WB-Analysis of the attack on the Nakula and Antareja machines in January 2002

RVS-RR-05-02

Lars Molske <lars.molske@uni-bielefeld.de>
Damian Nowak <damian.nowak@uni-bielefeld.de>
Peter B. Ladkin <ladkin@rvs.uni-bielefeld.de>

June 30, 2005

Contents

Chapter 1

Introduction

1.1 About this paper

This document presents a causal analysis of a security-related incident at the *Networks and Distributed Systems Group* (AG RVS)[1] in January 2002. Its goal is to reveal what happened during a series of partly remote attacks on two machines hosted in the RVS at the University of Bielefeld. We used the WBA Method developed by Peter B. Ladkin and the RVS Group. WB-Analysis is a formal a posteriori failure analysis technique, based on formal semantics and logic. Using WBA, we analyzed and explained the history of this accident. For a brief description we added a part from the abstract of the paper [1], which contains the forensic analysis of the incident performed by I Made Wiranya and Avinanta Tarigan. We performed our analysis based on this report.

[1] German: Arbeitsgruppe Rechnernetze und Verteilte Systeme (AG RVS)

1.2 Abstract taken from the source document

> ”On 18th January 2002, we received a security alert. There is a mass attack launched from Nakula machine. The intruder has gained the root privilege in Nakula machine. He wants to grab the credit card number, sniff and launch the other mass-scan and attack. After collecting password for Antareja machine, he accessed Antareja an tried to do a local exploit. However he was not been successful to get the root privilege.”

1.3 Brief overview of the events

In this section we will present a short overview over the events happened in January 2002. We will provide this information to summarize the detailed report so that the reader of this document get an idea of what happened without wade through the full report.

1.3.1 18th January 2002

User *koko*, an Indonesian student, was remotely logged in on Nakula. He worked via the internet from Jakarta. He noticed user *made* was logged in and also user *root*. So he thought *made* was performing administrative tasks. He tried to contact *made* via chat and instant messenger, but got no response. After several tries without a reaction of *made*, user *koko* informed the RVS administrative staff.

1.3.2 18th January 2002, 22:56

made remotely logged in on Nakula using ARCOR[2] services. He found several anomalies regarding the system’s behavior. The secure shell daemon (sshd) was unable to deliver service outside the RVS network, the sendmail was getting down frequently and the network connection was very slow. After his first view *made* informed *avinanta*.

[2] German ISP, www.arcor.de

1.3.3 18th January 2002, 23:05

avinanta logged in on Nakula and Antareja in order to find the source of the abnormal behavior. He found several files in hidden directories belonging to exploit programs and rootkits. At this point, they were sure that the systems were cracked by an intruder.

1.3.4 19th January 2002, 00:40

Some research showed that nearly all log files in /var/log were deleted. At this point, the decision was taken to shut down both machines to prevent further loss of evidence.

1.3.5 19th January 2002, 00:50

A mail from the administrator of the technical faculty reached the RVS about mass scanning on hosts in the technical faculty from hosts within the RVS.

1.4 Presentation of the affected systems

In this short system presentation we will mention only those pieces of installed software which were important for the analysis.

1.4.1 Profile of the Nakula machine

Nakula was and still is a webpublishing platform, hosting the most popular web site about information technology known in Indonesia. Most of the papers were written in Indonesian language. This could have made Nakula a nice target system for Indonesian hacker groups. The system had about ten active users, mainly students from Jakarta. All of them were personally known by *made* and *avinanta*. Additionally Nakula offered mail and database services.

- Operating system: SuSE Linux 7.2, Kernel 2.4.4
- Apache 1.3.12
- PHP 4.2.06
- sendmail with SMTP, POP3 and IMAP
- OpenSSH
- ProFTP
- MySQL

1.4.2 Profile of the Antareja machine

Antareja was a experimental system used to test video conferencing between Bielefeld and Jakarta. Therefore, some video conferencing tools and measurement tools were installed in addition to the base system which provides also services for mail and webpublishing. Antareja was installed in December 2001, so only active for a few months. There were only a few active users and the machine was not well known amongst the public.

- Operating system: SuSE Linux 7.3, Kernel 2.4.10
- Apache 1.3.12
- PHP 4.2.06
- sendmail with SMTP, POP3 and IMAP
- OpenSSH
- ProFTP
- PostgreSQL

1.4.3 Network infrastructure

Both machines were connected directly to the internet via a switch provided by the HRZ[3]. No special security measurements such as a central perimeter firewall or an intrusion detecting system were provided, but the HRZ offered a guarantee that no sniffing in the University's switched network will be possible.

[3] Hochschulrechenzentrum, http://www.uni-bielefeld.de/hrz,
Central computing service department of the University of Bielefeld

1.5 Information about the forensic report

Altogether, the forensics team had to spent a total of about one man month on the investigation - including their report and the fixing of the caused damage.

1.5.1 Problems concerning the forensics

When the intruder noticed that he might have been detected, he deleted log files and tried to cover his operations as well as he could. Due to that, it was difficult for the analysts to examine the systems and reveal what happened.

Their goal was to find out how the intruder gained access to the systems, how he got root rights on Nakula, who he was and what he aimed for. So they used several tools for recovering deleted files and got at least partial recovered log files containing important information.

Based on this information, the analysts simulated different attack scenarios and came to the conviction that only the following attack scenario was possible due to technical requisites, such as lack of proper remote exploits at this time.

1.5.2 One possible attack scenario

The analysts came to the conviction that only this scenario would be possible:

- Intruder had access to university's network
- He was able to use techniques that forced the switch to forwarding all traffic to his machine (ARP spoofing and sniffing)
- He found login/password combination for Nakula machine in unencrypted FTP traffic
- He used this information to login on Nakula

Reaching his first goal, he must have went on employing Nakula

- He must have used an local exploit to gain root access (e.g. suid exploit) due to the fact that no proper remote exploit for SuSE 7.2 existed at that time

- He installed a root kit
- He launched a sniffer attack on the network
- He was able to gain login/password combination for ANTAREJA machine

At this point he must have reached all he wanted on NAKULA till then and switched over to ANTAREJA using the gained and valid login data.

- He tried to use the same exploits he also used on NAKULA, but was not successful due to the usage of SuSE 7.3 on ANTAREJA.
- He was not successful to gain root access on ANTAREJA, although he tried until he was discovered.

1.5.3 Conclusions drawn from the forensic report

After the complete forensic analysis the two analysts came to the following conclusions:

- Probable motivation of the intruder:
  - Use machines as launching pads for further attacks
  - Gain root access to as many hosts as possible
  - Sniff credit card numbers
  - Prepare distributed denial-of-service attacks
- Probable intruders identity:
  - Romanian hacker tazmania using his own root kit
- Switched networks do not always guarantee sniffing protection

According to this, they suggested several improvements concerning the University's network and computational services:

- University level intrusion detection system
- Better log-mechanisms, e.g. usage of an external log-server
- A reliable mechanism to notify system administrators
- Development of proper security policies

Chapter 2

The WB-Analysis

2.1 About WBA

When a particular unwanted behavior of a system has happened, it is advisable to analyze it and see what exactly went wrong and caused the chain of events to happen as it did, and not the way it was intended to. This way one may be able to prevent a similar incident in the future.

The here used Why-Because Analysis developed by Peter B. Ladkin and the RVS Group is a formal, rigorous reasoning method to develop relatively sufficient and sound causal explanations for any incident. The underlying technique is based on formal semantics and logic to ensure the accurate and objective results. Furthermore it supplies methods to even prove the correctness of these explanations. The response to an incident should be based on correct reasoning as it is provided by WBA, otherwise one might not be successful in the goal of preventing future recurrences of a similar and unwanted sequence of events.

To get an overview what really happened, one first creates a list of facts. In a list of facts, all the facts found in the source report(s) are extracted to catchwords non-valuated and combined in a new document. During this process, it's important to keep your goal in mind. Not every fact happened during the eyed time span might be important or even causally relevant for the regarded scenario. Of course, you should always allow revision on this initial judgement in the further process. Especially if you notice that you are stuck and that facts are missing.

The proper application of the WB-Analysis results in a WB-Graph, which visualizes the failure scenario. This Graph is a "complete statement of the causal relations between all events and system states of significance for casually explaining the failure scenario."[2] The WB-Graph is constructed by applying the Counterfactual Test pairwise to the facts stated in list of facts. Given two actually happened events, states or processes, A and B, the Counterfactual Test asks the question if B would not have happened if A had not. If the answer is yes the test is successfully passed and an edge between the two nodes is drawn. B is then counterfactual dependent on A. If it fails, no edge is drawn. Further details on the WBA-method, its underlying formal details and information about the formal foundations may be found in "Causal System Analysis"[3].

2.2 What makes this analysis different

Most of the WB-Analyses conducted have been analyses of safety-related cases like transportation accidents in commercial aviation or railway systems. They were dealing with accidents (unwanted events) of rather open, heterogenous and complex systems - the domain for which WBA was originally developed.

In this case, we have two big differences compared to the analyses to date: The first one is, that we are dealing with a security-related case. The second one is, that we have a high degree of human interaction, which was absolutely necessary for the incident to happen as it did. The affected IT-systems were functioning as they were designed to, but their behavior leading to the accident was precipitated by someone on purpose. Many events and states of the system were the results of human decisions and by that reason hard to prove by the Counterfactual Test.

And this leads to other complications with this case: The intruder's motivation plays a major role as necessary causal factor for many events. Such a problem might be solved by modeling the intruders as a rule based human agent - but in this case that's nearly impossible due to the fact that he was just not following rules. With his goal in mind, he adapted his procedures and did what ever he could and had to to find a way to his goal, avoid detection and bypass security precautions.

In addition to that, there were quite a few facts which were not clearly observable (like the attackers motivation) or simply deleted (like some log files). So, we had to base them on conclusions and plausible, coherent assumptions, partly given by the forensics team, partly drawn by ourselves.

2.3 Defining the accident

In many safety-related cases, you might not have a hard time defining what the event regarded as accident might be. If a plane crashes into the ground, the "accident" is quite obvious. But in our case, we came up with a couple of plausible alternatives. As the starting point of any analysis, this is a very important question.

So, what should we regard as the accident, what should we use as root-point? The intrusion itself? Or better the cost of money? Other possibilities would be the loss of system-resources or the loss of manpower. We settled for the fact that the intruder caused a loss of RVS resources in general though he could not reach his (assumed) aim to sniff credit card numbers. Nevertheless he caused damage by flooding the switch, by causing downtime of the systems and by causing additional expenditure (examination and recovery of the systems).

As you can see in section 2.4.2, this uncertainty and abstract definition of the accident will lead to several WB-Graphs.

2.4 Results of the WBA

In the following chapter, we will present our working results, namely the list of facts and the different WB-Graphs.

2.4.1 List of facts

Due to the many obscurities regarding the exact course of action leading to the accident, we could finalize our list of facts only after completing and checking our graphs carefully. Here it is, the final version. For each fact the justification is included.

Legend:

- GF: Given fact in the world
- CC: Causal conclusion
- BF: Based on another fact in the list
- RP: Fact given by the report

List of facts:

1. Loss of resources

    CC:
    2) Attacker used Nakula unauthorized,
    Attacker used Antareja unauthorized
    38) Temporary loss of Antareja machine and services
    42) Specific loss of manpower resources
    44) Temporary loss of Nakula machine and services
    Recall: The the definition of the accident varies slightly between the graphs and according to that this explanation shall be varied.

2. Attacker used Nakula unauthorized

    GF: The intruder was not authorized for usage.
    BF: Usage must be authorized: Fact 5: ”Only trusted users are authorized to use RVS hosts”

BF: Intruder gained the login/password combination illegally by sniffing (Fact 6: "Attacker gained valid login/password combination for NAKULA machine")
BF: Intruder used NAKULA by and after logging in (Fact 3: "Attacker used gained login/password combination for NAKULA machine").

3. Attacker used gained login/password combination for NAKULA machine

   RP: Page 42-45, Logins by user *made* from IP addresses the real user *made* never used.

4. Assumption: Attackers motivation: infiltrate hosts

   RP: Page 54, Conclusion
   RP: Page 3, Intension of the attacker

5. Only trusted users are authorized to use RVS hosts

   GF: Only users authorized and in charge of a valid login may use the RVS systems.

6. Attacker gained valid login/password combination for NAKULA machine

   BF: Fact 7
   BF: Fact 3
   CC: The attacker was able to log in an NAKULA, so he must have gained the login

7. Attacker sniffed network traffic

   RP/CC: The report states out, that this is the only possibility for the intruder to gain the valid login/password combination. It could not have been else.

8. Login/password combination for NAKULA machine transmitted in clear text

BF: Fact 9
GF/CC: Unencrypted FTP traffic entails clear text transmission of the login procedure.

9. Unencrypted FTP connections used

   RP/CC: Page 7/Page 2. The FTP service was offered and it must have been used in order that the attacker could gain the login data.

10. Unencrypted FTP service offered on Nakula

    RP: Page 7, The RVS decided to use ProFTPD to fulfil their need for file transfer.

11. ProFTPD installed and running on Nakula

    RP: Page 7

12. Need for FTP service in the RVS

    GF

13. Switch operates in broadcast mode

    RP: Page 28

14. Switch is configured to switch to broadcast mode when flooded

    CC/BF: The switch operated in broadcast mode (Fact 13), otherwise the sniffing would not have been possible.

15. Attacker flooded switch

    RP: Page 54/Page 3, Sniffing in switched environment only possible through flooding/ARP spoofing.

16. Attacker accessed University Intranet

    CC/BF: The intruder must have accessed the University's Intranet, otherwise he would not have been able to sniff the intranet (Fact 7).

17. Assumption: Attackers motivation: Collect data from network traffic

    RP: Page 54/Page 3, Sniffing in switched environment only possible through flooding/ARP spoofing

18. Attacker able to access University Intranet

    RP: Page 8, there was no other way.

19. Insufficient network security provided by HRZ

    GF: At the time of the incident there was a lack of a perimeter firewall at the University of Bielefeld.

20. HRZ guaranteed protection against sniffer attacks in a switched network environment

    RP: Page 7

21. Attacker used ANTAREJA unauthorized

    GF: The intruder was not authorized for usage.
    BF: Usage must be authorized: Fact 5: "Only trusted users are authorized to use RVS hosts"
    BF: Intruder gained the login/password combination illegally by sniffing (Fact 21: "Attacker gained valid login/password combination for ANTAREJA machine")
    BF: Intruder used NAKULA by and after logging in (Fact 22: "Attacker used gained login/password combination for ANTAREJA machine").

22. Attacker used gained login/password combination for ANTAREJA machine

    RP: Page 45, login from IP ranges the users *made* and *avinanta* never used.

23. Attacker gained valid login/password combination for ANTAREJA machine

    RP: Page 19, Sniffer result

24. Login/password combination for Antareja machine transmitted in clear text

    GF: This is how FTP works
    RP: Result in log on Page 45

25. Attacker sniffed network traffic using Nakula

    RP: Page 45

26. Unencrypted FTP connections used

    RP/CC: Page 7/Page 45. The FTP service was offered and it must have been used, otherwise the sniffer log on page 19 would not contain entries.

27. Unencrypted FTP service offered on Antareja

    RP: Page 7
    BF: Fact 28

28. ProFTPD installed and running on Antareja

    RP: Page 7

29. Attacker installed and launched linsniffer undetected

    RP: Page 15, Existence of "linsniffer"
    RP: Page 19, Sniffer log

30. Assumption: Attackers motivation: collect further data from network traffic

    RP: Page 54, Conclusion
    RP: Page 3, Intension of the attacker

31. Attacker gained root access on Nakula

    RP: Page 11, Mails in root mailbox

32. Attacker installed rootkit on Nakula

    RP: Page 13, Replacement of several files against root kit files detected

33. Assumption: Attackers motivation: Hide operations, avoid detection

    RP: Page 13, Root kit is used to hide the attackers existence

34. Assumption: Attackers motivation: Gain root access on host

    RP: Page 54, Conclusion
    RP: Page 3, Intension of the attacker

35. Local exploit on Nakula

    RP: Page 11, Gain of root privileges only possible through local or remote exploit
    RP: Page 52, No signs for a working remote exploit found on Nakula, but for a local exploit

36. RVS decision: FTP login equals SSH login on Antareja

    GF

37. RVS decision: FTP login equals SSH login on Nakula

    GF

38. RVS decision: Use ProFTP to fulfil need

    GF: This decision was based on the guarantee given by the HRZ

39. Temporary loss of Antareja machine and services

    RP: Page 9, Decision to shutdown Antareja
    CC: Antareja was shutdown, so the services offered by this machine were unavailable for a period of time.

40. Shutdown of Antareja to prevent further loss of evidence

    RP: Page 9

41. Examination of Antareja

    RP: Page 9

42. Detection by RVS: Unauthorized use of Antareja

RP: Page 9

43. RVS decision: Policy: All Incidents must be examined

    GF

44. Specific loss of manpower resources

    RP/CC: Page 9, The examination of the machines required several hours of work.

45. RVS Decision: Reinstallation of Nakula

    GF according to one of the investigators

46. Temporary loss of Nakula machine and services

    RP: Page 9, Decision to shutdown Nakula
    CC: Nakula was shutdown, so the services offered by this machine were unavailable for a period of time.

47. Shutdown of Nakula to prevent further loss of evidence

    RP: Page 9, Decision to shutdown Nakula

48. Examination of Nakula

    RP: Page 9

49. Detection by RVS: Unauthorized use use of Nakula

    RP: Page 9

2.4.2 Why different graphs?

As previously stated, our definition of the accident ”Loss of resources” turned out not to be specific enough to build only one graph which covers the whole incident.

We have a base of 5 graphs, which will first be described one after the other. Some graphs tie up to others, and some are just sub-graphs. For a better summing up, we colored the points of contact.

- The Nakula graph (Page 22)

  If "loss of resources" is interpreted in it's most direct way, the unauthorized use of the Nakula machine alone is a sufficient necessary causal factor for the accident. Nothing else had to happen to trigger a general loss of any resources. Therefore, this graph is relatively small and abstains from many facts.

  Note that this graph can be divided in two parts, a upper and a lower part. The only connection between these two runs through node "1.1.1.1: Attacker gained valid login/password combination for Nakula machine". This "single point of failure" is very well visible here. The contact point for further graphs "1.1: Attacker used Nakula unauthorized" is coloured in red.

- The Antareja graph (Page 23)

  In the Nakula graph, the accident was interpreted in a very general manner - otherwise the Causal Completeness Test would have failed. The Causal Completeness Test makes sure, that every NCF stated really was necessary for an event to happen. If we settle for a more specific "Loss of resources", namely the loss of resources on both machines, we have to include the scenes regarding Antareja into our graph and end up with two NCFs - "1.1: Attacker used Nakula unauthorized" and "1.2: Attacker used Antareja unauthorized".

  Note that we basically have the same "single point of failure" in the Antareja sub-graph. The Nakula sub-graph is left out in this case, but the contact point is coloured red. The Antareja contact point for further graphs is coloured blue.

- The Nakula & Antareja graph (Page 24)

  This graph is a combination of the Nakula sub-graph and the Antareja sub-graph. The contact points are still coloured like stated above.

