CORONA
EMERGENCY
LECTURE

Security of Distributed Software

Prof. Dr.-Ing. Martin Gaedke
Chemnitz University of Technology
Department of Computer Science
Professorship of Distributed and Self-organizing Systems

http://vsr.informatik.tu-chemnitz.de

Section

IDENTITY INFORMATION IN DIRECTORY SERVICES

Directory Service

- Directory Service is a special ‘Name Service‘
- Property-based requests
  - Comparison: full-name DNS request
  - Similar to ‘Yellow Pages‘
- OSI X.500 is the ‘classical‘ Directory Service
  - However, the complex ‘Directory Access Protocol‘ (DAP) prevented it from becoming more widespread.
- LDAP: Lightweight Directory Access Protocol
  - Standardized by IETF

X.500, LDAP: Namespace (1)

Base element: Entry

(Attribute, Value)
(Attribute, Value)
(Attribute, Value)
...

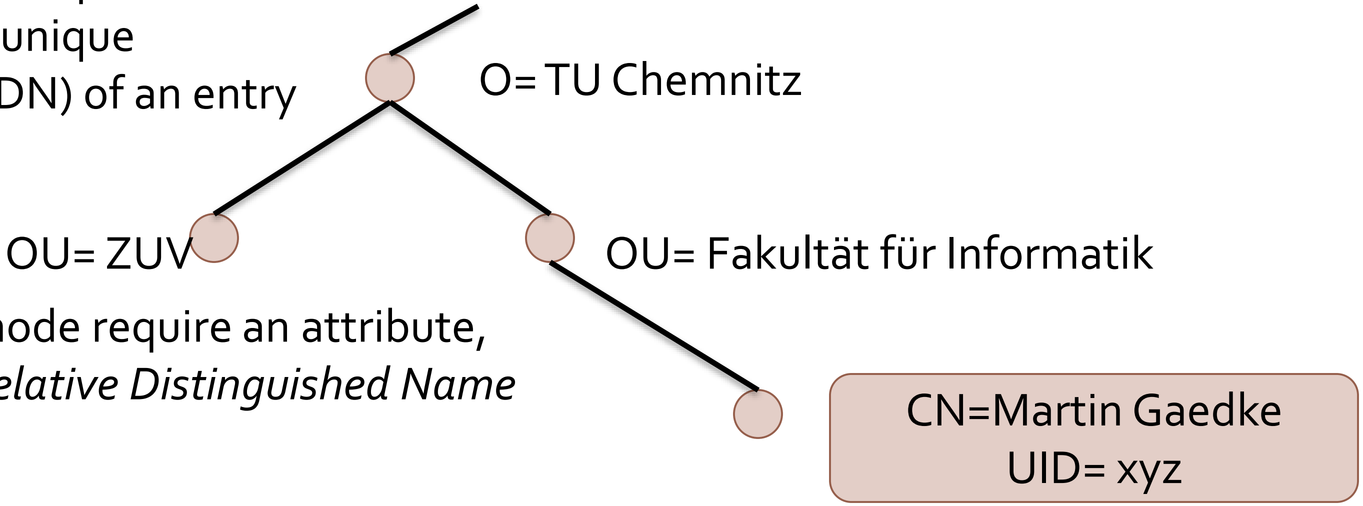
Attribute type

Example

(O, TU Chemnitz)
(OU, Fakultät für Informatik)
(CN, Martin Gaedke)
(EMAIL, gaedke@cs.tu-chemnitz.de)
...

An entry can serve as a container and reference a (sub-) directory -> hierarchical structuring

Comma-separated line-up of RNDs comprises a unique *Distinguished Name* (DN) of an entry



Entries within one node require an attribute, which serves as a *Relative Distinguished Name* (RDN)

LDAP, X.500: Namespace (2)

Typical container attributes:

Object Class Type	Attribute Name	Explanation
Country	c	Can provide geographical structure
Locale	l	Can subdivide country container
Organization	o	Can provide political structure
Organizational unit	ou	Can subdivide organization container

Further typical entry attributes:

Attribute	Explanation
cn	Common name
st	State
street	Street address
dc	Domain component
uid	User identity

LDAP, X.500: Namespace (3)

- Collection of all entries in a X.500-directory is called '*Directory Information Base*'
- Name-tree constructed by an RDN sequence is called '*Directory Information Tree*'
- Hierarchical structure enables 'Delegation of Management' and distributed implementation
- LDAP Schema defines the exact class definitions and the according class structure rules, attribute types, syntax and 'matching'

Comparison: Network management information models

LDAP: Operations (1)

Category	LDAP Operation
Session	**Bind, unbind, abandon**
Request/Retreival	**Search, compare**
Entry modification	**Add, modify, modifyRDN, delete**
Extensions	**Extended**

- Client-Server architecture
- LDAP typically works over TCP
  - CLDAP over UDP
- Applications with an incorporated LDAP-Client are called *directory-enabled applications*
  - *Directory-Enabled Networking (DEN)*
  - Example: Active Directory (Microsoft)

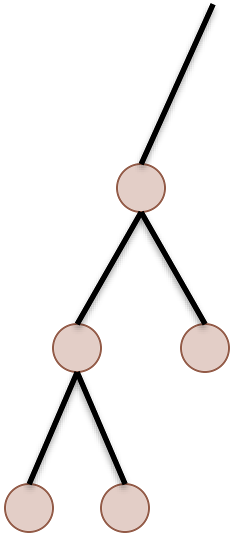
LDAP: Operations (2)

Search: required parameters

- Base DN
- Scope: base, one, subtree
- Filter: Attribute type, comparator, attribute value
  - Multiple triples allowed

