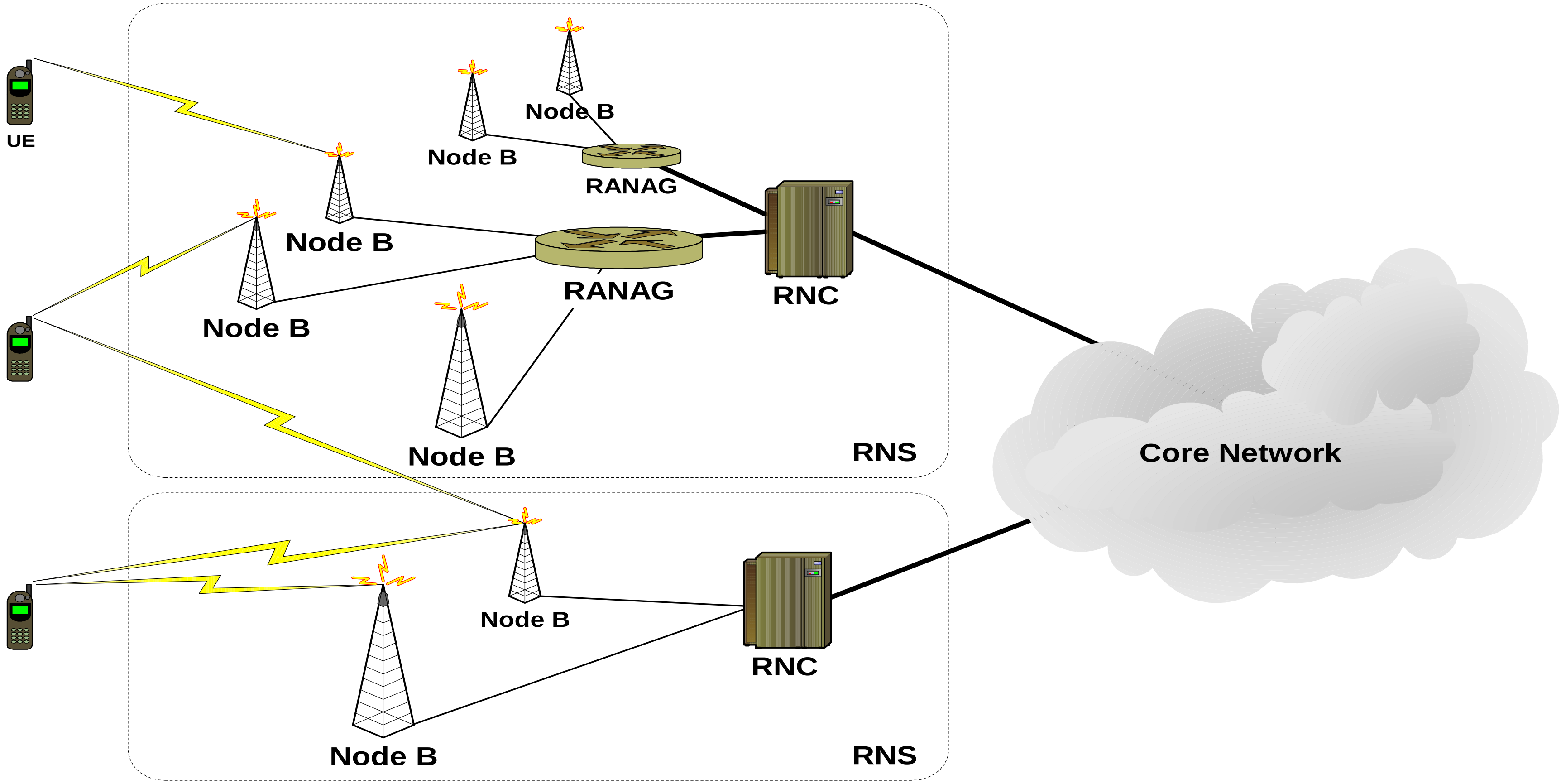
UTRAN Operation System Security

Juha Utriainen

Presentation contents

- Introduction to the context of the thesis study
- Presentation of the operation systems security solution
- Methods used in the thesis work
- Results of the study