- The RVS-Loss graph (Page 25)

  If we modify our interpretation of the accident again, we end up with the RVS-Loss graph. Up to now, we only regarded the loss of system resources as necessary and sufficient for the accident. The loss of manpower resources and the loss of machine availability was suppressed till now. But that's all about to change.

In this case we have a total of five necessary causal factors which form a set of together sufficient causal factors. There are the nodes "1.1: Attacker used NAKULA unauthorized" and "1.2: Attacker used ANTAREJA unauthorized" like in the first graphs, but additional to that we have "1.4: Temporary loss of NAKULA machine and services", "1.3: Specific loss of manpower resources" and "1.5: Temporary loss of ANTAREJA machine and services". The NAKULA sub-graph is blinded out as well as the ANTAREJA sub-graph.

- The complete graph (Page 26)

  The complete graph is nothing else than the RVS-Loss graph with full sub-graphs. All events and facts come out in this one.

2.4.3 The WB-graphs

For improved visibility, the WB-Graphs can be found one by one each on a new page.

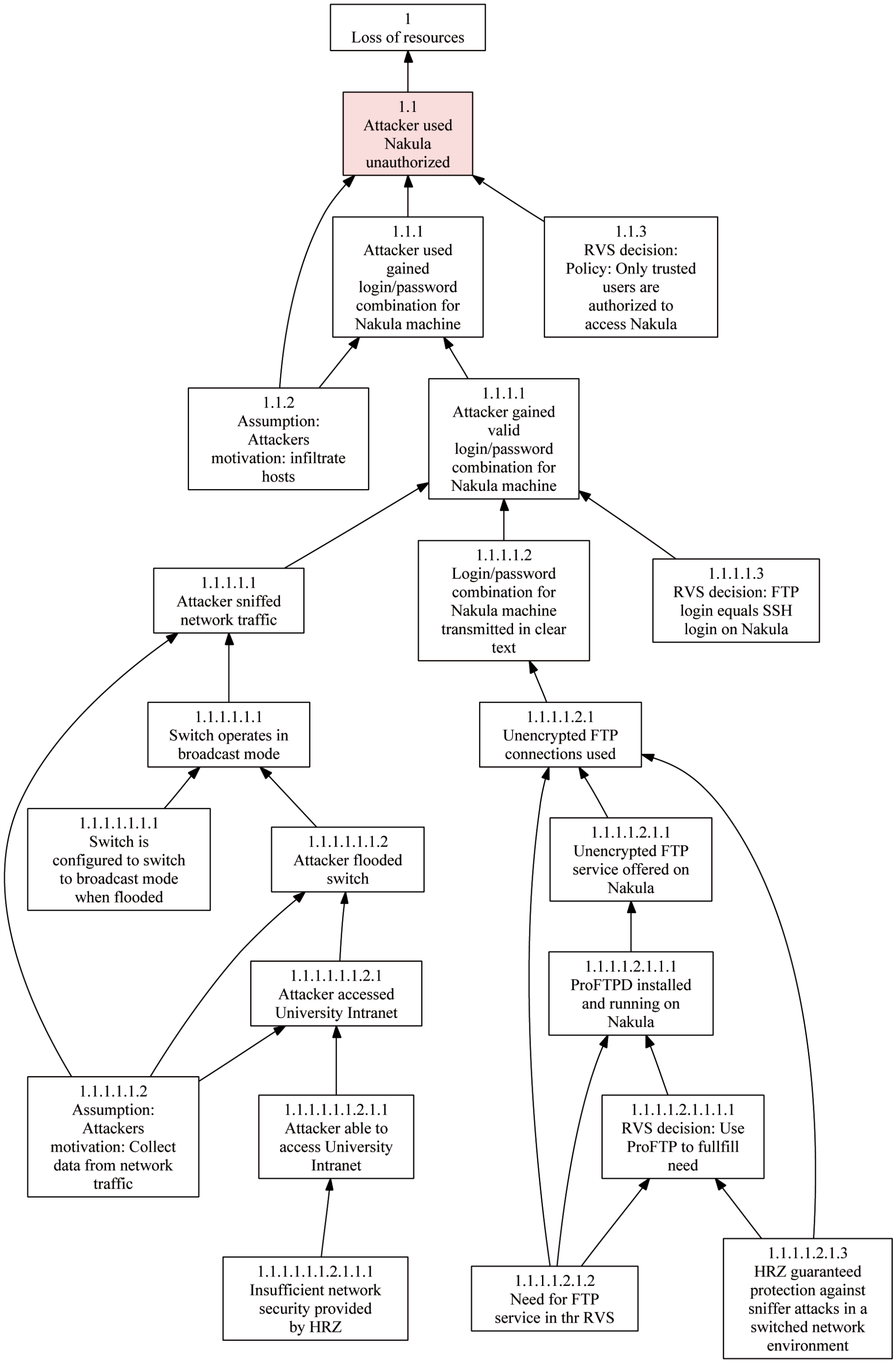
1
Loss of resources
1.1
Attacker used Nakula unauthorized
1.1.1
Attacker used gained login/password combination for Nakula machine
1.1.3
RVS decision: Policy: Only trusted users are authorized to access Nakula
1.1.2
Assumption: Attackers motivation: infiltrate hosts
1.1.1.1
Attacker gained valid login/password combination for Nakula machine
1.1.1.1.1
Attacker sniffed network traffic
1.1.1.1.2
Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3
RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1.1
Switch operates in broadcast mode
1.1.1.1.2.1
Unencrypted FTP connections used
1.1.1.1.1.1.1
Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.2
Attacker flooded switch
1.1.1.1.2.1.1
Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.2.1
Attacker accessed University Intranet
1.1.1.1.2.1.1.1
ProFTPD installed and running on Nakula
1.1.1.1.1.2
Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.1.1.2.1.1
Attacker able to access University Intranet
1.1.1.1.2.1.1.1.1
RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.1.2.1.1.1
Insufficient network security provided by HRZ
1.1.1.1.2.1.2
Need for FTP service in thr RVS
1.1.1.1.2.1.3
HRZ guaranteed protection against sniffer attacks in a switched network environment

Figure 2.1: The Nakula graph

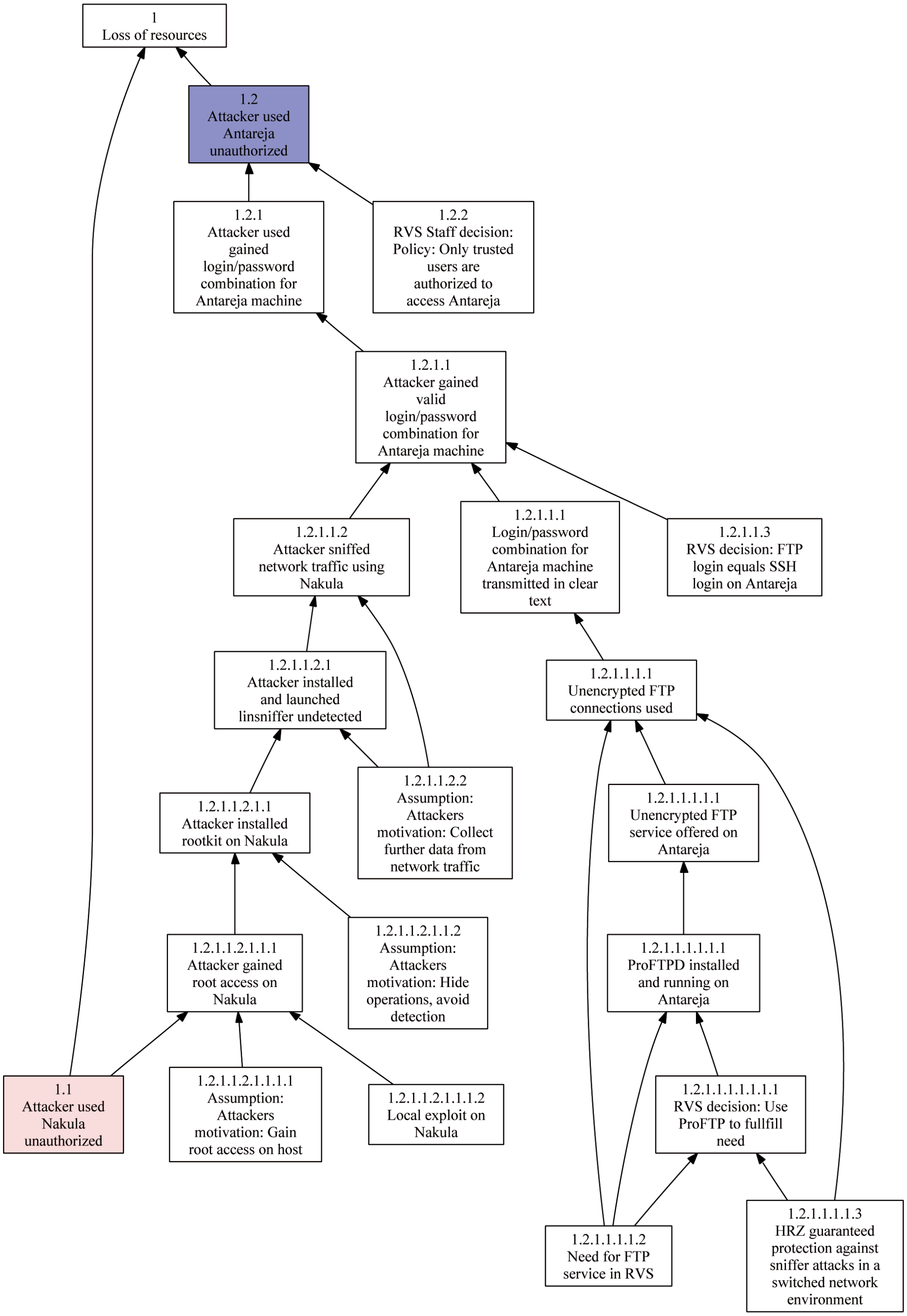
1 Loss of resources
1.2 Attacker used Antareja unauthorized
1.2.1 Attacker used gained login/password combination for Antareja machine
1.2.2 RVS Staff decision: Policy: Only trusted users are authorized to access Antareja
1.2.1.1 Attacker gained valid login/password combination for Antareja machine
1.2.1.1.2 Attacker sniffed network traffic using Nakula
1.2.1.1.1 Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.3 RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.2.1 Attacker installed and launched linsniffer undetected
1.2.1.1.1.1 Unencrypted FTP connections used
1.2.1.1.2.1.1 Attacker installed rootkit on Nakula
1.2.1.1.2.2 Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.1.1.1 Unencrypted FTP service offered on Antareja
1.2.1.1.2.1.1.1 Attacker gained root access on Nakula
1.2.1.1.2.1.1.2 Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.1.1.1.1 ProFTPD installed and running on Antareja
1.1 Attacker used Nakula unauthorized
1.2.1.1.2.1.1.1.1 Assumption: Attackers motivation: Gain root access on host
1.2.1.1.2.1.1.1.2 Local exploit on Nakula
1.2.1.1.1.1.1.1.1 RVS decision: Use ProFTP to fullfill need
1.2.1.1.1.1.3 HRZ guaranteed protection against sniffer attacks in a switched network environment
1.2.1.1.1.1.2 Need for FTP service in RVS

Figure 2.2: The ANTAREJA graph

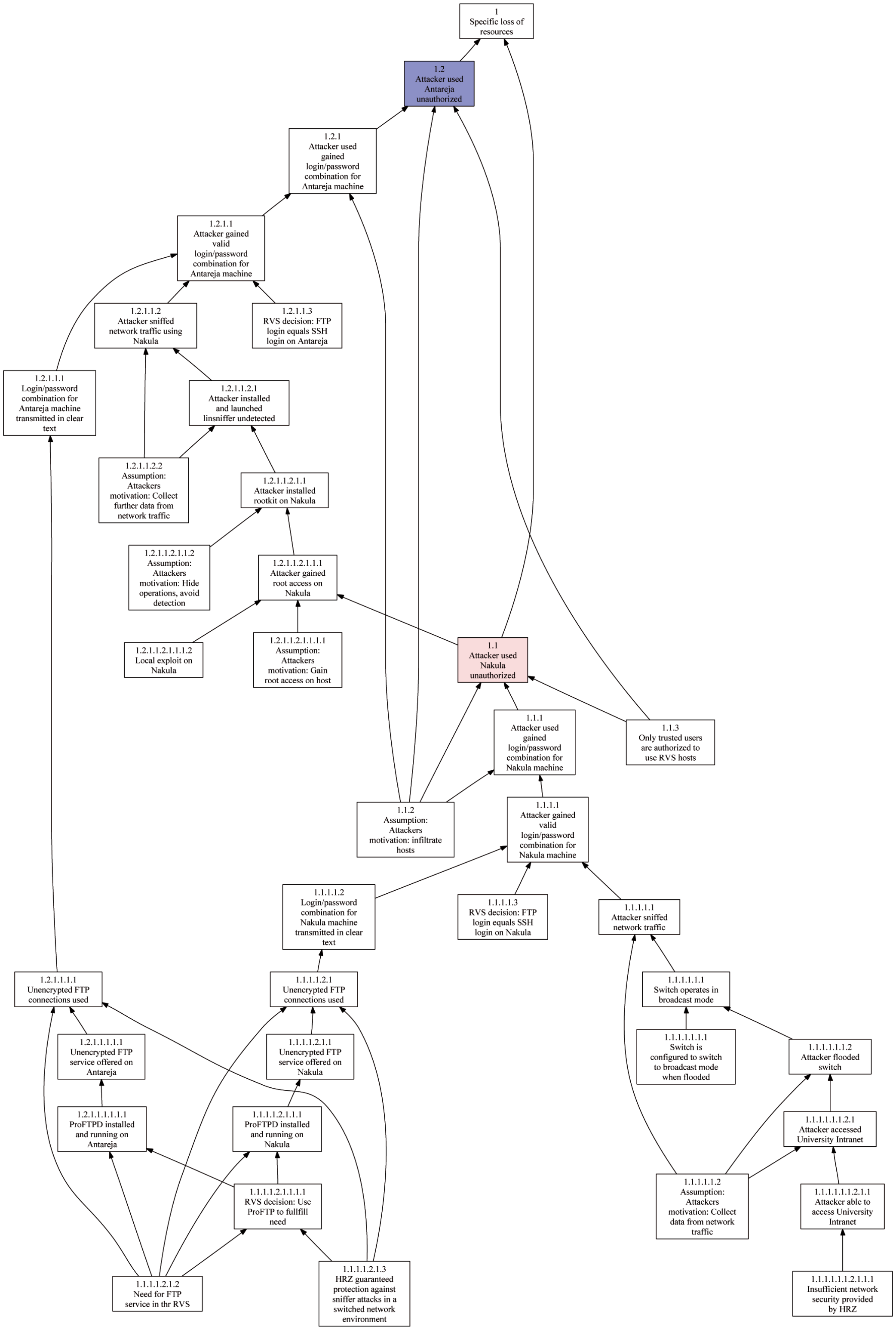
1 Specific loss of resources
1.2 Attacker used Antareja unauthorized
1.2.1 Attacker used gained login/password combination for Antareja machine
1.2.1.1 Attacker gained valid login/password combination for Antareja machine
1.2.1.1.2 Attacker sniffed network traffic using Nakula
1.2.1.1.3 RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.1 Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.2.1 Attacker installed and launched linsniffer undetected
1.2.1.1.2.2 Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.2.1.1 Attacker installed rootkit on Nakula
1.2.1.1.2.1.1.2 Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.2.1.1.1 Attacker gained root access on Nakula
1.2.1.1.2.1.1.1.2 Local exploit on Nakula
1.2.1.1.2.1.1.1.1 Assumption: Attackers motivation: Gain root access on host
1.1 Attacker used Nakula unauthorized
1.1.1 Attacker used gained login/password combination for Nakula machine
1.1.3 Only trusted users are authorized to use RVS hosts
1.1.2 Assumption: Attackers motivation: infiltrate hosts
1.1.1.1 Attacker gained valid login/password combination for Nakula machine
1.1.1.1.2 Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3 RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1 Attacker sniffed network traffic
1.2.1.1.1.1 Unencrypted FTP connections used
1.1.1.1.2.1 Unencrypted FTP connections used
1.1.1.1.1.1 Switch operates in broadcast mode
1.2.1.1.1.1.1 Unencrypted FTP service offered on Antareja
1.1.1.1.2.1.1 Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.1 Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.2 Attacker flooded switch
1.2.1.1.1.1.1.1 ProFTPD installed and running on Antareja
1.1.1.1.2.1.1.1 ProFTPD installed and running on Nakula
1.1.1.1.1.1.2.1 Attacker accessed University Intranet
1.1.1.1.2.1.1.1.1 RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.2 Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.1.1.2.1.1 Attacker able to access University Intranet
1.1.1.1.2.1.3 HRZ guaranteed protection against sniffer attacks in a switched network environment
1.1.1.1.2.1.2 Need for FTP service in thr RVS
1.1.1.1.1.1.2.1.1.1 Insufficient network security provided by HRZ

Figure 2.3: The Nakula & Antareja graph

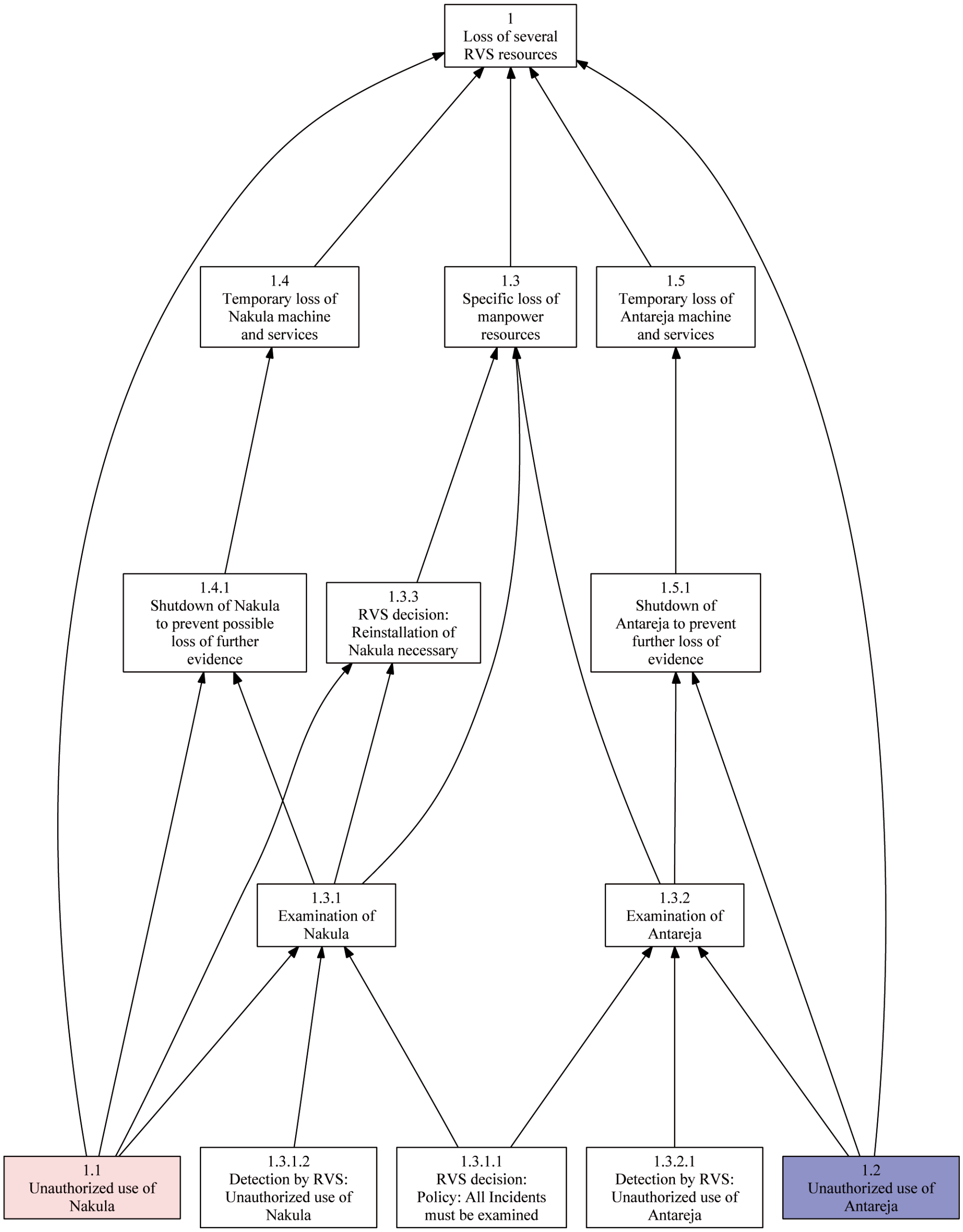
1
Loss of several RVS resources
1.4
Temporary loss of Nakula machine and services
1.3
Specific loss of manpower resources
1.5
Temporary loss of Antareja machine and services
1.4.1
Shutdown of Nakula to prevent possible loss of further evidence
1.3.3
RVS decision: Reinstallation of Nakula necessary
1.5.1
Shutdown of Antareja to prevent further loss of evidence
1.3.1
Examination of Nakula
1.3.2
Examination of Antareja
1.1
Unauthorized use of Nakula
1.3.1.2
Detection by RVS: Unauthorized use of Nakula
1.3.1.1
RVS decision: Policy: All Incidents must be examined
1.3.2.1
Detection by RVS: Unauthorized use of Antareja
1.2
Unauthorized use of Antareja

