Security Analysis of Remote Tower Control

By:
Joseph Brian Musanje Kasozi
Male Henry Kenneth

Date: April 2015

1. TARGET OF EVALUATION

The main target of the analysis is the Remote Tower control center.This will provide Air traffic control services for more than one airport by a single operator in a remote location therefore eliminating an individual control tower located on the individual airport premises. The Remote tower is expected to offer a full range of air traffic services such that the airspace users are not negatively impacted compared to the traditional local control tower. Furthermore the analysis focuses on the Identity & access management, web application & database, networking and infrastructure.

In order to analyse the threats and risks of the remote tower control center,the following assumptions were considered.

- All the already existing features ,services and systems etc are secured
- All the new features, services and systems need to be secured
- There is also some channel of communication between the Remote tower and the airport
- The new features are compatible with the current airport system

2. SUMMARY OF FINDINGS

In identity and access management, some of the main identified assets included, domain naming service, directory service, information server and out of the window system. these assets can be affected by the unauthorised access to data by employees and denial of service attack launched by an attacker or malicious employee. The proposed controls to these threats include installation of intrusion detection systems and segregation of duties

For web application and database security,system identification information, encryption and decryption service and the network configurations were considered to be the main assets.these assets face cross-site scripting and SQL injections as some of the main threats.These threats could be mitigated or eliminated by integration of the database server into the security gateway and eliminating flaws

Routers and switches ,remote tower control communication and operating systems were the main assets identified in the networking and infrastructure. All these assets are faced by a risk ,loss and destruction of infrastructure which can be brought about by malicious employees or hackers

manipulating management parameters, however these threats can be controlled by installation of firewalls, setting up security policies and installation of electronic access control systems.

3. DESCRIPTION OF METHOD APPLICATIONS TO ANALYSE THE REMOTE TOWER CONTROL CENTER

In this section we detail all the assumptions, findings and application for the three main security phenomenons ,That is Identity and access management,web application and database ,networking and infrastructure security, Further in this section we identified the different ways in which the assets will be protected. In Security management, following the lecture slide " Information Security Management by professor Fabio Massacci, there is a list of question to be answered to ensure that security is upheld. these include[4]

- Which assets do we need to protect?
- How do we decide what to do?
- What can we do to counter those threats?

In quest to answering these questions in the case study of the Remote tower center, we used mainly two methods, SCREAM and CORAS to give answer to the question in the all aspects of the study

3.1 Identity and Access Management

3.1.1 Summary of assumptions and finding

Identity and access management for the RTC is a very important section in the security of the whole center.Therefore we identified a number of key point including primary assets, supporting assets, threats and treatments which were based on the impact of the risk to the RTC assuming that the security of the RTC will have an impact on the already existing features ,processes and services at the airports. Some of the main identified assets included, domain naming service, directory service, information server and out of the window system. we assumed that the RTC has got many parties to interact with it which include the users and the systems. For proper access and management, the above mentioned assets have to be protected to eliminate intruders and unauthorised access.Some of the threats that might harm the mentioned assets include unauthorized access to information which might result from social engineering or misuse of client application.The proposed controls to these threats include installation of intrusion

detection systems since this is extremely effective in preventing and detecting unauthorised access to vital assets.Segregation of duties whose primary role is differentiate employees duties. hence limiting employees from doing what is not meant for them.This evaluation was conducted in two sections; identity management was conducted with SecRAM. while CORAS was with access management. All the main results of the analysis were obtained from the documents provided for the case study and these include; the remote tower case study, SESAR ATM Security risk Assessment Method, EATM Pre-event threat controls,EATM Post-event threat controls and EATM threat catalogue

3.1.2 Process used to analyze Authentication Requirements

At Step 1 we identified the primary assets and assessed their impact on the Remote Tower Centre(RTC) (see table 1.1 and 1.2 in the document "D1-G15-SecRAM_artifact.xlsx". The main primary assets identified where based on the "The Remote Tower case Study "document which entails how the RTC concept will work . For Example we identified the primary asset, Directory service which is responsible for storing and providing all user information for accessing the RTC domain. The Domain name server which is responsible for locating and identifying systems and services over a network. An identity provider, a service responsible for providing unique identities to users and systems who will interact with RTC system

