WB-Analysis of the Nakula & Antareja Incident

A WB-Analysis of a system security-related incident

5.5th Bieleschweig Workshop
Bielefeld, June 6-7 2005

R|V|S
Rechnernetze und Verteilte Systeme

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Overview

- Introduction
- The WB-Analysis
- Conclusion
- Discussion

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Summary of the Incident

- 18th January 2002
  - Student “koko" from Jakarta was working on Nakula
  - He noticed users “made" and “root" working on the system
  - So he tried to contact “made" but got no response
  - After several tries he informed the RVS
- 18th January 2002, 22:56
  - “made" logged in on Nakula remotely and found anomalies:
    - sshd delivered no service to clients outside the RVS network
    - sendmail was getting down frequently
    - Remote connection through ARCOR-ISP was very slow
  - “made" informed “avinanta"

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Summary of the Incident

- 18th January 2002, 23:05
  - “avinanta” logged in on Nakula remotely and tried to find the source of the abnormal behaviour
  - He logged in on Antareja and realized that sendmail was influenced by a strange .procmail in /home/avinanta containing a program, which was used to gain root access
  - He also discovered several strange files, including root kit files
  - “avinanta” and “made” both agreed that the systems must have been cracked

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Summary of the Incident

- 19th January 2002, 00:40
  - Check of /var/log showed that all log files had been deleted
  - Both machines were shutdown immediately to prevent the intruder from deleted any evidence he had left on the machines
- 19th January 2002, 00:50
  - RVS received notification about mass-scans:
    - From Techfak administrator about scans targeting hosts belonging to the Techfak network

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Presentation of the systems

- Nakula
  - Profile of the Nakula machine
    - Operating System: SuSE Linux 7.2, Kernel 2.4.4
    - Apache 1.3.12, PHP 4.2.06
    - Sendmail, SMTP, POP3, IMAP
    - OpenSSH, ProFTP
    - MySQL
  - Not more than 10 active users
  - One of the most popular sites about information technology in Indonesia

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Presentation of the systems

- Antareja
  - Profile of the Antareja machine
    - Operating System: SuSE Linux 7.3, Kernel 2.4.10
    - Apache 1.3.12, PHP 4.2.06
    - Sendmail, SMTP, POP3, IMAP
    - OpenSSH, ProFTP
    - PostgreSQL
  - New machine, active since December 2001
  - Used to test video conference connection between Bielefeld and Jakarta
  - Not well known, few active users

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Presentation of the systems

- Infrastructure
  - Both machines are directly connected to the Internet via switches provided by the Hochschulrechenzentrum (HRZ)
  - No central perimeter firewall
  - No Intrusion Detection System
  - HRZ guarantee:
    Sniffing of network traffic in the switched universities network environment not possible!

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Problems performing the forensics

- Lack of valid evidence
  - Intruder deleted log-files
  - Log-files could only be partially recovered
  - Intruder tried to cover his traces
  - Intruders motivation not obvious
- Leads to different possible attack scenarios
  - Analysts tried to reconstruct the chain of events by simulating the attack based on the tools and evidences found on the machines
  - Results in the conviction, that only one attack scenario was possible

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Only possible attack scenario

- Getting started
  - Intruder had access to universities 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

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Only possible attack scenario

- On Nakula machine
  - No applicable SuSE 7.2 remote exploit was known at that time (e.g. no lpd installed)
  - He must have used an local exploit to gain root access (suid exploit)
  - Installed root kit
  - Launched sniffer attack on the network
  - Gained login/password combination for Antareja machine
- On Antareja machine
  - He tried to use same exploits also used on Nakula, but was not successful due to usage of SuSE 7.3 on Antareja
  - He was not successful to gain root access on Antareja, although he tried until he was discovered

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Conclusion of the forensic analysis

- 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 attack
- Switched network environments
  - Do not always guarantee sniffing protection
- Probable intruders identity:
  - Romanian hacker tazmania using his own root kit

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Conclusion of the forensic analysis

- Suggested improvements:
  - University level Intrusion Detection System
  - Better log-mechanisms, e.g. usage of an external log-server
  - Mechanism to notify system administrator
  - Development of proper security policies

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Part II:

The WB-Analysis

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

What makes this WB-Analysis different?

