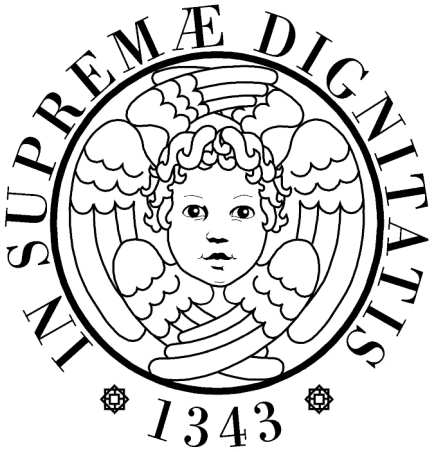
Threat Assessment & Remediation Analysis (TARA): "SAPIENT" case of study.

Mariano Basile

23rd July 2016



Contents

1 Introduction

1.1 High-level System Overview

SAPIENT is a client-server application for air-traffic control aimed at building a 4D map of environmental conditions of the sky to support air-traffic management (ATM). A client peer is located on an aircraft whereas the server(s) is(are) located in the ground network. Typically, during a flight, a client monitors the surrounding conditions of the sky from several viewpoints, including weather and communication quality. Then, the client reports sensed data to a SAPIENT server.

SAPIENT uses monitored data, possibly received from aircrafts, to build a global view of the system and send air-traffic management (ATM) commands. For example, given the weather conditions and the communication quality in a certain area, SAPIENT may command an aircraft that is flying by that area "to switch from a data link L to another one, L', before communication on the former link L is lost".

The main actors involved in the SAPIENT system are represented in Figure 1. The whole architecture can be divided into several domains: the application domain, the data link domain (DL), the core network domain, and the air-traffic control domain. These domains will be briefly introduced below.

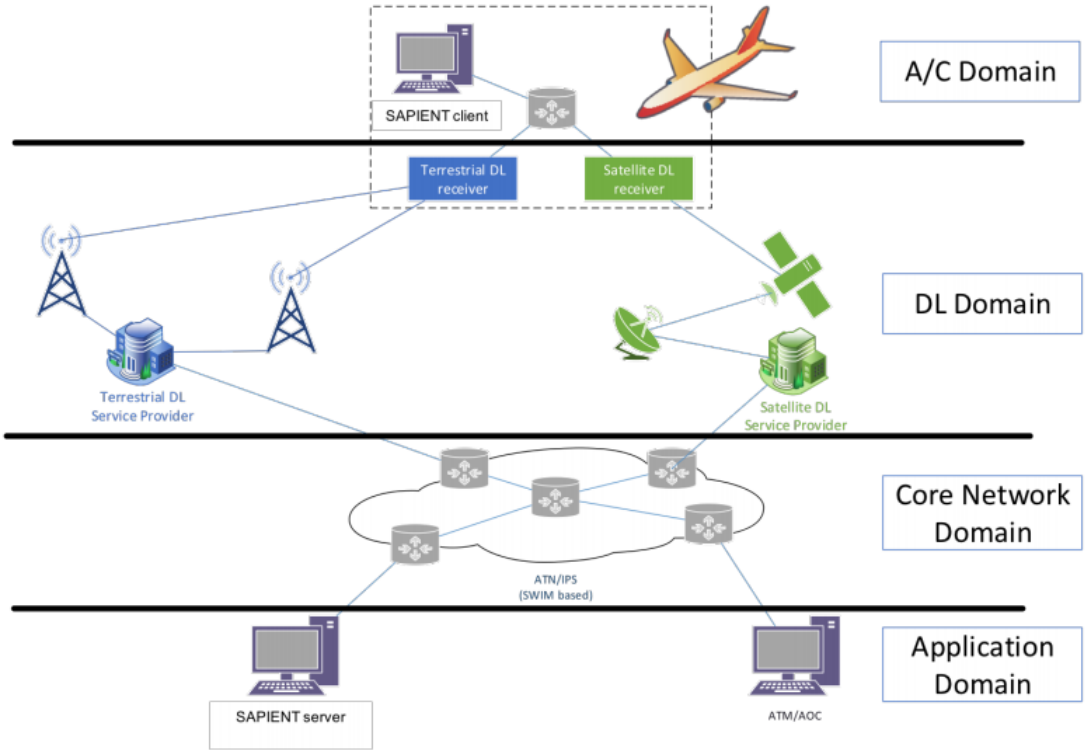


Figure 1: High-level representation of the SAPIENT system

The application domain includes all the applications that will be used either for the purpose of the SAPIENT system or for other ATM1 operations. The core network encompasses the core elements of the ATN/IPS, e.g. IPv6 routers, that are used to provide

connectivity for the ground network. That is, above the layer 2, SAPIENT service will run on the IPS suite2.

