing the detailed mitigation techniques. The labels are propagated to other more abstract mitigation techniques (e.g. Strengthen WEP) and NFRs based on the type of contributions (e.g. ++, +, -, --, or decompositions such as AND- or OR-decomposition denoted with a single- or double-bar respectively) and their satisficing status, resulting in a *Satisfied* label (check-mark), *Denied* label (cross-mark), *Weakly Satisfied* (W+), *Weakly Denied* (W-), *Undecided* (u), or *Conflicting* (lightning bolt), using the label evaluation procedure defined in the NFR Framework [Chu00].

Reference

Source of Knowledge

The source of knowledge section identifies the source of information for the context, problem, and solution of the pattern, which may be combined from different sources to construct a meaningful threat and mitigation pattern.

Experience

The Experience section documents known uses of mitigation techniques or the pattern itself, preferably with postmortem lessons learned and insights.

4 Wireless WEP Breaking TVM Pattern

Synopsis

The **Wireless WEP Breaking** (TVM pattern) is concerned with **confidentiality of Intranet** (security objective) that may be compromised via a **wireless network** (facility), by **WEP encryption key breaking** (threat) that exploits **Weak encryption of wireless WEP** (vulnerability), that could lead to **unauthorized access to the intranet** (undesirable outcome) that may negatively affects the **confidentiality of the intranet** (security objective).

The **Weak encryption of wireless WEP** (vulnerability) could be mitigated by **using a wireless network that uses WPA, WPA2, IPSEC, VPN, or SSL/TLS** (risk transfer measure) that changes the facility to that with a more acceptable vulnerability. Alternatively, the **WEP encryption breaking** (threat) may be prevented by **strengthen WEP that uses at least 104-bit, frequently rotating the WEP key, using with WPA or VPN, or controlling access based on MAC addresses** (preventive measures), and/or contained by **isolating the affected facility** (quarantine measure). These mitigation solutions have positive and/or negative consequences upon **Availability, Cost, Administration Need, and Usability** (NFRs).

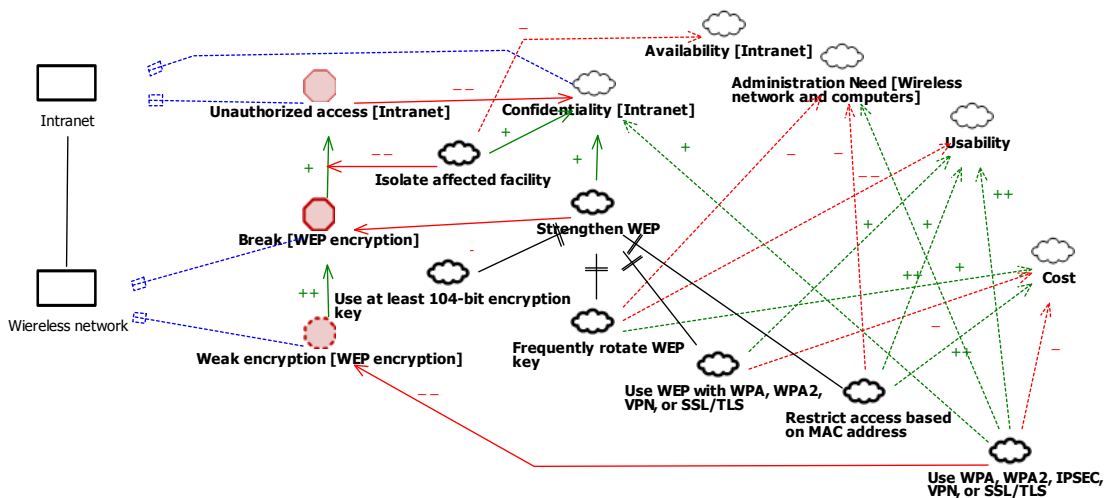


Figure 3. A Wireless WEP Breaking Threat and Vulnerability Mitigation Pattern

Context

Asset

Intranet

An internal network that has direct or indirect access to sensitive information desirable by hostile agents.

Facility

Wireless network

Wireless network provides a convenient and cost effective means for data communication, especially for locations that are not designed with data network in mind or require connectivity with mobile devices such as at retail stores. Because wireless signal can be intercepted by any wireless devices within the signal range, most private wireless networks are configured to encrypt transmitted data. WEP is the first widely used encryption technique used by the first generation wireless networks. It uses a simple symmetric

encryption method with a short key length (24 or 104 bits). Later generations of wireless networks support WPA or WPAs that use a more secure encryption method such as AES with a longer key length.