- Security-related incident
  - Most WB-Analyses have been safety-related
  - Many facts are not clearly observable and are based on plausible and coherent assumptions (including the attackers motivations)
  - Behaviour of the system precipitated by intruder
- High level of human interaction
  - Intruders motivation was necessary for this incident to happen
  - Missing of rule-based behaviour makes the modelling of the human agent difficult
  - Intruder able to adapt his procedures
  - System worked as specified

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

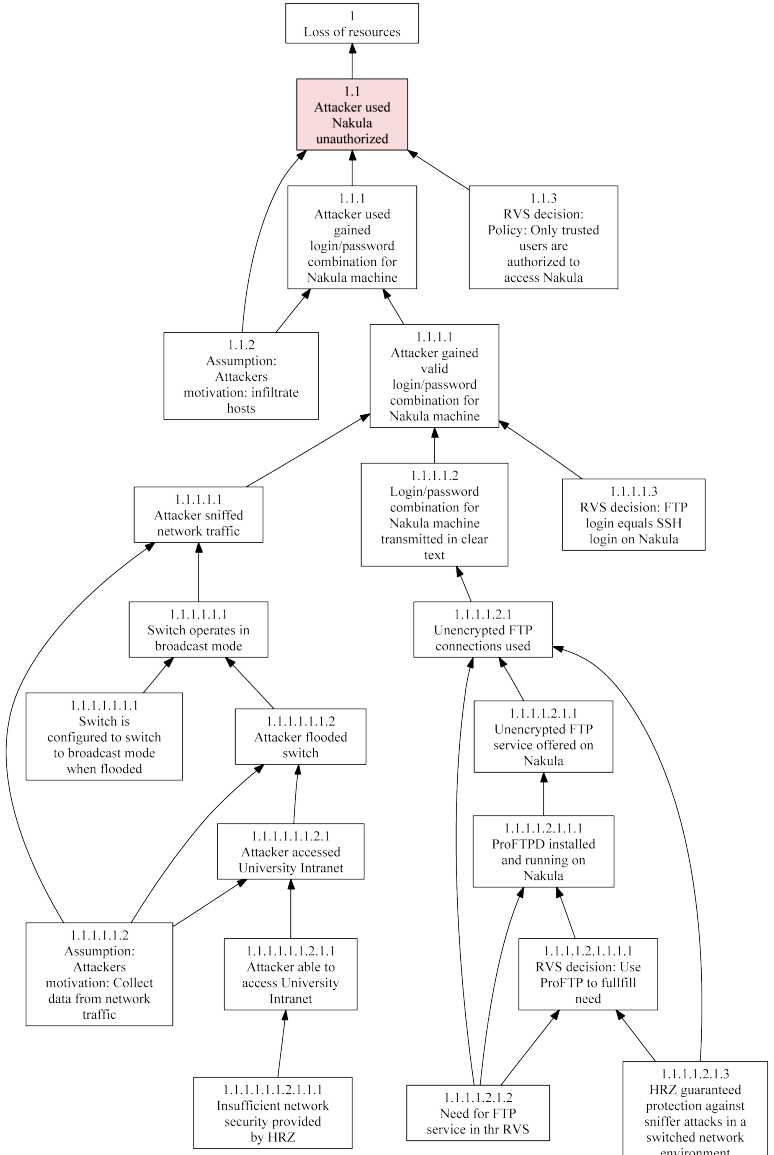
What is considered to be the accident?

- Possibilities:
  - Loss of system-resources?
  - Cost of money?
  - Loss of manpower?
  - Infiltration of systems by Intruder?
  - …
- Choice: Loss of (RVS-) resources (in general)
  - But: This abstract definition of the accident leads to several WB-Graphs, as we will see

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

The Nakula graph

- Accident: Loss of (system) resources
- Necessary causal factor for the accident:
  - *1.1: "Unauthorized use of Nakula"* alone is a sufficient causal factor for a not further specified *"Loss of resources"*
- All other graphs require a more specific definition of *"Loss of resources"*