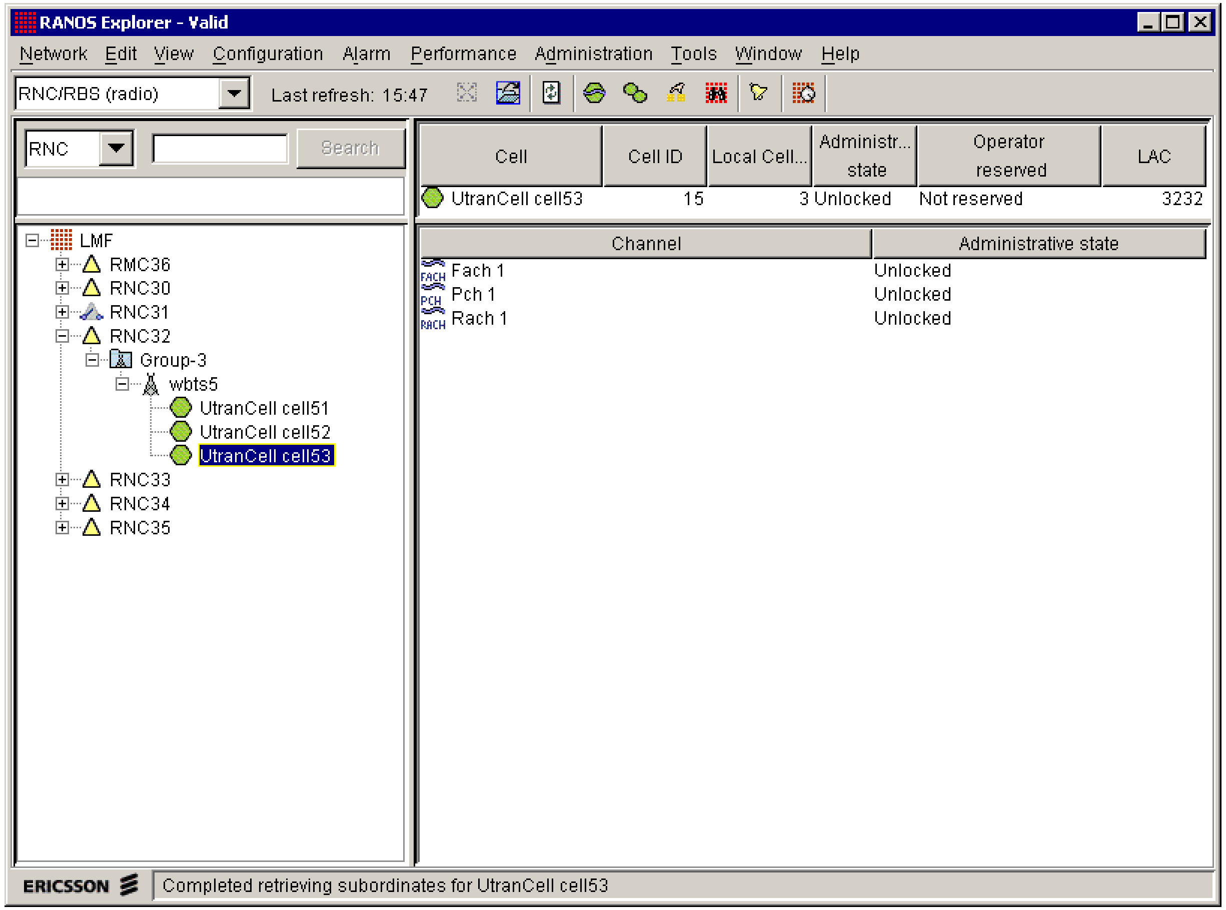
Universal Terrestrial Radio Access Network UTRAN



ERICSSON RAN Operation Support RANOS

- Subnetwork manager
- Controls three different element types:
  - Node B:s (NB)
  - Radio Network Controllers (RNC)
  - RAN Aggregators (RANAG)
- Basic functions
  - Configuration management
  - Software management
  - Product inventory
  - Fault management
  - Performance Monitoring