In particular, end-to-end communication will take place over TCP or UDP. The model of the core network, i.e., topology, link bandwidth and delay, routing etc. should be provided by partners with the relevant expertise. The data link domain includes all the ground-to-air data links that can be used to transport both SAPIENT and ATM/AOC data.

Two data links will be considered within the SAPIENT simulator: - A terrestrial DL, running LDACS, consisting of several antennas located on a floorplan (at given 3D coordinates), between which seamless layer-2 handover may occur; - A satellite DL, where an orbiting satellite relays communication between the A/C and a ground station.

The air-traffic control models the A/Cs as communication end-points, e.g. running SAPIENT and/or ATM/AOC applications, mobility models, mission duration (take-off/landing) etc. The internal structure of an A/C, if any such exists, needs to be clarified by partners with the relevant expertise.

For instance: is the A/C a single endpoint, or is it a network itself? In case, what is a model of the A/C network? A/C are of course mobile. The trajectory of an A/C will be modelled as a waypoint model, i.e. a sequence of tuples <3Dcoordinates, speed>, meaning that the aircraft moves at the specified constant speed towards the next waypoint. Figure 2 provides another end-to-end view of the system.

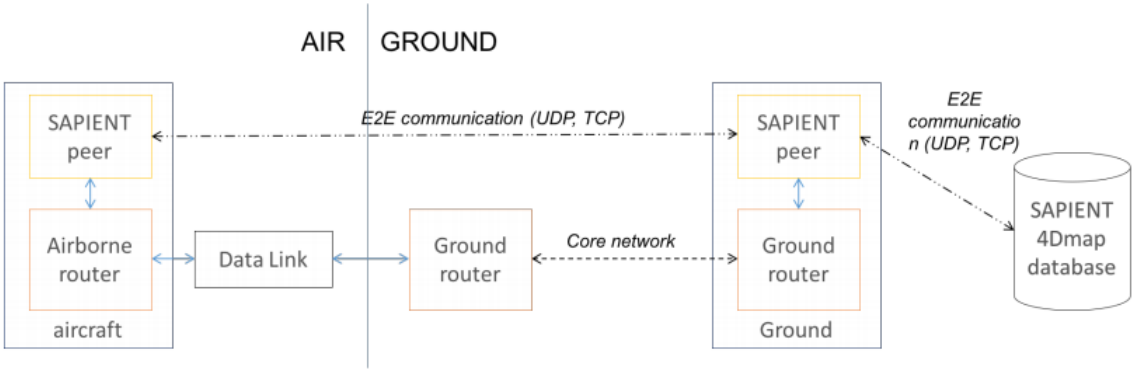


Figure 2: End-to-end view of SAPIENT

2 Threat Assessment & Remediation Analysis (TARA)

2.1 Assessment Methodology

TARA assessments are conducted on selected cyber assets. **A cyber asset is defined as any IT asset used to store, transport, and/or process information within an enterprise, including servers, clients systems, network appliances, etc**.
The objectives of a TARA assessment are:

- To identify and prioritize high-risk adversarial Tactics, Techniques, and Procedures (TTPs) that a cyber asset may be susceptible to;
- To identify and prioritize countermeasures (CMs) effective against those TTPs;
- To recommend CMs that can reduce the susceptibility of a cyber asset to attack;

Each TARA assessment is comprised of two analysis steps:

- **Cyber Threat Susceptibility Assessment (CTSA);**
- **Cyber Risk Remediation Analysis (CRRA);**

The CTSA step identifies and evaluates the susceptibility of a cyber asset to attack relative to a set of TTPs. The CRRA step identifies a set of countermeasures that reduce the susceptibility or lessen the effects of a cyber attack.
The deliverable of a TARA assessment is a set of recommended steps to reduce or minimize susceptibility of a cyber asset to attack.