At Step 2 we identified the supporting assets of the primary assets identified at step 1 which are detailed in the table 2 in the document "D1-G15-SecRAM_artifact.xlsx". For example we identified the supporting assets as server computers and storage devices. Based on the overall impact most of the assets have an impact greater than four(4), this shows that most of the identified assets need to be secured if the RTC identity management and authentication is to be managed and secured as justified in the same document in column K (justification)

At step 3 we identified threats to our supporting assets from Step 2 see table 3 "D1-G15-SecRAM_artifact.xlsx". The main threats identified are Unauthorised access to data, denial of service attacker and corruption application data For instance, the supporting asset server computers may be affected by corruption of application data . All the Weights where assigned to the threats depending on the level at which it harms the primary assets thereby

assigning them the overall impact of the primary assets on the CIA triad.This conclusion was based on the information from the document "EATM THREAT CATALOGUE Vo.10"

At Step 4 we evaluated the impact and risk level of the threats identified at Step 3 (see table 4.1 and 4.2 in the document "D1-G15-SecRAM_artifact.xlsx"). The main threats that should be mitigated are the following threats Unauthorised access to data, denial of service attacks, hacking, data interception and corruption application data .

At Step 5, we proposed the security controls that are reported in the worksheet "step 5 risk treatment" in document "D1-G15-SecRAM_artifact.xlsx". We selected these security controls based on the documents EATM Pre-event threat controls and EATM Post-event threat controls and others based on our own experiences. For example to control the threat of hacking that would affect the server computer on which most of the information will be stored we proposed a pre-control measure, Penetration Testing. This will mitigate the impact of hacking as well controlling it from happening. This would keep the information on the servers safe by controlling the Denial of Service Attack. But since the servers are really very important to the case study then we assumed that what if the hacker again finds a way of going behind the server and entering the RTC domain. Here we proposed some post-controls that would mitigate the harm the Denial of service attack which is Reconfigurable Data Messaging Systems

3.1.3 Process used to find Access Control Requirements

We have used the CORAS method to analyse the access control requirements. This method is made up of eight(8) steps. Step one was not performed by this group but from the document % the remote tower case study% we were able to extract information about the customer thus performing step 2 and 3 as detailed in the next sections.

Step 2. In this step we studied the documents provided to deeply understand the case study and the risk analysis to be performed. We further detailed the target and objectives of the the analysis as in the document "D1-G15-CORAS-artifact.ppt" on slide six (6).

- TARGET : The main focus and target of the analysis is the Remote Tower control(All the systems)
- The analysis is also focusing at protecting both the direct and indirect assets involved with the RTC
- To protect and enhance on the airport transport navigation
- To analyse the Access Management of the RTC

Step 3 the results are a list of assets detailed in the asset diagram on slide 8 of the "D1-G15-CORAS-artifact.ppt" . We defined these assets from the document "Remote Tower case Study".More results giving a high level risk analysis are reported in the table on slide 9

The results of Step 4 are the likelihood and consequence scales for each asset, target definition and risk evaluation matrix, which is reported on slides 11-20 in document "D1-G15-CORAS-artifact.ppt. We identified the following list of assets for further risk assessment, OTW system, airport communication, information server, signal and sensor system and alarm system. For example, in the risk assessment, the asset "information server" was identified because it manages all the information about the users, services and the entire remote air traffic control system.

In Step 5 and 6 we identified the main threats for the assets from Step 4. The corresponding threat diagrams reported on slides 23-24 in document "D1-G15-CORAS-artifact.ppt". We identified these threats based on the EATM threat catalogue document and the remote Tower case study document. For example on slide 21 we assume that threat "hacker" can lead to the unwanted incident "leaking of confidential information" by spoofing and exploring the vulnerability of no intrusion detectors in the remote tower center scenario. Other vulnerability that can be exploited by the hacker include weak regulation policies, that can enable a hacker to perform a threat scenario of social engineering and hence leaking confidential information again.

At Step 7 we evaluate the risk based on the matrices proposed at Step 4 (see matrices and risk diagrams on slides 30-34 in document "D1-G15-CORAS-artifact.ppt"). Based on the results of this step we can conclude that the main risks that need to be treated are leakage of information, loss of infrastructure and system breakdown.

At Step 8, to mitigate the major risks we proposed some security controls that are reported in diagrams on slide 38-41 in document "D1-G15-CORAS-artifact.ppt". We selected these security controls based on EATM Pre-event threat controls and EATM Post-event threat controls. For example, in the diagram on slide 38, to mitigate the risk "capturing wrong information" we proposed the treatment performing a data input credibility check. This would reduce the risk

level from unacceptable to monitor. The complete summary of results can be found in the document "D4-G15-summary_of_results.xlsx" submitted as integral part of the current report.

