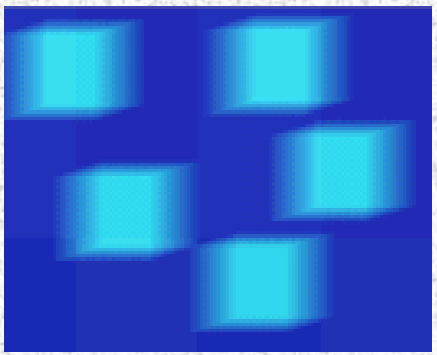
Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA05)
July 7th-8th, 2005, Vienna

# Combining IDS and Honeynet Methods for Improved Detection and Automatic Isolation of Compromised Systems

*B.Tödtmann, S.Riebach, E.P. Rathgeb*



Dipl. Wirt.-Inf. Stephan Riebach
Computer Networking Technology Group
Institute for Experimental Mathematics (IEM) and
Institute for Computer Science and
Business Information Systems (ICB)
University Duisburg-Essen, Germany

# Overview

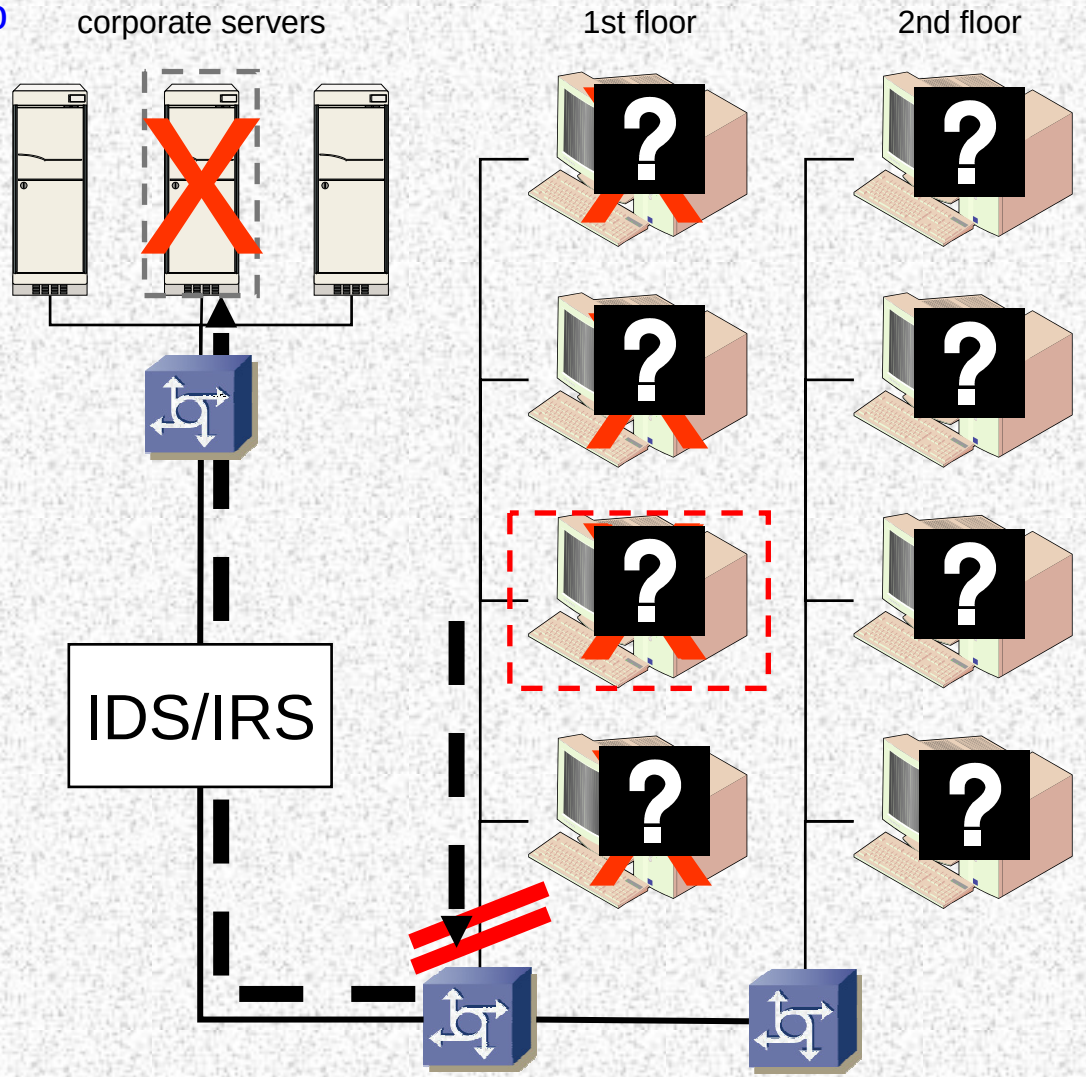
1. Introduction and motivation
2. IDS/IRS: concepts and limitations
3. Automated isolation of suspicious systems
4. Prototype implementation
5. Conclusion and Outlook