Figure 2.4: The RVS-Loss graph

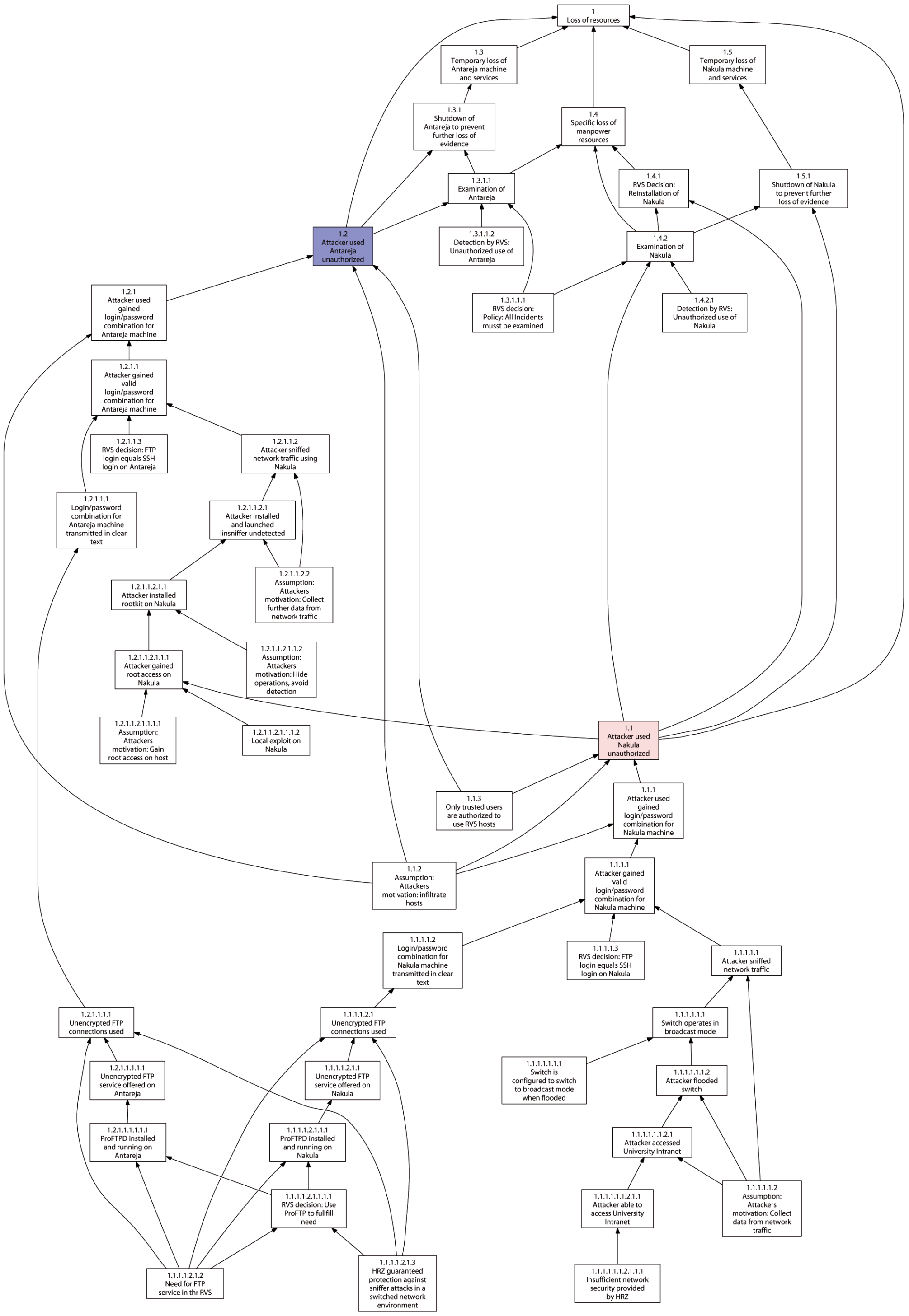
1 Loss of resources
1.3 Temporary loss of Antareja machine and services
1.5 Temporary loss of Nakula machine and services
1.3.1 Shutdown of Antareja to prevent further loss of evidence
1.4 Specific loss of manpower resources
1.3.1.1 Examination of Antareja
1.4.1 RVS Decision: Reinstallation of Nakula
1.5.1 Shutdown of Nakula to prevent further loss of evidence
1.2 Attacker used Antareja unauthorized
1.3.1.1.2 Detection by RVS: Unauthorized use of Antareja
1.4.2 Examination of Nakula
1.2.1 Attacker used gained login/password combination for Antareja machine
1.3.1.1.1 RVS decision: Policy: All Incidents musst be examined
1.4.2.1 Detection by RVS: Unauthorized use of Nakula
1.2.1.1 Attacker gained valid login/password combination for Antareja machine
1.2.1.1.3 RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.2 Attacker sniffed network traffic using Nakula
1.2.1.1.1 Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.2.1 Attacker installed and launched linsniffer undetected
1.2.1.1.2.1.1 Attacker installed rootkit on Nakula
1.2.1.1.2.2 Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.2.1.1.1 Attacker gained root access on Nakula
1.2.1.1.2.1.1.2 Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.2.1.1.1.1 Assumption: Attackers motivation: Gain root access on host
1.2.1.1.2.1.1.1.2 Local exploit on Nakula
1.1 Attacker used Nakula unauthorized
1.1.3 Only trusted users are authorized to use RVS hosts
1.1.1 Attacker used gained login/password combination for Nakula machine
1.1.2 Assumption: Attackers motivation: infiltrate hosts
1.1.1.1 Attacker gained valid login/password combination for Nakula machine
1.1.1.1.2 Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3 RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1 Attacker sniffed network traffic
1.2.1.1.1.1 Unencrypted FTP connections used
1.1.1.1.2.1 Unencrypted FTP connections used
1.1.1.1.1.1 Switch operates in broadcast mode
1.2.1.1.1.1.1 Unencrypted FTP service offered on Antareja
1.1.1.1.2.1.1 Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.1 Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.2 Attacker flooded switch
1.2.1.1.1.1.1.1 ProFTPD installed and running on Antareja
1.1.1.1.2.1.1.1 ProFTPD installed and running on Nakula
1.1.1.1.1.1.2.1 Attacker accessed University Intranet
1.1.1.1.2.1.1.1.1 RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.1.2.1.1 Attacker able to access University Intranet
1.1.1.1.1.2 Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.2.1.3 HRZ guaranteed protection against sniffer attacks in a switched network environment
1.1.1.1.2.1.2 Need for FTP service in thr RVS
1.1.1.1.1.1.2.1.1.1 Insufficient network security provided by HRZ

Figure 2.5: The complete graph

2.5 Playing with the graphs

Unfortunately, the graphs and their relations are quite complex. The coherences do not show well and so we tried to clarify them. In this chapter we will present some prospects to approach this goal.

2.5.1 Marking the sub-graphs

Though the complete graph is only the combination of the different subgraphs, this is difficult to ascertain. It sure helps to colourize the sub-graphs. And that looks like the following graph.

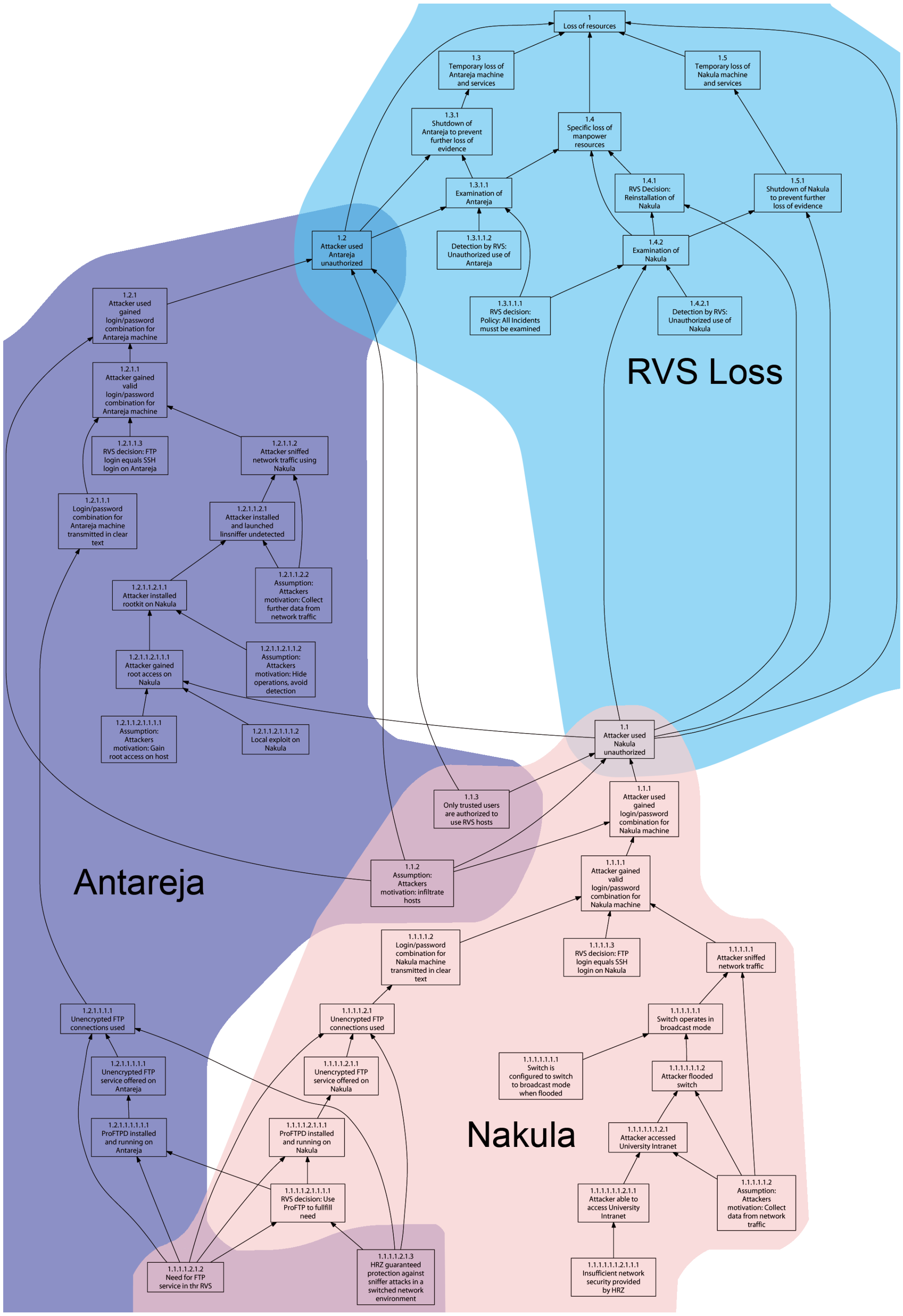
1
Loss of resources
1.3
Temporary loss of Antareja machine and services
1.5
Temporary loss of Nakula machine and services
1.3.1
Shutdown of Antareja to prevent further loss of evidence
1.4
Specific loss of manpower resources
1.3.1.1
Examination of Antareja
1.4.1
RVS Decision: Reinstallation of Nakula
1.5.1
Shutdown of Nakula to prevent further loss of evidence
1.2
Attacker used Antareja unauthorized
1.3.1.1.2
Detection by RVS: Unauthorized use of Antareja
1.4.2
Examination of Nakula
1.3.1.1.1
RVS decision: Policy: All Incidents musst be examined
1.4.2.1
Detection by RVS: Unauthorized use of Nakula
RVS Loss
1.2.1
Attacker used gained login/password combination for Antareja machine
1.2.1.1
Attacker gained valid login/password combination for Antareja machine
1.2.1.1.3
RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.2
Attacker sniffed network traffic using Nakula
1.2.1.1.1
Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.2.1
Attacker installed and launched linsniffer undetected
1.2.1.1.2.2
Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.2.1.1
Attacker installed rootkit on Nakula
1.2.1.1.2.1.1.2
Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.2.1.1.1
Attacker gained root access on Nakula
1.2.1.1.2.1.1.1.1
Assumption: Attackers motivation: Gain root access on host
1.2.1.1.2.1.1.1.2
Local exploit on Nakula
1.1
Attacker used Nakula unauthorized
1.1.3
Only trusted users are authorized to use RVS hosts
1.1.1
Attacker used gained login/password combination for Nakula machine
1.1.2
Assumption: Attackers motivation: infiltrate hosts
Antareja
1.1.1.1
Attacker gained valid login/password combination for Nakula machine
1.1.1.1.2
Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3
RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1
Attacker sniffed network traffic
1.2.1.1.1.1
Unencrypted FTP connections used
1.1.1.1.2.1
Unencrypted FTP connections used
1.1.1.1.1.1
Switch operates in broadcast mode
1.2.1.1.1.1.1
Unencrypted FTP service offered on Antareja
1.1.1.1.2.1.1
Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.1
Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.2
Attacker flooded switch
1.2.1.1.1.1.1.1
ProFTPD installed and running on Antareja
1.1.1.1.2.1.1.1
ProFTPD installed and running on Nakula
Nakula
1.1.1.1.1.1.2.1
Attacker accessed University Intranet
1.1.1.1.2.1.1.1.1
RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.1.1.2.1.1
Attacker able to access University Intranet
1.1.1.1.1.2
Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.2.1.3
HRZ guaranteed protection against sniffer attacks in a switched network environment
1.1.1.1.2.1.2
Need for FTP service in thr RVS
1.1.1.1.1.1.1.2.1.1.1
Insufficient network security provided by HRZ

Figure 2.6: The complete graph with coloured sub-graphs

2.5.2 Marking out control areas

If we have a closer look at the nodes, we can allocate facts which could not even be mitigated if one wanted to: facts which just don't lie under one's control. And then there are facts which could be mitigated. It's trivial to realise that, while trying to prevent further similar accidents, the concentration should be on those facts which are in fact controllable.

So we tried to apply this idea and came up with the graph on the following page displaying the whole WB-Graph with marked control areas. We differentiate three control areas:

- Blue: Human-control area
  The nodes lying under the direct control of the defender. So we could interfere here.

- Yellow: Attacker-control area
  The defender has no direct options for manipulation. It's quite useless to regard them as possible candidates for direct removal, so they can be blinded out simply because you can't change anything here.

- Green: Technical-control area
  This nodes are of pure technical interest, e.g. "1.1.1.1.1.1: Switch operates in broadcast mode". These might be possible candidates for removal and should be considered as important aspirants for further inspection.

The uncoloured nodes don't lie under anyone's control and are causal results.