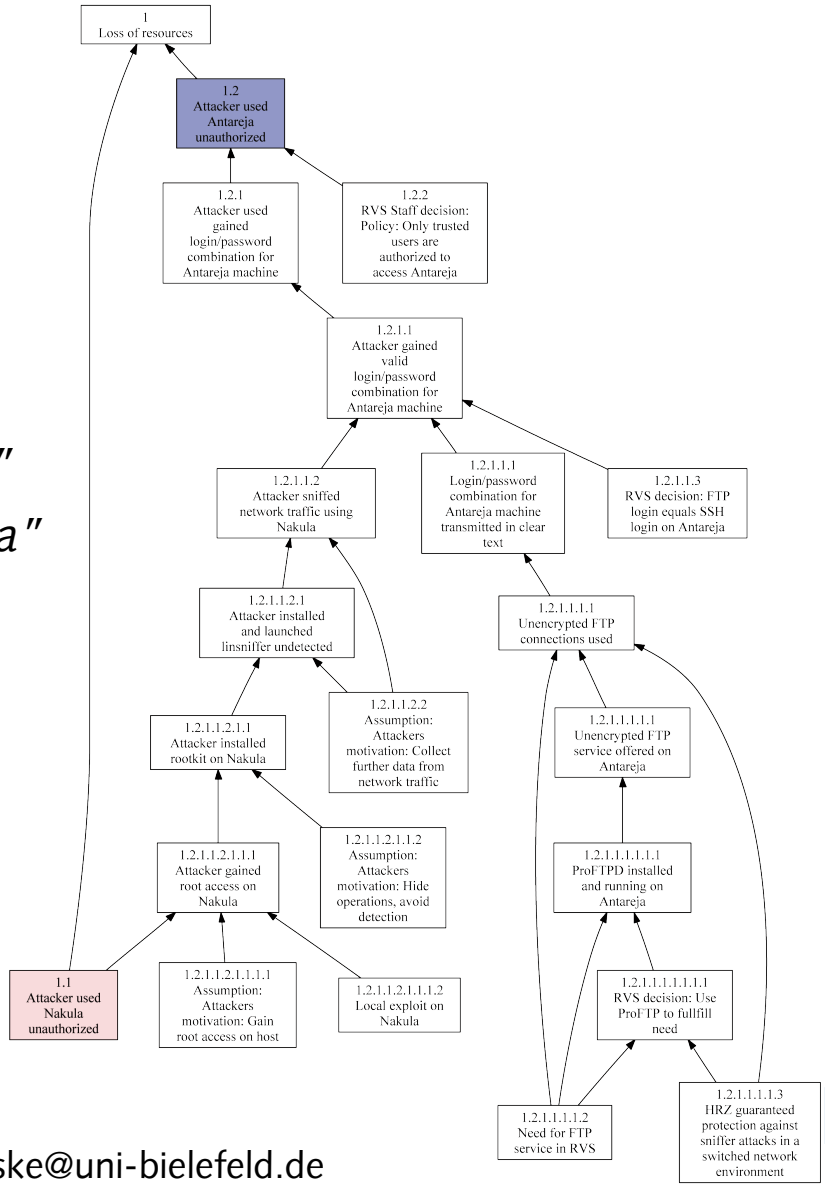
RVS Rechnernetze und Verteilte Systeme

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

The Antareja graph

- Accident: Loss of (specific amount of system) resources
- Necessary causal factors for the accident
  - *1.1: "Unauthorized use of Nakula"*
  - *1.2: "Unauthorized use of Antareja"*