Search: optional parameters

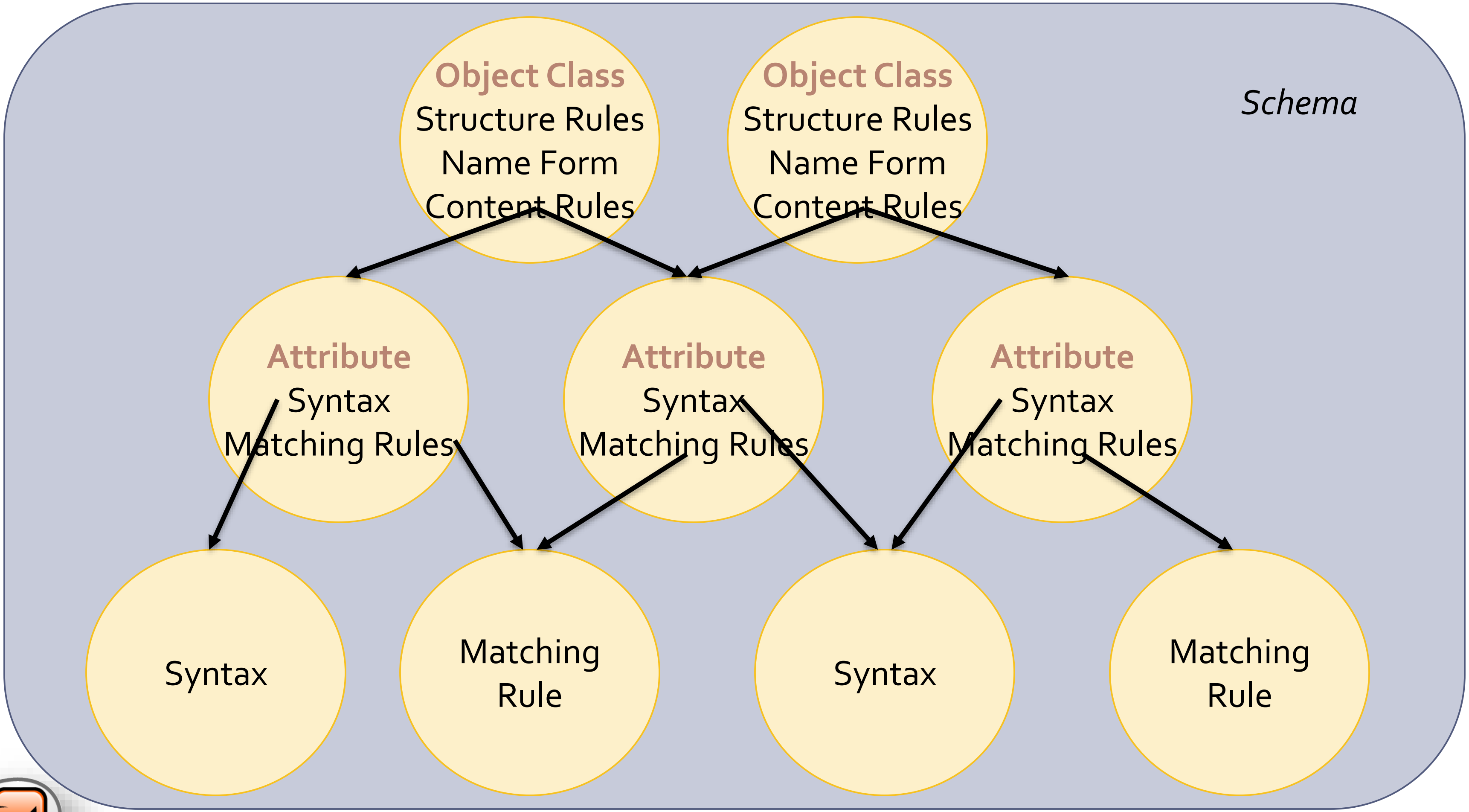
- Which attributes should be returned?
- Size limit
- Time limit
- …



LDAP API for C defined in RFC 1823

LDAP: Schema

- Specification of classes, attributes, matching rules
- Important: Consistency-check



Person Description

- Abstract class ‘top‘ (OID 2.5.6.1)
- Class ‘person‘ (OID 2.5.6.6)
  - Must contain: Surname (SN) | Common Name (CN)
  - May contain: userPassword | telephoneNumber | seeAlso | description
- Class ‘organizational person‘ (OID 2.5.6.7)
  - May contain: title | telexNumber | ...