3 Cyber Threat Susceptibility Assessment (CTSA)

CTSA quantitatively assesses a system's inability to resist cyber attack over a range of adversary Tactics, Techniques, and Procedures (TTPs) and produces a Threat Matrix, which provides a ranked list of TTPs that each cyber asset is susceptible to.
CTSA consists of the following steps:

1. Establish assessment scope;
2. Identify candidate TTP;
3. Eliminate implausible TTPs;
4. Apply scoring model;
5. Construct the threat matrix;

3.1 Establish assessment scope

The scope of CTSA is defined in terms of the cyber assets evaluated against a specified range of TTPs.
In our scenario we've found three (3) cyber assets and fifteen (15) TTPs selected from the open source Capec catalog (http://capec.mitre.org/).

3.2 Cyber Assets

- **Sapient Server (including Sapient 4D-MAP DB)**: A SAPIENT server uses monitored data, possibly received from aircrafts, to build a 4D map of environmental conditions of the sky to support air-traffic management (ATM).
- **Radio channel – Satellite channel**: ground-to-air (and viceversa) data links that can be used to transport both SAPIENT and ATM/AOC data.
- **Airborne router**: It is used to provide connectivity for the air-traffic control domain (e.g for the SAPIENT client to let it transmit sensed data).

3.2.1 Assumptions on the system

1. We do not take into account ATM/AOC machines since control towers already made full use for the purpose of sending air-traffic management (ATM) commands.

   Because of that we can suppose that some form of security already exists.
2. The same reasoning can be applied for the ATN/IPS network: here we assumed it is either a private network or the 'public' Internet but in which some secure form of communication have been implemented (e.g VPN, IPSEC, SSL, etc) and appropriate security policies have been applied.
3. If the assumption of trusted airline pilots holds then the Sapient client, which during a flight monitors the surrounding conditions of the sky and reports sensed data to a SAPIENT server, can also be considered a trusted source of information.
4. The radio channel and the satellite channel transmit info in clear.

3.3 Range of TTPs

ID	TTP Name	Source Reference
1	Interception	CAPEC-117
2	Excavation	CAPEC-116
3	Footprinting	CAPEC-169
4	Flooding	CAPEC-125
5	Fault Injection	CAPEC-624
6	Content Spoofing	CAPEC-148
7	Communication Channel Manipulation	CAPEC-216
8	Functionality Bypass	CAPEC-554
9	Brute Force	CAPEC-112
10	Exploiting Trust in Client (man in the middle, create malicious client, removing important client functionality)	CAPEC-22
11	Contaminate Resource	CAPEC-548
12	Infrastructure Manipulation	CAPEC-161
13	Audit Log Manipulation	CAPEC-268
14	Local Execution of Code	CAPEC-549
15	Malicious Logic Insertion	CAPEC-441

Figure 3: Involved CAPEC attack patterns

3.4 TTP Plausibility

The following table assesses the plausibility of each candidate TTPs as attack vectors for the various cyber assets, based on the available documentation.

Id	TTP Name	Source Reference	Plausible?	Rationale
1	Interception	CAPEC-117	YES	It usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties the attacker is passive however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. ***Involved c.as:*** **Radio channel – Satellite channel, Airborne router**
2	Excavation	CAPEC-116	YES	An adversary actively probes the target in a manner that is designed to solicit information relevant to system security.Ordinary interaction with the target may reveal info like stack traces, configuration information, path information, or database design ***Involved c.as:*** **Sapient Server**

3	Footprinting	CAPEC-169	Yes	It consists of using tools to learn as much as possible about the composition, configuration, and security mechanisms of the targeted application, system or network.Any system that can be detected can be footprinted. ***Involved c.as:*** **Sapient Server, Airborne router, Sapient client**
4	Flooding	CAPEC-125	YES	An attacker consumes the resources of a target by rapidly engaging in a large number of interactions with the target. ***Involved c.as:*** **Sapient Server**
5	Fault Injection	CAPEC-624	YES	An attacker uses disruptive signals (e.g. electromagnetic pulses, laser pulses etc.) to cause faulty behavior in electronic devices (terrestrial antennas, ground stations). ***Involved c.as:*** **Radio channel - Satellite channel**