Security objective

Confidentiality of the Intranet

Intranet should be accessible to only authorized personnel and devices.

Affected NFRs

Availability

How a mitigation technique affects the availability of the intranet.

Cost

The monetary expense that incurs with a particular mitigation technique.

Administration Need

How much recurring administration support a mitigation technique needs after it has been implemented.

Usability

Ease of use for end users to use a particular mitigation technique.

Security Problems

Undesirable Outcome

Unauthorized access to the intranet

An unauthorized access to the intranet by a hostile agent could lead to other undesirable outcomes such as stolen credit card information.

Threat

Breaking of WEP encryption key

If a sufficiently large amount of encrypted data can be collected, for example over the air from a parking lot outside a retail store [tjx], it can be used to crack the encryption key [no clothes].

Vulnerability

Weak encryption of WEP

WEP uses 24 bits or 104 bits for encryption key and a simple symmetric encryption method. It has been proven to be easy to crack [Arb02].

Mitigating Solutions

Impact Prevention and Control

Not available

Threat Containment

Isolate affected facility

A log of data communication with MAC addresses could be collected and examined. The affected wireless network or intermediate sub-networks may be disabled or isolated to prevent access to sensitive asset such as credit card information.

Positive Consequences

Make (++) cost, as most wireless access point equipment should already support this option.

Negative Consequences

Hurt (-) availability of the intranet if the affected area is disabled or isolated from the rest of the network, as legitimate use of the network from and to the affected facility would be restricted.

Threat Prevention

Using WEP with at least 104 bits for encryption.

Using a longer key length makes it harder and more time consuming to break. The PCI DSS recommends this option [PCI05 section 4.1.1], however, it has been shown to be easy to crack [Tews07].

Positive Consequences

Make (++) cost, as most wireless access point equipment should already support this option.

Negative Consequences

Break (--) security, as 104-bit WEP is still highly vulnerable [Tews07].

Rotating WEP key every quarter and after each critical personnel change.

This mitigation technique is recommended by PCI DSS [PCI05 section 4.1.1], but appears to be effective in guarding against previously authorized users, such as ex-employees, to gain access after they are no longer authorized (e.g. after employment termination), therefore, not a direct mitigation of the WEP breaking threat.

Positive Consequences

Help (+) cost, as no additional equipment is required.

Negative Consequences:

Hurt (-) toward administration needs for ongoing key rotation support.

Break (--) usability, as users or network administrators have to reconfigure the wireless computers and devices whenever the key is rotated.

Hurt (-) availability, as any wireless device or computer that is not reconfigured with the new key in time before the key is rotated would not have access to the network.

Using with a more secure supplemental technologies such as WPA or VPN

PCI recommends this technique to be used with WEP encryption. While it is reasonable to use WEP with VPN, but, it appears to be impractical to use both WEP and WPA encryptions in the same wireless network as most wireless access points allow either method for encryption if both technologies are supported.

Positive Consequences

Make (++) security

Negative Consequences:

Hurt (-) administration needs

Break (--) cost, if new equipment or software is required.

Restricting access by MAC address

Most wireless access point equipment support access control by MAC address so that only allowed devices may access the network. This mitigation is recommended by PCI DSS [PCI05 section 4.1.1].

Positive Consequences

Make (++) cost, as no additional equipment is required

Negative Consequences

Hurt (-) administration need, as network administrator needs to update all relevant wireless access points whenever a device is authorized or de-authorized from the networks.

Vulnerability Risk Transfer ☁

Using a more secure encryption

Use encryption methods, such as WPA, WPA2, VPN, or SSL/TLS [PCI 4.1] that use harder to break encryption methods. This mitigation is recommended by PCI DSS [PCI05 section 4.1.1].

Positive Consequences

Make (++) security

Make (++) usability, as connecting network devices and computers do not require re-configuration once they have been set up to use the new encryption technology reconfiguration

Negative Consequences

Break (--) cost, new equipment or software is required if it is not already supported.