# Introduction & Motivation

- mobile/wireless computing rapidly changed situation in corporate networks
  - in the past: single network entry point, fixed stations
  - today: mobile stations that move out of the corporate network
- mobile computing decreases system administrators control level
  - stations move in non-secured areas, e.g. public and home networks
- “on the road” those systems can be infected within a few minutes
  - less secured systems fully exposed to the internet
- corporate firewalls protect a LAN against attacks from the Internet
  - Sunday: University Bochum, Hacker gained access to 40.000 mailboxes
- common IDS are passive systems: attack → detection → log-file
- IRS can cause negative side effects due to false positives
- IDS limitations
  - misuse detection: false negatives because of unknown attacks, false positives for non-customized rules
  - anomaly detection: false positives in training phase, software changes

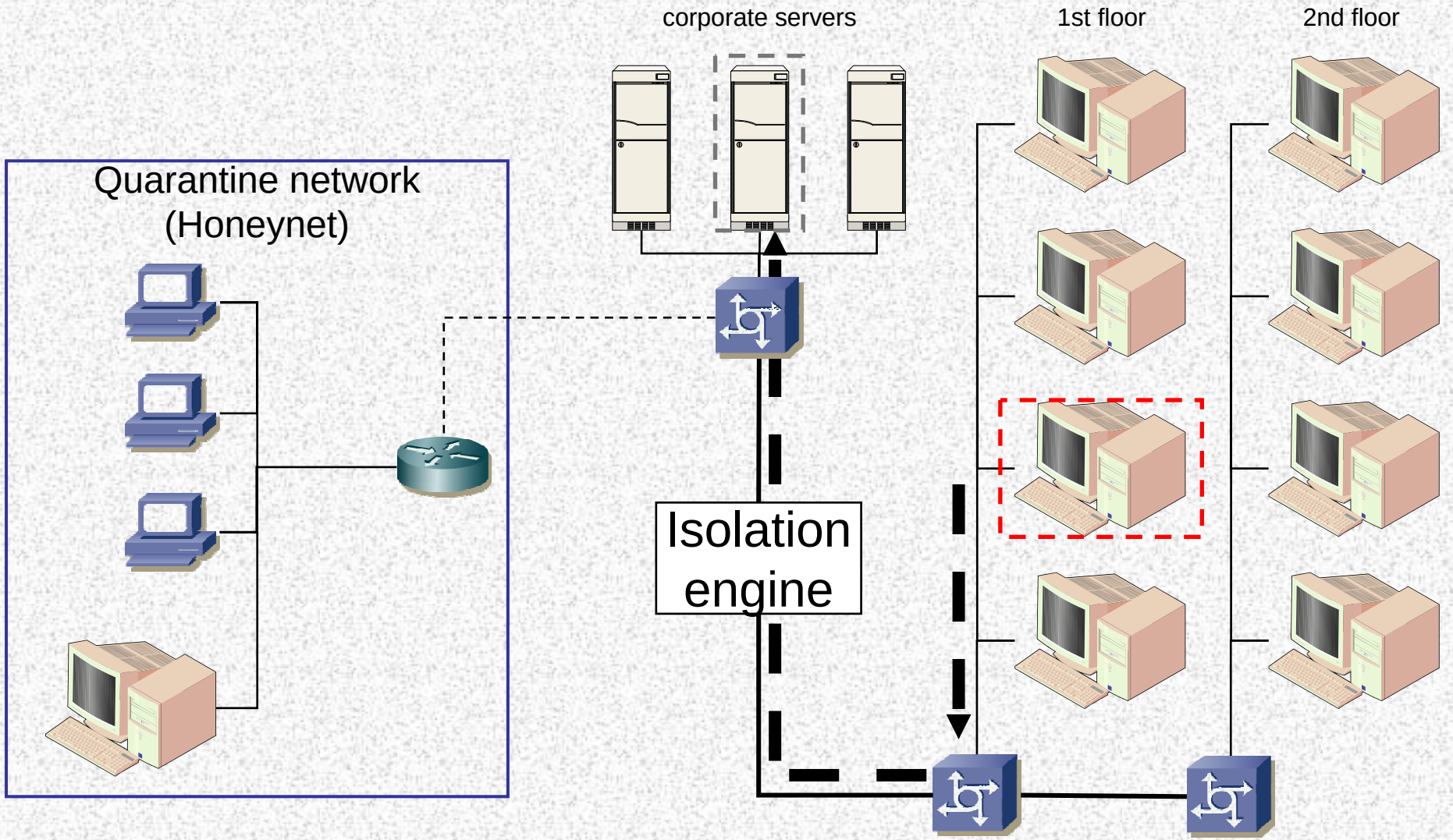
# Impact of Intrusion Response

- a station becomes suspicious due to scans
- common IRS alternatives
  - session locking
  - connection disabling
  - server disabling
- problems of Intrusion Response
  - suspicion cannot be proven
  - station may belong to CEO ☺
  - every change of network-based software causes IR
- in general: false positives cause significant damage
  - denial of service
  - staff cannot work
  - trust in IT will be decreased
  - problem of costs



# Our approach: isolation

Computer Networking Technology Group
Institute for Experimental Mathematics
University Duisburg-Essen, Germany



# Automated isolation of suspicious systems
## How it works

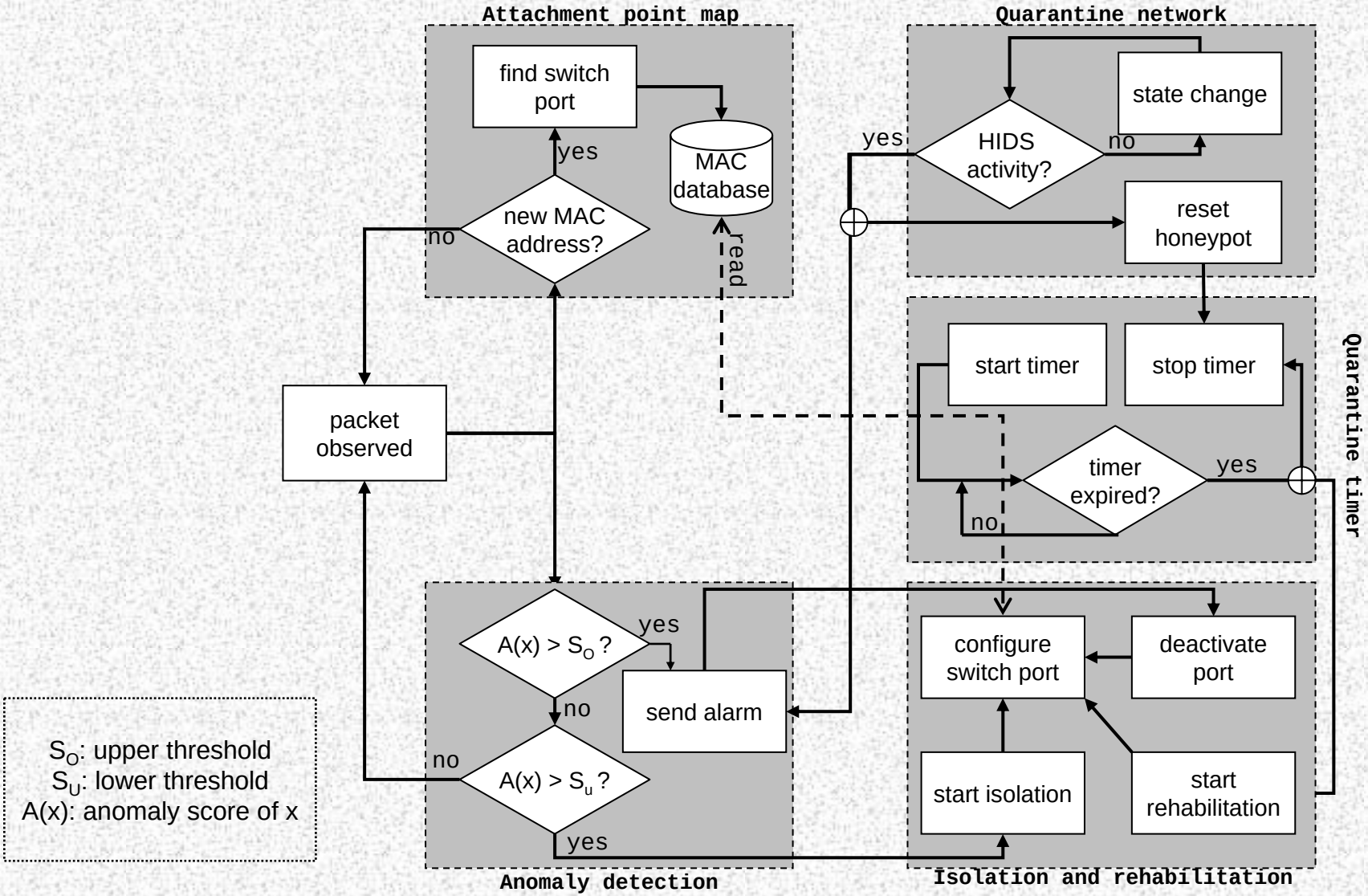
Computer Networking Technology Group
Institute for Experimental Mathematics
University Duisburg-Essen, Germany