RANOS Explorer

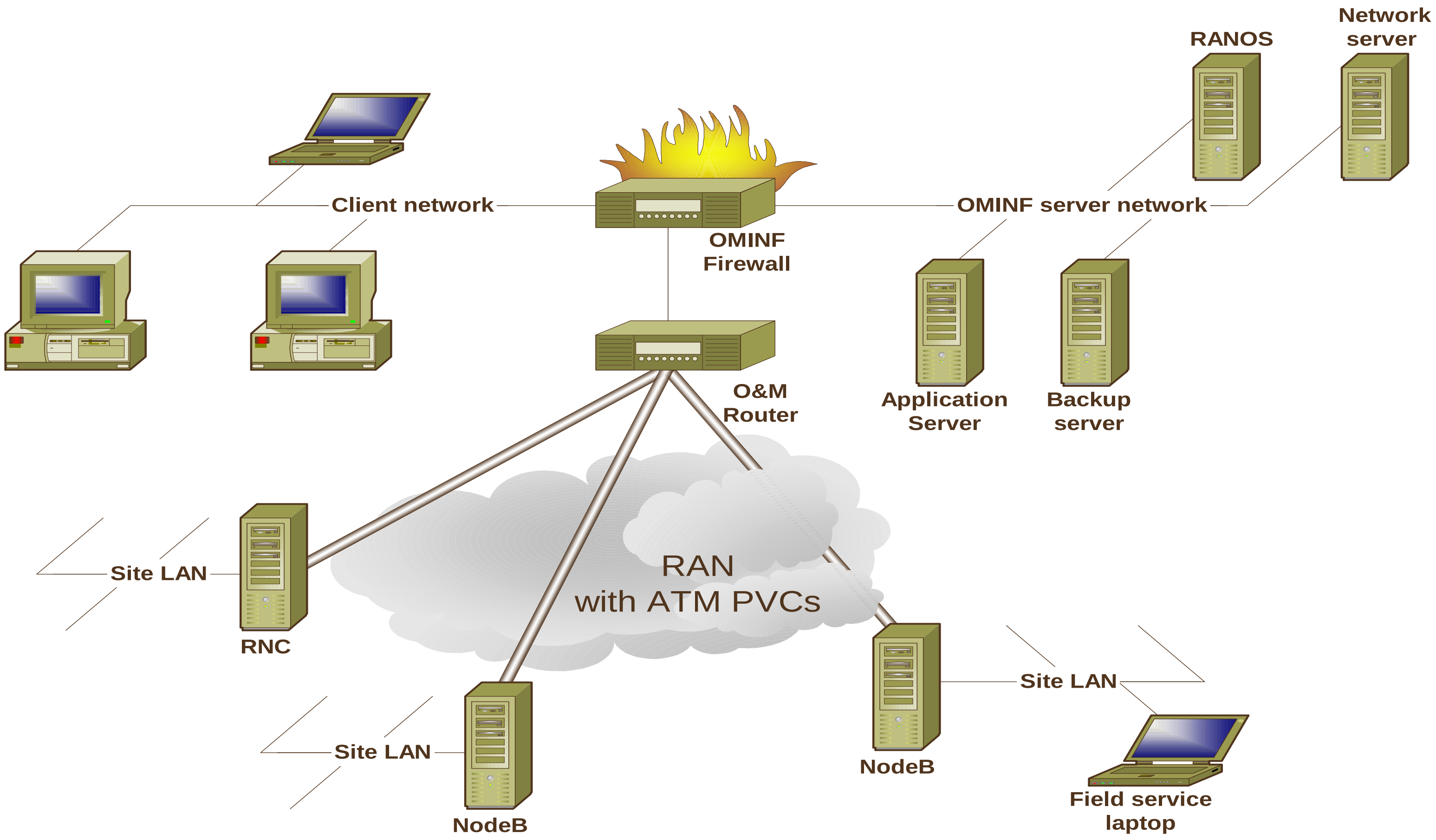


Cell	Cell ID	Local Cell...	Administr... state	Operator reserved	LAC
UtranCell cell53	15	3	Unlocked	Not reserved	3232

