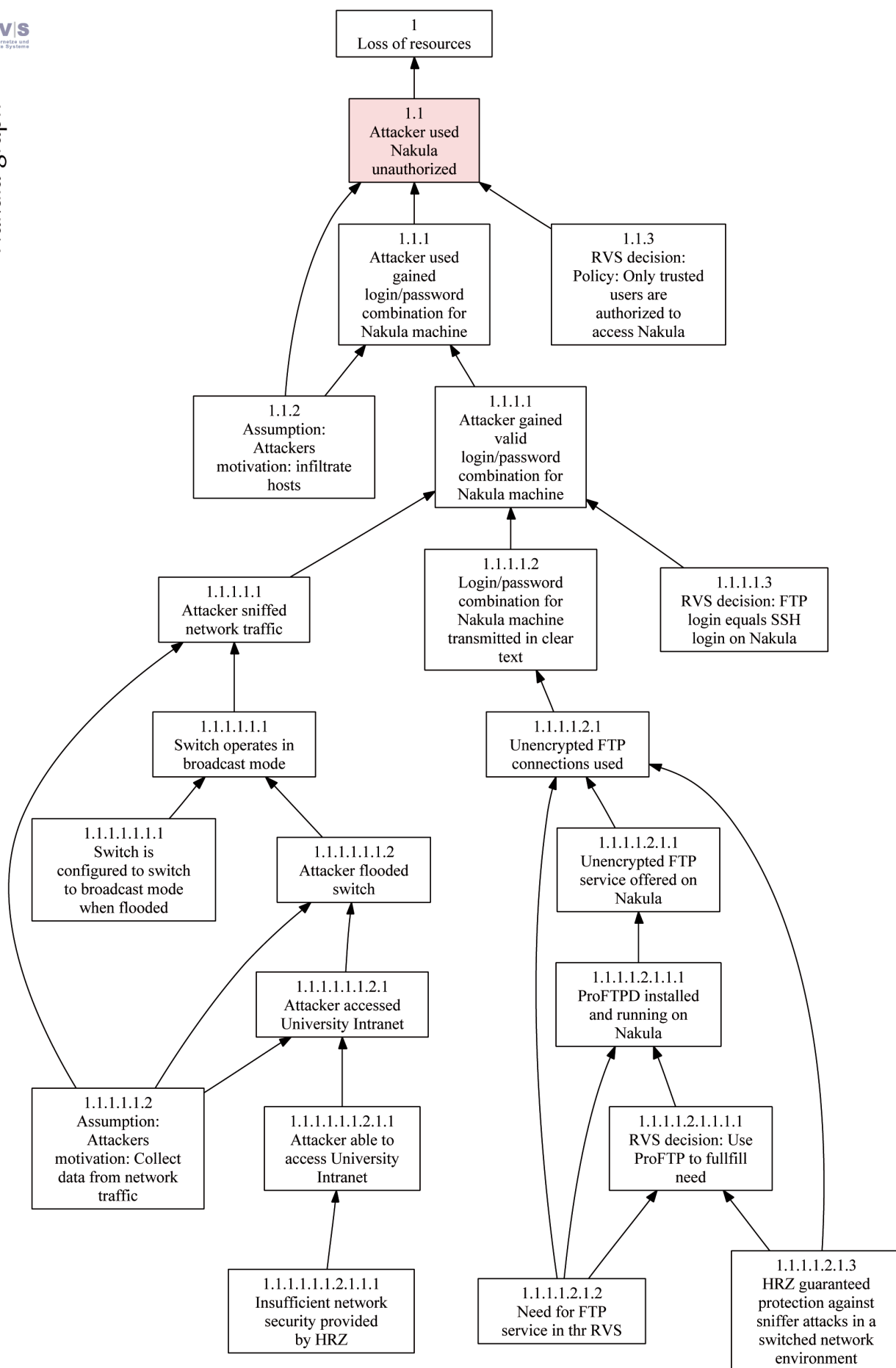


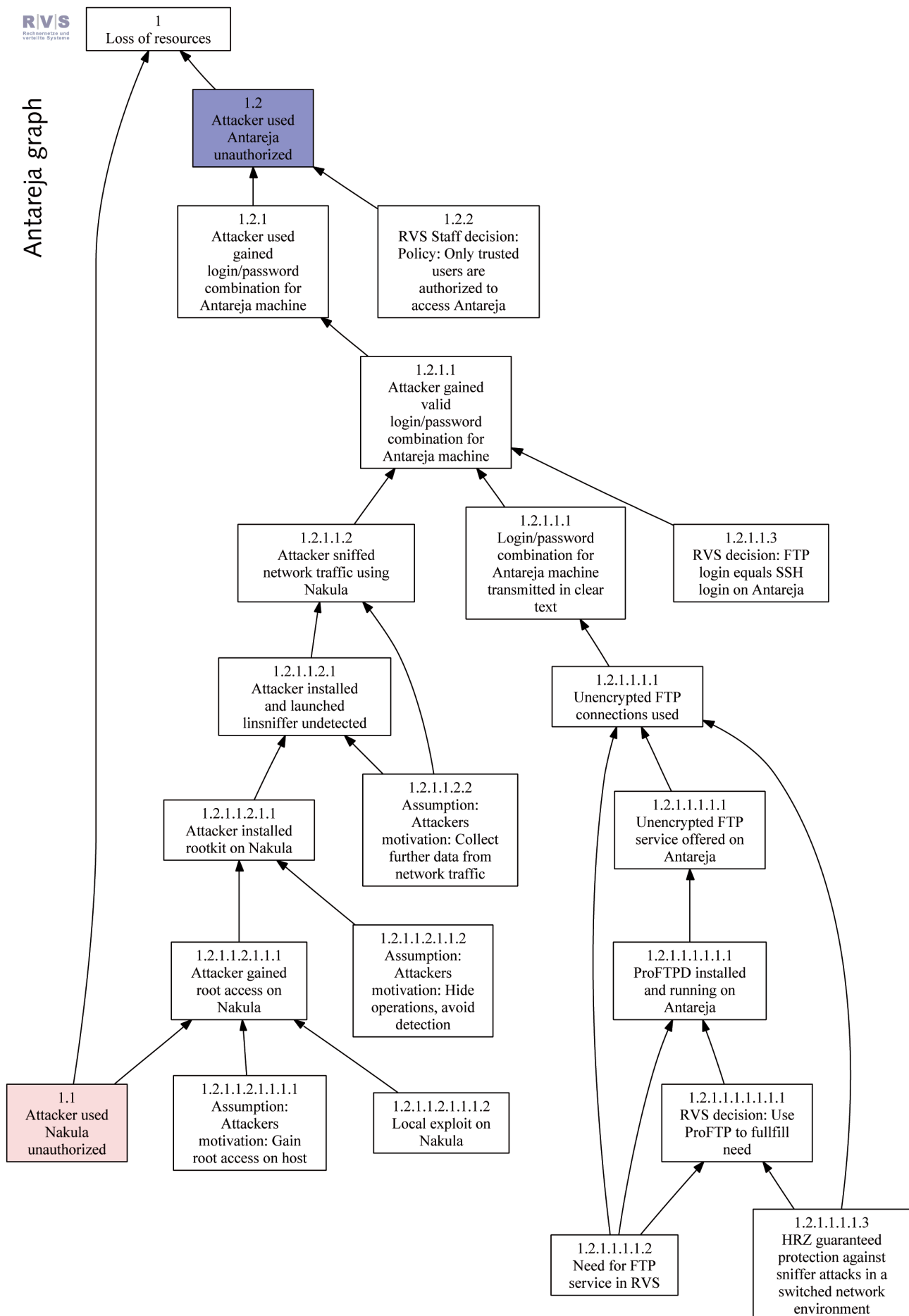