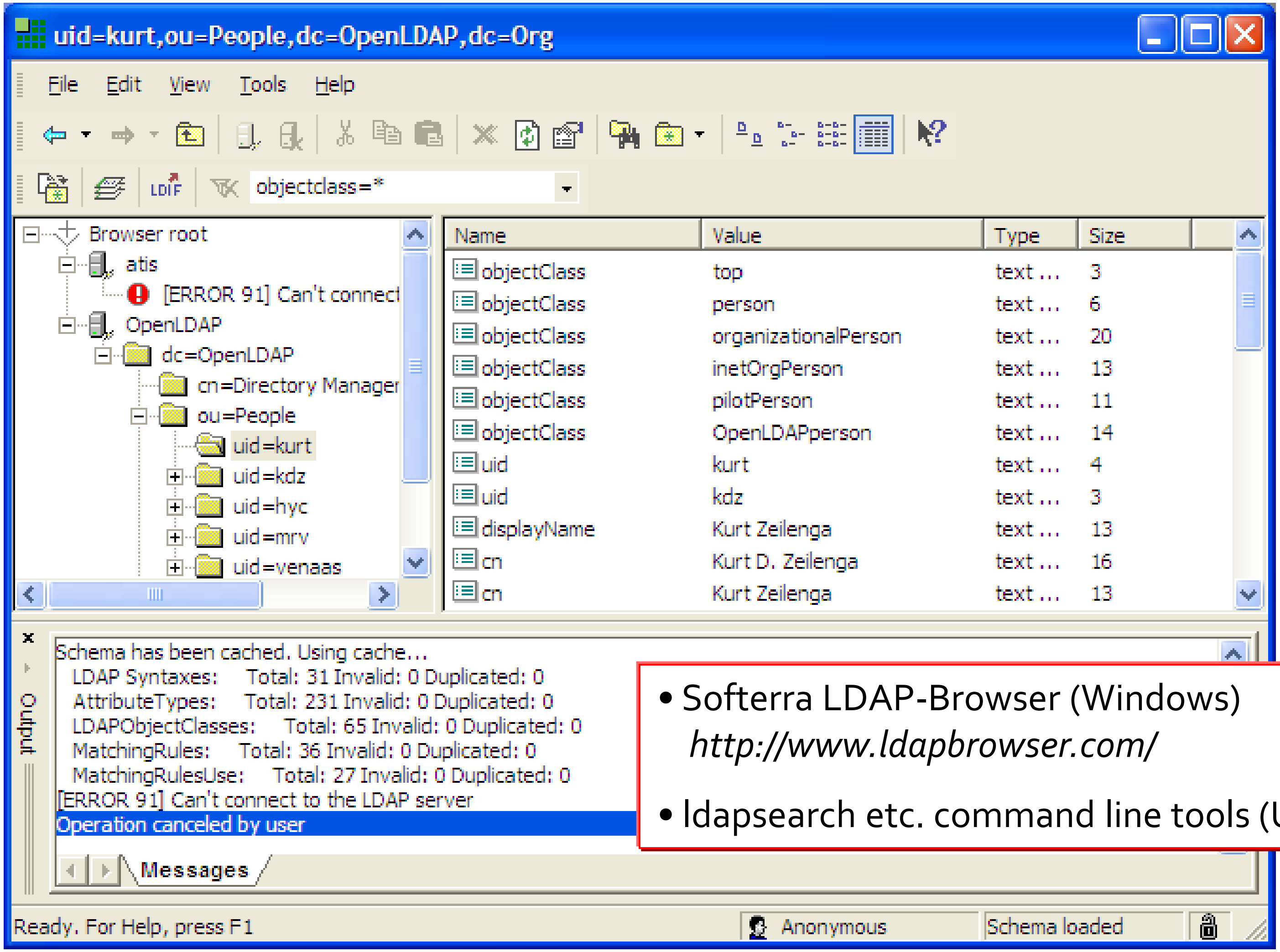
RFC 2256

- Class ‘interOrgPerson‘ (OID 2.16.840.1.113730.3.2.2)
  - May contain: carLicense | employeeNumber | photo | ...

RFC 2798

- In scope of the Internet2-Initiative: Definition of a ‘EduPerson‘.

Tool: LDAP-Browser



Name	Value	Type	Size
objectClass	top	text ...	3
objectClass	person	text ...	6
objectClass	organizationalPerson	text ...	20
objectClass	inetOrgPerson	text ...	13
objectClass	pilotPerson	text ...	11
objectClass	OpenLDAPperson	text ...	14
uid	kurt	text ...	4
uid	kdz	text ...	3
displayName	Kurt Zeilenga	text ...	13
cn	Kurt D. Zeilenga	text ...	16
cn	Kurt Zeilenga	text ...	13

```
Schema has been cached. Using cache...
  LDAP Syntaxes:    Total: 31 Invalid: 0 Duplicated: 0
  AttributeTypes:   Total: 231 Invalid: 0 Duplicated: 0
  LDAPObjectClasses:    Total: 65 Invalid: 0 Duplicated: 0
  MatchingRules:   Total: 36 Invalid: 0 Duplicated: 0
  MatchingRulesUse:    Total: 27 Invalid: 0 Duplicated: 0
[ERROR 91] Can't connect to the LDAP server
Operation canceled by user
```

- Softerra LDAP-Browser (Windows)
  http://www.ldapbrowser.com/
- ldapsearch etc. command line tools (Unix)

LDAP: Directory Management

Distribution approaches:

- *Replication*: Copy of a partition in another directory or on a different server
  - Single-Master, Multi-Master
  - Decision on performance and safety
- *Referral*: Requestor will be referred to another directory
- *Chaining*: LDAP server executes the referral itself and provides the answer to the client
- *Aliases*: References

- How are directories merged?

Directory Integration

- Sources: What are the sources?
- Synchronisation: How is the data compared?
- Data authority: Who does the data belong to or Who is authoritatively responsible for the data?
- Data consumers: Who requres that data?
- **Data protection: Which data can be disclosed to whom?**

- Meta-directories are currently only popular on the provider side

Chapter 5

MANAGEMENT OF ACCESS RIGHTS

Authorization

- *Authorization* is the process of verification and access right assignment for a resource/service to a subject
  - Not to be confused with *Authentication* (process of verification of claimed properties)

- Access Control is a process of access rights management and control

Access Matrix

Attention: Highly simplified!