Selection Patterns

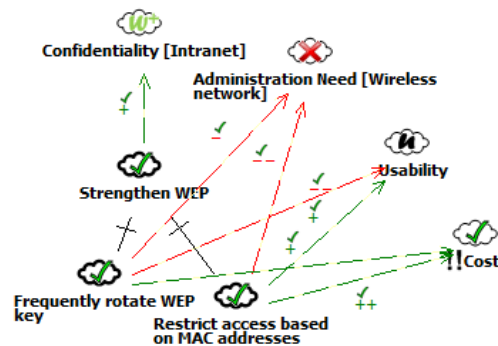
!!Cost, Confidentiality, Administration Need, Usability

Recommended Mitigations:

- Strengthen WEP, including
 - rotating WEP keys
 - restricting access based on MAC addresses

NFRs achievement:

- Cost (satisfied)
- Confidentiality (weakly-satisfied)
- Administration Need (denied)
- Usability (undecided)



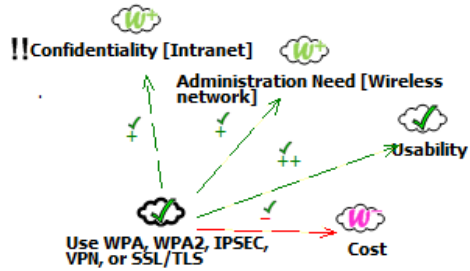
!! Confidentiality, Administration Need, Usability, Cost

Recommended Mitigations:

- Use WPA, WPA2, IPSEC, VPN, or SSL/TLS

NFRs achievement:

- Confidentiality (weakly-satisfied)
- Administration Need (satisfied)
- Usability (satisfied)
- Cost (weakly-denied)



Reference

Source of Knowledge

PCI DSS 1.1

Experience

Over 700 organizations are compliant with and using the PCI DSS [Vis09]

5 Remote Access Masquerading TVM Pattern

Synopsis

The **Remote Access Masquerading** (TVM pattern) is concerned with **confidentiality of corporate server** (security objective) that may be compromised via **remote users logging in to a server using ID and password** (facility), by a **hacker masquerading as a valid user using stolen ID and password** (threat) that exploits **easily stolen ID/passwords that are due to the use of easy to guess simple passwords, undesirable user behavior and social engineering, or hackable ID/password**, (vulnerability), that could lead to an **unauthorized access to the server** (undesirable outcome) that negatively affects the **confidentiality of the corporate server** (security objective).

The **easily stolen ID/passwords** (vulnerability) could be mitigated by **using secure passwords that employ strong passwords (non-dictionary words and frequently changed passwords), user education, training, and enforcement, and encrypting stored and transmitted IDs and passwords** (risk transfer measure) that change the facility to that with a more acceptable vulnerability. Alternatively, **hacker masquerading as a valid user using stolen ID and password** (threat) may be prevented by **implementing two-factor authentication that uses ID/password with certificate/token based authentication or ID/password with biometrics based authentication** (preventive measures). In the case that those mitigation techniques were unsuccessful, **stolen credit card information** (undesirable outcome) may be prevented or controlled by **not storing card sensitive authentication data** (impact prevention and control) to limit the impacts on the **confidentiality of credit card information** (security objective). These mitigation solutions have positive and/or negative consequences upon **Usability and Cost** (NFRs).

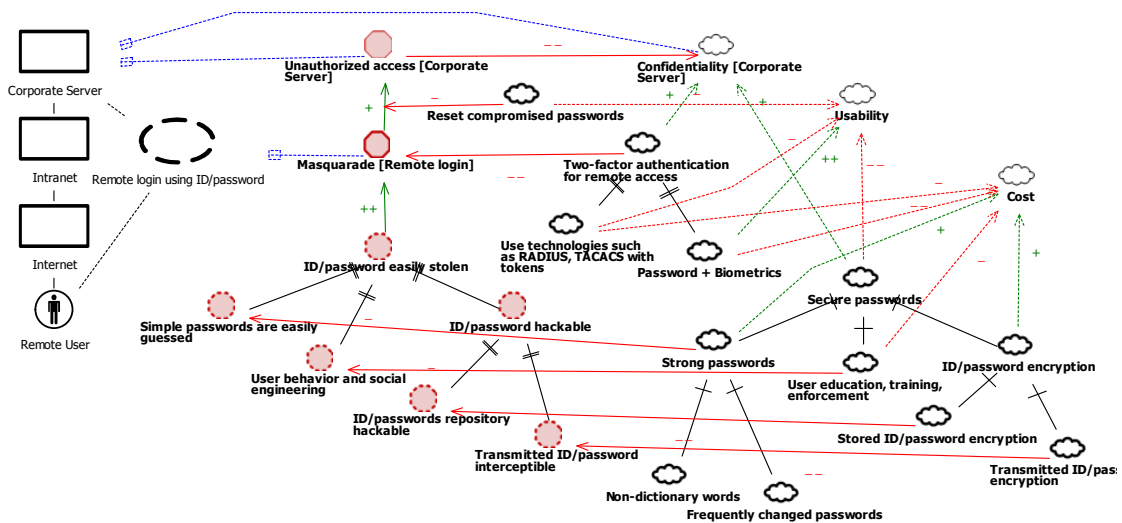


Figure 4. A Remote Access Masquerading Threat and Vulnerability Mitigation Pattern