This figure helps to focus on important events where the system's stakeholder has direct access. During this process, it makes sense to think about nodes you could, but you don't want to eliminate by intuition like "1.4.2.1: Detection by RVS: Unauthorized use of NAKULA" (q.v. chapter 2.5.4). Closing your eyes doesn't really make the accident go away. ;-)

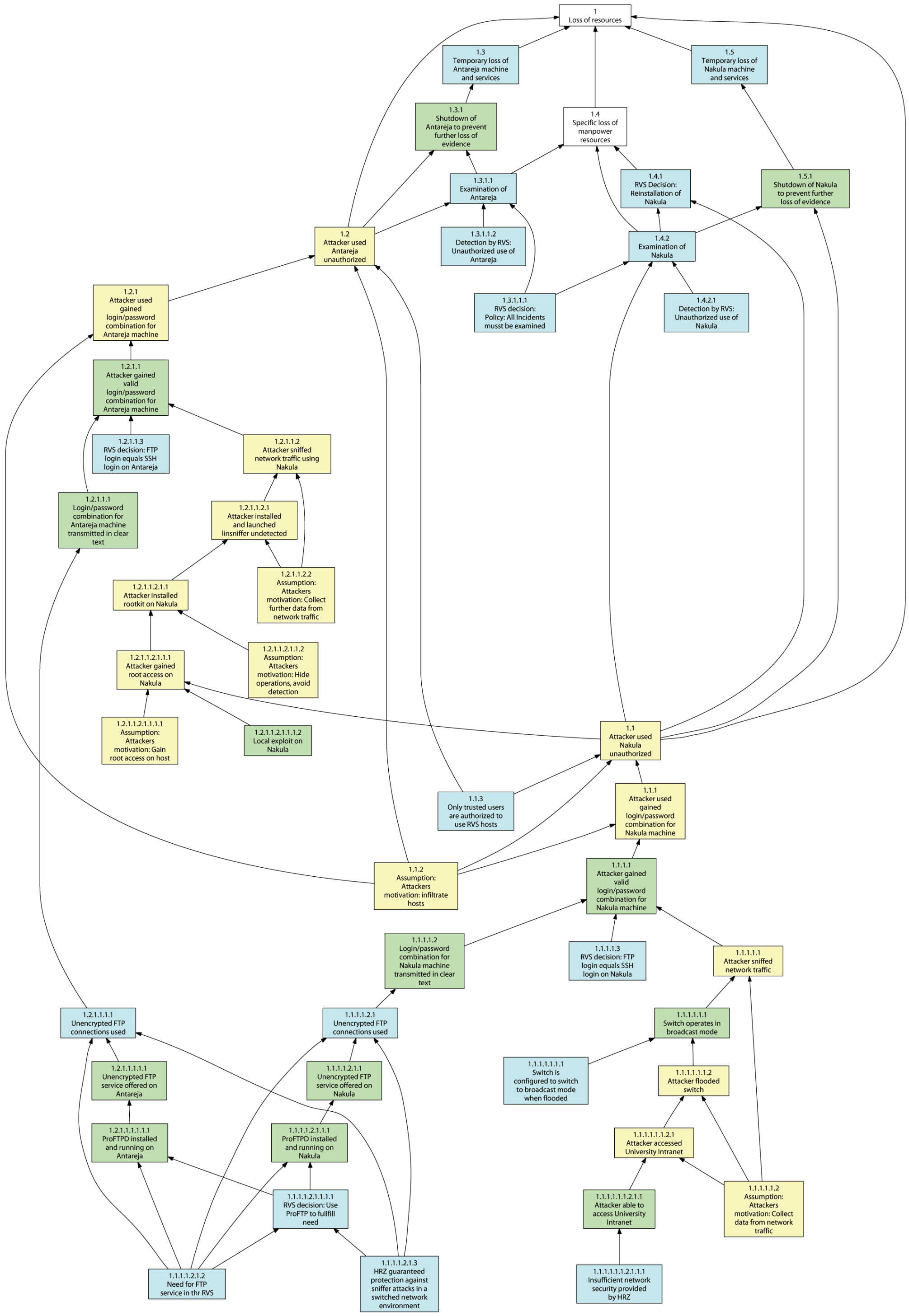
1
Loss of resources
1.3
Temporary loss of Antareja machine and services
1.5
Temporary loss of Nakula machine and services
1.3.1
Shutdown of Antareja to prevent further loss of evidence
1.4
Specific loss of manpower resources
1.3.1.1
Examination of Antareja
1.4.1
RVS Decision: Reinstallation of Nakula
1.5.1
Shutdown of Nakula to prevent further loss of evidence
1.2
Attacker used Antareja unauthorized
1.3.1.1.2
Detection by RVS: Unauthorized use of Antareja
1.4.2
Examination of Nakula
1.2.1
Attacker used gained login/password combination for Antareja machine
1.3.1.1.1
RVS decision: Policy: All Incidents musst be examined
1.4.2.1
Detection by RVS: Unauthorized use of Nakula
1.2.1.1
Attacker gained valid login/password combination for Antareja machine
1.2.1.1.3
RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.2
Attacker sniffed network traffic using Nakula
1.2.1.1.1
Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.2.1
Attacker installed and launched linsniffer undetected
1.2.1.1.2.2
Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.2.1.1
Attacker installed rootkit on Nakula
1.2.1.1.2.1.1.1
Attacker gained root access on Nakula
1.2.1.1.2.1.1.2
Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.2.1.1.1.1
Assumption: Attackers motivation: Gain root access on host
1.2.1.1.2.1.1.1.2
Local exploit on Nakula
1.1
Attacker used Nakula unauthorized
1.1.3
Only trusted users are authorized to use RVS hosts
1.1.1
Attacker used gained login/password combination for Nakula machine
1.1.2
Assumption: Attackers motivation: infiltrate hosts
1.1.1.1
Attacker gained valid login/password combination for Nakula machine
1.1.1.1.2
Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3
RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1
Attacker sniffed network traffic
1.2.1.1.1.1
Unencrypted FTP connections used
1.1.1.1.2.1
Unencrypted FTP connections used
1.1.1.1.1.1
Switch operates in broadcast mode
1.1.1.1.1.1.1
Switch is configured to switch to broadcast mode when flooded
1.2.1.1.1.1.1
Unencrypted FTP service offered on Antareja
1.1.1.1.2.1.1
Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.2
Attacker flooded switch
1.2.1.1.1.1.1.1
ProFTPD installed and running on Antareja
1.1.1.1.2.1.1.1
ProFTPD installed and running on Nakula
1.1.1.1.1.1.2.1
Attacker accessed University Intranet
1.1.1.1.2.1.1.1.1
RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.1.2.1.1
Attacker able to access University Intranet
1.1.1.1.1.2
Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.2.1.2
Need for FTP service in thr RVS
1.1.1.1.2.1.3
HRZ guaranteed protection against sniffer attacks in a switched network environment
1.1.1.1.1.1.2.1.1.1
Insufficient network security provided by HRZ

Figure 2.7: The complete graph with coloured control areas

2.5.3 Allow transitivity

The counterfactual definition of the notion *necessary causal factor* as stated by Lewis in "Causal System Analysis"[3] is a binary, non-transitive relation. Imagine three temporally successive events - A, B and C. Let's say A is a necessary causal factor for B, and B is a necessary causal factor for C. Than A is not necessarily a causal factor for C. Transitivity is not given.

If we allow transitivity, and therefore use Lewis's definition of *cause*[4] as transitive closure of the notion of *causal factor*, we will save some edges and improve serenity. So, thats what we did.

Below we append three versions of each graph. In each first graph the edges we removed in the next step are marked by a red X. Each third graph is a complete recreation of the "transitive reduced" graph using *ybedit* (q.v. Appendix B).

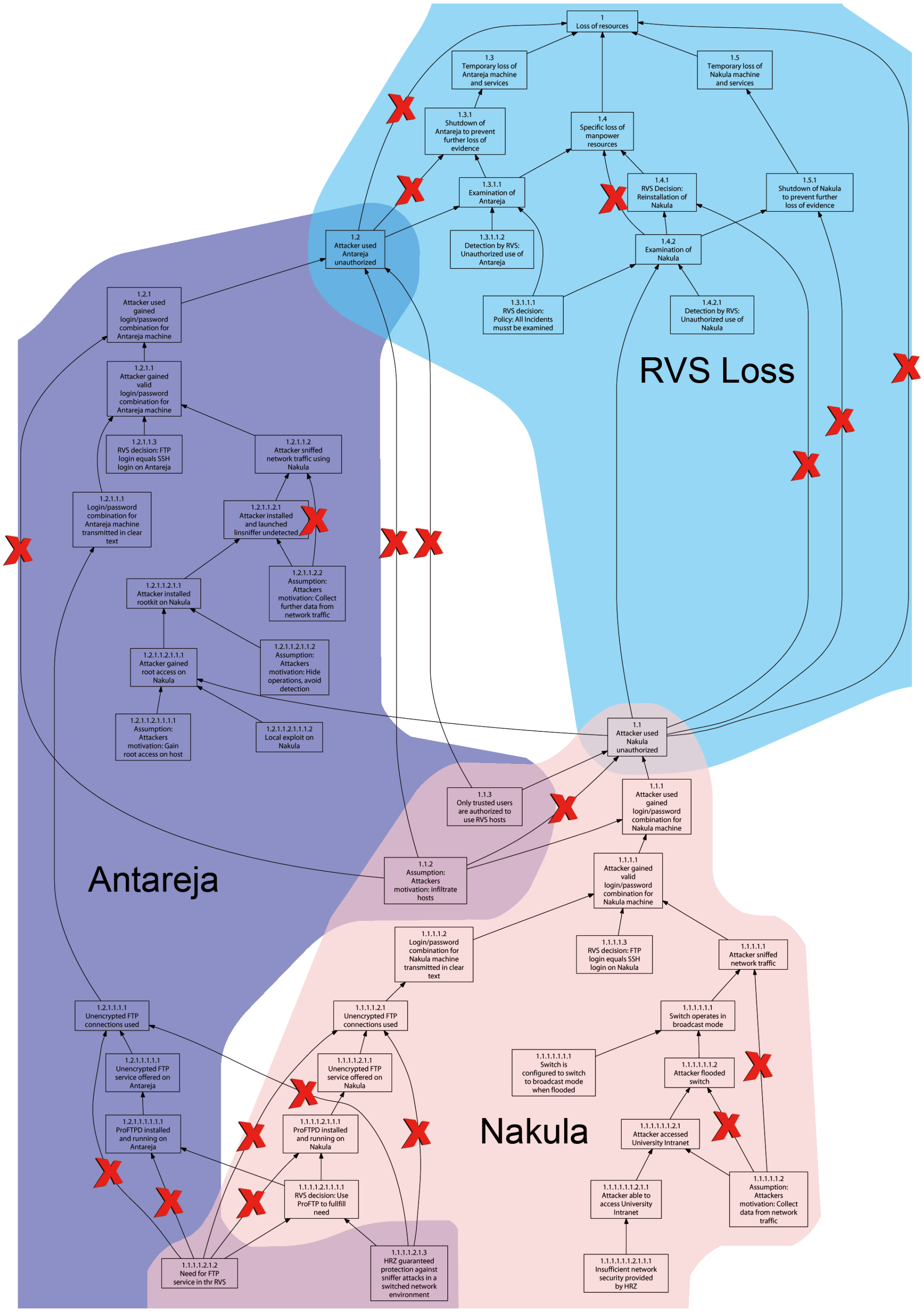
RVS Loss
Antareja
Nakula
1 Loss of resources
1.3 Temporary loss of Antareja machine and services
1.5 Temporary loss of Nakula machine and services
1.3.1 Shutdown of Antareja to prevent further loss of evidence
1.4 Specific loss of manpower resources
1.3.1.1 Examination of Antareja
1.4.1 RVS Decision: Reinstallation of Nakula
1.5.1 Shutdown of Nakula to prevent further loss of evidence
1.2 Attacker used Antareja unauthorized
1.3.1.1.2 Detection by RVS: Unauthorized use of Antareja
1.4.2 Examination of Nakula
1.3.1.1.1 RVS decision: Policy: All Incidents musst be examined
1.4.2.1 Detection by RVS: Unauthorized use of Nakula
1.2.1 Attacker used gained login/password combination for Antareja machine
1.2.1.1 Attacker gained valid login/password combination for Antareja machine
1.2.1.1.3 RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.2 Attacker sniffed network traffic using Nakula
1.2.1.1.1 Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.2.1 Attacker installed and launched linsniffer undetected
1.2.1.1.2.2 Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.2.1.1 Attacker installed rootkit on Nakula
1.2.1.1.2.1.1.1 Attacker gained root access on Nakula
1.2.1.1.2.1.1.2 Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.2.1.1.1.1 Assumption: Attackers motivation: Gain root access on host
1.2.1.1.2.1.1.1.2 Local exploit on Nakula
1.1 Attacker used Nakula unauthorized
1.1.3 Only trusted users are authorized to use RVS hosts
1.1.1 Attacker used gained login/password combination for Nakula machine
1.1.2 Assumption: Attackers motivation: infiltrate hosts
1.1.1.1 Attacker gained valid login/password combination for Nakula machine
1.1.1.1.2 Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3 RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1 Attacker sniffed network traffic
1.2.1.1.1.1 Unencrypted FTP connections used
1.1.1.1.2.1 Unencrypted FTP connections used
1.1.1.1.1.1 Switch operates in broadcast mode
1.2.1.1.1.1.1 Unencrypted FTP service offered on Antareja
1.1.1.1.2.1.1 Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.1 Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.2 Attacker flooded switch
1.2.1.1.1.1.1.1 ProFTPD installed and running on Antareja
1.1.1.1.2.1.1.1 ProFTPD installed and running on Nakula
1.1.1.1.1.1.2.1 Attacker accessed University Intranet
1.1.1.1.2.1.1.1.1 RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.1.2.1.1 Attacker able to access University Intranet
1.1.1.1.1.2 Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.2.1.2 Need for FTP service in thr RVS
1.1.1.1.2.1.3 HRZ guaranteed protection against sniffer attacks in a switched network environment
1.1.1.1.1.1.2.1.1.1 Insufficient network security provided by HRZ

Figure 2.8: Complete coloured graph: removable edges

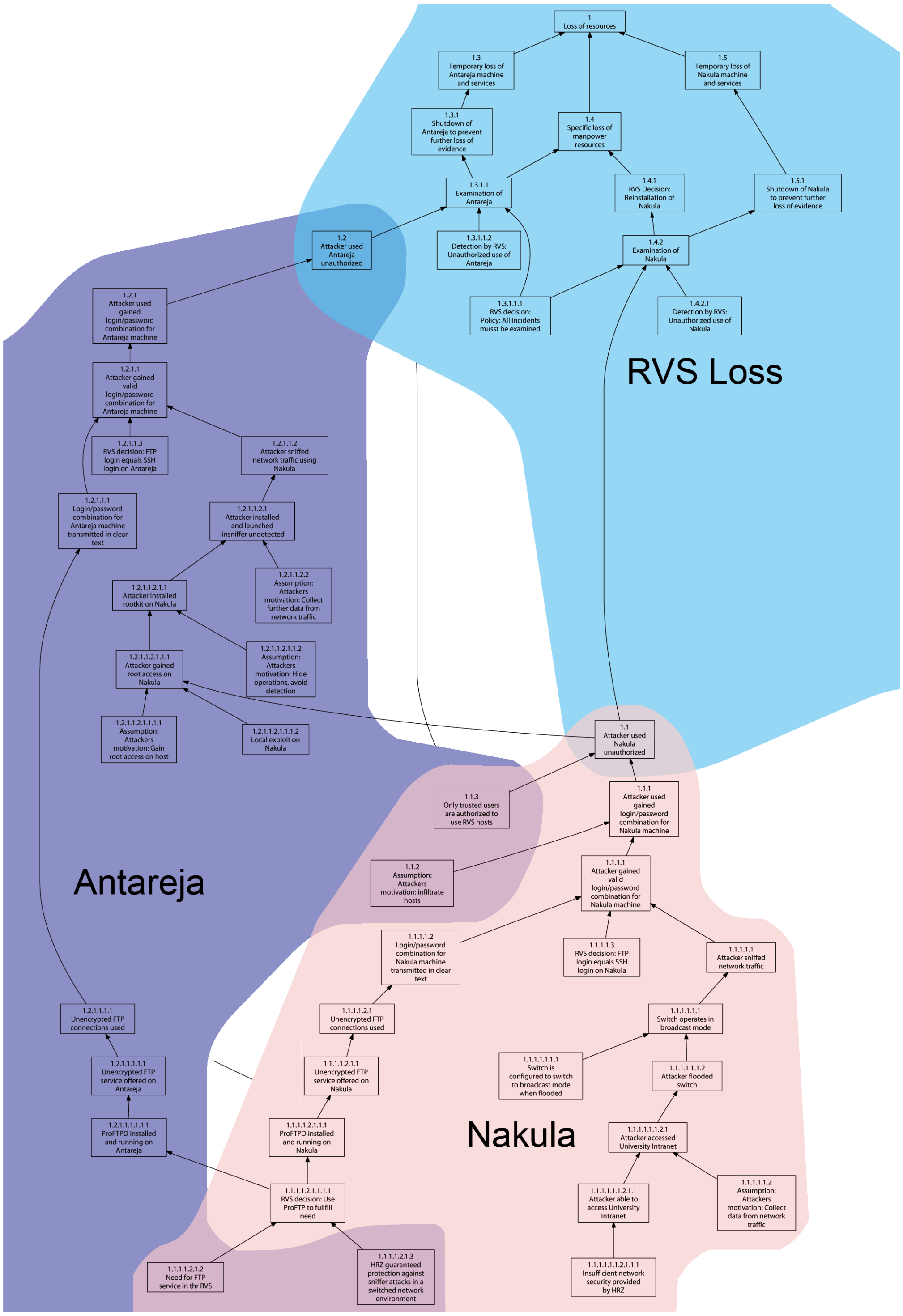
1 Loss of resources
1.3 Temporary loss of Antareja machine and services
1.5 Temporary loss of Nakula machine and services
1.3.1 Shutdown of Antareja to prevent further loss of evidence
1.4 Specific loss of manpower resources
1.3.1.1 Examination of Antareja
1.4.1 RVS Decision: Reinstallation of Nakula
1.5.1 Shutdown of Nakula to prevent further loss of evidence
1.2 Attacker used Antareja unauthorized
1.3.1.1.2 Detection by RVS: Unauthorized use of Antareja
1.4.2 Examination of Nakula
1.2.1 Attacker used gained login/password combination for Antareja machine
1.3.1.1.1 RVS decision: Policy: All Incidents musst be examined
1.4.2.1 Detection by RVS: Unauthorized use of Nakula
RVS Loss
1.2.1.1 Attacker gained valid login/password combination for Antareja machine
1.2.1.1.3 RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.2 Attacker sniffed network traffic using Nakula
1.2.1.1.1 Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.2.1 Attacker installed and launched linsniffer undetected
1.2.1.1.2.2 Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.2.1.1 Attacker installed rootkit on Nakula
1.2.1.1.2.1.1.1 Attacker gained root access on Nakula
1.2.1.1.2.1.1.2 Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.2.1.1.1.1 Assumption: Attackers motivation: Gain root access on host
1.2.1.1.2.1.1.1.2 Local exploit on Nakula
1.1 Attacker used Nakula unauthorized
1.1.3 Only trusted users are authorized to use RVS hosts
1.1.1 Attacker used gained login/password combination for Nakula machine
Antareja
1.1.2 Assumption: Attackers motivation: infiltrate hosts
1.1.1.1 Attacker gained valid login/password combination for Nakula machine
1.1.1.1.2 Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3 RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1 Attacker sniffed network traffic
1.2.1.1.1.1 Unencrypted FTP connections used
1.1.1.1.2.1 Unencrypted FTP connections used
1.1.1.1.1.1 Switch operates in broadcast mode
1.2.1.1.1.1.1 Unencrypted FTP service offered on Antareja
1.1.1.1.2.1.1 Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.1 Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.2 Attacker flooded switch
1.2.1.1.1.1.1.1 ProFTPD installed and running on Antareja
1.1.1.1.2.1.1.1 ProFTPD installed and running on Nakula
Nakula
1.1.1.1.1.1.2.1 Attacker accessed University Intranet
1.1.1.1.2.1.1.1.1 RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.1.2.1.1 Attacker able to access University Intranet
1.1.1.1.1.2 Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.2.1.2 Need for FTP service in thr RVS
1.1.1.1.2.1.3 HRZ guaranteed protection against sniffer attacks in a switched network environment
1.1.1.1.1.1.2.1.1.1 Insufficient network security provided by HRZ

