2nd Annual review
Florence 15 November 2013

nSHIELD

Attack surface metrics approach

Responsible of the activity: Andrea Morgagni – Selex-ES

Presenter: Andrea Fiaschetti – Univ. "La Sapienza"

ARTEMIS

References

BASELINE

OSSTMM 3 The Open Source security Methodology Manual – Contemporary security Testing and Analysis – created by Pete Herzog – Developed by ISECOM – 2010

An Attack Surface Metric - Pratyusa K. Manadhata, Member, IEEE, and Jeannette M. Wing, - IEEE Transactions on Software Engineering, 2010

DAMAGE POTENTIAL-EFFORT RATIO

Common Criteria – Common Methodology for Information Technology Security Evaluation – Evaluation methodology, September 2012, Version 3.1, Revision 4

WEAKNESS WEIGHTED

Purpose and base concepts (1/2)

TARGET: Quantify how a nSHIELD system is resistent to **ATTACK** to its **SURFACE (Actual SPD level).**

SYSTEM'S ATTACK SURFACE is the set of ways in which an attacker can enter the system and potentially cause damage.

Purpose and base concepts (2/2)

- **Threat** is the origin of the fault chain (fault -> errors -> failures) for the dependability concerns and as the potential for abuse of protected assets by the system for security concerns.
- The **Attacker** is the threat agent, it is a malicious human activity or non malicious event
- An attacker uses **nSHIELD's entry and exit** points to attack the system.
- It is introduced an **entry and exit point framework** (formally modeled through I/O automata)
- A threat, to be effective, must interact either directly or indirectly with the asset. To separate the threat from the asset we need to avoid a possible interaction. Therefore it is possible to have **total (100) SPD level** if the threat and the asset are completely separated from each other. Otherwise SPD level indicates **a measure for assurance protection of the asset** which is provided by the controls you put on the asset or the **degree to which you lessen the impact of the threat**.

Actual SPD level definition (1/3)

Each system has interactive points, we refer them as **POROSITY** which is further categorized as one of 3 elements:

- **Complexity:** number of components critical for the dependability of the nSHIELD system;
- **Access**: number of different places where the interaction can occur (direct entry and exit points);
- **Trust**: each relationship that exists where the system accepts interaction freely from its component or another system within the scope (indirect entry and exit points)

Access “pores” leads to define the concept of **damage potential – effort ratio (der)**, which is a consistent measure of the lack of separation that each access pore introduces.

Actual SPD level definition (2/3)

To minimize the Attack surface we introduce **CONTROLS** divided in 2 classes and 10 categories:

Class	Category
Interactive controls	Authentication
	Idemnification
	Resilience
	Subjugation
	Availability
Process controls	Non-repudiation
	Confidentiality
	Privacy
	Integrity
	Alarm

Actual SPD level definition (3/3)

Controls minimize the attack surface, but they can themselves increase it if they have **LIMITATIONS** (particular events that affect how well our controls can work)

LIMITATIONS are classified in five types:

- **Vulnerability**
- **Weakness**
- **Concern**
- **Exposure**
- **Anomaly**

In Actual SDP level definition it was considered the introduction of a weight of a particular limitation (Vulnerability) wich is based on the concept of **attack potential** described in the **Common Criteria** standard and used in pSHIELD SPD metrics.

Actual SPD level calculation (1/2)

In this approach was used an operational metric and so must be considered the usual problems that this choice can lead.

The SPD level is a scale measurement of the attack surface, the amount of uncontrolled interactions with a target, which is calculated by the quantitative balance between operations, limitations, and controls.

Its calculation can be divided in two phases.