Handout

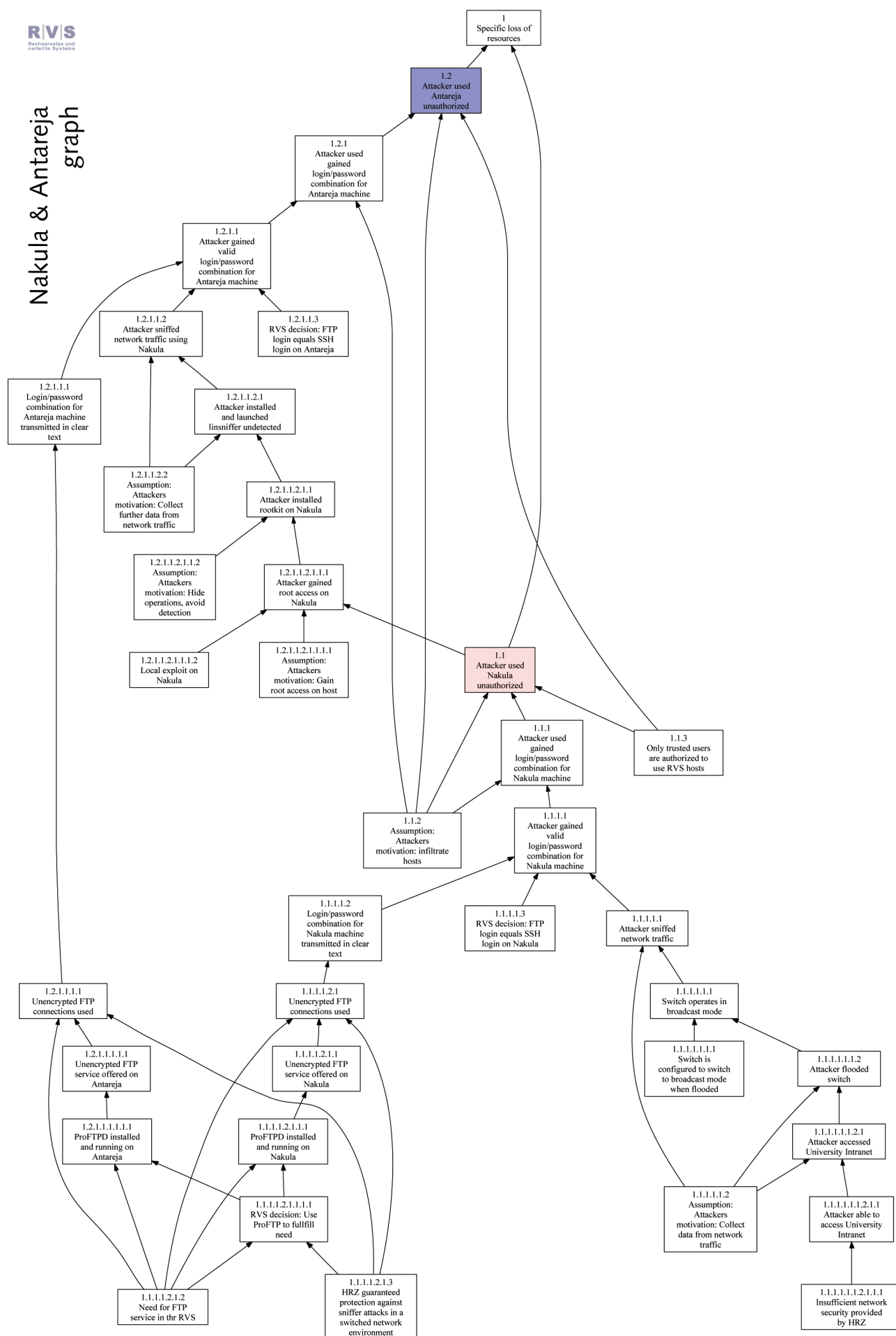