Channel	Administrative state
Fach 1	Unlocked
Pch 1	Unlocked
Rach 1	Unlocked

Completed retrieving subordinates for UtranCell cell53

Operation and Maintenance Infrastructure OMINF

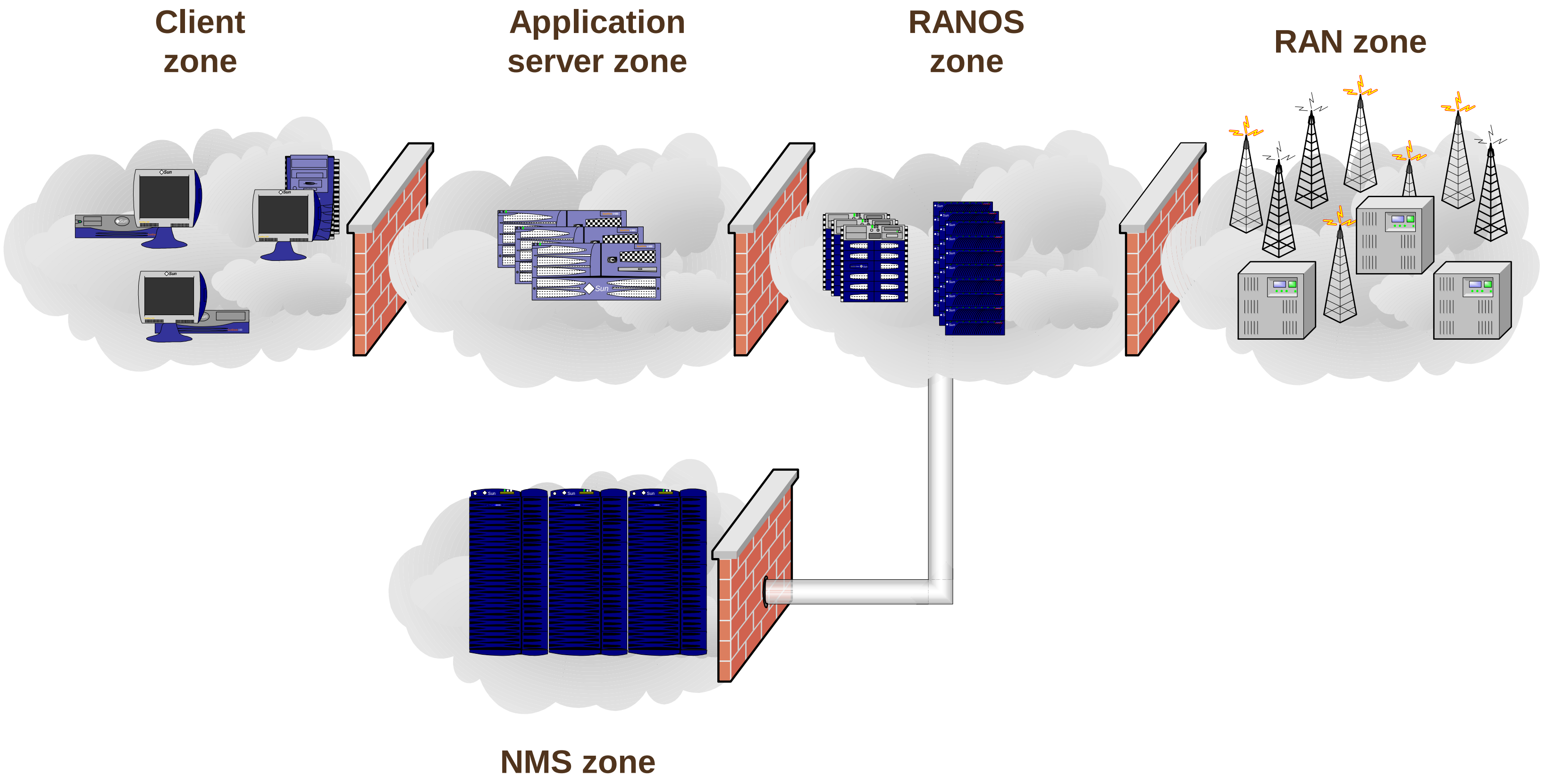


Security solution

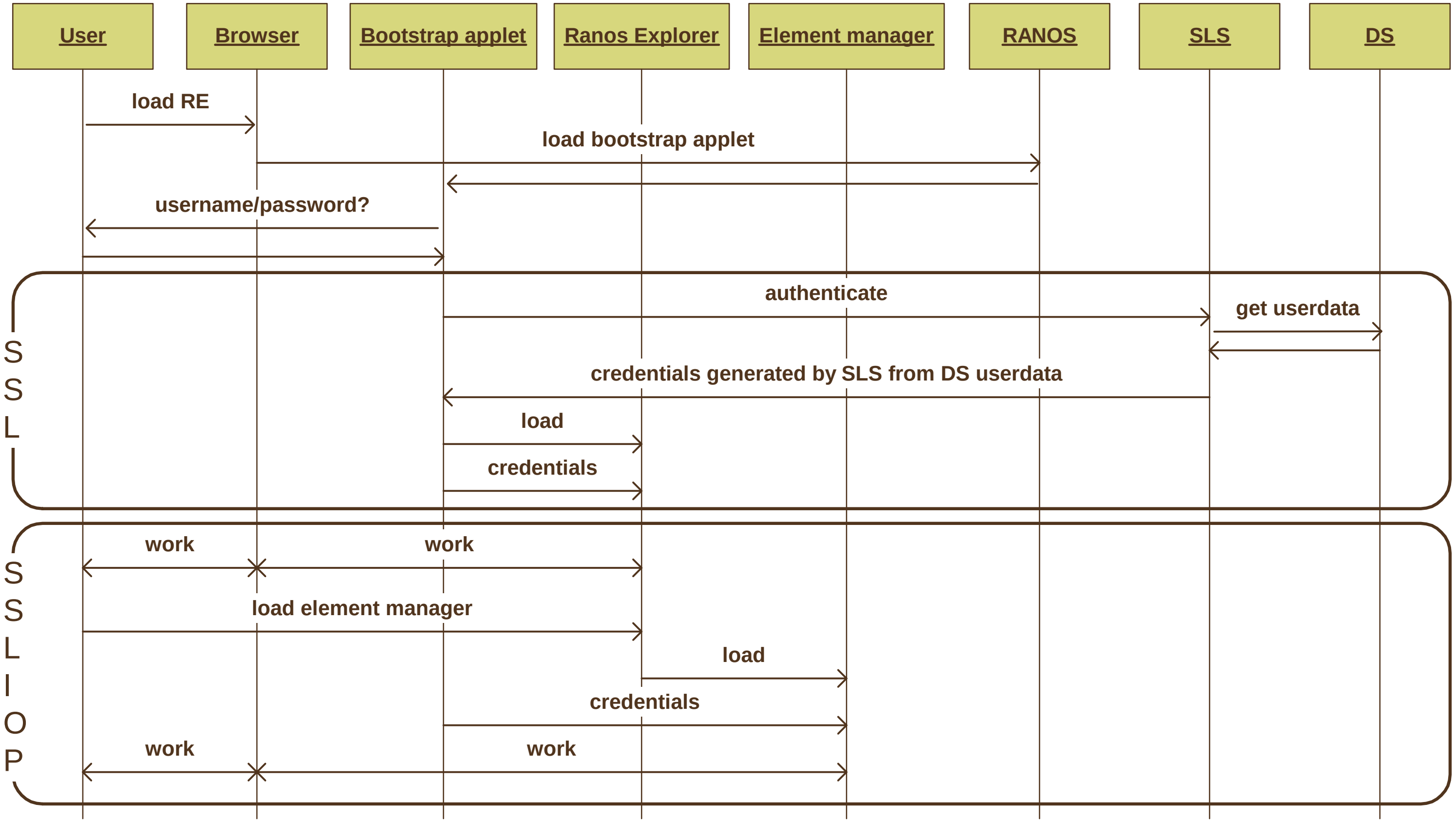
OMINF Security Solution

- Consists of software and security documentation
- Splits the O&M network to five firewall protected security zones
- Activates secure protocols for O&M traffic (IIOP and SSH)
- Introduces two new servers into OMINF network:
  - Single Logon Server (SLS) authenticating and generating temporary online and standalone offline certificates for users
  - Public Key Support Server (PKS) generating certificates for servers
- Authorization of user actions is done by Telecom Security Services daemon (TSS) usually running in RANOS server
- Documentation contains firewall configuration guide and RANOS Server Security Guide

OMINF Security Zones



Authentication and authorization



Security evaluation methodology

Security evaluation workflow

- Risk assessment
- Policy and other documentation evaluation
- Vulnerability scanning
- Architectural evaluation
- Penetration testing

Risk assessment

- Manual and intellectual work that cannot be automated
- Should be part of the security policy development process
- Describes threats
  - Information theft
  - Resource theft
  - Service delivery break
  - Other system dependent threats
- Profiles enemies and their motives
  - Professional intruders
  - Script kiddies
- Evaluates threat realization possibility and impact