Figure 2.9: Complete coloured graph using the definition of *cause*

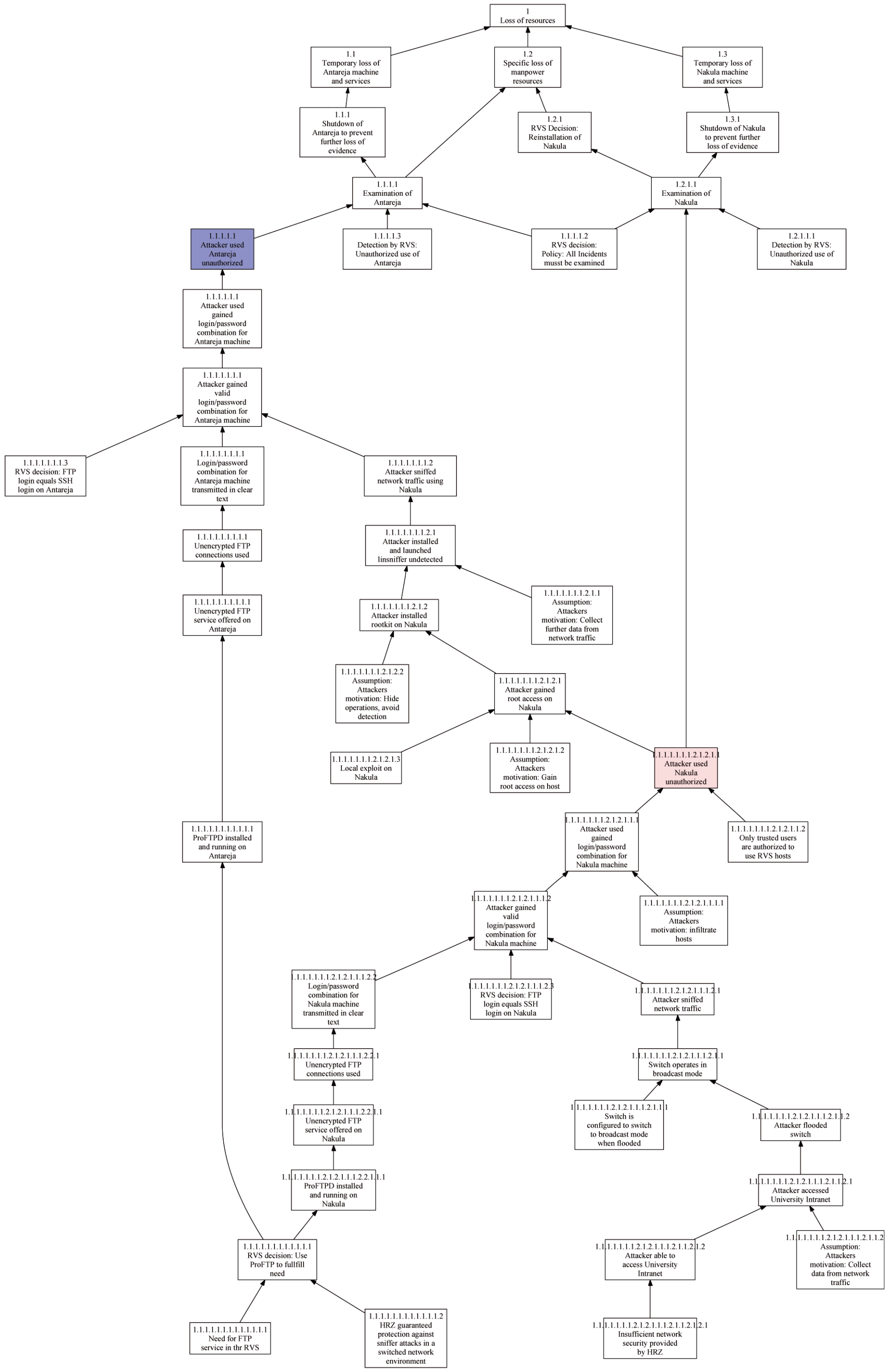
1
Loss of resources
1.1
Temporary loss of Antareja machine and services
1.2
Specific loss of manpower resources
1.3
Temporary loss of Nakula machine and services
1.1.1
Shutdown of Antareja to prevent further loss of evidence
1.2.1
RVS Decision: Reinstallation of Nakula
1.3.1
Shutdown of Nakula to prevent further loss of evidence
1.1.1.1
Examination of Antareja
1.2.1.1
Examination of Nakula
1.1.1.1.1
Attacker used Antareja unauthorized
1.1.1.1.3
Detection by RVS: Unauthorized use of Antareja
1.1.1.1.2
RVS decision: Policy: All Incidents musst be examined
1.2.1.1.1
Detection by RVS: Unauthorized use of Nakula
1.1.1.1.1.1
Attacker used gained login/password combination for Antareja machine
1.1.1.1.1.1.1
Attacker gained valid login/password combination for Antareja machine
1.1.1.1.1.1.1.3
RVS decision: FTP login equals SSH login on Antareja
1.1.1.1.1.1.1.1
Login/password combination for Antareja machine transmitted in clear text
1.1.1.1.1.1.1.2
Attacker sniffed network traffic using Nakula
1.1.1.1.1.1.1.1.1
Unencrypted FTP connections used
1.1.1.1.1.1.1.2.1
Attacker installed and launched linsniffer undetected
1.1.1.1.1.1.1.1.1.1
Unencrypted FTP service offered on Antareja
1.1.1.1.1.1.1.2.1.2
Attacker installed rootkit on Nakula
1.1.1.1.1.1.1.2.1.1
Assumption: Attackers motivation: Collect further data from network traffic
1.1.1.1.1.1.1.2.1.2.2
Assumption: Attackers motivation: Hide operations, avoid detection
1.1.1.1.1.1.1.2.1.2.1
Attacker gained root access on Nakula
1.1.1.1.1.1.1.2.1.2.1.3
Local exploit on Nakula
1.1.1.1.1.1.1.2.1.2.1.2
Assumption: Attackers motivation: Gain root access on host
1.1.1.1.1.1.1.2.1.2.1.1
Attacker used Nakula unauthorized
1.1.1.1.1.1.1.1.1.1.1
ProFTPD installed and running on Antareja
1.1.1.1.1.1.1.2.1.2.1.1.1
Attacker used gained login/password combination for Nakula machine
1.1.1.1.1.1.1.2.1.2.1.1.2
Only trusted users are authorized to use RVS hosts
1.1.1.1.1.1.1.2.1.2.1.1.1.2
Attacker gained valid login/password combination for Nakula machine
1.1.1.1.1.1.1.2.1.2.1.1.1.1
Assumption: Attackers motivation: infiltrate hosts
1.1.1.1.1.1.1.2.1.2.1.1.1.2.2
Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.1.1.1.2.1.2.1.1.1.2.3
RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1.1.1.2.1.2.1.1.1.2.1
Attacker sniffed network traffic
1.1.1.1.1.1.1.2.1.2.1.1.1.2.2.1
Unencrypted FTP connections used
1.1.1.1.1.1.1.2.1.2.1.1.1.2.1.1
Switch operates in broadcast mode
1.1.1.1.1.1.1.2.1.2.1.1.1.2.1.1.1
Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.1.2.1.2.1.1.1.2.1.1.2
Attacker flooded switch
1.1.1.1.1.1.1.2.1.2.1.1.1.2.2.1.1
Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.1.2.1.2.1.1.1.2.2.1.1.1
ProFTPD installed and running on Nakula
1.1.1.1.1.1.1.2.1.2.1.1.1.2.1.1.2.1
Attacker accessed University Intranet
1.1.1.1.1.1.1.1.1.1.1.1
RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.1.1.2.1.2.1.1.1.2.1.1.2.1.2
Attacker able to access University Intranet
1.1.1.1.1.1.1.2.1.2.1.1.1.2.1.1.2.1.1.2
Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.1.1.1.1.1.1.1.1.1
Need for FTP service in thr RVS
1.1.1.1.1.1.1.1.1.1.1.1.2
HRZ guaranteed protection against sniffer attacks in a switched network environment
1.1.1.1.1.1.1.2.1.2.1.1.1.2.1.1.2.1.2.1
Insufficient network security provided by HRZ

Figure 2.10: Reformated complete graph using the definition of *cause*

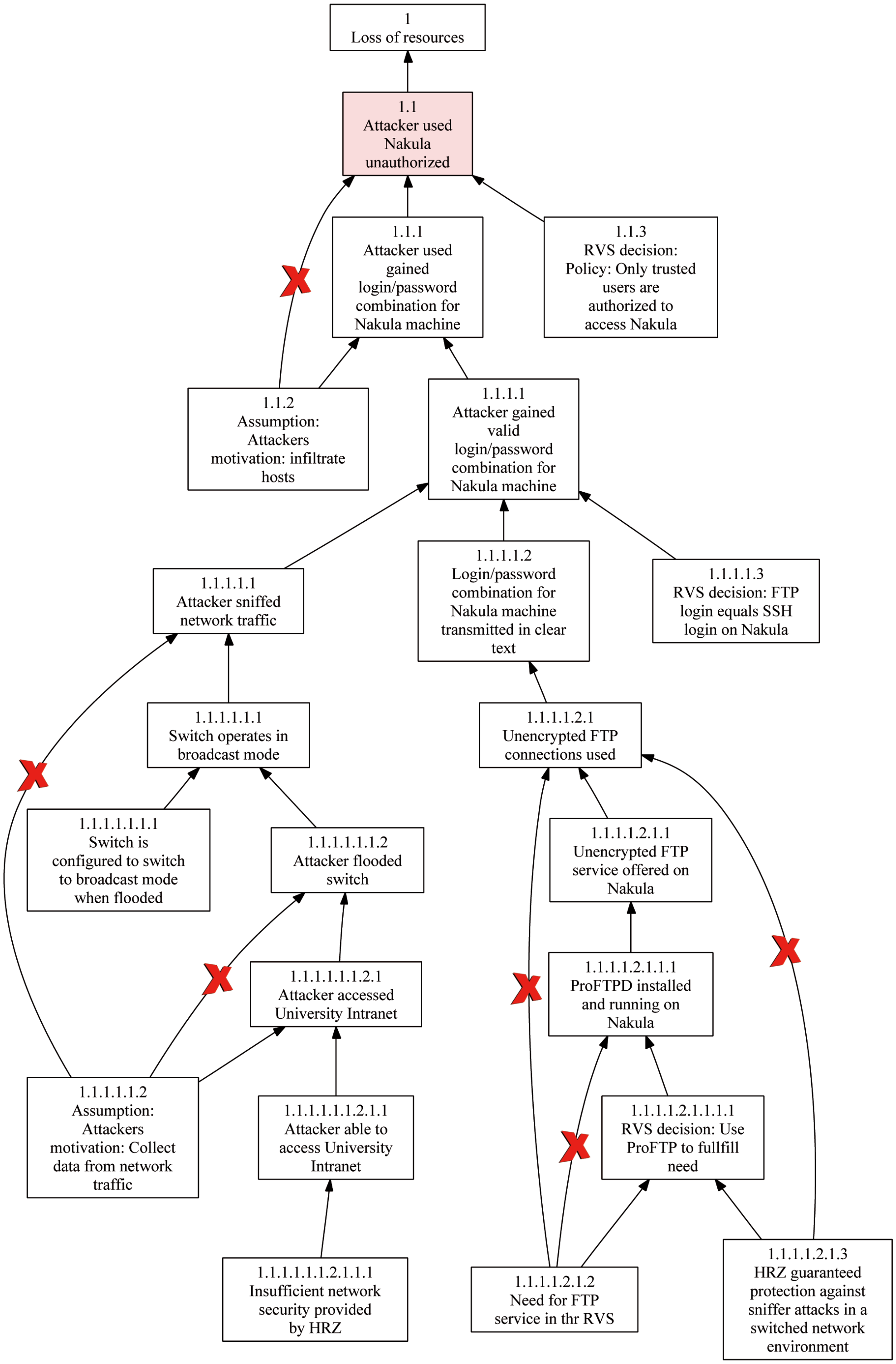
1
Loss of resources
1.1
Attacker used Nakula unauthorized
1.1.1
Attacker used gained login/password combination for Nakula machine
1.1.3
RVS decision: Policy: Only trusted users are authorized to access Nakula
1.1.2
Assumption: Attackers motivation: infiltrate hosts
1.1.1.1
Attacker gained valid login/password combination for Nakula machine
1.1.1.1.1
Attacker sniffed network traffic
1.1.1.1.2
Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3
RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1.1
Switch operates in broadcast mode
1.1.1.1.2.1
Unencrypted FTP connections used
1.1.1.1.1.1.1
Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.2
Attacker flooded switch
1.1.1.1.2.1.1
Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.2.1
Attacker accessed University Intranet
1.1.1.1.2.1.1.1
ProFTPD installed and running on Nakula
1.1.1.1.1.2
Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.1.1.2.1.1
Attacker able to access University Intranet
1.1.1.1.2.1.1.1.1
RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.1.2.1.1.1
Insufficient network security provided by HRZ
1.1.1.1.2.1.2
Need for FTP service in thr RVS
1.1.1.1.2.1.3
HRZ guaranteed protection against sniffer attacks in a switched network environment

Figure 2.11: Nakula graph: removable edges

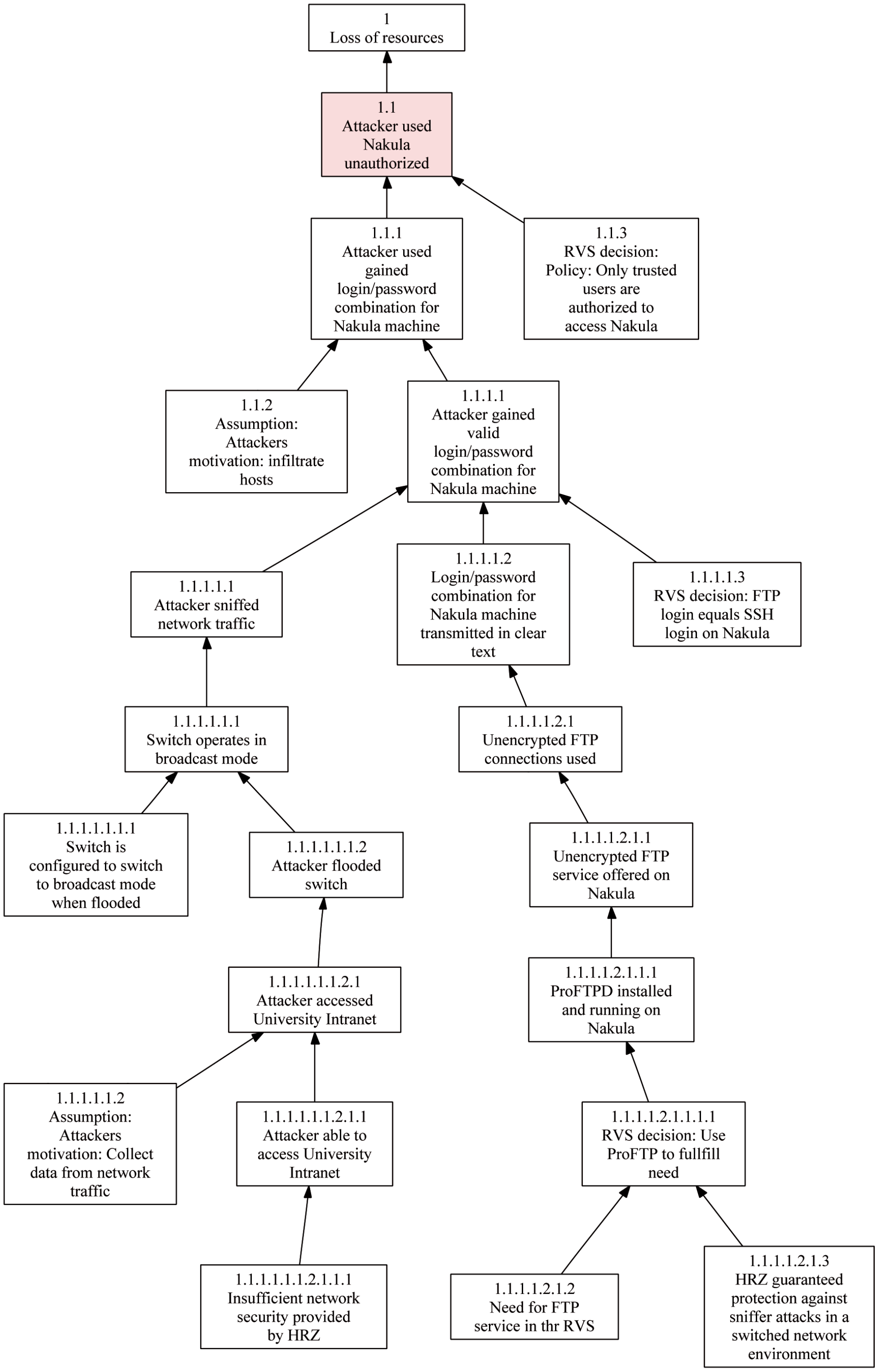
1
Loss of resources
1.1
Attacker used Nakula unauthorized
1.1.1
Attacker used gained login/password combination for Nakula machine
1.1.3
RVS decision: Policy: Only trusted users are authorized to access Nakula
1.1.2
Assumption: Attackers motivation: infiltrate hosts
1.1.1.1
Attacker gained valid login/password combination for Nakula machine
1.1.1.1.1
Attacker sniffed network traffic
1.1.1.1.2
Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3
RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1.1
Switch operates in broadcast mode
1.1.1.1.2.1
Unencrypted FTP connections used
1.1.1.1.1.1.1
Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.2
Attacker flooded switch
1.1.1.1.2.1.1
Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.2.1
Attacker accessed University Intranet
1.1.1.1.2.1.1.1
ProFTPD installed and running on Nakula
1.1.1.1.1.2
Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.1.1.2.1.1
Attacker able to access University Intranet
1.1.1.1.2.1.1.1.1
RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.1.2.1.1.1
Insufficient network security provided by HRZ
1.1.1.1.2.1.2
Need for FTP service in thr RVS
1.1.1.1.2.1.3
HRZ guaranteed protection against sniffer attacks in a switched network environment