3.2 Web Application and Database Security

3.2.1 Summary of assumptions and finding (1/2 pages)

When analysing security of a web application and database the following two question were put in mind. and throughout the evaluation we provided answers as proposed in the lecture slides[2]

- "What if the "it" on the other side is not who s/he claims to be?"
- " What if the "it" on the other side does not send the right data?"

How will the application authenticate the user who accesses it or how will the application validate the data that it receives. Assuming that the application is to be developed, we proposed a number of solutions depending on the possible threats that might harm the performance of the application .

The web application manages different sorts of information but all these are supported by "supporting assets". For example we identified protocol information , system identification information ,domain naming service and application source code among others as the main primary assets but these are also supported by assets like database, web server, client application, web browser, network devices and third party softwares like operating systems[3]. .

All these assets are faced by threats which pose a risk on each of them damaging the availability integrity and confidentiality of the given asset. These threats include web spoofing, systematic trying-out of passwords, malicious software, SQL injection among others as documented in the %Web Application secram-G15.xls ,sheet step 3. Threats%. The evaluation showed that all the threats need to be treated because they all have an impact on the application which is not allowed or unacceptable. The possible solutions proposed include protection against active content, separation of data networks, secure connection of background systems to web applications (using SSL/TLS).

3.2.2 Process used to analyze Application Security Requirements

At Step 1 we identified the primary assets and assessed their impact on the operation of web application and database. (see sheet step 1.1 Primary Assets and 1.2 in the document

"D2-G15-SecRAM-artifact.xlsx"). We identified up to nine main assets and they all have a high impact on the web application performance these include user identification information, system identification information, protocol information, session information among other as in the document mentioned above.

At Step 2 we identified supporting assets for the list of primary assets from Step 1 as in the document "D2-G15-SecRAM-artifact.xlsx". For example, the primary asset user identification information we identified a number of supporting assets which include web browsers, database, third party softwares. We based on the Remote tower case study document and our own experience with web applications.

At Step 3 we identified threats to the supporting assets from Step 2 (see step.3 Threats in the document "D2-G15-SecRAM-artifact.xlsx"). For example, the main threats to the supporting asset application server has the following threats; denial of services, malicious software, DNS spoofing, errors in configuration and operation and use of insecure protocols in public networks. This is because we assumed that supporting asset "application server" is to host the entire application hence being the major threat target. On addition we assumed that for now the security is not strong enough to stop the different threats like DNS spoofing and error in configurations. We based the results on the "IT-Grundschutz-Catalogues", "EATM threat catalogue" and also on our own experience.

At Step 4 we evaluated the impact and risk level of the threats identified at Step 3 (see Sheet 4.1 Impact evaluation in the document "D2-G15-SecRAM-artifact.xlsx"). We identified mainly twenty one threats and concluded that they all need to be mitigated because they have a high risk level and impact on the application and RTC at large.

At Step 5 we proposed a set of security controls to mitigate all the threats identified at Steps 3-4 (see Sheet 5 Risk Treatment in the document "D2-G15-SecRAM-artifact.xlsx"). We selected these security controls based on the documents "IT-Grundschutz-Catalogues","EATM Pre-Event Threat Controls","EATM Post-Event Threat Controls", and our own experience. For example, to mitigate the threat DNS Spoofing, we proposed to implement secure communication with a centralised logging server (Use of TLS/SSL) as a security pre control because it can reduce the risk down to monitor level according to the document "IT-Grundschutz-Catalogues".and also we

proposed a post event control training the security administrators. This can lower the risk just incase the threat was able to go past the pre control. The complete summary of results can be found in the document "D4-G15-summary_of_results.xlsx" submitted as integral part of the report.

3.3 Network and Infrastructural Security

3.3.1 Summary of assumptions and finding

In the analysis of the networking and infrastructure security we presumed to answer two questions ie.

• Which visible assets do we need to protect?

• What are the imposing threats and what can we do to counter them?

We identified the important assets which included switches and routers, IT cabling , server rooms, Mobile devices, operating systems, out of the window system. All of these assets are prior to threats that is to say, malicious employee, hackers, sloopy employee , thieves and many more which can impose risks which include access to confidential information,manipulation of management of parameters,denial of service ,system malfunction.