Context

Asset

Corporate server

A corporate server on the or central network.

Facility

A login facility that allows remote users on a network outside the corporate network to login for accessing the server.

Security objective

Confidentiality of the server

Corporate servers should be accessible to only authorized personnel.

Affected NFRs

Cost

The monetary expense that incurs with a particular mitigation technique.

Usability

Ease of use for end users to use a particular mitigation technique

Security Problems

Undesirable Outcome

Unauthorized access to the server

A server accessible to a hostile agent that could lead to other undesirable outcomes.

Threat

Masquerading as a valid user

A hostile agent may masquerade as an authorized user login using stolen ID and password to gain access to the server.

Vulnerability

Easily stolen ID and password

Using ID and password is a common authentication method. However, IDs and passwords can be stolen if the passwords are easy to guess (e.g. using words that exist in a dictionary), some unsuspecting users may leave written ID and password nearby the computer as a reminder, or IDs and passwords that are stored and transmitted in clear text.

Mitigating Solutions

Impact Prevention and Control

Not available

Threat Containment

Resetting the password or disabling the account

If an ID and password is suspected to have been used improperly, the user may change the password, or the organization may reset the password to a new system generated password, or disable the account.

Positive Consequences

Make (++) cost, as no additional equipment or software is required

Negative Consequences

Hurt (-) usability, as users have to remember the new password or re-activate the account.

Threat Prevention



Use two-factor authentication

Two-factor authentication that ID/password with security token, certificate, or biometric based authentication could prevent user masquerading based on ID and password alone. The additional authentication factor may be RADIUS or TACACS, secure ID, VPN with personal certificate, or biometrics such as finger print or facial recognition, or retina scan technologies. This mitigation is recommended by PCI DSS [PCI05 section 8.3].

Positive Consequences

Make (++) usability for biometrics based authentication, as users do not need to memorize an additional password or carry a special device.

Negative Consequences

Hurt (-) cost, as it is costly to acquire token devices or to collect and maintain biometrics samples.

Hurt (-) usability for token based authentication, as users need to carry a physical device, which can be lost or misplaced.

Vulnerability Risk Transfer



Not available. It is unlikely that ID and password based authentication could be replaced since it is widely supported by most computing platforms and is cost effective.

Selection Patterns

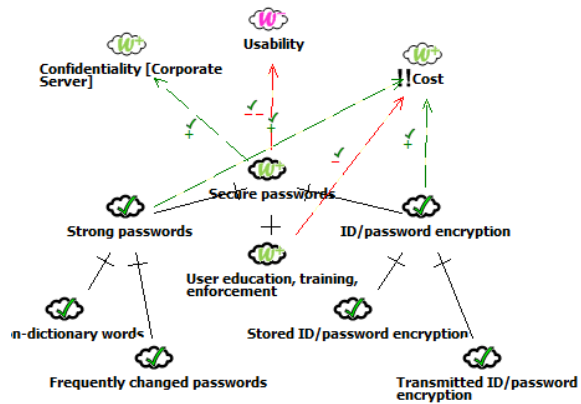
!! Cost, ! Confidentiality, Usability

Recommended Mitigations:

- Secure passwords, consisting of
 - strong passwords,
 - user education, training, enforcement,
 - ID/password encryption

NFRs achievement:

- Cost (weakly-satisfied)
- Confidentiality (weakly-satisfied)
- Usability (weakly-denied)



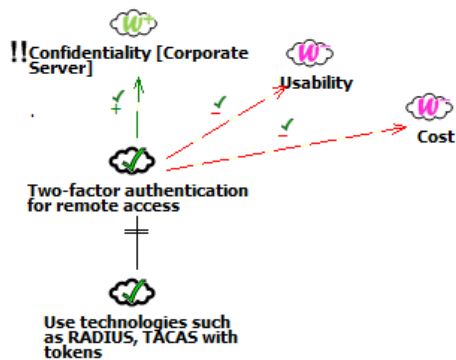
!! Confidentiality, !Usability, Cost

Recommended Mitigations:

- Two-factor authentication, using
 - Using technologies such as RADIUS, TACAC

NFRs achievement:

- Confidentiality (weakly-satisfied)
- Usability (weakly-denied)
- Cost (weakly-denied)



Reference

Source of Knowledge

PCI DSS 1.1

Experience

Over 700 organizations are compliant with and using the PCI DSS [Vis09]

6 Malicious Transfer of Sensitive Data TVM Pattern

Synopsis

The **Malicious Transfer of Sensitive Data** (TVM pattern) is concerned with **confidentiality of sensitive data** (security objective) that may be compromised via **an internal host, intranet, the Internet, and external host, and data transfer capability** (facility), by **malicious transfer of sensitive data to a malicious external host** (threat) that exploits **making connection can be made to any external host** (vulnerability), which may be required by some legitimate applications, that could lead to **stolen sensitive data** (undesirable outcome) that may negatively affects the **confidentiality of the sensitive data** (security objective).

The **malicious transfer of sensitive data to a malicious external host** (threat) may be prevented by **restricting outbound traffic to that which is necessary for the cardholder data environment [PCI05 section 1.3.5], denying all outbound traffic not specifically allowed, and restricting outbound traffic from sensitive data processing applications to IP addresses within the DMZ** (preventive measures), and/or contained by **isolating affected facility** (threat containment). In the case that those mitigation techniques were unsuccessful, **stolen sensitive data** (undesirable outcome) may be prevented or controlled by **not storing complete data** and/or **storing the data in a different form that is not useful for hostile agents** (impact prevention and control) to limit the impacts on the **confidentiality of sensitive** (security objective). These mitigation solutions have positive and/or negative consequences upon **confidentiality, availability, and cost** (NFRs).

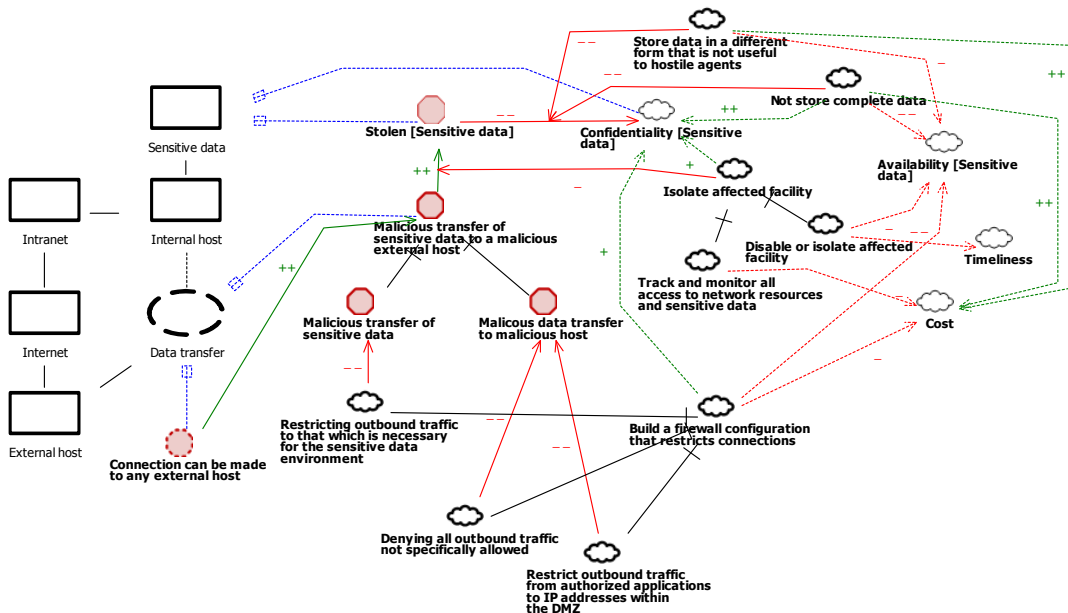


Figure 5. A Malicious Transfer of Sensitive Data Threat Mitigation Pattern

Context

Asset

Sensitive data

Sensitive data such as credit card information.

Facility

Internal host, Intranet, Internet, External host

Network connection that allows data transfer from intranet to malicious network or host via the Internet.