Figure 2.12: Nakula graph using the definition of *cause*

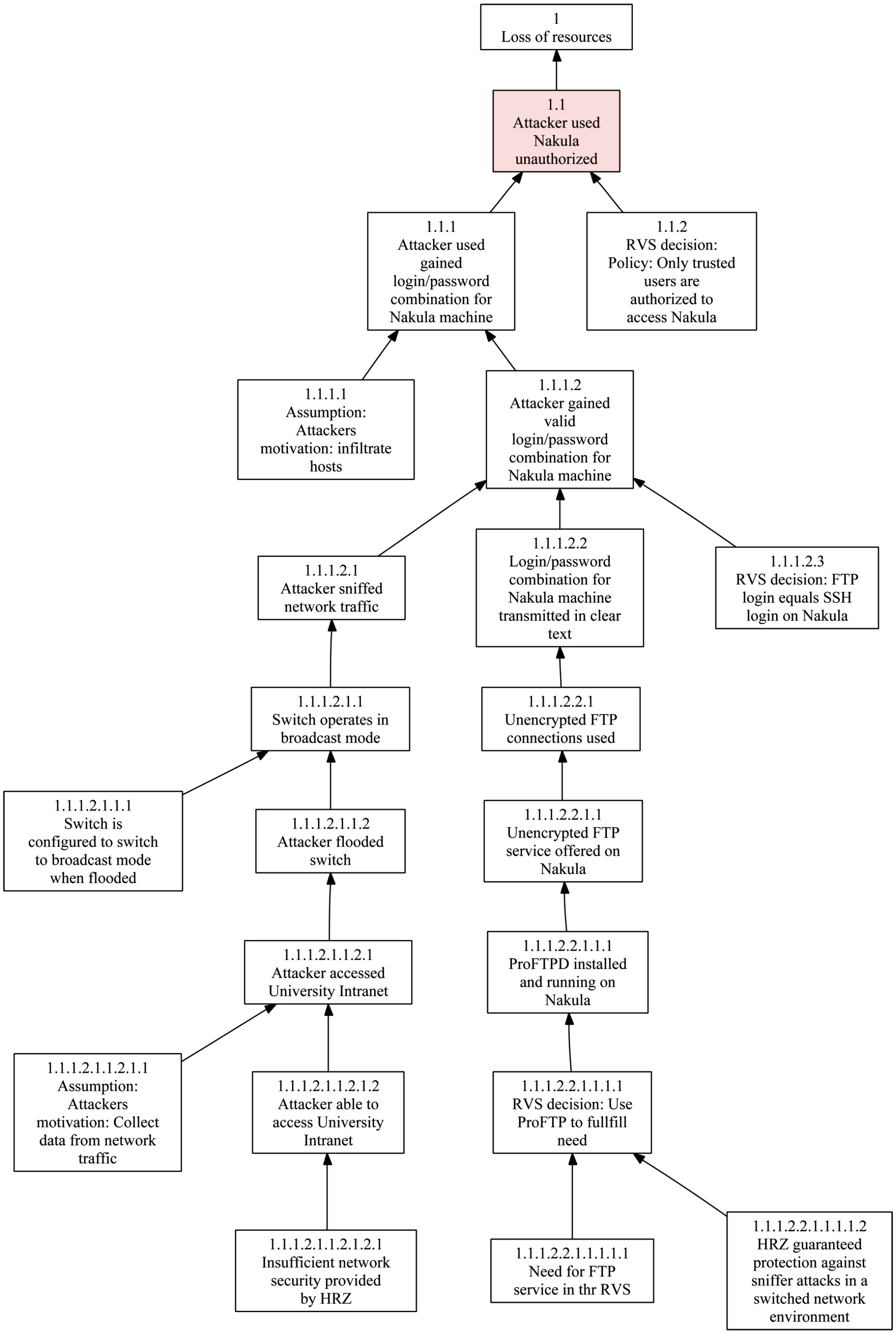
1 Loss of resources
1.1 Attacker used Nakula unauthorized
1.1.1 Attacker used gained login/password combination for Nakula machine
1.1.2 RVS decision: Policy: Only trusted users are authorized to access Nakula
1.1.1.1 Assumption: Attackers motivation: infiltrate hosts
1.1.1.2 Attacker gained valid login/password combination for Nakula machine
1.1.1.2.1 Attacker sniffed network traffic
1.1.1.2.2 Login/password combination for Nakula machine transmitted in clear text
1.1.1.2.3 RVS decision: FTP login equals SSH login on Nakula
1.1.1.2.1.1 Switch operates in broadcast mode
1.1.1.2.2.1 Unencrypted FTP connections used
1.1.1.2.1.1.1 Switch is configured to switch to broadcast mode when flooded
1.1.1.2.1.1.2 Attacker flooded switch
1.1.1.2.2.1.1 Unencrypted FTP service offered on Nakula
1.1.1.2.1.1.2.1 Attacker accessed University Intranet
1.1.1.2.2.1.1.1 ProFTPD installed and running on Nakula
1.1.1.2.1.1.2.1.1 Assumption: Attackers motivation: Collect data from network traffic
1.1.1.2.1.1.2.1.2 Attacker able to access University Intranet
1.1.1.2.2.1.1.1.1 RVS decision: Use ProFTP to fullfill need
1.1.1.2.1.1.2.1.2.1 Insufficient network security provided by HRZ
1.1.1.2.2.1.1.1.1.1 Need for FTP service in thr RVS
1.1.1.2.2.1.1.1.1.2 HRZ guaranteed protection against sniffer attacks in a switched network environment

Figure 2.13: Reformated Nakula graph using the definition of *cause*

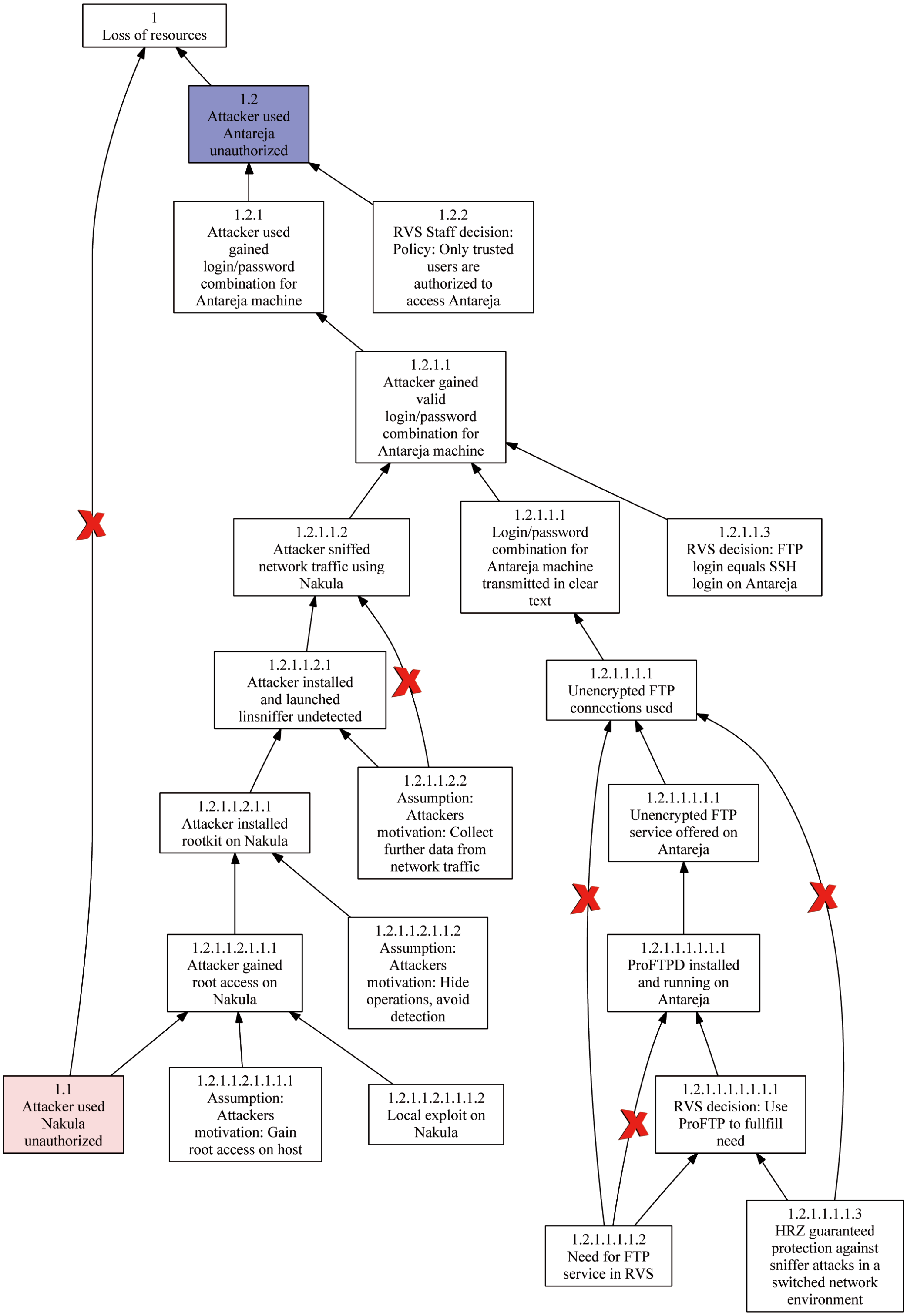
1
Loss of resources
1.2
Attacker used Antareja unauthorized
1.2.1
Attacker used gained login/password combination for Antareja machine
1.2.2
RVS Staff decision: Policy: Only trusted users are authorized to access Antareja
1.2.1.1
Attacker gained valid login/password combination for Antareja machine
1.2.1.1.2
Attacker sniffed network traffic using Nakula
1.2.1.1.1
Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.3
RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.2.1
Attacker installed and launched linsniffer undetected
1.2.1.1.1.1
Unencrypted FTP connections used
1.2.1.1.2.1.1
Attacker installed rootkit on Nakula
1.2.1.1.2.2
Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.1.1.1
Unencrypted FTP service offered on Antareja
1.2.1.1.2.1.1.1
Attacker gained root access on Nakula
1.2.1.1.2.1.1.2
Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.1.1.1.1
ProFTPD installed and running on Antareja
1.1
Attacker used Nakula unauthorized
1.2.1.1.2.1.1.1.1
Assumption: Attackers motivation: Gain root access on host
1.2.1.1.2.1.1.1.2
Local exploit on Nakula
1.2.1.1.1.1.1.1.1
RVS decision: Use ProFTP to fullfill need
1.2.1.1.1.1.2
Need for FTP service in RVS
1.2.1.1.1.1.3
HRZ guaranteed protection against sniffer attacks in a switched network environment

Figure 2.14: Antareja graph: removable edges

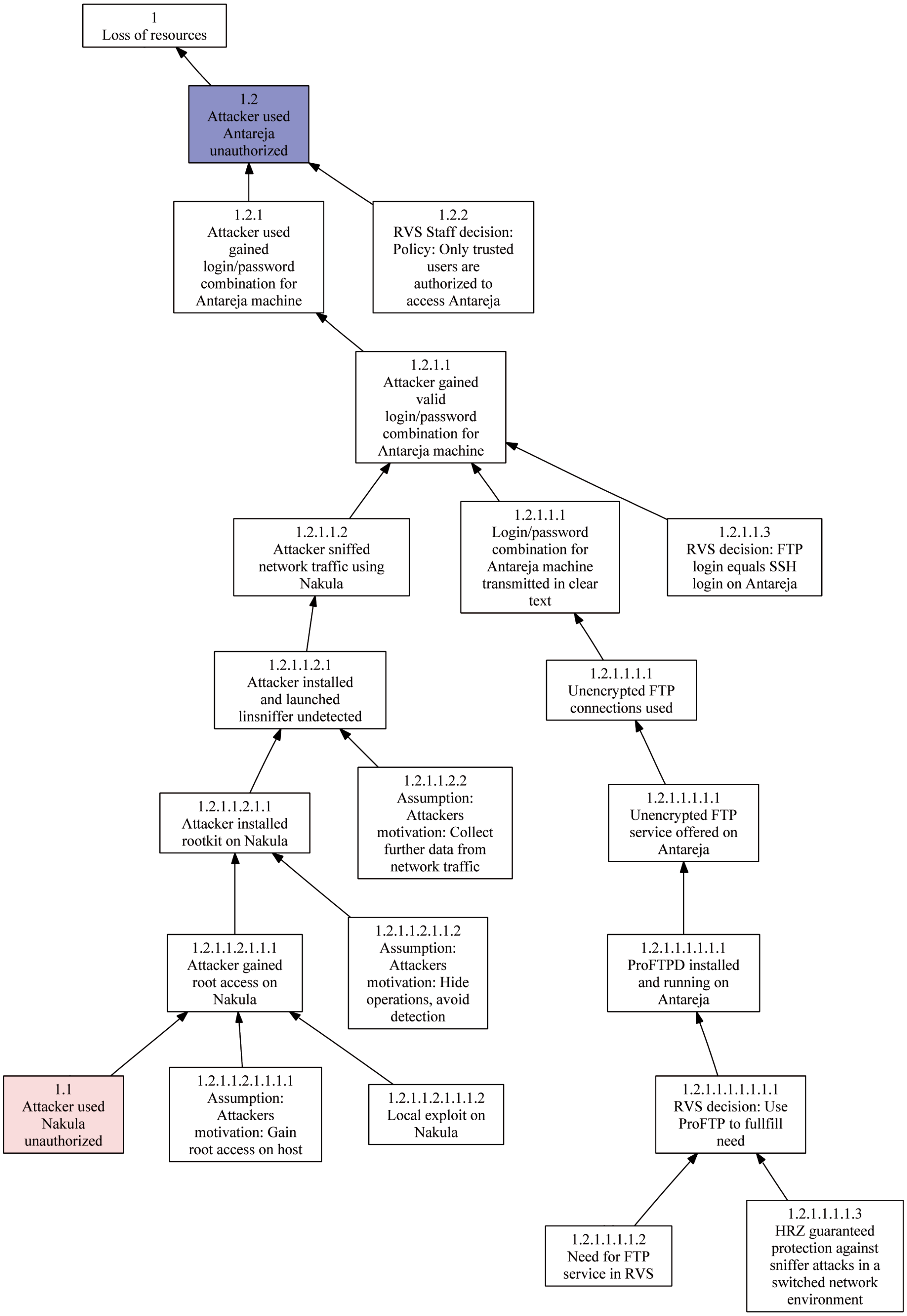
1
Loss of resources
1.2
Attacker used Antareja unauthorized
1.2.1
Attacker used gained login/password combination for Antareja machine
1.2.2
RVS Staff decision: Policy: Only trusted users are authorized to access Antareja
1.2.1.1
Attacker gained valid login/password combination for Antareja machine
1.2.1.1.2
Attacker sniffed network traffic using Nakula
1.2.1.1.1
Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.3
RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.2.1
Attacker installed and launched linsniffer undetected
1.2.1.1.1.1
Unencrypted FTP connections used
1.2.1.1.2.1.1
Attacker installed rootkit on Nakula
1.2.1.1.2.2
Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.1.1.1
Unencrypted FTP service offered on Antareja
1.2.1.1.2.1.1.1
Attacker gained root access on Nakula
1.2.1.1.2.1.1.2
Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.1.1.1.1
ProFTPD installed and running on Antareja
1.1
Attacker used Nakula unauthorized
1.2.1.1.2.1.1.1.1
Assumption: Attackers motivation: Gain root access on host
1.2.1.1.2.1.1.1.2
Local exploit on Nakula
1.2.1.1.1.1.1.1.1
RVS decision: Use ProFTP to fullfill need
1.2.1.1.1.1.1.2
Need for FTP service in RVS
1.2.1.1.1.1.1.3
HRZ guaranteed protection against sniffer attacks in a switched network environment