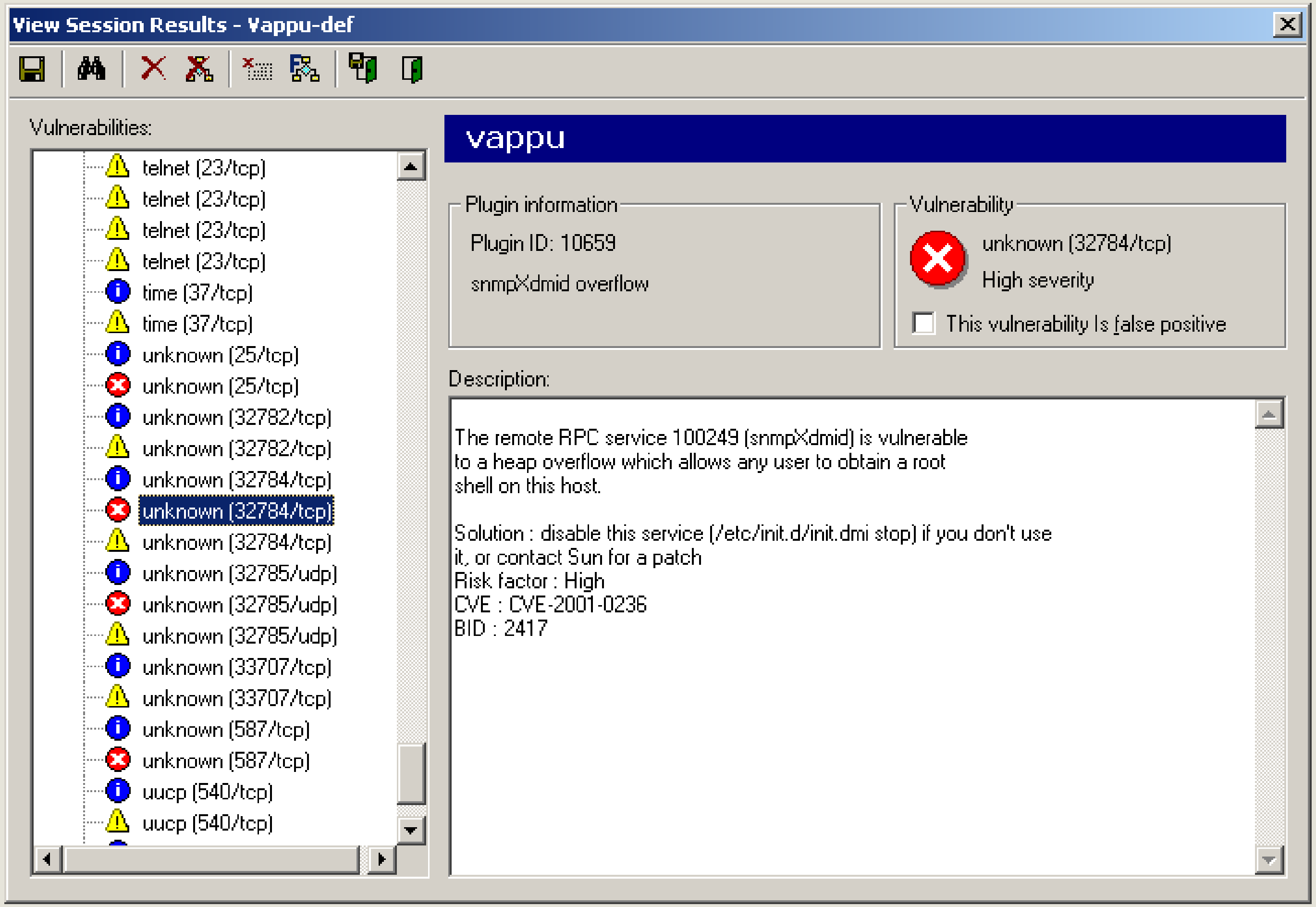
Security documentation

- Security policy
  - Contains risk analysis
  - Describes methods to minimize risk realization and impact
  - Should also contain security breach detection mechanisms and recovery procedures
- Other documentation
  - Security architecture documentation
  - Configuration guides
  - User documentation for administrators and users

Vulnerability scanning

- Automated evaluation of current security status
- Basic part of the system protection
- Hacker view of the system, using tools that hackers use
- Seeks for known vulnerabilities
  - Open ports
  - Old software revisions
- Some tools test if the vulnerability can be exploited
- Gives detailed and readily applicable information
- Open source tools, like Nessus, are available and highly capable

Vulnerability scan report example



View Session Results - Vappu-def

Vulnerabilities:

- ⚠ telnet (23/tcp)
- ⚠ telnet (23/tcp)
- ⚠ telnet (23/tcp)
- ⚠ telnet (23/tcp)
- ⓘ time (37/tcp)
- ⚠ time (37/tcp)
- ⓘ unknown (25/tcp)
- ✖ unknown (25/tcp)
- ⓘ unknown (32782/tcp)
- ⚠ unknown (32782/tcp)
- ⓘ unknown (32784/tcp)
- ✖ unknown (32784/tcp)
- ⚠ unknown (32784/tcp)
- ⓘ unknown (32785/udp)
- ✖ unknown (32785/udp)
- ⚠ unknown (32785/udp)
- ⓘ unknown (33707/tcp)
- ⚠ unknown (33707/tcp)
- ⓘ unknown (587/tcp)
- ✖ unknown (587/tcp)
- ⓘ uucp (540/tcp)
- ⚠ uucp (540/tcp)

vappu

Plugin information

Plugin ID: 10659

snmpXdmid overflow

Vulnerability

✖ unknown (32784/tcp)

High severity

□ This vulnerability Is false positive

Description:

The remote RPC service 100249 (snmpXdmid) is vulnerable
to a heap overflow which allows any user to obtain a root
shell on this host.

Solution : disable this service (/etc/init.d/init.dmi stop) if you don't use
it, or contact Sun for a patch
Risk factor : High
CVE : CVE-2001-0236
BID : 2417

Architectural security evaluation

- Completes the vulnerability scanning
- Seeks for security infrastructure design errors
  - Covert channels
  - Missing policy enforcement elements
- Produces information that is not available for intruders
- Manual work requiring security expertise

Penetration testing

- Demonstrates system vulnerability
- Used to scare stakeholders
- May be done blindly without previous evaluation
- Does not have security proofing power

Results

Results of the thesis study

- Security package blocks outside attacks effectively
- Security documentation is incomplete
- Patch delivery process is immature
- Intrusion detection mechanism needs refinement
- Few acute findings that are now patched

Questions?