Access Control Matrix

Subjects	Objects				
	Datei 1	Datei 2	Datei 3	Datei 4	…
Bill	Owner, r, w, x	-	-	r, w	
Joe	r, x	r, w	r	r	
Anne	a, c, d	Owner, r, x	r	…	

Subject's view → Capabilities

Object's view → Access Control Lists (ACLs)

Group- & role-based access rights management:

- Complexity reduction by clustering users into 'role groups'
- Inheritance relationships in rights management
- Permissions based on roles

Access Control Lists

- *Principal* is a user, group or process that can be authenticated
- Simply put, ACL is a set of resources, principals and corresponding access rights

Resource	Principal	Privilege
/home/Alice/script.sh	Alice	Read, Write, Execute
	Bob	Read
	Others	-

Access Control Models

- Discretionary Access Control (DAC)
  - Access rights are assigned per user. Owner of a resource can pass his own rights.
- Mandatory Access Control (MAC)
  - Rights passing is not allowed. The system alone decides on which user has access to which resources (for example, Security-Levels)
- Role-Based Access Control (RBAC)
  - User could potentially be assigned multiple roles. Access rights are role-based.

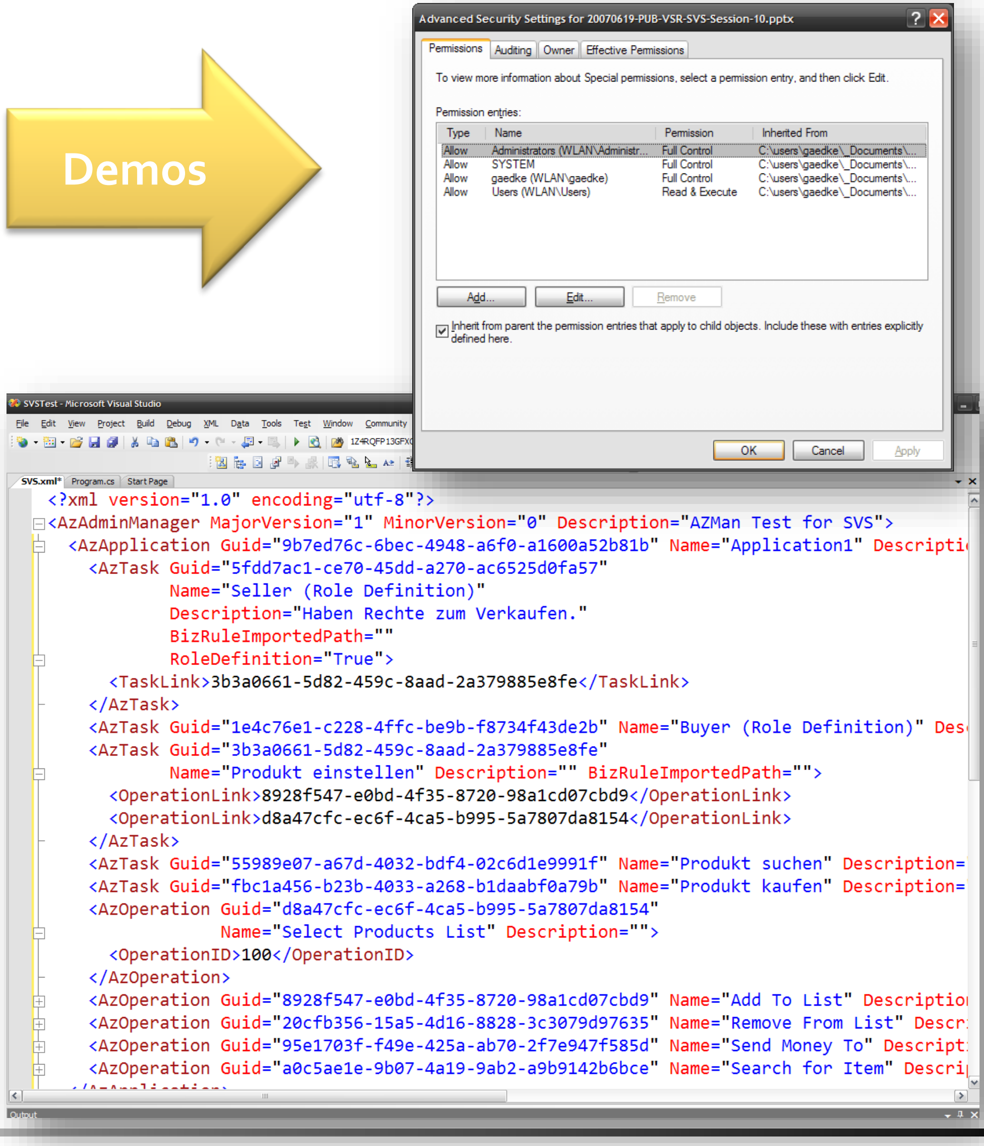
Realization in Operating Systems

- Unix/Linux:
  - Data/directories are associated to an inode descriptor (contains ID of the owner, ID of the group, ACL etc.)
  - Assignment of rights to the file owner, group, everyone else
- Windows 2000/XP/Vista/7
  - Permissions/restrictions can be assigned to individual users and groups
  - Security descriptors contain owner-ID, group-ID, Access Control Elements with Allow/Deny entries, logging operations

Examples / Demos / Concepts

- Concepts
  - ACLs & Groups
  - Roles
- What are the conceptual differences?
  - Why are roles typical for LOB applications?

Demos



Advanced Security Settings for 20070619-PUB-VSR-SVS-Session-10.pptx

To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From
Allow	Administrators (WLAN\Administr...	Full Control	C:\users\gaedke_Documents\...
Allow	SYSTEM	Full Control	C:\users\gaedke_Documents\...
Allow	gaedke (WLAN\gaedke)	Full Control	C:\users\gaedke_Documents\...
Allow	Users (WLAN\Users)	Read & Execute	C:\users\gaedke_Documents\...