Figure 2.15: Antareja graph using the definition of *cause*

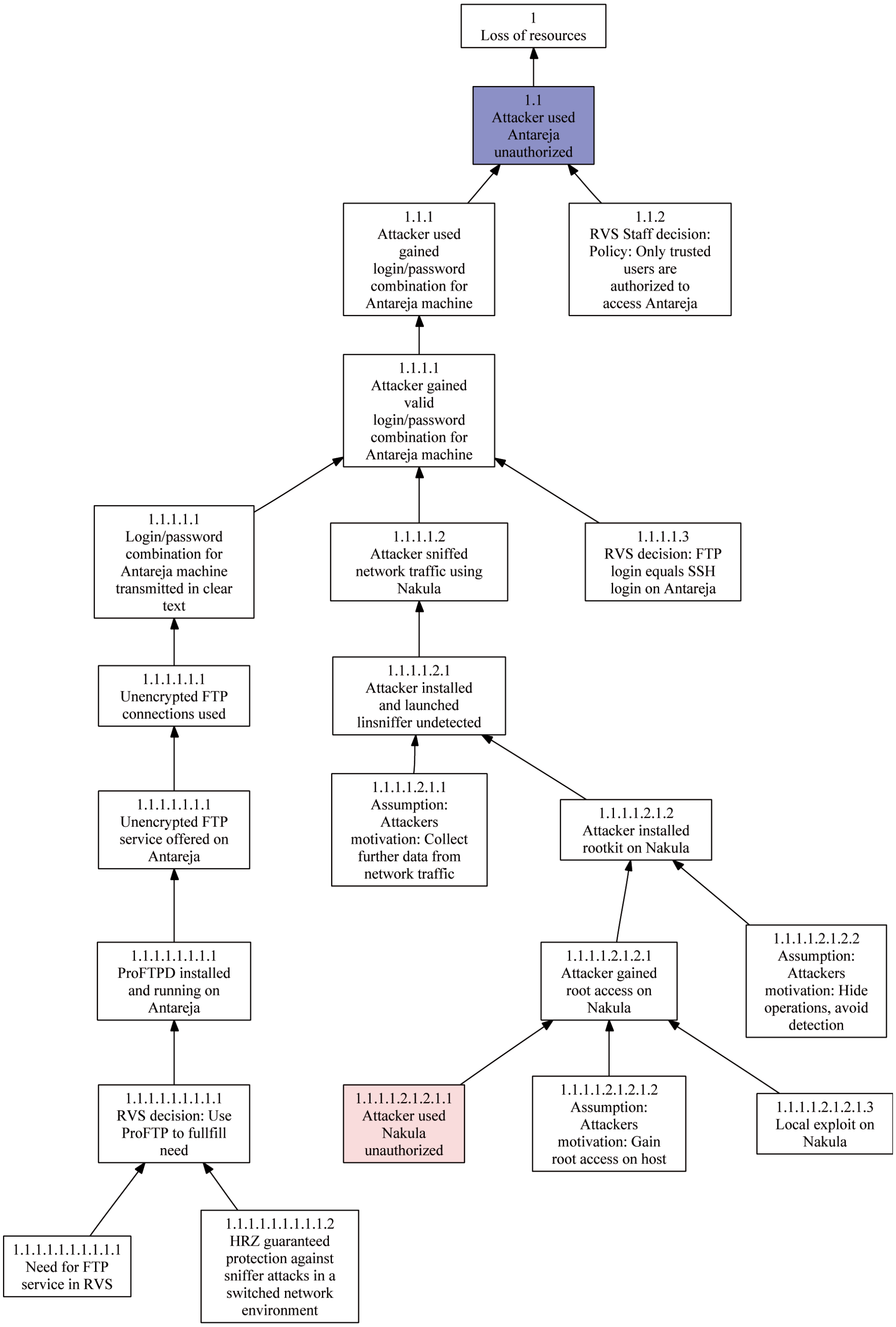

Figure 2.16: Reformated Antareja graph using the definition of *cause*

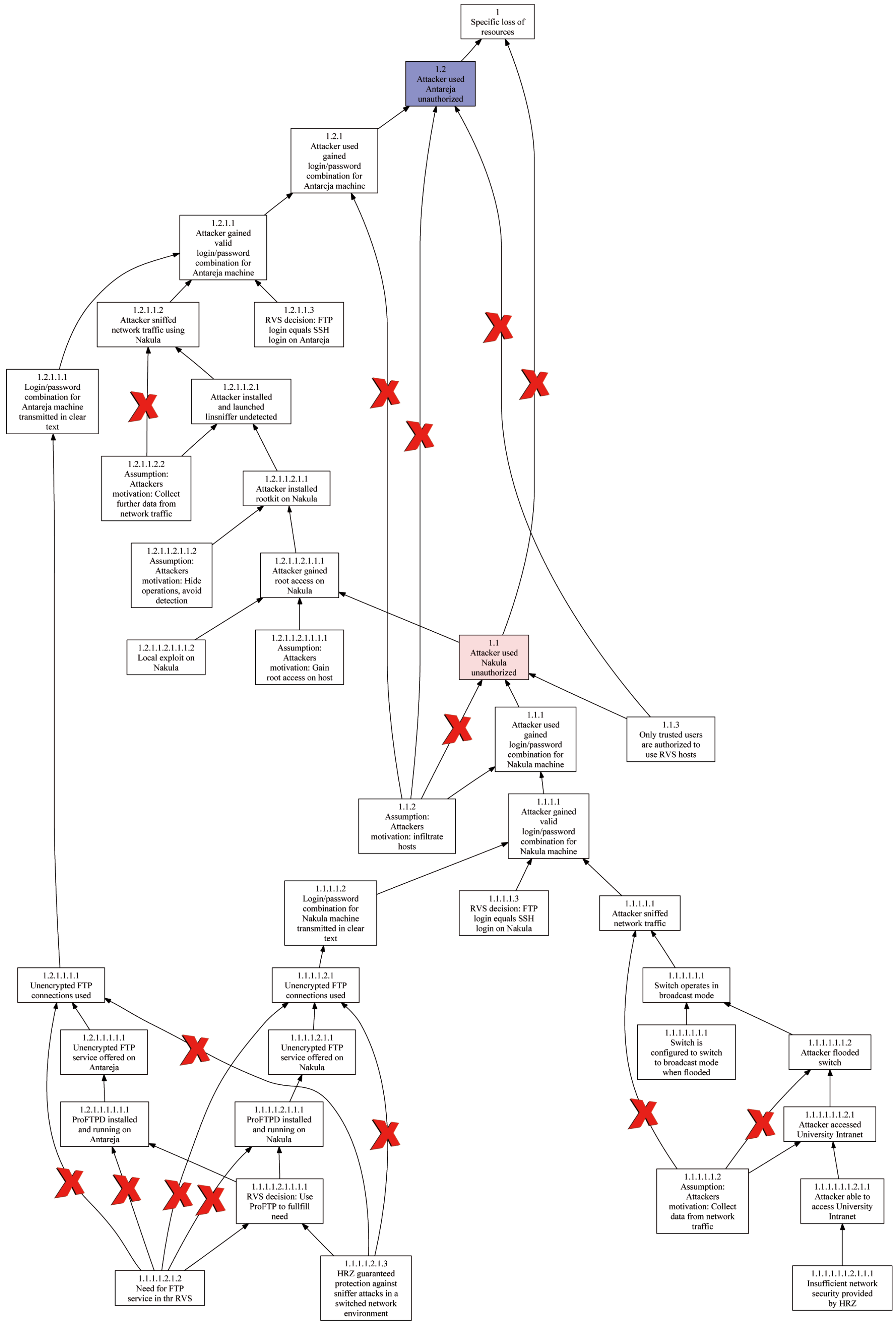
1 Specific loss of resources
1.2 Attacker used Antareja unauthorized
1.2.1 Attacker used gained login/password combination for Antareja machine
1.2.1.1 Attacker gained valid login/password combination for Antareja machine
1.2.1.1.2 Attacker sniffed network traffic using Nakula
1.2.1.1.3 RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.1 Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.2.1 Attacker installed and launched linsniffer undetected
1.2.1.1.2.2 Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.2.1.1 Attacker installed rootkit on Nakula
1.2.1.1.2.1.1.2 Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.2.1.1.1 Attacker gained root access on Nakula
1.2.1.1.2.1.1.1.2 Local exploit on Nakula
1.2.1.1.2.1.1.1.1 Assumption: Attackers motivation: Gain root access on host
1.1 Attacker used Nakula unauthorized
1.1.1 Attacker used gained login/password combination for Nakula machine
1.1.3 Only trusted users are authorized to use RVS hosts
1.1.2 Assumption: Attackers motivation: infiltrate hosts
1.1.1.1 Attacker gained valid login/password combination for Nakula machine
1.1.1.1.2 Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3 RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1 Attacker sniffed network traffic
1.2.1.1.1.1 Unencrypted FTP connections used
1.1.1.1.2.1 Unencrypted FTP connections used
1.1.1.1.1.1 Switch operates in broadcast mode
1.2.1.1.1.1.1 Unencrypted FTP service offered on Antareja
1.1.1.1.2.1.1 Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.1 Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.2 Attacker flooded switch
1.2.1.1.1.1.1.1 ProFTPD installed and running on Antareja
1.1.1.1.2.1.1.1 ProFTPD installed and running on Nakula
1.1.1.1.1.1.2.1 Attacker accessed University Intranet
1.1.1.1.2.1.1.1.1 RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.2 Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.1.1.2.1.1 Attacker able to access University Intranet
1.1.1.1.2.1.3 HRZ guaranteed protection against sniffer attacks in a switched network environment
1.1.1.1.2.1.2 Need for FTP service in thr RVS
1.1.1.1.1.1.2.1.1.1 Insufficient network security provided by HRZ

Figure 2.17: Nakula & Antareja graph: removable edges

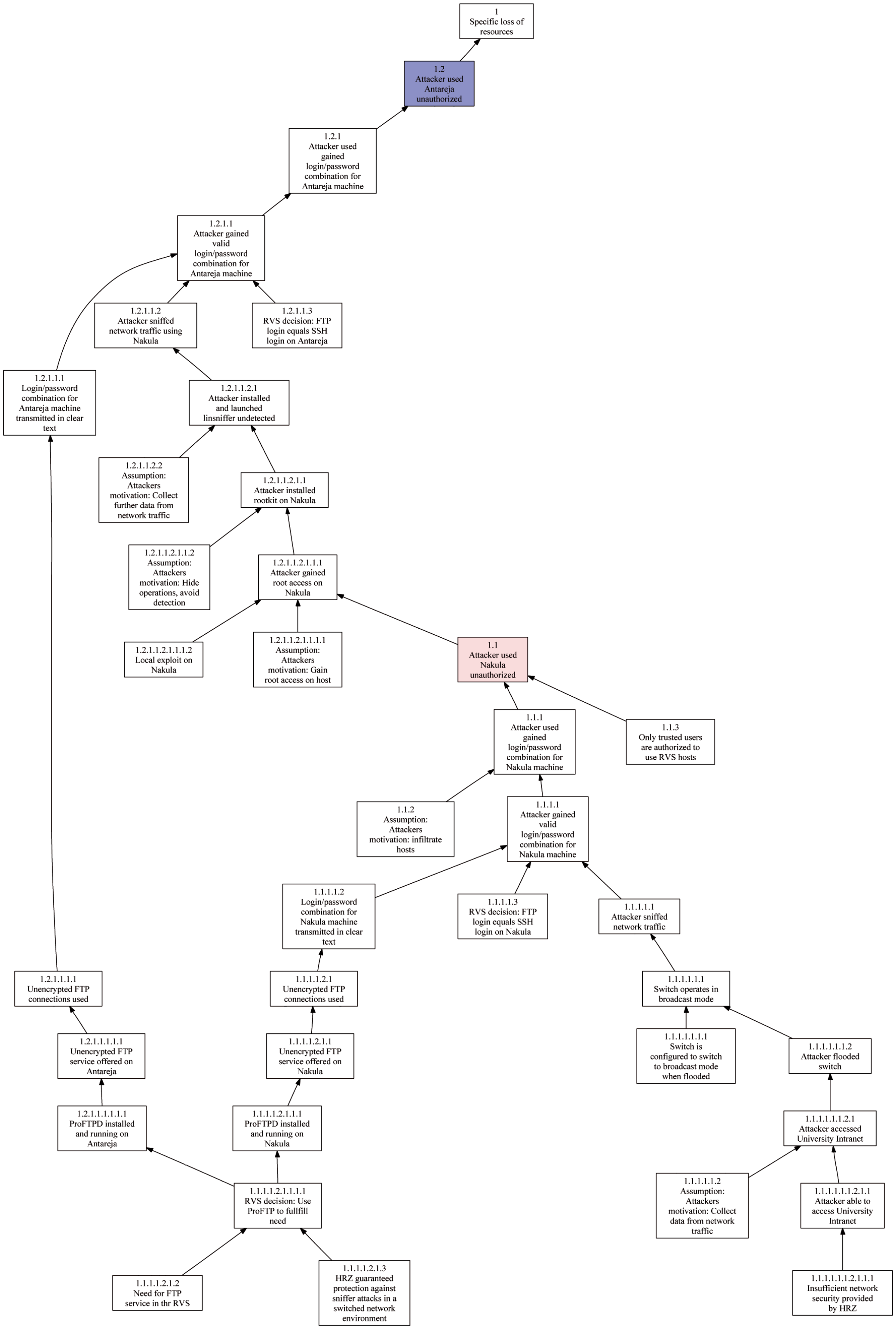
1
Specific loss of resources
1.2
Attacker used Antareja unauthorized
1.2.1
Attacker used gained login/password combination for Antareja machine
1.2.1.1
Attacker gained valid login/password combination for Antareja machine
1.2.1.1.2
Attacker sniffed network traffic using Nakula
1.2.1.1.3
RVS decision: FTP login equals SSH login on Antareja
1.2.1.1.1
Login/password combination for Antareja machine transmitted in clear text
1.2.1.1.2.1
Attacker installed and launched linsniffer undetected
1.2.1.1.2.2
Assumption: Attackers motivation: Collect further data from network traffic
1.2.1.1.2.1.1
Attacker installed rootkit on Nakula
1.2.1.1.2.1.1.2
Assumption: Attackers motivation: Hide operations, avoid detection
1.2.1.1.2.1.1.1
Attacker gained root access on Nakula
1.2.1.1.2.1.1.1.2
Local exploit on Nakula
1.2.1.1.2.1.1.1.1
Assumption: Attackers motivation: Gain root access on host
1.1
Attacker used Nakula unauthorized
1.1.1
Attacker used gained login/password combination for Nakula machine
1.1.3
Only trusted users are authorized to use RVS hosts
1.1.2
Assumption: Attackers motivation: infiltrate hosts
1.1.1.1
Attacker gained valid login/password combination for Nakula machine
1.1.1.1.2
Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.3
RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.1
Attacker sniffed network traffic
1.2.1.1.1.1
Unencrypted FTP connections used
1.1.1.1.2.1
Unencrypted FTP connections used
1.1.1.1.1.1
Switch operates in broadcast mode
1.2.1.1.1.1.1
Unencrypted FTP service offered on Antareja
1.1.1.1.2.1.1
Unencrypted FTP service offered on Nakula
1.1.1.1.1.1.1
Switch is configured to switch to broadcast mode when flooded
1.1.1.1.1.1.2
Attacker flooded switch
1.2.1.1.1.1.1.1
ProFTPD installed and running on Antareja
1.1.1.1.2.1.1.1
ProFTPD installed and running on Nakula
1.1.1.1.1.1.2.1
Attacker accessed University Intranet
1.1.1.1.2.1.1.1.1
RVS decision: Use ProFTP to fullfill need
1.1.1.1.1.2
Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.1.1.2.1.1
Attacker able to access University Intranet
1.1.1.1.2.1.2
Need for FTP service in thr RVS
1.1.1.1.2.1.3
HRZ guaranteed protection against sniffer attacks in a switched network environment
1.1.1.1.1.1.2.1.1.1
Insufficient network security provided by HRZ

Figure 2.18: Nakula & Antareja graph using the definition of *cause*

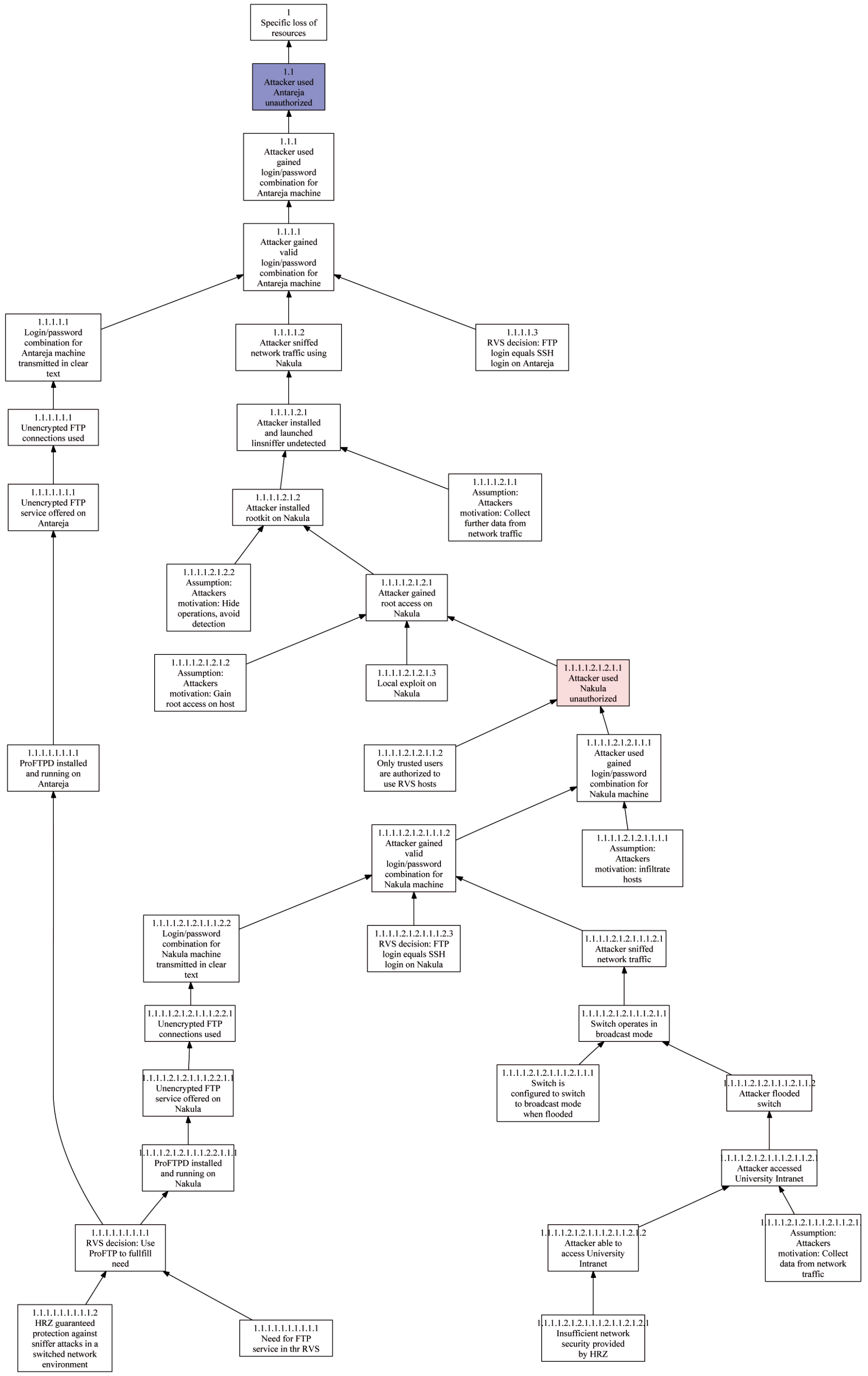
1 Specific loss of resources
1.1 Attacker used Antareja unauthorized
1.1.1 Attacker used gained login/password combination for Antareja machine
1.1.1.1 Attacker gained valid login/password combination for Antareja machine
1.1.1.1.1 Login/password combination for Antareja machine transmitted in clear text
1.1.1.1.2 Attacker sniffed network traffic using Nakula
1.1.1.1.3 RVS decision: FTP login equals SSH login on Antareja
1.1.1.1.1.1 Unencrypted FTP connections used
1.1.1.1.2.1 Attacker installed and launched linsniffer undetected
1.1.1.1.1.1.1 Unencrypted FTP service offered on Antareja
1.1.1.1.2.1.2 Attacker installed rootkit on Nakula
1.1.1.1.2.1.1 Assumption: Attackers motivation: Collect further data from network traffic
1.1.1.1.2.1.2.2 Assumption: Attackers motivation: Hide operations, avoid detection
1.1.1.1.2.1.2.1 Attacker gained root access on Nakula
1.1.1.1.2.1.2.1.2 Assumption: Attackers motivation: Gain root access on host
1.1.1.1.2.1.2.1.3 Local exploit on Nakula
1.1.1.1.2.1.2.1.1 Attacker used Nakula unauthorized
1.1.1.1.1.1.1.1.1 ProFTPD installed and running on Antareja
1.1.1.1.2.1.2.1.1.2 Only trusted users are authorized to use RVS hosts
1.1.1.1.2.1.2.1.1.1 Attacker used gained login/password combination for Nakula machine
1.1.1.1.2.1.2.1.1.1.2 Attacker gained valid login/password combination for Nakula machine
1.1.1.1.2.1.2.1.1.1.1 Assumption: Attackers motivation: infiltrate hosts
1.1.1.1.2.1.2.1.1.1.2.2 Login/password combination for Nakula machine transmitted in clear text
1.1.1.1.2.1.2.1.1.1.2.3 RVS decision: FTP login equals SSH login on Nakula
1.1.1.1.2.1.2.1.1.1.2.1 Attacker sniffed network traffic
1.1.1.1.2.1.2.1.1.1.2.2.1 Unencrypted FTP connections used
1.1.1.1.2.1.2.1.1.1.2.1.1 Switch operates in broadcast mode
1.1.1.1.2.1.2.1.1.1.2.2.1.1 Unencrypted FTP service offered on Nakula
1.1.1.1.2.1.2.1.1.1.2.1.1.1 Switch is configured to switch to broadcast mode when flooded
1.1.1.1.2.1.2.1.1.1.2.1.1.2 Attacker flooded switch
1.1.1.1.2.1.2.1.1.1.2.2.1.1.1 ProFTPD installed and running on Nakula
1.1.1.1.2.1.2.1.1.1.2.1.1.2.1 Attacker accessed University Intranet
1.1.1.1.1.1.1.1.1.1 RVS decision: Use ProFTP to fullfill need
1.1.1.1.2.1.2.1.1.1.2.1.1.2.1.2 Attacker able to access University Intranet
1.1.1.1.2.1.2.1.1.1.2.1.1.2.1.1 Assumption: Attackers motivation: Collect data from network traffic
1.1.1.1.1.1.1.1.1.1.2 HRZ guaranteed protection against sniffer attacks in a switched network environment
1.1.1.1.1.1.1.1.1.1.1 Need for FTP service in thr RVS
1.1.1.1.2.1.2.1.1.1.2.1.1.2.1.2.1 Insufficient network security provided by HRZ