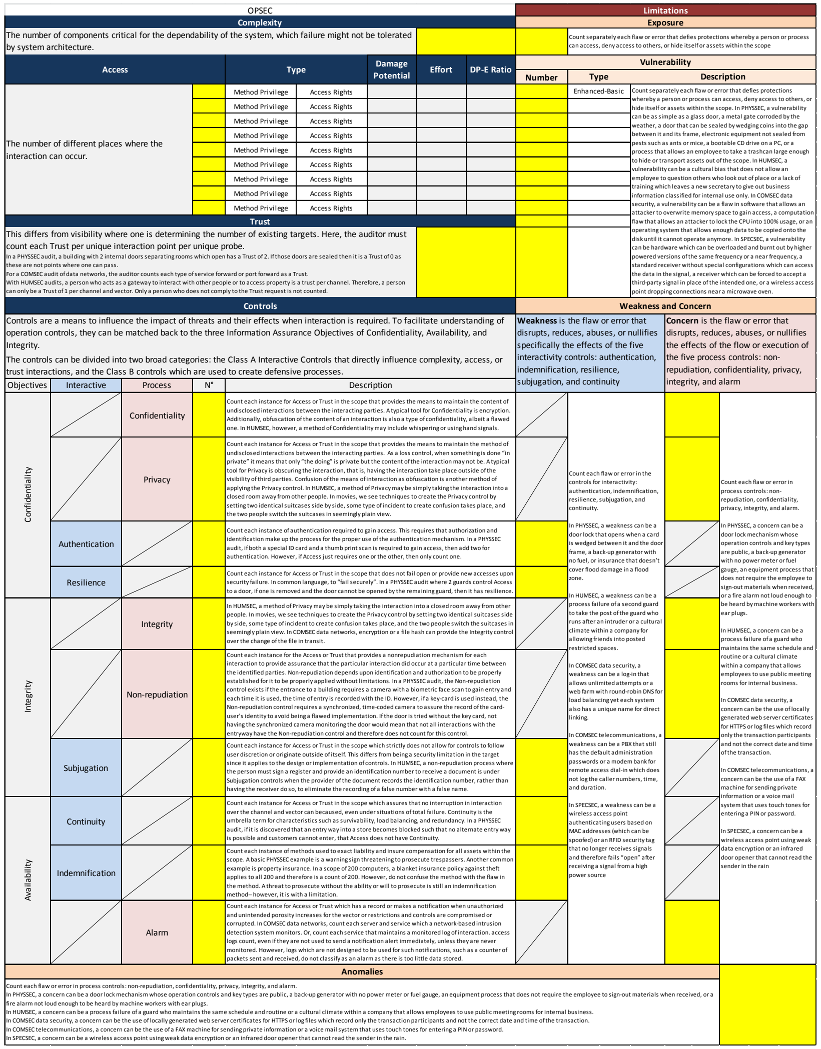
Actual SPD level calculation (2/2)

1. **Data collection** (see Data Collection Form) - for each component, subsystem and finally for the whole nSHIELD system must be considered:
   - Porosity data (complexity, access and trust attributes);
   - Controls in place;
   - Limitations found in the control (weighted with attack potential calculated as described in Common Criteria standard)

2. **Insertion of data collected in the calculation engine** (see Actual SPD Level calculation engine) – The output of this phase is the Actual SPD Level calculated througth the following formula (defined in D2.8)

$$\mathbf{\mathit{ActSPDL} = 100 + \mathit{ActSPDL\Delta} - 1/100 \times (\mathit{OpSec}_{base} \times \mathit{FC}_{base} - \mathit{OpSec}_{base} \times \mathit{SecLim}_{base} + \mathit{FC}_{base} \times \mathit{SecLim}_{base}}$$

Data Collection Form



OPSEC

Complexity

The number of components critical for the dependability of the system, which failure might not be tolerated by system architecture.

Access		Type		Damage Potential	Effort	DP-E Ratio
The number of different places where the interaction can occur.		Method Privilege	Access Rights			
		Method Privilege	Access Rights			
		Method Privilege	Access Rights			
		Method Privilege	Access Rights			
		Method Privilege	Access Rights			
		Method Privilege	Access Rights			
		Method Privilege	Access Rights			
		Method Privilege	Access Rights			
		Method Privilege	Access Rights			

Trust

This differs from visibility where one is determining the number of existing targets. Here, the auditor must count each Trust per unique interaction point per unique probe.

In a PHYSSEC audit, a building with 2 internal doors separating rooms which open has a Trust of 2. If those doors are sealed then it is a Trust of 0 as these are not points where one can pass.

For a COMSEC audit of data networks, the auditor counts each type of service forward or port forward as a Trust.