6	Content Spoofing	CAPEC-148	YES	An attacker modifies content to make it contain something other than what the original content was while keeping the apparent source of the content unchanged. Any content could be spoofed, at the source or while it is in transit. ***Involved c.as:*** **Sapient Server, Airborne router, Radio channel - Satellite channel**
7	Communication Channel Manipulation	CAPEC-216	YES	Usually affects communication by manipulating security setting or protocol's parameters. ***Involved c.as:*** **Radio channel - Satellite channel**
8	Functionality Bypass	CAPEC-554	YES	An adversary attacks a system by bypassing some or all functionality intended to protect it. Often, a system user will think that protection is in place, but the functionality behind those protections has been disabled. ***Involved c.as:*** **Sapient Server, Airborne router, Sapient client**

9	Brute Force	CAPEC-112	YES	In this attack, some asset (information, functionality, identity, etc.) is protected by a finite secret value. Examples of secrets can include passwords (Sapient server), encryption keys, database lookup keys (Sapient DB). ***Involved c.as:*** **Airborne router, Sapient Server, Sapient Client**
10	Exploiting Trust in Client (Man in the Middle, create malicious client, removing important client functionality)	CAPEC-22	YES	An attack of this type exploits vulnerabilities in client/server communication. It leverages the implicit trust a server places in the client, or more importantly, that which the server believes is the client. An attacker executes this type of attack by placing themselves in the communication channel between client and server. ***Involved c.as:*** **Sapient Server, Radio channel - Satellite channel**

11	Contaminate Resource	CAPEC-548	YES	An adversary contaminates information systems including devices and networks. The information system, device or network is unavailable while the spill is investigated and mitigated. ***Involved c.as:*** **Sapient Server, Airborne router, Radio channel - Satellite channel Sapient client**
12	Infrastructure Manipulation	CAPEC-161	YES	An attacker exploits characteristics of the infrastructure of a network in order to perpetrate attacks or information gathering.Most often, this involves manipulation of the routing of network messages so, instead of arriving at their proper destination, they are directed towards an entity of the attacker, usually a server controlled by the attacker. ***Involved c.as:*** **Airborne router, Radio channel - Satellite channel**

13	Audit Log Manipulation	CAPEC-268	Yes	The attacker injects, manipulates, deletes, or forges malicious log entries into the log file, in an attempt to mislead an audit of the log file or cover tracks of an attack. ***Involved c.as:*** **Sapient Server**
14	Local Execution of Code	CAPEC-549	Yes	An adversary installs and executes malicious code on the target system in an effort to achieve a negative technical impact. ***Involved c.as:*** **Sapient Server, Sapient client, Airborne router**
15	Malicious Logic Insertion	CAPEC-441	Yes	An attacker installs or adds malicious logic (either sw or hw) into a seemingly benign component of the system. This logic is often hidden from the user of the system and works behind the scenes to achieve negative impacts. ***Involved c.as:*** **Sapient Server, Airborne router, Sapient client**

3.5 TTP Risk Scoring

Candidate TTPs are then ranked using a scoring model.
The TTP scoring model assesses the risk associated with each TTP based on a range of criteria. **For each TTP, the score (1 to 5) assigned to each criteria only considers the attack's success onto the system: NO MATTER WHERE. (i.e. the susceptible cyber assets which may be involved)**.
The risk score associated to each TTP is then computed as the scores' average assigned to each TTP's criteria.
This ranking helps set priorities on where to apply security measures to reduce the system's susceptibility to cyber attack.

Factors for assessing TTP Risk					
Factor Range	1	2	3	4	5
How localized are the effects posed by this TTP?	no noticeable effects	effects limited to targeted asset	targeted asset and supporting network	noticable effects to external enclave/domain	effects experienced globally
How long would it take to recover from this TTP once the attack was detected?	no recovery needed	< 1 hour	< 24 hours	< 72 hours	> 72 hours
What is the estimated cost to restore or replace affected cyber asset?	no restoration required	< $10K	< $20K	< $50K	> $50K
How serious an impact is loss of data confidentiality resulting from successful application of this TTP?	no adverse effects	limited adverse effects	serious adverse effects	severe adverse impact	catastrophic impact
How serious an impact is loss of data integrity resulting from successful application of this TTP?	no adverse effetcs	limited adverse effects	serious adverse effects	severe adverse impact	catastrophic impact
How serious an impact is loss of system availability resulting from successful application of this TTP?	no adverse effects	limited adverse effects	serious adverse effects	severe adverse impact	catastrophic impact
Is there evidence of this TTP's use in a security incident database?	Incident database not consulted	evidence of TTP use possible	confirmed evidence of TTP use in database	frequent use of TTP reported	widespread use of TTP reported
What level of skill or specific knowledge is required by the adversary to apply this TTP?	no specific skills required	generic technical skills	some knowledge of targeted system	detail knowledge of targeted system	knowledge of both mission and targeted system
Would resources be required or consumed in order to apply this TTP?	no resources required	minimal resources required	some resources required	significant resources required	resources required and consumed
How detectable is this TTP when it is applied?	not detectable	detection possible with specialized monitoring	detection likely with specialized monitoring	detection likely with routine monitoring	TTP obvious without monitoring
Would residual evidence left behind by this TTP lead to attribution?	no residual evidence	some residual evidence, attribution unlikely	attribution possible from characteristics of the TTP	same or similar TTPs previously attributed	signature attack TTP used by adversary