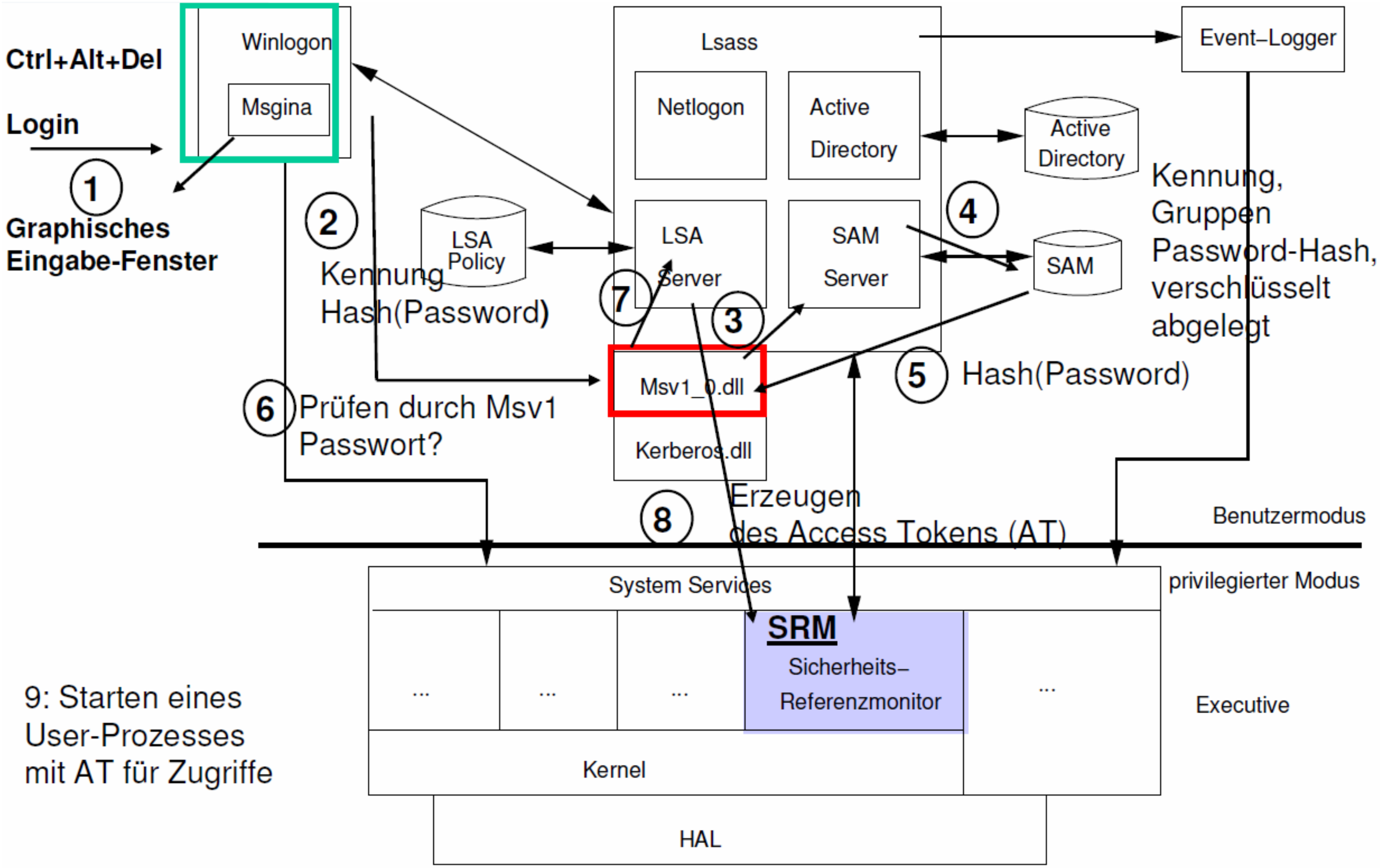
☑ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.

SVSTest - Microsoft Visual Studio

```
<?xml version="1.0" encoding="utf-8"?>
<AzAdminManager MajorVersion="1" MinorVersion="0" Description="AZMan Test for SVS">
  <AzApplication Guid="9b7ed76c-6bec-4948-a6f0-a1600a52b81b" Name="Application1" Descripti
    <AzTask Guid="5fdd7ac1-ce70-45dd-a270-ac6525d0fa57"
            Name="Seller (Role Definition)"
            Description="Haben Rechte zum Verkaufen."
            BizRuleImportedPath=""
            RoleDefinition="True">
      <TaskLink>3b3a0661-5d82-459c-8aad-2a379885e8fe</TaskLink>
    </AzTask>
    <AzTask Guid="1e4c76e1-c228-4ffc-be9b-f8734f43de2b" Name="Buyer (Role Definition)" Des
    <AzTask Guid="3b3a0661-5d82-459c-8aad-2a379885e8fe"
            Name="Produkt einstellen" Description="" BizRuleImportedPath="">
      <OperationLink>8928f547-e0bd-4f35-8720-98a1cd07cbd9</OperationLink>
      <OperationLink>d8a47cfc-ec6f-4ca5-b995-5a7807da8154</OperationLink>
    </AzTask>
    <AzTask Guid="55989e07-a67d-4032-bdf4-02c6d1e9991f" Name="Produkt suchen" Description=
    <AzTask Guid="fbc1a456-b23b-4033-a268-b1daabf0a79b" Name="Produkt kaufen" Description=
    <AzOperation Guid="d8a47cfc-ec6f-4ca5-b995-5a7807da8154"
                 Name="Select Products List" Description="">
      <OperationID>100</OperationID>
    </AzOperation>
    <AzOperation Guid="8928f547-e0bd-4f35-8720-98a1cd07cbd9" Name="Add To List" Descriptio
    <AzOperation Guid="20cfb356-15a5-4d16-8828-3c3079d97635" Name="Remove From List" Descr
    <AzOperation Guid="95e1703f-f49e-425a-ab70-2f7e947f585d" Name="Send Money To" Descript
    <AzOperation Guid="a0c5ae1e-9b07-4a19-9ab2-a9b9142b6bce" Name="Search for Item" Descri
  </AzApplication>
```