With HUMSEC audits, a person who acts as a gateway to interact with other people or to access property is a trust per channel. Therefore, a person can only be a Trust of 1 per channel and vector. Only a person who does not comply to the Trust request is not counted.

Limitations

Exposure

Count separately each flaw or error that defies protections whereby a person or process can access, deny access to others, or hide itself or assets within the scope

Vulnerability

Number	Type	Description
	Enhanced-Basic	Count separately each flaw or error that defies protections whereby a person or process can access, deny access to others, or hide itself or assets within the scope. In PHYSSEC, a vulnerability can be as simple as a glass door, a metal gate corroded by the weather, a door that can be sealed by wedging coins into the gap between it and its frame, electronic equipment not sealed from pests such as ants or mice, a bootable CD drive on a PC, or a process that allows an employee to take a trashcan large enough to hide or transport assets out of the scope. In HUMSEC, a vulnerability can be a cultural bias that does not allow an employee to question others who look out of place or a lack of training which leaves a new secretary to give out business information classified for internal use only. In COMSEC data security, a vulnerability can be a flaw in software that allows an attacker to overwrite memory space to gain access, a computation flaw that allows an attacker to lock the CPU into 100% usage, or an operating system that allows enough data to be copied onto the disk until it cannot operate anymore. In SPECSEC, a vulnerability can be hardware which can be overloaded and burnt out by higher powered versions of the same frequency or a near frequency, a standard receiver without special configurations which can access the data in the signal, a receiver which can be forced to accept a third-party signal in place of the intended one, or a wireless access point dropping connections near a microwave oven.

Controls

Controls are a means to influence the impact of threats and their effects when interaction is required. To facilitate understanding of operation controls, they can be matched back to the three Information Assurance Objectives of Confidentiality, Availability, and Integrity.

The controls can be divided into two broad categories: the Class A Interactive Controls that directly influence complexity, access, or trust interactions, and the Class B controls which are used to create defensive processes.

Weakness and Concern

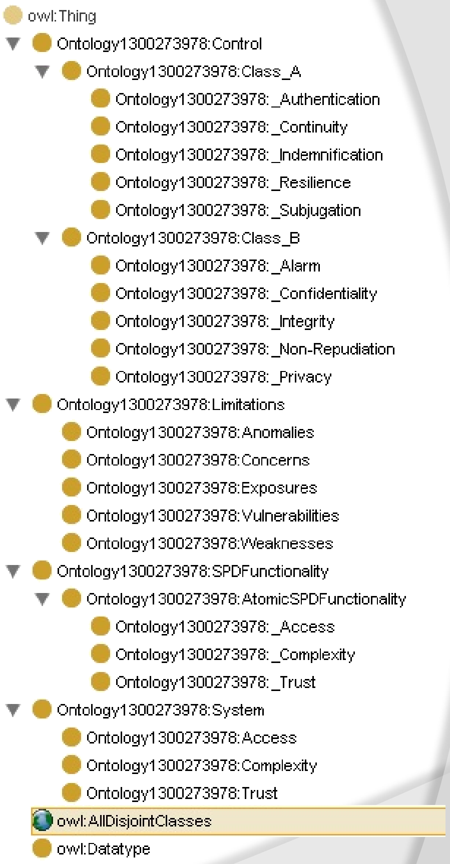
Weakness is the flaw or error that disrupts, reduces, abuses, or nullifies specifically the effects of the five interactivity controls: authentication, indemnification, resilience, subjugation, and continuity

Concern is the flaw or error that disrupts, reduces, abuses, or nullifies the effects of the flow or execution of the five process controls: non-repudiation, confidentiality, privacy, integrity, and alarm