Figure 4: TTP Risk Scoring Model

3.6 TTP Risk Scoring for the SAPIENT case of study

TTP ID	TTP Name	Source Reference	Criteria 1	Criteria 2	Criteria 3	Criteria 4	Criteria 5	Criteria 6	Criteria 7	Criteria 8	Criteria 9	Criteria 10	Criteria 11	Risk Score
9	Brute Force	CAPEC-112	5	5	4	5	5	5	4	4	4	4	5	4,54545455
8	Functionality Bypass	CAPEC-554	5	5	5	5	5	5	4	5	5	2	2	4,36363636
4	Flooding	CAPEC-125	5	5	4	1	1	5	2	5	5	5	5	3,90909091
10	Exploiting Trust in Client (Man in the Middle, Create Malicious Client, Removing Important Client Functionality)	CAPEC-22	5	5	3	5	5	5	2	5	3	2	2	3,81818182
15	Malicious Logic Insertion	CAPEC-441	5	5	4	1	5	5	1	4	5	4	2	3,72727273
6	Content Spoofing	CAPEC-148	5	4	2	5	5	5	1	5	3	2	2	3,54545455
12	Infrastructure Manipulation	CAPEC-161	3	2	2	5	1	5	1	4	4	4	3	3,09090909
14	Local Execution of Code	CAPEC-549	5	4	3	2	2	5	1	5	2	2	3	3,09090909
11	Contaminate Resource	CAPEC-548	3	3	3	1	1	5	1	4	3	4	2	2,72727273
1	Interception	CAPEC-117	3	2	1	5	3	3	1	4	2	1	2	2,45454545
3	Footprinting	CAPEC-169	2	4	2	5	1	1	2	3	2	2	2	2,36363636
2	Excavation	CAPEC-116	2	1	1	3	1	1	4	2	4	3	3	2,27272727
13	Audit Log Manipulation	CAPEC-268	2	4	2	1	1	1	1	4	2	4	3	2,27272727
7	Communication Channel Manipulation	CAPEC-216	3	3	2	1	3	3	1	2	2	3	1	2,18181818
5	Fault Injection	CAPEC-624	4	1	2	1	1	4	1	3	2	1	1	1,90909091

3.7 Threat Matrix

CTSA produces a Threat Matrix: the latter is generated by using the (already computed) TTP Risk Scoring,which lists plausible TTPs ranked by decreasing risk score and their mapping to cyber assets as a function of adversary type (External, Insider, Trusted Insider).

If a cyber asset is susceptible to a TTP, its risk score is transferred to that cyber asset.

The mapping of TTPs to threat actors, e.g. external, insider, and/or trusted insider, estimates the proximity of the adversary to the cyber asset that is minimally needed to conduct the TTP.

The Threat Matrix is also useful to tabulate an aggregate susceptibility to cyber attacks for each cyber asset considered in the assessment.

This matrix is used in the follow-on Cyber Risk Remediation Analysis (CRRA) to identify potential mitigation strategies to address TTP susceptibilities.