Nakula & Antareja Incident

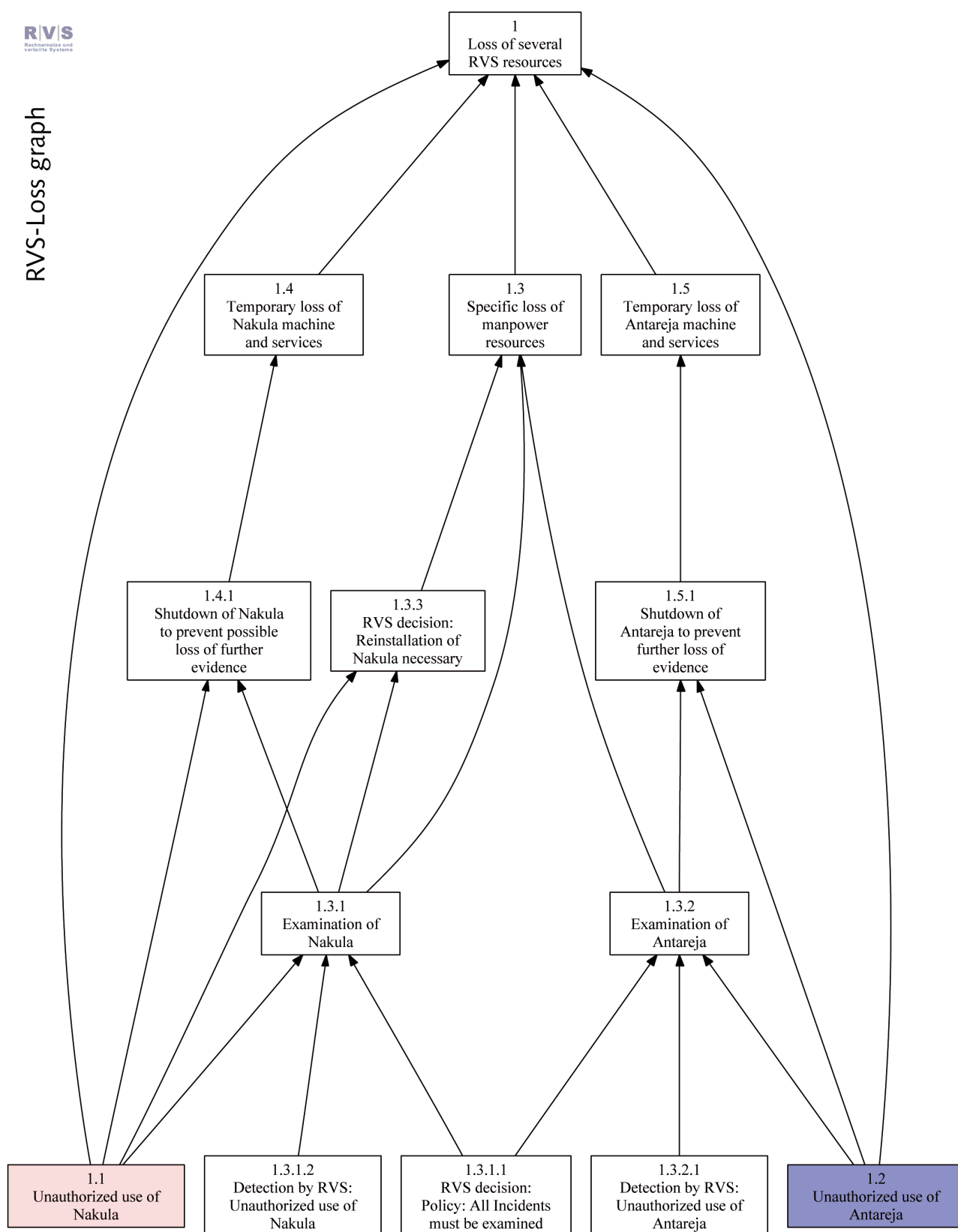