form a set of sufficient causal factors for this *"Loss of resources"*



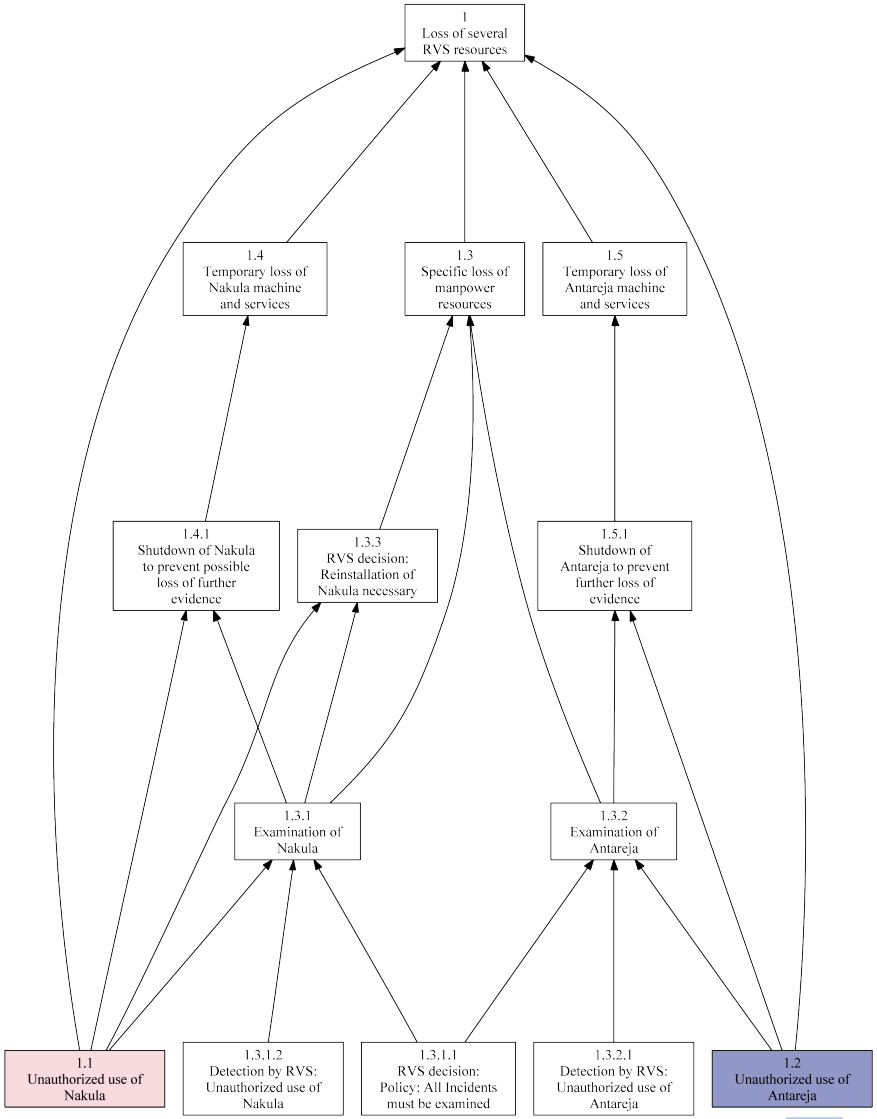
RVS Rechnernetze und Verteilte Systeme

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

The RVS-Loss graph

- Loss of several RVS resources
- Necessary causal factors for the accident
  - *1.1: "Unauthorized use of Nakula"*
  - *1.2: "Unauthorized use of Antareja"*
  - *1.3: "Specific loss of manpower resources"*
  - *1.4: "Temporary loss of Nakula machine and services"*
  - *1.5: "Temporary loss of Antareja machine and services"*

  form a set of sufficient causal factors for the *"Loss of several RVS resources"*