3.8 Threat Matrix for the SAPIENT case of study

				Sapient Server			Radio ch. - Satellite ch.			Airborne Router		
TTP ID	TTP Name	Source Reference	Risk Score	Ext.	Ins.	T. Ins.	Ext.	Ins.	T. Ins.	Ext.	Ins.	T. Ins.
9	Brute Force	CAPEC-112	4,54	4,54								4,54
8	Functionality Bypass	CAPEC-554	4,36	4,36								4,36
4	Flooding	CAPEC-125	3,9	3,9								
10	Exploiting Trust in Client (Man in the Middle, create malicious client, removing important client functionality)	CAPEC-22	3,81				3,81					
15	Malicious Logic Insertion	CAPEC-441	3,72			3,72						3,72
6	Content Spoofing	CAPEC-148	3,54				3,54					3,54
12	Infrastructure Manipulation	CAPEC-161	3,09				3,09			3,09		3,09
14	Local Execution of Code	CAPEC-549	3,09			3,09						3,09
11	Contaminate Resource	CAPEC-548	2,72	2,72		2,72	2,72					2,72
1	Interception	CAPEC-117	2,45				2,45			2,45		
3	Footprinting	CAPEC-169	2,36	2,36						2,36		
2	Excavation	CAPEC-116	2,27	2,27								
13	Audit Log Manipulation	CAPEC-268	2,27	2,27		2,27						
7	Communication Channel Manipulation	CAPEC-216	2,18				2,18					
5	Fault Injection	CAPEC-624	1,9				1,9					
		Aggregate Susceptibility		22,42	0	11,8	19,69	0	0	7,9	0	25,06
					34,22			**19,69**			**32,96**	

For presentation purposes, colors are used to bin TTPs into severity categories based on risk score, as follows:

- TTPs with a risk score in the range [4.0...5.0] pose serious risk and appear in red;
- TTPs with a risk score in the range [2.5...3.9] pose moderate risk and appear in yellow;
- TTPs with a risk score in the range [1.0...2.4] pose minimal risk and appear in blue.

4 Cyber Risk Remediation Analysis (CRRA)

Cyber Risk Remediation Analysis (CRRA) is an approach for selecting countermeasures (CMs) to reduce a cyber asset's susceptibility to attack over a range of Tactics, Techniques, and Procedures (TTPs).
CRRA is performed separately for each cyber asset and consists of the following steps:

1. Select which TTPs to mitigate
2. Identify plausible countermeasures
3. Assess countermeasure merit
4. Identify an optimal CM solution
5. Prepare recommendations

4.1 CRRA: More in deep

The first step is to select a list of TTPs to mitigate. There are several strategies to perform this selection. One strategy is to focus only on the highest scoring TTPs in the Threat Matrix for each cyber asset.
CRRA employs a mapping table to represent the many-to-many mapping between TTPs and countermeasures (CMs). This mapping is used to identify candidate CMs for a given set of TTPs.
Each CM to TTP mapping is characterized by the mitigation value.
A 2-character notation is used to represent mitigation effectiveness within the mapping table, where the first character signifies the type of mitigation from the list: (N)eutralize, (D)etect, (L)imit and (R)ecover. The second character represents the degree of effectiveness from the list: (L)ow, (M)edium, (H)igh, and (V)ery high.
The objective of CRRA is to identify an optimal list of CMs for a specified range of TTPs. To identify an optimal list of CMs, it is first necessary to assess the relative merit of each CM.
The approach calculates a utility/cost (U/C) ratio for each CM and uses these U/C ratios to rank CMs based on their relative merit.
To assess the utility of each CM, a score is assigned to each mitigation effectiveness:

Ordinal Value	Mitigation Effectiveness Scoring			
	Detect	**Neutralize**	**Limit**	**Recover**
Very High	DV=7	NV=11	LV=9	RV=7
High	DH=5	NH=9	LH=7	RH=5
Medium	DM=3	NM=7	LM=5	RM=3
Low	DL=1	NL=5	LL=3	RL=1

Figure 5: Mitigation Effectiveness Scoring

The utility of each CM can now be calculated by summing the scores over the range of TTPs mitigated. The second factor in calculating the U/C ratio is CM cost.
The cost of a CM should consider the cost to develop, integrate, and maintain the CM over the operational life of the system. Whatever model is used to assess cost, its valuation should map to a linear scale of [1...5] in order to be used to calculate U/C ratios.
A CM Ranking Table can facilitate the calculation of U/C ratios over the range of CMs identified in a TTP/CM mapping table.
The table is constructed by inverting the contents of the TTP/CM mapping table and adding some columns to tabulate the CM merit scoring.
U/C ratios are calculated for each CM once utility and cost values have been assigned. The last step to construct this table is to order the rows by decreasing U/C ratio.
An optimal CM solution is the set of CMs that provides effective mitigation over a specified range of TTPs at the lowest cost.
What constitutes "effective mitigation" is determined by a CM selection strategy.
A CM selection strategy establishes a basis for filtering the range of potential solutions, i.e., the solution space, which can grow exponentially with the number of CMs.
For example, a CM selection strategy could require that the following conditions hold in order to qualify as a viable solution:

1. At least one highly effective CM must be selected for each TTP (it is the one that has been choosen).

2. Less effective CMs may be combined to satisfy #1.

3. A Detect CM is required for TTPs that have no Neutralize CMs.

Identification of an optimal CM solution can be performed manually by walking the CM Ranking table.
The final CRRA step is to translate the CM solution list into well-formed recommendations.