Security objective

Confidentiality of the sensitive data

The sensitive data is accessible to only authorized personnel.

Affected NFRs

Cost

The monetary expense that incurs with a particular mitigation technique.

Availability

How a mitigation technique affects the availability of the sensitive data.

Usability

Ease of use for end users to use a particular mitigation technique

Timeliness

How quickly a mitigation technique mitigates a security problem.

Security Problems

Undesirable Outcome

Stolen sensitive data

Sensitive data is obtained by a hostile agent.

Threat

Malicious transfer of sensitive data to a malicious external host

The threat is composed of two sub-problems: malicious transfer of sensitive data and malicious transfer to a malicious external host.

Vulnerability

Connection can be made to any external host

A network connection can be made between any host on the intranet with any host on the Internet by default, allowing a malicious connection to be used for a malicious intent. Standard data transfer facility such as ftp may be used to transfer sensitive information to a malicious host.

Mitigating Solutions

Impact Prevention and Control

Not store complete data

In some cases, sensitive information would not be useful to hostile agents if a piece of information is missing or not stored. For example, credit card numbers would not be useful to hackers without the associated sensitive authentication code or expiration date. [PCI05 section 3.2]

Positive Consequences

Make (++) cost, as no additional equipment or software development are required

Negative Consequences

Break (--) availability of sensitive data for legitimate purposes that requires the missing information.

Storing data in a different form that is not useful to hostile agents

Information, such as driver license number, that is needed for authentication purposes may be stored in a different form without retaining the original information, for example, as an one-way hashed value, which can still be used for authentication, but would not be useful to hostile agents. If the original information needs to be retained, it may be stored in an encrypted form. Using hashed values and encryption are recommended by the PCI DSS [PCI05 section 3.4].

Positive Consequences

Make (++) cost, as no additional equipment or software development are required

Negative Consequences

Break (--) availability of payment card information for legitimate purposes where the missing information is needed.

Threat Containment



Isolating affected facility

Network traffic may be logged and frequently monitored [PCI05 section x] to detect potentially malicious connectivity or activities on the sensitive asset, for example, a connection to known malicious destination or file transfer of sensitive files to unauthorized destinations. If that occurs, the suspected origin host or sub-network may be isolated or disabled.

Positive Consequences

Make (+) cost, as no additional equipment is required although would some incur labor cost for the personnel to monitor the network log.

Negative Consequences

Break (--) availability of facility for legitimate use, if disabled or isolated from the rest of the network.

Hurt (-) timeliness of threat mitigation, as detecting and recovering after the fact take time and may not be in time to prevent large damages.

Threat Prevention



Restricting outbound traffic

Malicious network connection and data transfer can be prevented by restricting outbound traffic to that which is necessary for sensitive data environment [PCI05 section 1.3.5], which can be achieved via the use of a firewall equipment or software.

Positive Consequences

Make (++) proprietary of network connection and data transfer usage

Negative Consequences

Hurt (-) availability of unplanned but legitimate network connections and data transfer

Hurt (-) cost, as a separate environment must be dedicated for sensitive information

Vulnerability Risk Transfer



Not available. Network connection and data transfer are basic network facilities that are essential and cannot be easily replaced.

Selection Patterns

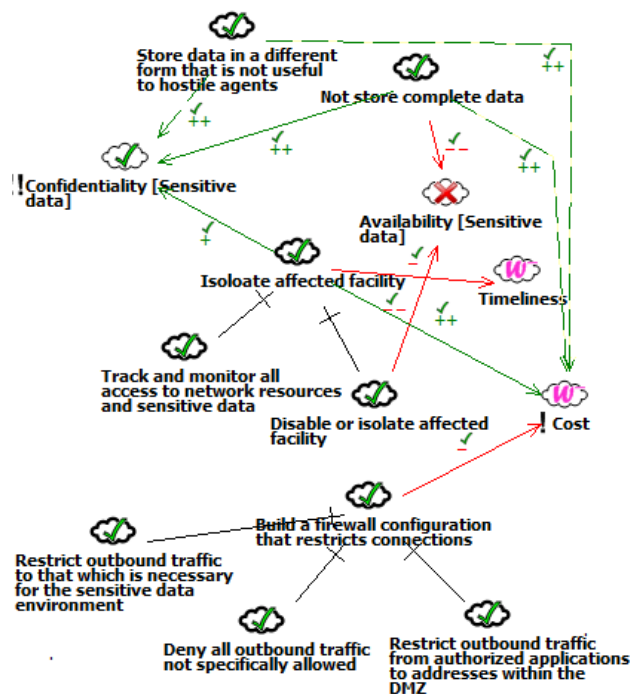
!! Confidentiality, ! Cost, Availability