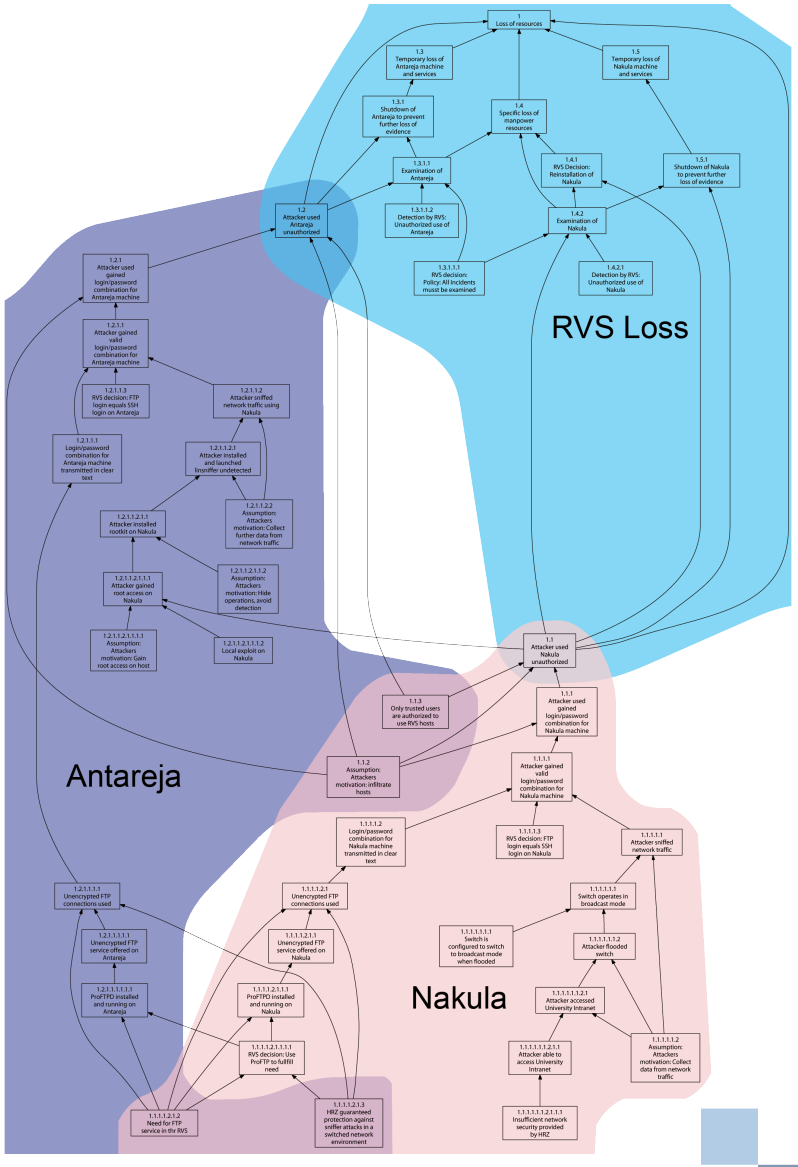
RVS Rechnernetze und Verteilte Systeme

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

The complete graph

- Accident: Loss of resources (complete)
- Necessary causal factors for the accident
  - *1.1: "Unauthorized use of Nakula"*
  - *1.2: "Unauthorized use of Antareja"*
  - *1.3: "Specific loss of manpower resources"*
  - *1.4: "Temporary loss of Nakula machine and services"*
  - *1.5: "Temporary loss of Antareja machine and services"*

  form a set of sufficient causal factors for this *"Loss of resources"*
- Colouring marks sub graphs



RVS Rechnernetze und Verteilte Systeme

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

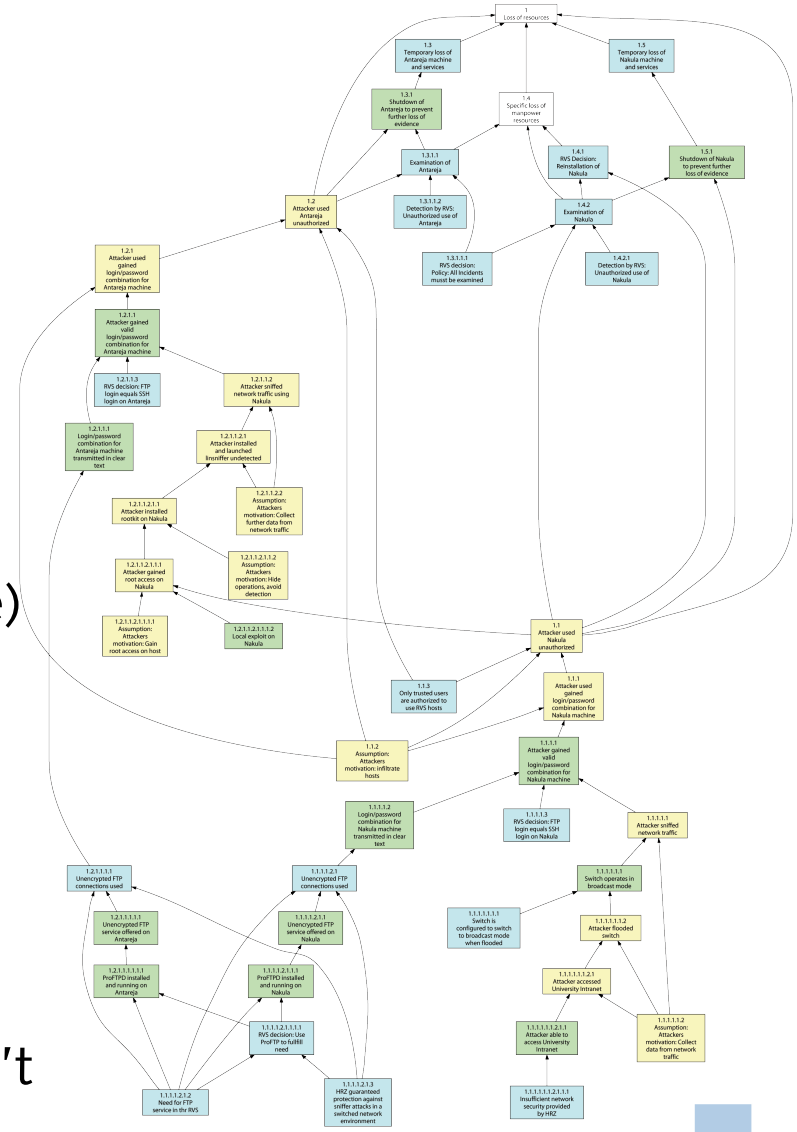
Many graphs… Where to look at?