4.2 Applying CRRA for the SAPIENT case of study

4.2.1 SAPIENT Server

- **TTPs to mitigate**

We focused on the first four top ranked TTPs in the Threat Matrix for the SAPIENT server. The following table lists the TTPs from the Threat Matrix:

Sapient Server	TTP Description
Brute Force	CAPEC-112
Functionality Bypass	CAPEC-554
Flooding	CAPEC-125
Malicious Logic Insertion	CAPEC-441

- **Candidate Countermeasures (CMs)**

CM Id	CM Name
C001	Use Strong Password
C002	Lock out accounts after a defined number of incorrect password attempts
C003	Use Captchas
C004	Use a network Intrusion Detection System (IDS) and an Intrusion Protection Systems (IPS)
C005	Use strong authentication
C006	Block all unnecessary ports at the firewall
C007	Use well configured ACLs
C008	Use resource and bandwidth throttling technique
C009	Stay current with the latest operating system service packs and software patches

- **TTP/CM Mapping Table**

CM Id	Mitigation effectiveness (by Capec Id)				
	112	554	125	441	
C001	LV	LH			
C002	NV	NV			
C003	NV	LV			
C004		NH	LV	LV	
C005	LV	LV		LV	
C006		LV	LV		
C007		NM	LV	DM	
C008		LL	LV	RL	
C009		LL	LM	DH	
C010					

- **CM Ranking Table**

	Neutralize			Limit				Detect		Recover	CM Merit Scoring		
CM ID	NV = 11	NH = 9	NM = 7	LV = 9	LH = 7	LM = 5	LL =3	DH = 5	DM = 3	RL = 1	Utility	Cost	U/C ratio
C003	112			554							20	1	20
C006				554 - 125							18	1	18
C001				112	554						16	1	16
C004		554		125 - 441							27	2	13,5
C005				112 - 554 - 441							27	2	13,5
C009						125	554	441			13	1	13
C007			554	125					441		19	2	9,5
C008				125			554			441	13	2	6,5
C002	112 - 554										22	4	5,5

- **Identify an Optimal CM solution set**

Solution	List of Countermeasures	Cost
1	C003, C002, C001, C005, C004, C007, C008	**14**
2	C003, C001, C005, C006, C004	**7**
3	C003, C002, C008, C007, C006, C004, C005, C009	**15**

Solution 2 identifies a list of CMs that mitigate the list of TTPs with the lowest overall cost over the range of solutions evaluated.

- **Tara Recommendations**

1. **Use strong authentication mechanism**: This countermeasure is high effective at limiting *functionaly bypass attacks*, *malicious logic insertion (malicious software insertion)* and *brute force attacks* too.

2. **Use strong passwords**: This is another common countermeasure which results very effective at limiting *brute force attacks*.

3. **Use captchas**: This countermeasure is very high effective at neutralizing *brute force attacks* to which the Sapient Servers (and Sapient DB) may be subject to.

4. **Use a network Intrusion Detection System (IDS) and an Intrusion Protection Systems (IPS)**: This countermeasure is high effective at limiting *functionaly bypass attacks*, *flooding attacks* and *malicious logic insertion (again malicious software insertion) attacks* too.

5. **Block all unnecessary ports at the firewall**: This countermeasure is high effective at limiting *functionaly bypass attacks* and *flooding attacks* too.