- anomaly-based NIDS flags a suspicious system
- isolation engine “moves” the system into a Honeynet
  - layer 2 based switch technology → VLANs
- traffic observation
  - due to restrictive firewall rules usual traffic will be possible from inside the Honeynet, such as SMTP, HTTP etc.
  - all other traffic is redirected to Honeypots
- quarantine timer
  - if the IDS (HIDS and/or NIDS) inside of the Honeynet reports any further malicious activity → permanent deactivation
  - if no other activity occurs → rehabilitation

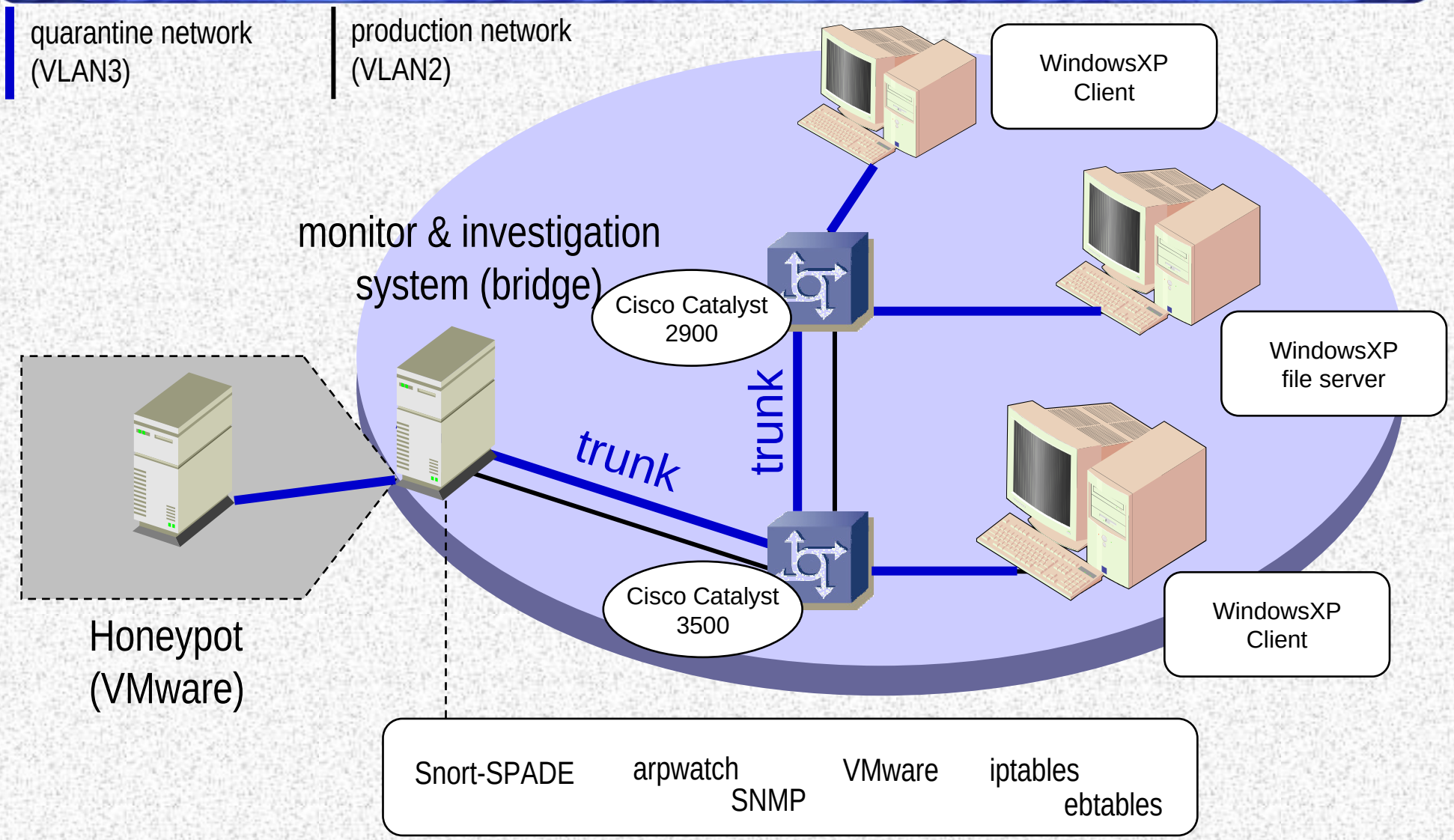
# Concept overview

- incident-driven system which combines well-known technologies
  - anomaly-based NIDS
  - Honeypots/Honeynets
  - IEEE 802.1q VLANs
  - SNMP messages
- starting incident is the alarm generated by NIDS
- choosing anomaly NIDS
  - detecting new attacks
  - improving NIDS accuracy
  - Honeynets for evaluation of alarms
- deploying Honeynets
  - controlled environment to observe suspicious systems → data control
  - powerful tools to detect attacks (NIDS/HIDS) → data capture
  - physical disjunction from production network

# HonIDS: process view



# Prototype Implementation



# Prototype implementation (II)

Computer Networking Technology Group
Institute for Experimental Mathematics
University Duisburg-Essen, Germany

- Snort-Spade anomaly NIDS
  - plugin for Snort
  - first prototypes with single-threshold
  - incident reporting via `syslog`
  - `syslog` sends all alerts to a `named pipe`
- Attachment point map
  - `arpwatch` to detect newly activated systems
  - the script "`mac2port`" automatically extracts a stations port when `arpwatch` "sees" a new station