Recommended Mitigations:

- Not store complete data (e.g. card authentication data)
- Isolate affected facility
 - Track and monitor all access to network resources and sensitive data
 - Disable or isolate affected facility
- Build a firewall configuration that restricts connections
 - Restricting outbound traffic to that which is necessary for the sensitive data environment
 - Denying all outbound traffic not specifically allowed
 - Restrict outbound traffic from authorized applications to IP addresses within the DMZ

NFRs achievement:

- Confidentiality (satisfied)
- Cost (weakly-denied)
- Availability (denied)
- Timeliness (weakly-denied)



Reference

Source of Knowledge

PCI DSS 1.1

Experience

Over 700 organizations are compliant with and using the PCI DSS [Vis09]

7 Related Work and Discussion

A large number of security patterns have been instrumental in capturing knowledge for achieving security at the architecture and design level [Fer01, Fer07, Sch05]. Our threat and vulnerability mitigation (TVM) patterns complement these security patterns with more formally represented security context (asset, facility, security objective and other NFRs), security problems, consequences, and guidelines for choosing security measures at the organizational level, where implementation specific details are available in the existing security patterns. Therefore, our TVM patterns can be seen and perhaps used as a bridge for transitioning from the requirements level to the architecture and design level.

The diagrammatic description of TVM patterns are based on a number of existing methods. Specifically, the notations representing asset and facility are adopted from the Problem Frames method [Jac00], which has been used for capturing patterns of domains and functions [Wir06] and adopted here to represent the embedded patterns of asset and facility. Security problems are represented using the notations from the Problem Interdependency Graph [Sup09] with an extension to represent vulnerabilities, while the notations for representing NFRs and solutions as (soft) goals are adopted from the NFR Framework [Chu00], which has been adopted for NFR-driven patterns selection [Gro01, Wei08]. The diagrams for the patterns in this paper were modeled using the RE-Tools¹ that supports integrated modeling using multiple notations.

While developing the concrete patterns using the meta-pattern as a template, we found that having a full understanding of security context and problems, and the classification of mitigating solutions helped make alternative exploration more complete. For example, we initially included only security measures from PCI DSS specification in the patterns. We found that in many cases, PCI DSS does not define complete mitigations for a set of vulnerability, threat, and undesirable outcome. In the case of the WEP Breaking pattern, while PCI DSS defines mitigations for vulnerability risk transfer and threat prevention, but it does not define threat containment, which prompted us to consider and capture a mitigation for isolating affected facility. In another case, for the Remote Access Masquerading pattern, while PCI DSS again defines mitigations for risk transfer and threat prevention, but does not define threat containment, which prompted us to consider password reset and account disabling as mitigating solutions to make the patterns more complete.

We also found that the approach presented in this paper has a number limitations. First, each TVM pattern, by capturing as many coherent mitigation alternatives as possible along the cause-effect chain between vulnerability, threat, and undesirable outcome, could be large and appear difficult to understand. The visual pattern is intended to provide a road map and visual cues to give a big picture of various concepts in the pattern and their relationships, but the pattern could still be difficult to understand for those that are not familiar with the visual pattern. Second, it appeared that some pieces of knowledge are common among many patterns, for example, "isolating affected facility" is a common mitigation in several TVM patterns that could have been extracted to a smaller pattern for reuse without having to repeat it in several larger patterns. However, our approach lacks the notation of pattern aggregation for capturing large grain knowledge composing of smaller grain patterns. Similarly, we envision that generalization could also be useful in reusing existing patterns to create specialized patterns with more specific knowledge for different situations and cases. For example, we could have a general pattern for mitigating encryption cracking that may be specialized by a pattern for mitigating WEP encryption cracking. Last, the TVM patterns in this paper appear to have a similar limitation experienced by some of existing patterns that pattern application during software development process is usually performed manually, where desirable solutions must be manually incorporated in requirements and design models. Although the TVM patterns in this paper are captured in a modeling tool, but due to the lack of support for systematic pattern application concept, desirable mitigation decisions must still be incorporated into requirements models manually.