Lars Molske, Damian Nowak

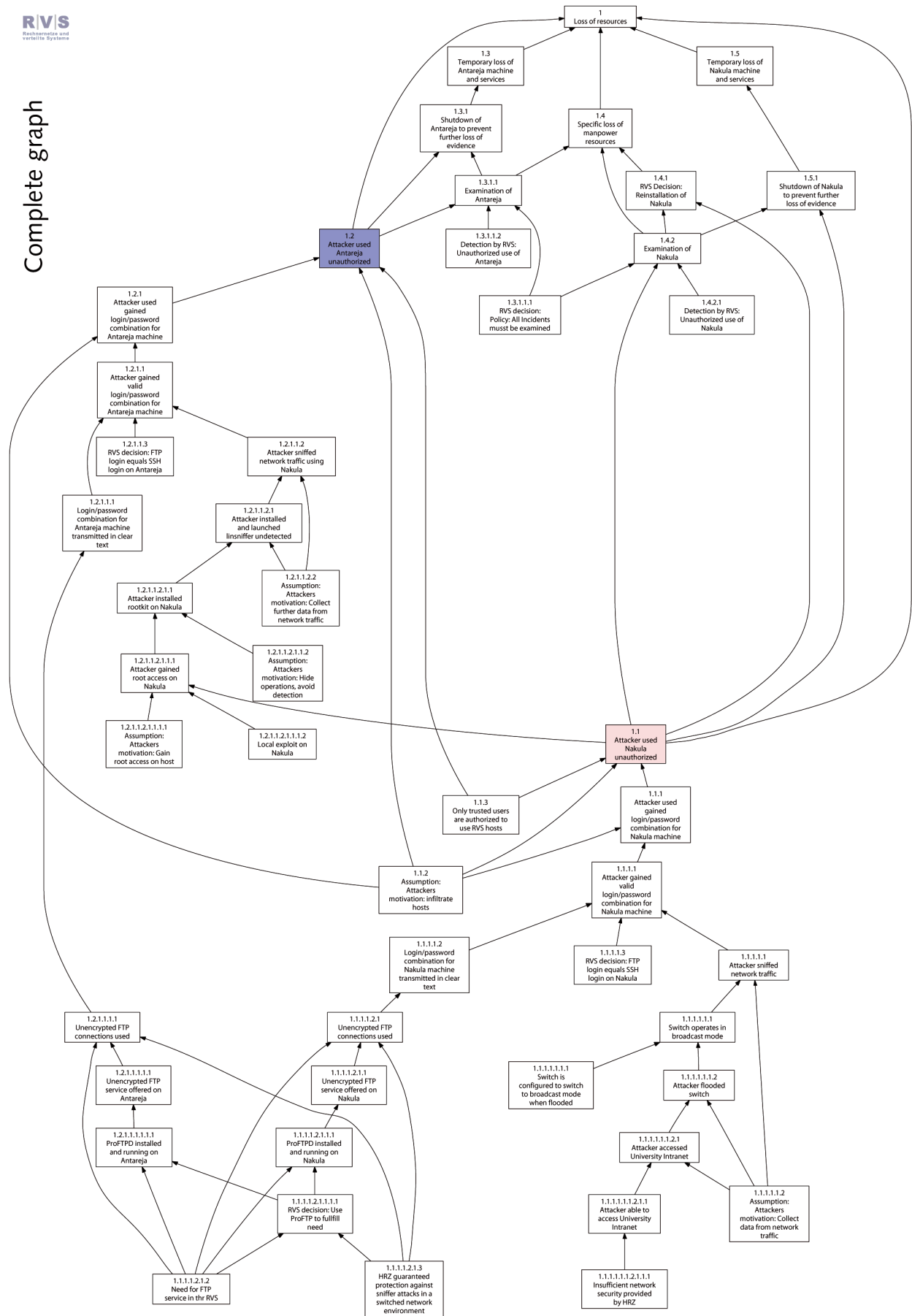
5.5th Bieleeschweig Workshop
Bielefeld, June 6-7 2005