  - `mac2port` sends SNMP requests to all switches
  - information stored in text files
- Isolation/Rehabilitation
  - Spade alarm triggers the isolation
  - sending SNMPv3 "set" request to switch to change VLAN
  - second message to clear switch MAC table

# Prototype implementation (III)

- Isolation/Rehabilitation
  - named pipes for total deactivation or rehabilitation (guilty/notguilty)
  - isolation function starts `qtimer` (20 min.)
- Quarantine network
  - VMware workstation with WindowsXP guest
  - guest in non-persistant mode
  - all filesystem changes are stored in REDO-logs
  - rebooting the Honeypot = set to unchanged state
- VMware based HIDS
  - requires guest filesystem FAT32, not NTFS
  - only changes of filesystem are stored → REDOs have finite size
  - periodically comparing $REDO_{now}$ with $REDO_{t\text{-}10sec}$ with xdelta
  - revealing newly created files
  - specialized for worm/virus detection

# Prototype implementation (IV)

- Bridge and filter configuration
  - bridge with 3 interfaces (2 physical for VLANs, 1 virtual)
  - netfilter under Linux with tools `iptables` and `ebtables`
  - `arp` traffic possible between VLAN2 and VLAN3
  - traffic from VLAN3 → VLAN2
    - harmless traffic (DNS, HTTP, SMB) is allowed
    - any other traffic redirected to Honeypot
- some example rules

```
ebtables -t nat -A PREROUTING -j ACCEPT --in-if eth0.3
   --protocol ip --ip-destination 0.0.0.0 --ip-protocol 17
   --ip-destination-port 53
iptables -t nat -A PREROUTING -j ACCEPT -m physdev
   --physdev-in eth0.3 --destination 0.0.0.0
   --protocol udp --destination-port 53
```