¹ www.utdallas.edu/~supakkul/tools/RE-Tools

8 Conclusion

In this paper, we have presented a meta-pattern and a pattern language (pattern catalog) for capturing knowledge of security context (asset, facility, and NFRs as driving forces), security problems (vulnerability, threat, and undesirable outcome), and mitigating solutions (risk transfer, threat prevention and containment, impact prevention and control) as well as sub-patterns for recommending suitable mitigation techniques based on NFRs and their criticality. The approach has been applied to develop a pattern language, consisting of three mitigation patterns that could have prevented the TJX credit card theft incident.

A number of improvements are being investigated, including a framework for relating patterns using aggregation and generalization concepts, and a method for systematically applying patterns in requirements models in a tool environment.

Reference

- [Ale77] C. Alexander, S. Ishikawa, and M. Silverstein, "A pattern language: towns, buildings, construction", Oxford Univ. Press, 1977
- [Gau07] S. Gaudin, "Banks Hit T.J. Maxx Owner With Class-Action Lawsuit", InformationWeek, Apr. 25, 2007
- [Gro01] D. Gross and E. Yu, "From non-functional requirements to design through patterns", Requirements Engineering, 6(1), pp. 18-36, Springer, 2001
- [Arb02] W. Arbaugh, N. Shankar, and Y. Wan, "Your 802.11 Wireless Network Has No Clothes", Wireless Communications, IEEE, 9(6), pp. 44-51, 2002
- [Boe89] B. Boehm, "Tutorial: Software Risk Management", IEEE Computer Society Press, 1989
- [Bra07] T. Bradley, A. Chuvakin, A. Elberg, and B.J. Koerner, "PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance", Syngress Publishing, 2007
- [Can07] Office Of The Privacy Commissioner Of Canada And Office Of The Information And Privacy Commissioner Of Alberta, Report of an Investigation into the Security, Collection and Retention of Personal Information of TJX Companies Inc. and Winners Merchant International L.P., Sep. 24, 2007
- [Chu00] L. Chung, B. A. Nixon, E. Yu, and J. Mylopoulos, "Non-Functional Requirements in Software Engineering", Kluwer Academic Publishers, 2000
- [FIS02] The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541)
- [Jac00] M. Jackson, "Problem Frames: Analyzing and structuring software development problems", Addison-Wesley Longman Publishing, 2000
- [Fer01] E. Fernandez and R. Pan, "A pattern language for security models", PLoP 2001
- [Fer07] E.B. Fernandez, J. Ballesteros, A.C. Desouza-Doucet, and M.M. Larrondo-Petrie, "Security Patterns for Physical Access Control Systems", Lecture Notes in Computer Science, 4602(259), Springer, 2007
- [Hil07] S. Hilley (editor), Computer Fraud and Security, Elsevier, Apr. 2007
- [Hil08] S. Hilley (editor), Computer Fraud and Security, Elsevier, Jan. 2008
- [Mes95] G. Meszaros and J. Doble, "A pattern language for pattern writing", PLoP95

- [PCI05] Payment Card Industry, "Data Security Standard v 1.1", 2005
- [Per07] J. Pereira, "Breaking The Code: How Credit-Card Data Went Out Wireless Door", The Wall Street Journal, May 4, 2007
- [Sch05] M. Schumacher, E. Fernandez, D. Hybertson, and F. Buschmann, "Security Patterns: Integrating security and systems engineering", John Wiley & Sons, 2005
- [Sup09] S. Supakkul and L. Chung, "Extending Problem Frames to Deal with Stakeholder Problems: An Agent- and Goal-Oriented Approach", Proc. the 24th ACM Symposium on Applied Computing (RE Track), March 9-12, 2009, Honolulu, pp. 389-394
- [Tew07] E. Tews, R.P. Weinmann, and A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds", Lecture Notes in Computer Science, 4867(188), Springer, 2007
- [Wir06] R. Wirfs-Brock, P. Taylor, and J. Noble, "Problem Frame Patterns", PLoP 2006
- [Wei08] M. Weiss and H. Mouratidis, "Selecting Security Patterns that Fulfill Security Requirements", Proc. 16th IEEE Intl. Requirements Engineering, 2008 (RE'08)
- [US08] United States of America v. Albert Gonzalez, United States District Court District of Massachusetts, 18 U.S.C. § 371, Aug. 5, 2008
- [Vis09] Visa Inc, " Global List of PCI DSS Validated Service Providers", <http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf>
- Ver08] Verizon, "Data Breach Investigation Report", 2009