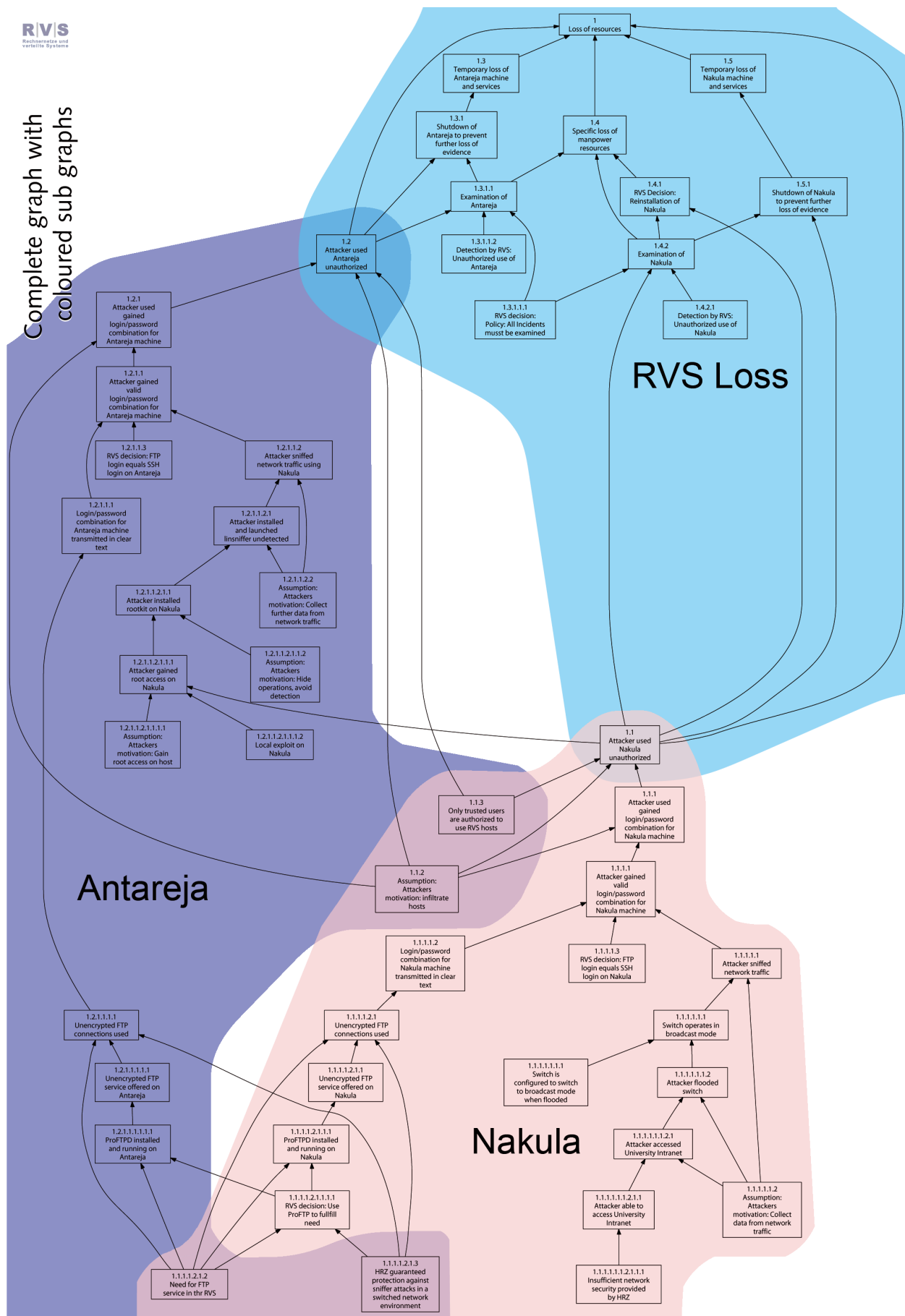


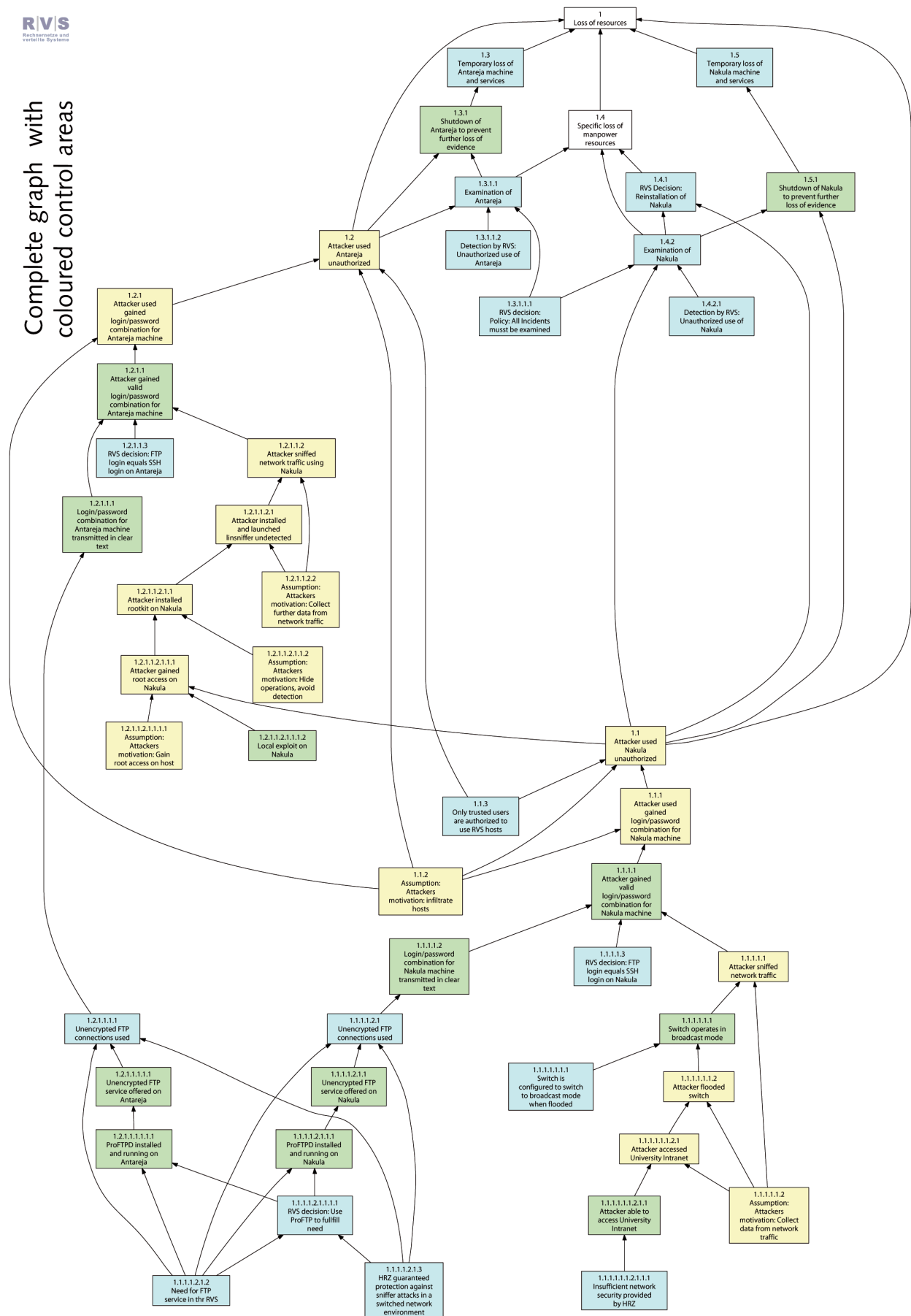












Factors meeting the presented criteria

Node	Description	Qualified by ¹
1.2.1.1.3:	RVS decision: FTP Login equals SSH Login on Antareja	L
1.2.1.1.2.1.1.1.2:	Local exploit on Nakula	L
1.1.1.1:	Attacker gained valid login/password comb. for Nakula mach.	SP
1.2.1.1:	Attacker gained valid login/password comb. for Antareja mach.	SP
1.1.1.1.3:	RVS decision: FTP Login equals SSH Login on Nakula	L
1.1.1.1.2.1:	Unencrypted FTP connections used on Nakula	4IO
1.2.1.1.1.1:	Unencrypted FTP connections used on Antareja	4IO
1.1.1.1.1.1.1:	Switch is configured to switch to broadcast mode when flooded	L
1.1.1.1.2.1.1.1.1:	RVS decision: Use ProFTP to fullfill need	4IO
1.1.1.1.2.1.3:	HRZ guaranteed protection against sniffer attacks	L, (3IO)
1.1.1.1.1.2.1.1.1:	Insufficient network security provided by HRZ	L

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

1.3.1.1:	Examination of Antareja	5IO
1.4.2:	Examination of Nakula	6IO
1.3.1.1.2:	Detection by RVS: Unauthorized use of Antareja	L
1.4.2.1:	Detection by RVS: Unauthorized use of Antareja	L
1.3.1.1:	RVS decision: Policy: All incidents must be examined	L
1.1.3:	Only trusted users are authorized to use RVS hosts	L
1.1.1.1.2.1.2:	Need for FTP service in the RVS	5IO, L

¹ xIO = Quantity of in- and out- edges, with x specifying the amount

L = Leaves

SP = Single point of failure