Example: Windows 2000/XP

Local Security Authority Subsystem Service (LSASS)



Quelle: C. Eckert

Discussion

- Identity- and access management is the technical foundation for IT-security management
- Radius, Kerberos, PKIs and LDAP form a basis for authentication and rights management for distributed systems
- ... and, especially, for integrated information management
  - Important for IT-security management for current-state detection, for example with respect to ITnetworks , consistency checks, ...
- Challenges:
  - Construction of an integrated directory
  - ‘Directory Enabled Applications‘; for example, combination of AAA and network management
  - Consistent right- and policy management
  - Data protection
- Trend: XML, Web Services

Chapter 6

INTERNET FIREWALLS

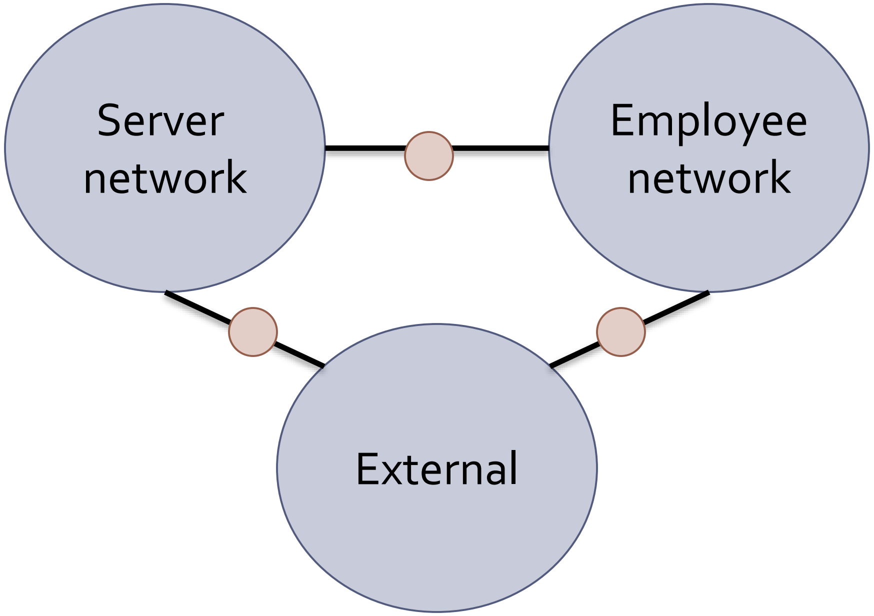
Definition and Fundamentals

- Hard- or software components, which control the interconnection point between two network areas.
- Implements security strategies by restricting packet forwarding.

Fundamentals:

- Packet filter
  - Entity, which selectively processes flowing packets according to pre-defined rules, in particular, preventing packet forwarding
- Proxy approaches
  - Representative of a client process
- Network Address Translation (NAT)
  - Address translation. Public and private addresses are distinguished
- Bastion Host
  - Computer with particularly high protection requirements; vulnerability mainly results from the computer‘s exposed location
- Dual-Homed Host
  - Computer with at least two network interfaces for two different subnets

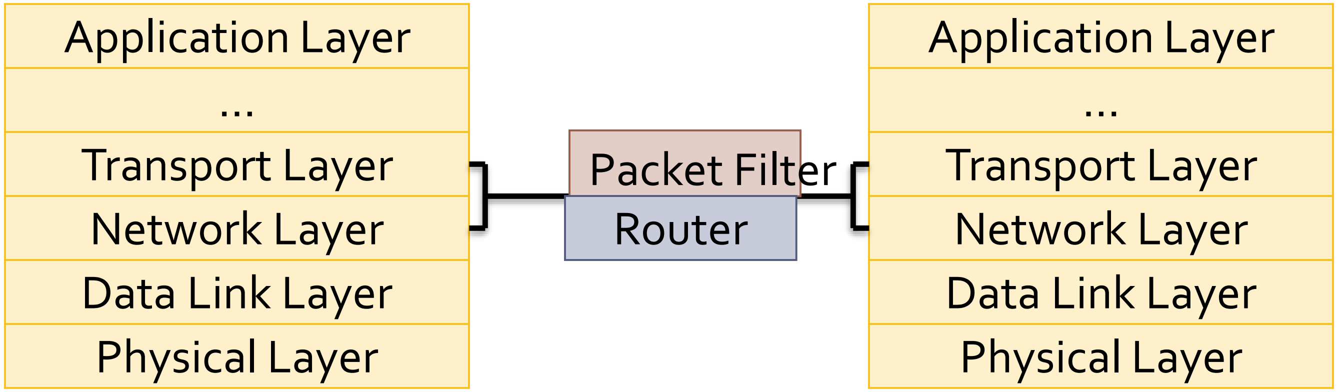
Illustration Packet Filter



Server network

Employee network

External



Application Layer

…

Transport Layer

Network Layer

Data Link Layer

Physical Layer

Packet Filter

Router

Application Layer

…

Transport Layer

Network Layer

Data Link Layer

Physical Layer

Filter Rules: University Case Study

Employee network →External
Protocols with access to all
Target computers

Protokoll	Ports
Finger	TCP 79
FTP [1]	TCP 20, 21
Ident	TCP 113
Ping	ICMP 8
SSH	TCP 22
SSH alternativer Port für SSH2	TCP 24
Telnet [1]	TCP 23
Whois	TCP 43
WWW	TCP 80