4.2.2 Radio channel - Satellite channel

- **TTPs to mitigate**

Here we focused on the first two top ranked TTPs in the Threat Matrix for the Radio Channel – Satellite Channel.
The following table lists the TTPs from the Threat Matrix**:**

Radio Channel – Satellite Channel	TTP Description
Exploiting trust in Client (Man in the Middle)	CAPEC-22
Content Spoofing	CAPEC-148

- **Candidate Countermeasures (CMs)**

CM Id	CM Name
C001	Use criptography
C002	Use Hashed Message Authentication Codes (HMACs)

- **TTP/CM Mapping Table**

CM Id	Mitigation effectiveness (by Capec Id)		
	22	148	
C001	**NH**	**NV**	
C002	**NH**	**NV**	

- **CM Ranking Table**

		Neutralize	CM Merit Scoring		
CM ID	NV = 11	NH = 9	Utility	Cost	U/C ratio
C001	148	22	20	3	6,67
C002	148	22	20	3	6,67

- **Identify an Optimal CM solution set**

Solution	List of Countermeasures	Cost
1	C001	3
2	C002	3

Either solution 1 or solution 2 can be used in this case.

- **Tara Recommendations**

- **Use criptography**: This countermeasure is high effective at neutralizing *Man in the Middle* and *Content Spoofing attack*. If data are encrypted before being transmitted to the involved ground station or to the RBS , that is after leaving the ATN/IPS network, the attacker can still intercept them but cannot read it or alter it. If the attacker blindly modifies the encrypted message, then the original recipient is unable to successfully decrypt it and, as a result, knows that it has been tampered with.

- **Use Hashed Message Authentication Codes (HMACs)**: This countermeasure is also high effective at neutralizing *Man in the Middle* and *Content Spoofing attack*. If an attacker alters the message, the recalculation of the HMAC at the recipient fails and the data can be rejected as invalid.

4.2.3 Airborne Router

- **TTPs to mitigate**

Here we focused on the first four top ranked TTPs in the Threat Matrix for the Airborne router.
The following table lists the TTPs from the Threat Matrix:

Sapient Server	TTP Description
Brute Force	CAPEC-112
Functionality Bypass	CAPEC-554
Malicious Logic Insertion	CAPEC-441
Content Spoofing	CAPEC-148

- **Candidate Countermeasures (CMs)**

CM Id	CM Name
C001	Avoid default password and use strong ones
C002	Deny access after a defined number of incorrect password attempts
C003	Well configure the firewall
C004	Update firmware regularly
C005	Use strong data encryption (WPA2)
C006	Well configured the Intrusion Protection Systems (IPS)

- **TTP/CM Mapping Table**

CM Id	Mitigation effectiveness (by Capec Id)				
	112	554	441	148	
C001	**LH**	**LH**	**LH**		
C002	**NV**	**NV**	**NV**		
C003		**LV**	**LV**		
C004		**LH**			
C005				**NV**	
C006	**DV,NH**	**LV**	**DH,LV**		

- **CM Ranking Table**

	Neutralize		Limit		Detect		CM Merit Scoring		
CM ID	NV = 11	NH = 9	LV = 9	LH = 7	DV = 7	DH = 5	Utility	Cost	U/C ratio
C002	112 -554 - 441						33	1	33
C001				112 -554 -441			21	1	21
C003			554 -441				18	2	16
C006	112		554		112	441	32	2	16
C004				554			7	1	7
C005	148						11	3	3,66667

- **Identify an Optimal CM solution set**

Solution	List of Countermeasures	Cost
1	C005,C006,C001,C003	**8**
2	C001,C002,C006,C005	**7**
3	C006,C003,C002,C005	**8**

Solution 2 identifies a list of CMs that mitigate the list of TTPs with the lowest overall cost over the range of solutions evaluated**.**

- **Tara Recommendations**

- **Avoid default password. Use strong ones**: This countermeasure is high effective at limiting *Brute Force attacks* for password cracking. Using default login (username/password combination), gives the attacker a head start.

- **Deny access after a defined number of incorrect password attempts**: This countermeasure is high effective at neutralizing *Brute Force* attacks too. Apply lockout policies limit the number of retry attempts that can be used to guess the password.

- **Use strong data encryption**: This countermeasure is high effective at neutralizing *Content Spoofing attacks*. A data encryption protocol as WPA2 allows to encrypt data as it travels in and out of the airborne, making it much more difficult to be read or altered by an attacker. If data are encrypted when leaving the airborne router and the same happens when data leave the ATN/IPS network, for the assumption of secure ATN/IPS network, the whole systems will result secure.

- **Well configured the Intrusion Protection Systems (IPS)**: This countermeasure is high effective at detecting and limiting *Functionality Bypass and Malicious Logic Insertion attacks.*