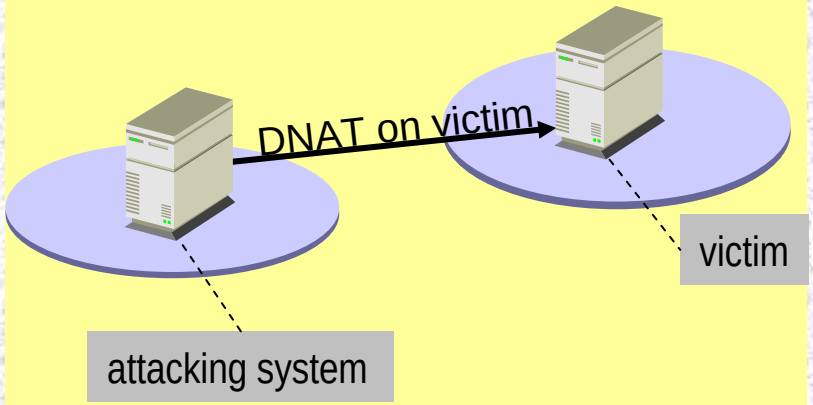
# Evaluation: Simulating false positive scenario and worm attack

Computer Networking Technology Group
Institute for Experimental Mathematics
University Duisburg-Essen, Germany

- Scenario A: Skype in the production network
  - client system scanned for peer nodes
  - activity flagged within 2-7 seconds
  - isolation to VLAN3 within 1 second
  - **total reaction time: 8 seconds**
  - HIDS reported no new EXE or DLL files
  - after 20 minutes successful rehabilitation
- Scenario B: Lovesan.A worm infection
  - execution of Lovesan.A on client
  - TCP scans were detected by SPADE
  - client was isolated to VLAN3
  - **total reaction time: 9 seconds**
  - the client infected the Honeypot
    - HIDS detected “MSBLAST.EXE”
  - deactivation of client’s switch port
- both clients (in A and B) could still access corporate servers

- reference times (worst case)

| | Test 1 | Test 2 | Test 3 |
|---|---|---|---|
| Lovesan.A | 13 sec. | 16 | 15 |
| Lovesan.F | 14 sec. | 11 | 16 |
| Sasser.A | 5 sec. | 4 | 6 |
| Sasser.B | 9 sec. | 8 | 7 |
| Welchia A,E,G,H | After activation all variants were inactive for at least 5 minutes | | |
| Randex.I | | | |

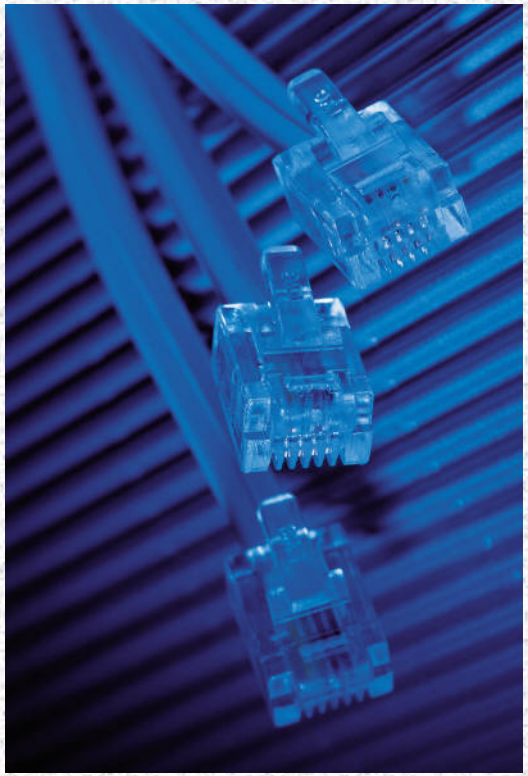


# Prototype limitations

- prototype supporting only one broadcast domain
  - VLANS cannot spread beyond a IP subnet
- SNMP mechanism requires equipment supporting VLAN-specific MIBs
- prototype allows isolation of only one system at a time
  - no multiple incident handling
  - multiple incident handling requires multiple VLANs and virtual honeynets
- VMware based HIDS is still not fully reliable
  - false negatives occurred (new DLLs and EXEs not found in REDO files)
- still no process monitoring HIDS deployed
- still no user traffic adjustment
  - starting the same suspicious but harmless software causes recurring isolation processes
  - rule-based customization affects the anomaly-based approach

# Conclusion & Outlook

- we demonstrate a way to deploy a two step IRS
  - combining IDS (security observation)
  - and Honeynets (forensics)
- our prototype improves LAN security
  - e.g. inhibit worm spreading in LANs
- alarms generated by anomaly-based IDS are validated
  - usage of Honeynet technology
- suspicious systems will not be deactivated
  - tolerable traffic limitations while observing
- future work
  - storing non-malicious activity
    - “calibration” of anomaly-based NIDS
  - multiple incident handling



# Thank you for your attention!