[1])Protocols with clear text passwords. These are only available on request

Employee network → External
Protocol with access to individual target machines

Protokoll	Ports	Server
ADSM/TSM	TCP 1501-1509	TSM-Server
DNS	UDP 53 (TCP 53)	Uni-Nameserver
NNTP	TCP 119	News-Server
Huelka	TCP 19991-19993, 37251	Huelka-Server
Imap[1]	TCP 143	Imap-Server
Imaps (secure Imap)	TCP 993	Imap-Server
Spop3 (Secure POP3)	TCP 995	POP-Server
SMTP	TCP 25	Mailserver
WWW-Cache	TCP 3128	Cache-Server

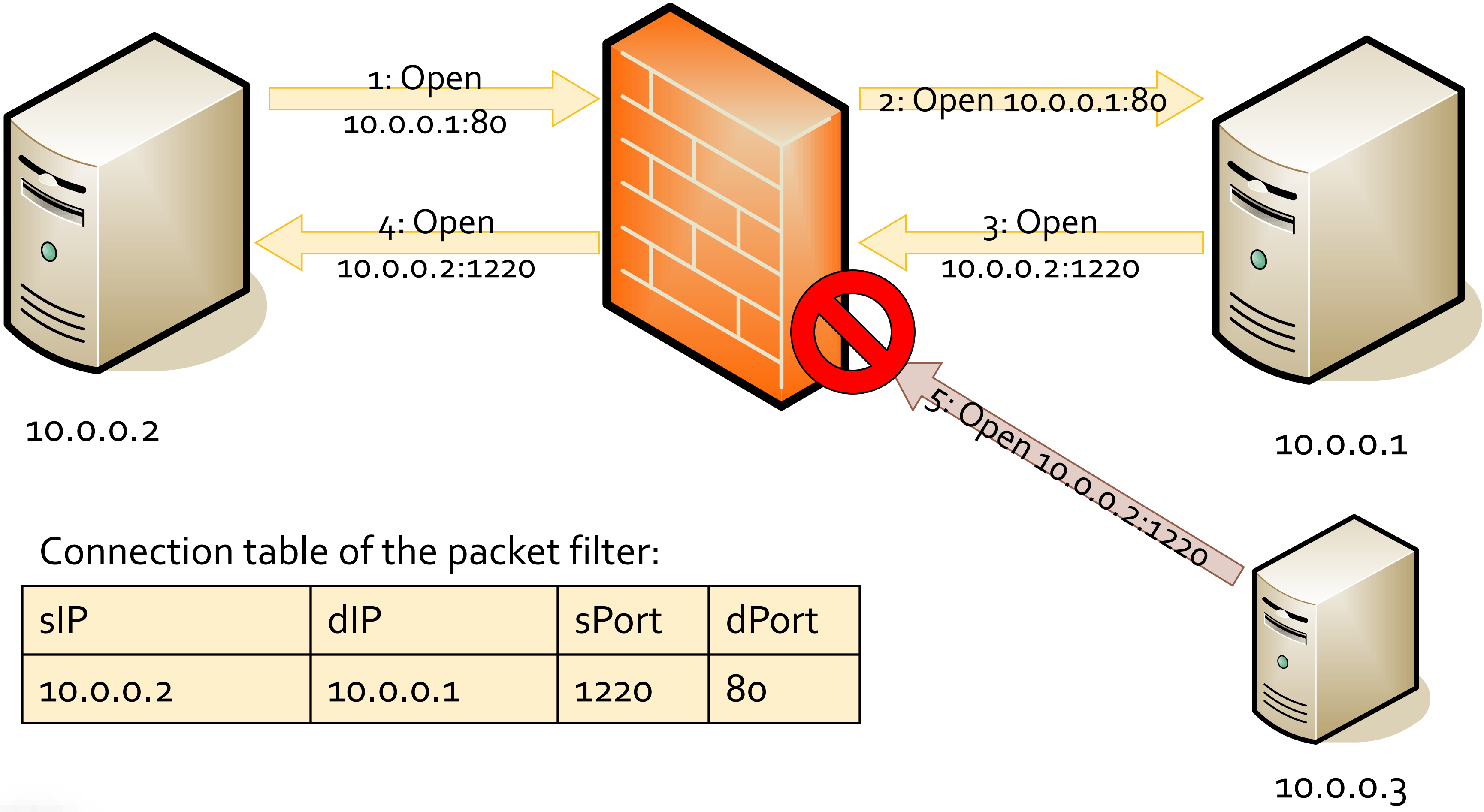
Router Filter Rules (Example)

Access-list	Acl number	Permit Deny	Protocol	Source Address and Mask	Destination Address and Mask	Eq Gt Lt Neq	UDP/TCP Port

```
deny icmp 129.12.0.0 0.0.255.255 any
deny udp any any eq 69
permit ip  192.70.120.11 any
```