Figure 2.19: Reformated Nakula & Antareja graph using the definition of *cause*

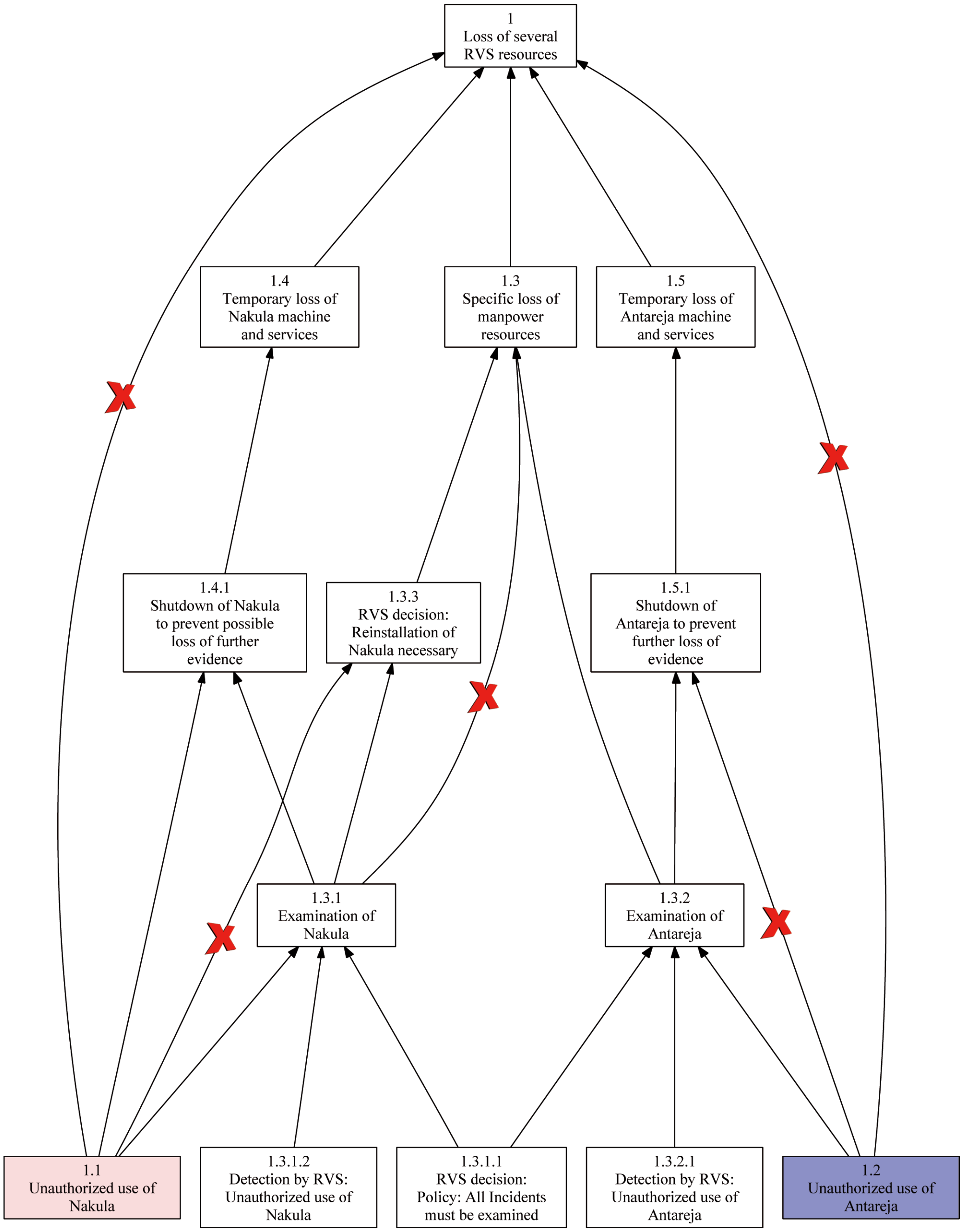
1
Loss of several RVS resources
1.4
Temporary loss of Nakula machine and services
1.3
Specific loss of manpower resources
1.5
Temporary loss of Antareja machine and services
1.4.1
Shutdown of Nakula to prevent possible loss of further evidence
1.3.3
RVS decision: Reinstallation of Nakula necessary
1.5.1
Shutdown of Antareja to prevent further loss of evidence
1.3.1
Examination of Nakula
1.3.2
Examination of Antareja
1.1
Unauthorized use of Nakula
1.3.1.2
Detection by RVS: Unauthorized use of Nakula
1.3.1.1
RVS decision: Policy: All Incidents must be examined
1.3.2.1
Detection by RVS: Unauthorized use of Antareja
1.2
Unauthorized use of Antareja

Figure 2.20: RVSLoss graph: removable edges

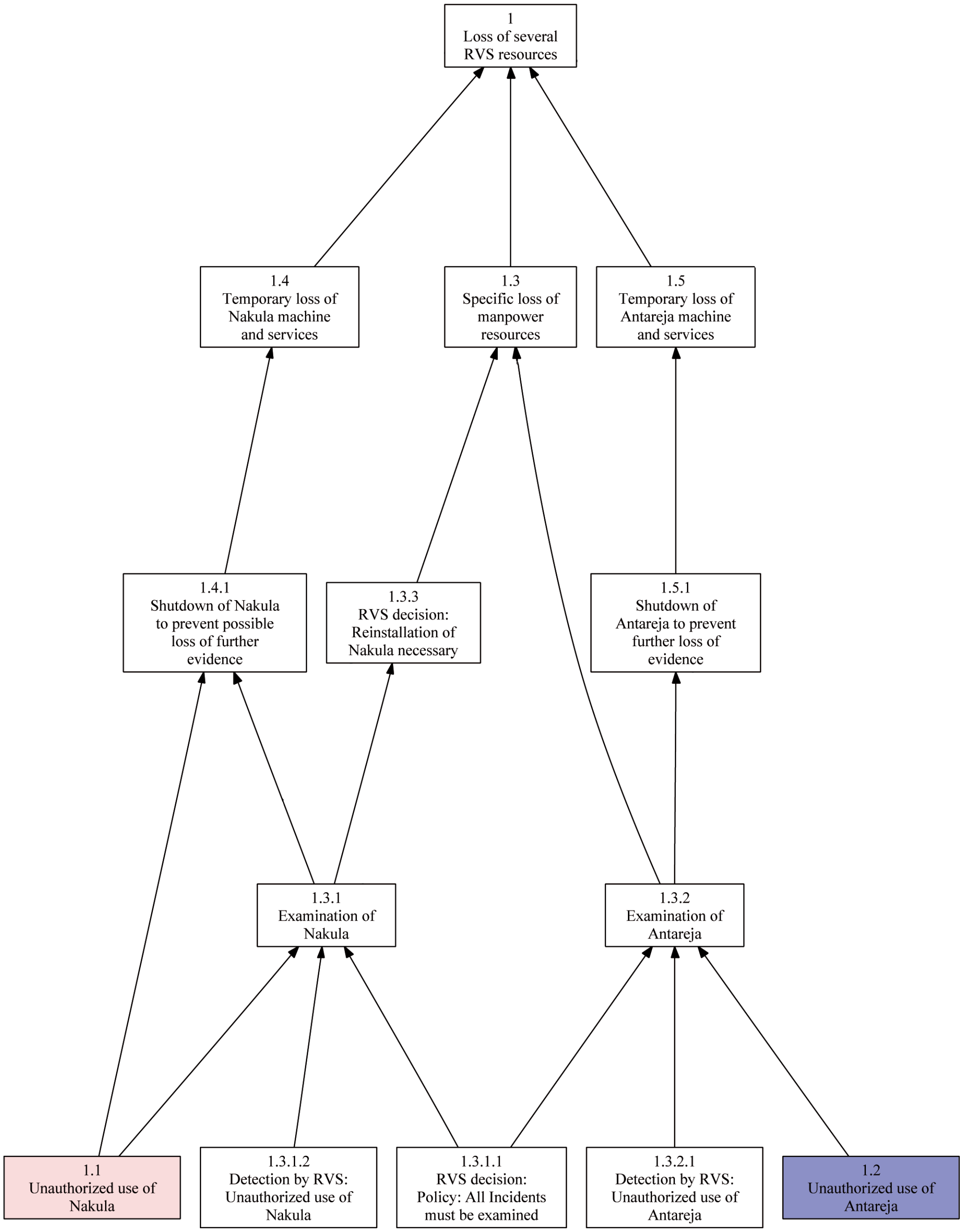
1
Loss of several RVS resources
1.4
Temporary loss of Nakula machine and services
1.3
Specific loss of manpower resources
1.5
Temporary loss of Antareja machine and services
1.4.1
Shutdown of Nakula to prevent possible loss of further evidence
1.3.3
RVS decision: Reinstallation of Nakula necessary
1.5.1
Shutdown of Antareja to prevent further loss of evidence
1.3.1
Examination of Nakula
1.3.2
Examination of Antareja
1.1
Unauthorized use of Nakula
1.3.1.2
Detection by RVS: Unauthorized use of Nakula
1.3.1.1
RVS decision: Policy: All Incidents must be examined
1.3.2.1
Detection by RVS: Unauthorized use of Antareja
1.2
Unauthorized use of Antareja

Figure 2.21: RVSLoss graph using the definition of *cause*

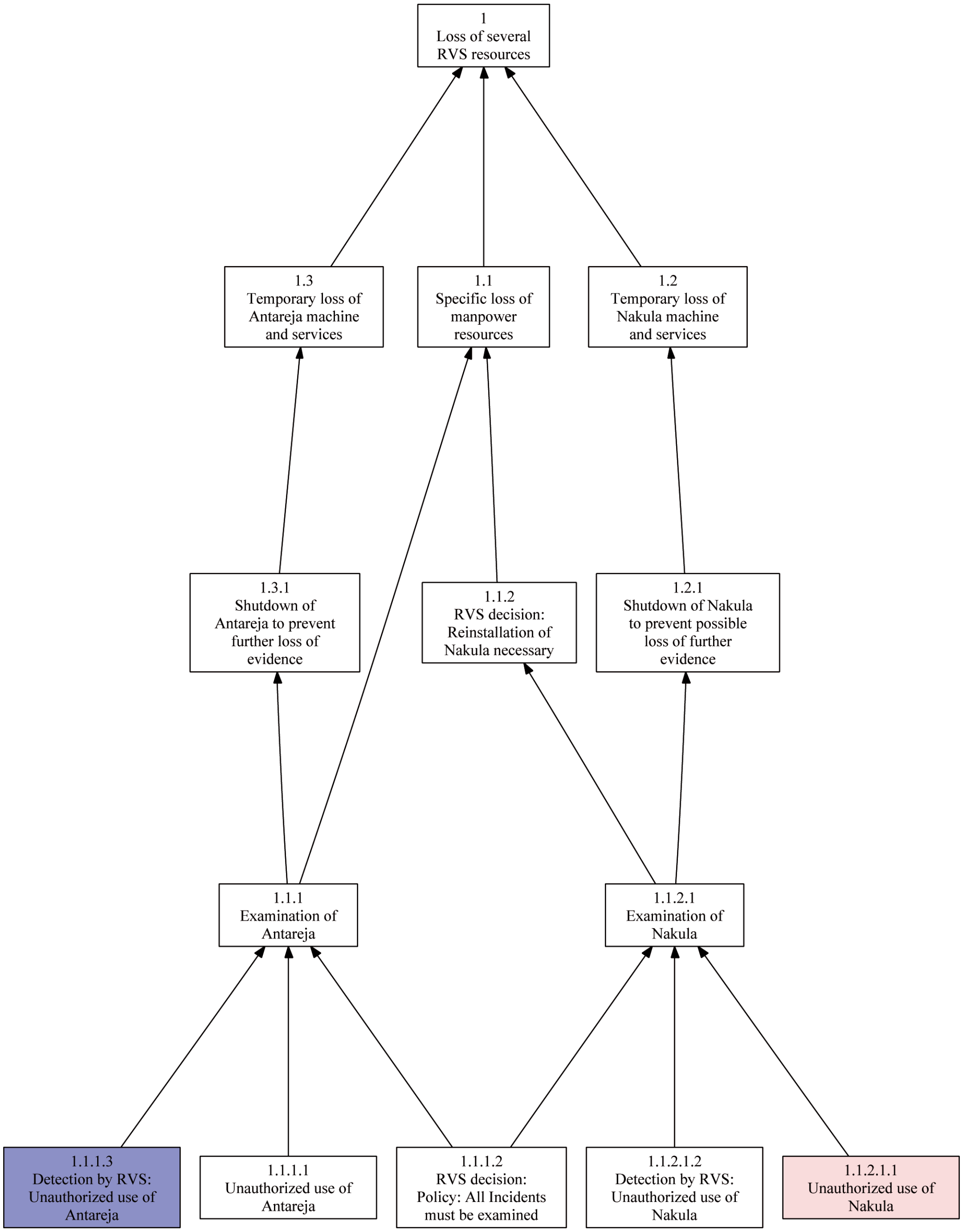
1
Loss of several RVS resources
1.3
Temporary loss of Antareja machine and services
1.1
Specific loss of manpower resources
1.2
Temporary loss of Nakula machine and services
1.3.1
Shutdown of Antareja to prevent further loss of evidence
1.1.2
RVS decision: Reinstallation of Nakula necessary
1.2.1
Shutdown of Nakula to prevent possible loss of further evidence
1.1.1
Examination of Antareja
1.1.2.1
Examination of Nakula
1.1.1.3
Detection by RVS: Unauthorized use of Antareja
1.1.1.1
Unauthorized use of Antareja
1.1.1.2
RVS decision: Policy: All Incidents must be examined
1.1.2.1.2
Detection by RVS: Unauthorized use of Nakula
1.1.2.1.1
Unauthorized use of Nakula

Figure 2.22: Reformated RVSLoss graph using the definition of *cause*

2.5.4 Focussing on the important nodes

We have included a total of 22 WB-Graphs in this document. Looking at such a mass of nodes and graphs, we started thinking about possible formalisms which could help to focus on the important events and facts in a WB-Graph. We came up with three criteria:

- Quantity of in- and out-going edges (InOut)
  Nodes with many edges must obviously exert important causal influence.
- "Single point of failure" (SPoF)
  The chain of events runs through this node, it must be a significant factor.
- Leaves (Lf)
  Notes without precursors are root causes for the accident. Mitigating these often circumvents many other accidents as well.

If we apply these criteria as well as the blending out of the uncontrollable facts as stated in chapter 2.5.2, we have good chances to reduce the amount of interesting facts by far. The complete graph counts a total of 49 nodes, after the application of the control areas 31 nodes remain.

Note: These formal criteria are simple and can be applied without the use of intuition. That means they can be smoothly implemented within a program, which reduces the amount of any WB-Graph without you raising only one finger.

After the execution of the criteria given (with in-/out egdes >3), we end up with the following factors:

- Node 1.2.1.1.3:
  RVS decision: FTP Login equals SSH Login on Antareja $_{(Lf)}$
- Node 1.2.1.1.2.1.1.1.2:
  Local exploit on Nakula $_{(Lf)}$
- Node 1.1.1.1:
  Attacker gained valid login/password comb. for Nakula machine $_{(SPoF)}$
- Node 1.2.1.1:
  Attacker gained valid login/password comb. for Antareja machine$_{(SPoF)}$

- Node 1.1.1.1.3:
  RVS decision: FTP Login equals SSH Login on Nakula $_{(Lf)}$
- Node 1.1.1.1.2.1:
  Unencrypted FTP connections used on Nakula $_{(4xInOut)}$
- Node 1.2.1.1.1.1:
  Unencrypted FTP connections used on Antareja $_{(4xInOut)}$
- Node 1.1.1.1.1.1.1.1:
  Switch is configured to switch to broadcast mode when flooded $_{(Lf)}$
- Node 1.1.1.1.2.1.1.1.1:
  RVS decision: Use ProFTP to fullfill need $_{(4xInOut)}$
- Node 1.1.1.1.2.1.3:
  HRZ guaranteed protection against sniffer attacks $_{(Lf+(3xInOut))}$
- Node 1.1.1.1.1.1.2.1.1.1:
  Insufficient network security provided by HRZ $_{(Lf)}$

The following facts meet the criteria, but we can intuitively judge that their direct elimination would not solve the problem:

- Node 1.3.1.1:
  Examination of Antareja $_{(5xInOut)}$
- Node 1.4.2:
  Examination of Nakula $_{(6xInOut)}$
- Node 1.3.1.1.2:
  Detection by RVS: Unauthorized use of Antareja $_{(Lf)}$
- Node 1.4.2.1:
  Detection by RVS: Unauthorized use of Antareja $_{(Lf)}$
- Node 1.3.1.1:
  RVS decision: Policy: All incidents must be examined $_{(Lf)}$
- Node 1.1.3:
  Only trusted users are authorized to use RVS hosts $_{(Lf)}$

- Node 1.1.1.1.2.1.2:
  Need for FTP service in the RVS $_{(5xInOut,Lf)}$

Starting with 49 nodes, we could isolate 18 nodes (and even 11 with a little intuition) which we might regard as important in our graph just by marking out non-controllable nodes and applying the formal criteria. That's a reduction of over 50% just by following some easy rules and a reduction of over 75% by looking and seeing. Cool.

Chapter 3

Conclusions

Despite the problems occurring during the analysis, we are able to determine one single-point of failure: The attacker was able to obtain valid usernames and passwords for Nakula and Antareja by sniffing the network traffic. This was made possible due to the fact that the affected computer systems in the RVS offered unencrypted FTP services. The RVS staff trusted the HRZ's assertion that the switched network infrastructure provided by them would not allow a sniffer attack and used ProFTPD to fulfil their need for a file transfer service.

During the log-in procedure of a FTP-session, username and password are transmitted unencrypted. By that reason, the attacker could read the clear text log-in data out of the sniffed data packets contrary to the HRZ's assertion. Thereafter he was able to log in and use the machines for his intentions.

3.1 Recommendations

So our recommendation is dual. First, the RVS should avoid the usage of unencrypted ftp-services. Second, rely conditions (like the one given by the HRZ) as basis for security-related decisions should be checked more thoroughly in the future. If these two circumstances had been eliminated before, this accident would not have been be possible. In fact they have been eliminated today and no clear-text login procedures to RVS machines are possible any more.

Independently from the RVS - further actions would also be applicable to prevent those incidents. One possibility is to make use of an Intrusion Detection System (IDS) or take precautions regarding network sniffing, but the recommendations given above are directly derived from the WB-Graph and thus evident. They are easy and reasonable to put into action and anyone can look at the graph and see that the mitigation removes nodes sufficient for all the consequent nodes and so for the accident itself.

3.2 Results of the WBA compared with the forensic analysis

As mentioned in the conclusions of the forensic report 1.5.3, the two authors suggested the usage of an IDS and other useful improvements to network security and forensics. What they did not express is, that the usage of unencrypted ftp-service was a crucial but simply removable factor to the whole story. Though the analysts were experienced and knew what they were dealing with, this analysis shows that intuition often omits conditions and facts. One reason for this might be that intuitive judgement is massively affected by the point of view - in this case by the point of view of a forensic analyst. Intuition might suggest the right steps, but the proof why these steps should be the right ones is missing.

The decision to install the FTP service was taken on the basis of the rely guarantee from the HRZ. This incident showed that the HRZ could not hold their guarantee and so all policy decisions based on this guarantee were potentially insecure. This WB-Analysis showed this straight forward. Without the HRZ guarantee, the RVS administrative staff might have taken another option to fulfil their need for file transfer services, e.g. they could have used sftp or other secure file transfer techniques like scp. Another problem was the configuration of the switches. The switches could have been configured to not allow spoofing techniques, but they have not been. This point in fact was one reason why the HRZ guarantee was obviously false and not justified. Even long time after the incident spoofing and sniffing was further possible, which showed that this incident was not even noticed - or when it was, that no actions had been taken by the HRZ.

3.3 WBA as a proper method for security-related incidents

Our work and this report shows that WBA applied on security-related incidents leads straight forward to the same objective result as it does for safety-related incidents. Also, no sophisticated mathematical skills or similar are necessary for a basic WBA, you just have to follow the method which can lead to different conclusions than intuitive judgement, with the difference that these objective conclusions are hard to counter because they are based on formal logic and semantics.

Appendix A

Acknowledgments

We would like to thank I Made Wiranya and Avinanta Tarigan for providing the report, helping us with the necessary technological background and answering our questions. Also we like to thank the whole RVS group, especially Jan Sanders, for critique and hints during our work.

Appendix B

Used Tools

During our work we used several tools including *ciedit* and *ybedit* for constructing the WB-Graphs, *Adobe Photoshop* for colouring and modifying the postscript graphics, *OpenOffice* for all document work like developing the list of facts and LaTeX which was used for typesetting this document.

List of Figures

Bibliography

[1] *Forensic Analysis on Nakula and Antareja Machine*
I Made Wiryana, Avinanta Tarigan, 2002.

[2] *A Quick Introduction to Why-Because Analysis*,
Peter B. Ladkin,
http://www.rvs.uni-bielefeld.de/research/WBA/introWB.ps
accessed 04.04.2005

[3] *Causal System Analysis. Formal Reasoning About Safety And Failure. Draft Version 2.0*,
Peter B. Ladkin,
2001, available from Author; to be published.

[4] *Causation*
David Lewis
In *Journal of Philosophy 70*, 1973, pages 556-67
And *Philosophical Papers, Volume II*, Oxford University Press, 1987