- Identifying key-nodes (NCFs):
  - Quantity of in- and out- going edges:
    - Nodes with many edges must obviously exert important causal influence
  - "Single point of failure":
    - The chain of events runs through one node, so it must be a significant factor
  - Leaves:
    - Nodes without precursors are the root causes for the accident
- Nodes with these properties should be further inspected

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Dropping even more nodes

- Not all factors can be mitigated
  - Due to lack of control
- Idea: Mark out the control areas
  - Attacker control area (yellow)
  - Human (defender) control area (blue)
  - Technical control area (green)
- Attacker controlled areas can be blinded out
  - You can't change anything there
  - Also check for facts you can't or don't want to change (intuition)



RVS Rechnernetze und Verteilte Systeme

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Applying the criteria

- If we focus on factors which
  - Are not attacker controlled or not controlled at all
  - Meet at least one of the criteria (note: In/Out > 3), the more the better
- We get the most important nodes like:
  - *Insufficient Network security provided by HRZ (1.1.1.1.1.1.2.1.1.1)*
  - *HRZ guaranteed protection against sniffer attacks (1.1.1.1.2.1.3)*
  - *Attacker gained valid login/password combination (1.1.1.1/2)*
  - *Need for FTP service in the RVS (1.1.1.1.2.1.2)*
  - *RVS decision: FTP-Login equals SSH login (1.1/2.1.1.3)*
  - …

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

OK – what does that mean?

- If we examine the identified nodes, we may find

  possibilities to prevent a similar accident in the future:
  - *1.1.1.1/1.2.1.1: "Attacker gained valid login/password combination"*
    - The attacker was able to gain login data by sniffing from the unencrypted FTP traffic.
  - *1.1.1.1.2.1.3: "HRZ guaranteed protection against sniffer attacks in the switched environment"*
    - This is a rely condition. The RVS trusted the HRZ and arranged their infrastructure according to their needs based on this assurance.

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Taking precautions

- Mitigate these two causes
  - *1.1.1.1/1.2.1.1: "Attacker gained valid login/password combination"*
    - No unencrypted FTP-service should be offered by RVS machines. An attacker could sniff for weeks and not gain a valid login.
  - *1.1.1.1.2.1.3: "HRZ guaranteed protection against sniffer attacks in the switched environment"*
    - The HRZ-guarantee was obviously not reliable. Rely-conditions should be checked thoroughly and more discerning in the future.
- This example leads to a successful prevention of a similar accident with little effort.

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Comparison with the forensic analysis

- Recall: Suggested improvements in the forensic analysis:
  - University level Intrusion Detection System
  - Better log-mechanisms
  - Mechanism to notify system administrator
  - Development of proper security policies
- The conclusions drawn from the WB-Analysis are missing
  - Though forensics were performed by experienced investigators
  - Intuition may suggest right steps – but why should these be the right ones?
  - The WBA-method leads to objective conclusions in security-related cases just by following the method!

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Comparison with the forensic analysis

- WBA is a proper method not only for safety analyses
  - Leads to objective conclusions
  - Conclusions hard to counter
  - No sophisticated mathematical skills or similar necessary
  - Just following the method
  - Can lead to other conclusions than intuitive judgement

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de

Thanks for your attention!

And now, time for questions and discussions

What about:

- Formalisms for the finding of important nodes
  - Colouring? Grouping?
- Modelling human behaviour in WB-analyses
  - How to cope with the Counterfactual-Test?
- Modelling unknown facts / assumptions with no rule-base available

R|V|S Rechnernetze und Verteilte Systeme

Lars Molske :: lars.molske@uni-bielefeld.de
Damian Nowak :: damian.nowak@uni-bielefeld.de