The complete summary of results can be found in the document "D4-G15-Summary_ of _results.xlsx" submitted as integral part of the current report**.**

3.3.2 Process used to analyze Network and Infrastructural Security Requirements

We have used the CORAS method to analyze the networking and infrastructure Security. The result of step one and two is the target of the analysis as shown in slide 6 of the "D3-G15-CORAS-artifact.pptx" document.

Step 3, the results of this step is a list of assets detailed in the asset diagram on slide 8 of the document "D3-G15-CORAS-artifact.pptx". We defined these assets from the documents "The Remote Tower case Study" and "IT-Grundschutz-Catalogues". More results are shown on slide 9 giving a high level risk analysis as reported in the table.

The results of Step 4 are asset table, likelihood and consequence scales for each asset, target definition and risk evaluation matrix, which reported at slides 11-26 in document

"D3-G15-CORAS-artifact.pptx". We identified the following list of assets for further risk assessment; switches and routers, remote tower control communication, OTW system, and operating systems. For example the asset "routers and switches" was identified because these are the intermediate devices in the network. They are needed to have a stable connection on the RTC.

At Step 5 and 6 we identified main threats for the assets from Step 4. The corresponding threat diagrams reported at slides 29-34 in document "D3-G15-CORAS-artifact.pptx". We identified these threats based on the document "EATM threat catalogue" ,"IT-Grundschutz-Catalogues" and the Remote Tower case study document. For example, as a result of poor monitoring and surveillance policy, this would lead to theft of both physical assets and information.This threat scenarios results into risks such as loss and destruction of infrastructure.

At Step 7 we evaluate the risk based on the matrices proposed at Step 4 (see matrices, risk diagrams and table on slide 36-44 in document " D3-G15-CORAS-artifact.pptx" . Based on the results of this step we can conclude that the main risks need to be treated are loss and destruction of infrastructure, denial of service attack, disabling the server while in operation, Access to confidential information and manipulation of management parameters.

At Step 8 to mitigate the major risks we proposed the security controls that are reported in diagrams on slides 48-51 in document % D3-G15-CORAS-artifact.pptx". We selected these security controls based on the documents "EATM Pre-event threat" ,"EATM Post-event threat controls" and "IT-Grundschutz-Catalogues". For example, in the diagram on slide 48, to mitigate the risk of line taping, we proposed a treatment to install well configured firewall and more others details in "D4-G15_summary_of_results" document because they can reduce the risk down to an acceptable or monitor level according to the "EATM Pre-event threat" , "EATM Post-event threat controls" and "IT-Grundschutz-Catalogues"

ANNEX

An integral part of the report we attach the following documents:

1. Summary of Results (see file "D4-G15-summary_of_results.xlsx").
2. [for CORAS D1] Powerpoint slides reporting the application of CORAS method on Identity management (see file "D1-G15-CORAS-artifact.ppt").
3. [for CORAS D3] Powerpoint slides reporting the application of CORAS method on Networking and infrastructure (see file "D3-G15-CORAS-artifact.ppt")
4. [for SecRAM] Excel document reporting the application of SecRAM method on Access management (see file "D1-G15-SecRAM_artifact.xlsx").
5. [for SecRAM] Excel document reporting the application of SecRAM method on Web application and Database (see file "D2-G15-SecRAM_artifact.xlsx").

REFERENCES

[1] Security management, Accessed on 13/11/2014 Availabel at https://en.wikipedia.org/wiki/Security_Management.

[2] Fabio Massacci lectureWebApplicationSecurity II ,Security Engineering,University of Trento , Available at https://securitylab.disi.unitn.it/lib/exe/fetch.php?media=teaching:seceng:2014:lecture-2014-15-webapplicationsecurity.pdf

[3] Fabio Massacci lectur Infrastructural Security - Introduction toOS Security ,Security Engineering,University of Trento , Available at https://securitylab.disi.unitn.it/lib/exe/fetch.php?media=teaching:seceng:2014:lecture-2014-17-os-vm-security.pdf

[4] IT-Grundschutz-Catalogues 13th version 2013, accessed on 4th/02/2014 at https://gsb.download.bva.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf

This work has been done by the undersigned students and has not been copied or otherwise derived from the work of others not explicitly cited and quoted.

Signature of Joseph Brian Musanje kasozi *Signature of Henry Kenneth Male*