Objectives	Interactive	Process	N°	Description				
Confidentiality		Confidentiality		Count each instance for Access or Trust in the scope that provides the means to maintain the content of undisclosed interactions between the interacting parties. A typical tool for Confidentiality is encryption. Additionally, obfuscation of the content of an interaction is also a type of confidentiality, albeit a flawed one. In HUMSEC, however, a method of Confidentiality may include whispering or using hand signals.		Count each flaw or error in the controls for interactivity: authentication, indemnification, resilience, subjugation, and continuity. In PHYSSEC, a weakness can be a door lock that opens when a card is wedged between it and the door frame, a back-up generator with no fuel, or insurance that doesn't cover flood damage in a flood zone. In HUMSEC, a weakness can be a process failure of a second guard to take the post of the guard who runs after an intruder or a cultural climate within a company for allowing friends into posted restricted spaces. In COMSEC data security, a weakness can be a log-in that allows unlimited attempts or a web farm with round-robin DNS for load balancing yet each system also has a unique name for direct linking. In COMSEC telecommunications, a weakness can be a PBX that still has the default administration passwords or a modem bank for remote access dial-in which does not log the caller numbers, time, and duration. In SPECSEC, a weakness can be a wireless access point authenticating users based on MAC addresses (which can be spoofed) or an RFID security tag that no longer receives signals and therefore fails "open" after receiving a signal from a high power source		Count each flaw or error in process controls: non-repudiation, confidentiality, privacy, integrity, and alarm. In PHYSSEC, a concern can be a door lock mechanism whose operation controls and key types are public, a back-up generator with no power meter or fuel gauge, an equipment process that does not require the employee to sign-out materials when received, or a fire alarm not loud enough to be heard by machine workers with ear plugs. In HUMSEC, a concern can be a process failure of a guard who maintains the same schedule and routine or a cultural climate within a company that allows employees to use public meeting rooms for internal business. In COMSEC data security, a concern can be the use of locally generated web server certificates for HTTPS or log files which record only the transaction participants and not the correct date and time of the transaction. In COMSEC telecommunications, a concern can be the use of a FAX machine for sending private information or a voice mail system that uses touch tones for entering a PIN or password. In SPECSEC, a concern can be a wireless access point using weak data encryption or an infrared door opener that cannot read the sender in the rain
		Privacy		Count each instance for Access or Trust in the scope that provides the means to maintain the method of undisclosed interactions between the interacting parties. As a loss control, when something is done "in private" it means that only "the doing" is private but the content of the interaction may not be. A typical tool for Privacy is obscuring the interaction, that is, having the interaction take place outside of the visibility of third parties. Confusion of the means of interaction as obfuscation is another method of applying the Privacy control. In HUMSEC, a method of Privacy may be simply taking the interaction into a closed room away from other people. In movies, we see techniques to create the Privacy control by setting two identical suitcases side by side, some type of incident to create confusion takes place, and the two people switch the suitcases in seemingly plain view.				
	Authentication			Count each instance of authentication required to gain access. This requires that authorization and identification make up the process for the proper use of the authentication mechanism. In a PHYSSEC audit, if both a special ID card and a thumb print scan is required to gain access, then add two for authentication. However, if Access just requires one or the other, then only count one.				
	Resilience			Count each instance for Access or Trust in the scope that does not fail open or provide new accesses upon security failure. In common language, to "fail securely". In a PHYSSEC audit where 2 guards control Access to a door, if one is removed and the door cannot be opened by the remaining guard, then it has resilience.				
Integrity		Integrity		In HUMSEC, a method of Privacy may be simply taking the interaction into a closed room away from other people. In movies, we see techniques to create the Privacy control by setting two identical suitcases side by side, some type of incident to create confusion takes place, and the two people switch the suitcases in seemingly plain view. In COMSEC data networks, encryption or a file hash can provide the Integrity control over the change of the file in transit.				
		Non-repudiation		Count each instance for the Access or Trust that provides a nonrepudiation mechanism for each interaction to provide assurance that the particular interaction did occur at a particular time between the identified parties. Non-repudiation depends upon identification and authorization to be properly established for it to be properly applied without limitations. In a PHYSSEC audit, the Non-repudiation control exists if the entrance to a building requires a camera with a biometric face scan to gain entry and each time it is used, the time of entry is recorded with the ID. However, if a key-card is used instead, the Non-repudiation control requires a synchronized, time-coded camera to assure the record of the card-user's identity to avoid being a flawed implementation. If the door is tried without the key card, not having the synchronized camera monitoring the door would mean that not all interactions with the entryway have the Non-repudiation control and therefore does not count for this control.				
	Subjugation			Count each instance for Access or Trust in the scope which strictly does not allow for controls to follow user discretion or originate outside of itself. This differs from being a security limitation in the target since it applies to the design or implementation of controls. In HUMSEC, a non-repudiation process where the person must sign a register and provide an identification number to receive a document is under Subjugation controls when the provider of the document records the identification number, rather than having the receiver do so, to eliminate the recording of a false number with a false name.				
Availability	Continuity			Count each instance for Access or Trust in the scope which assures that no interruption in interaction over the channel and vector can becaused, even under situations of total failure. Continuity is the umbrella term for characteristics such as survivability, load balancing, and redundancy. In a PHYSSEC audit, if it is discovered that an entry way into a store becomes blocked such that no alternate entry way is possible and customers cannot enter, that Access does not have Continuity.				
	Indemnification			Count each instance of methods used to exact liability and insure compensation for all assets within the scope. A basic PHYSSEC example is a warning sign threatening to prosecute trespassers. Another common example is property insurance. In a scope of 200 computers, a blanket insurance policy against theft applies to all 200 and therefore is a count of 200. However, do not confuse the method with the flaw in the method. A threat to prosecute without the ability or will to prosecute is still an indemnification method-- however, it is with a limitation.				
		Alarm		Count each instance for Access or Trust which has a record or makes a notification when unauthorized and unintended porosity increases for the vector or restrictions and controls are compromised or corrupted. In COMSEC data networks, count each server and service which a network-based intrusion detection system monitors. Or, count each service that maintains a monitored log of interaction. access logs count, even if they are not used to send a notification alert immediately, unless they are never monitored. However, logs which are not designed to be used for such notifications, such as a counter of packets sent and received, do not classify as an alarm as there is too little data stored.				

Anomalies

Count each flaw or error in process controls: non-repudiation, confidentiality, privacy, integrity, and alarm.
In PHYSSEC, a concern can be a door lock mechanism whose operation controls and key types are public, a back-up generator with no power meter or fuel gauge, an equipment process that does not require the employee to sign-out materials when received, or a fire alarm not loud enough to be heard by machine workers with ear plugs.
In HUMSEC, a concern can be a process failure of a guard who maintains the same schedule and routine or a cultural climate within a company that allows employees to use public meeting rooms for internal business.
In COMSEC data security, a concern can be the use of locally generated web server certificates for HTTPS or log files which record only the transaction participants and not the correct date and time of the transaction.
In COMSEC telecommunications, a concern can be the use of a FAX machine for sending private information or a voice mail system that uses touch tones for entering a PIN or password.
In SPECSEC, a concern can be a wireless access point using weak data encryption or an infrared door opener that cannot read the sender in the rain.



- owl:Thing
  - Ontology1300273978:Control
    - Ontology1300273978:Class_A
      - Ontology1300273978:_Authentication
      - Ontology1300273978:_Continuity
      - Ontology1300273978:_Indemnification
      - Ontology1300273978:_Resilience
      - Ontology1300273978:_Subjugation
    - Ontology1300273978:Class_B
      - Ontology1300273978:_Alarm
      - Ontology1300273978:_Confidentiality
      - Ontology1300273978:_Integrity
      - Ontology1300273978:_Non-Repudiation
      - Ontology1300273978:_Privacy
  - Ontology1300273978:Limitations
    - Ontology1300273978:Anomalies
    - Ontology1300273978:Concerns
    - Ontology1300273978:Exposures
    - Ontology1300273978:Vulnerabilities
    - Ontology1300273978:Weaknesses
  - Ontology1300273978:SPDFunctionality
    - Ontology1300273978:AtomicSPDFunctionality
      - Ontology1300273978:_Access
      - Ontology1300273978:_Complexity
      - Ontology1300273978:_Trust
  - Ontology1300273978:System
    - Ontology1300273978:Access
    - Ontology1300273978:Complexity
    - Ontology1300273978:Trust
  - owl:AllDisjointClasses
  - owl:Datatype

Conclusions

- Simple approach based on standard
- Technology Independent
- System scale Independend
- Fully deterministic
- Machine readable and machine executable (ready for automatic execution)
- The initial effort needed to identify parameters is balanced by the flexibility in future deployment
- An I/O automaton, $A = \langle sig(A);\ states(A);\ start(A);\ steps(A) \rangle$ is used to model the attack surface (entry/exit points): Forma Modelling

Thank you