- Linux environment tools: Iptables, ipchains, ipfilter …

Dynamic Packet Filter



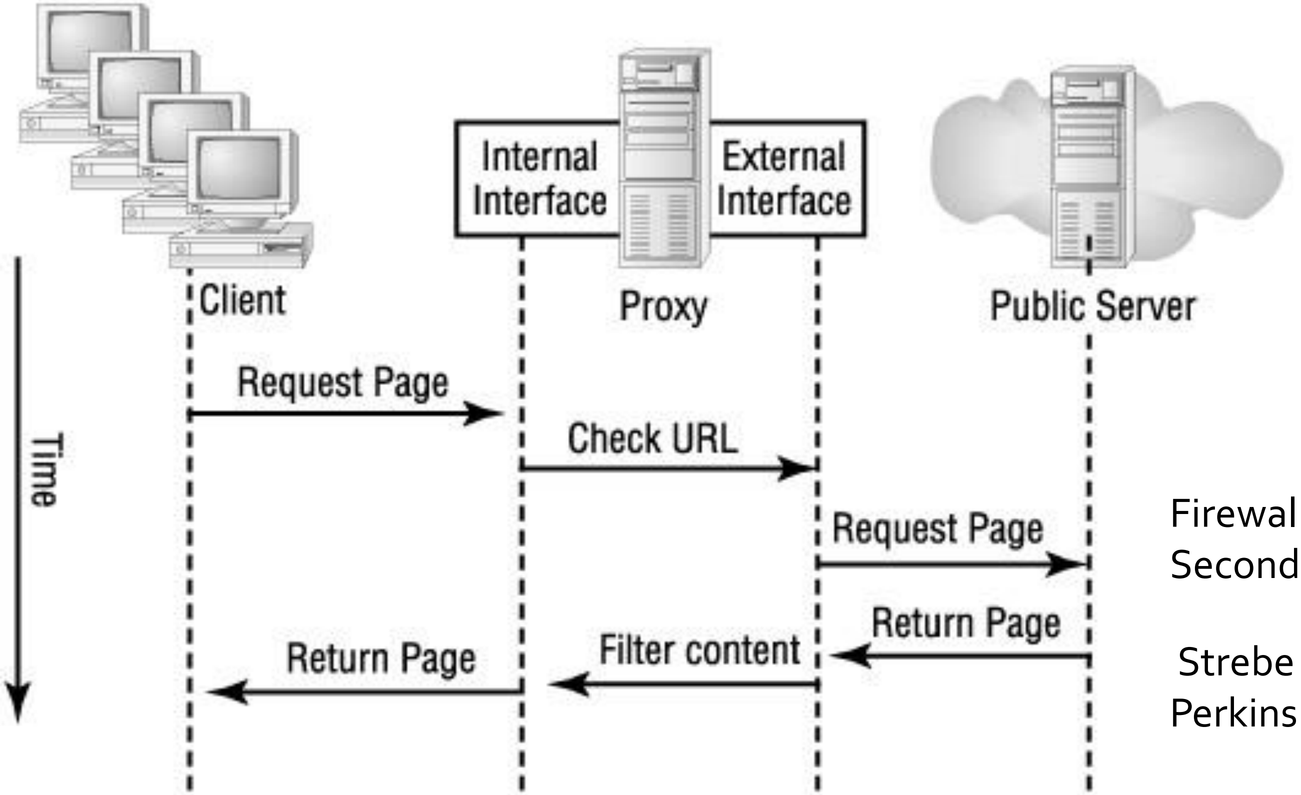
Connection table of the packet filter:

sIP	dIP	sPort	dPort
10.0.0.2	10.0.0.1	1220	80

Filter Table Guidelines

- “Default Deny“: Prohibit everything, which is not explicitly allowed
- Order: Filter table is usually processed sequentialy. Analysis is terminated after all the rules have been applied.
  - One should maintain a correct order
- Prevent spoofing attacks (see, for example, RFC 2827)
  - Packets coming from ‘outside‘ with ‘inside‘ addresses are rejected
  - Same holds in the other direction – if the source address is not an ‘inside‘ one
- Static filters: UDP blocking
- Controlled handling of ICMP
- Prevent Source-routing
- Efficiency: unnecessary filtering rules have to be removed

Proxy-Firewall



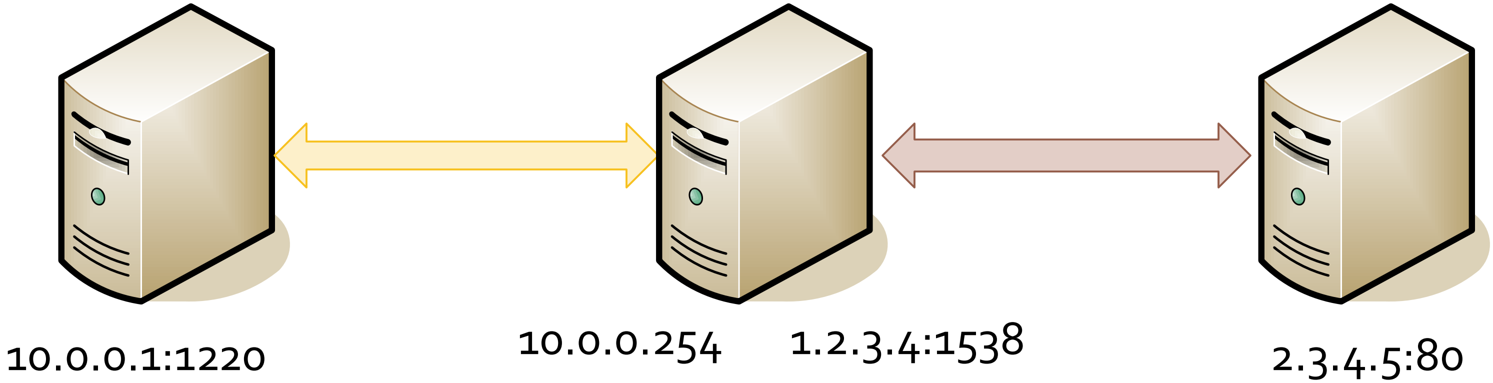
Firewalls 24Seven, Second Edition by Matthew

Strebe and Charles Perkins Sybex © 2002

- Typically, at transport layer or as an application proxy
- Transport layer: requires client code modification
- Application proxy: can perform service-specific controls

Network Address Translation

- Proxy concept at the network layer
- Initially: Preservation of the IPv4 address space
- Today: Internal network structure concealment
- In practice, giving up the end-to-end principle as it leads to numerous difficulties (for example, ftp)

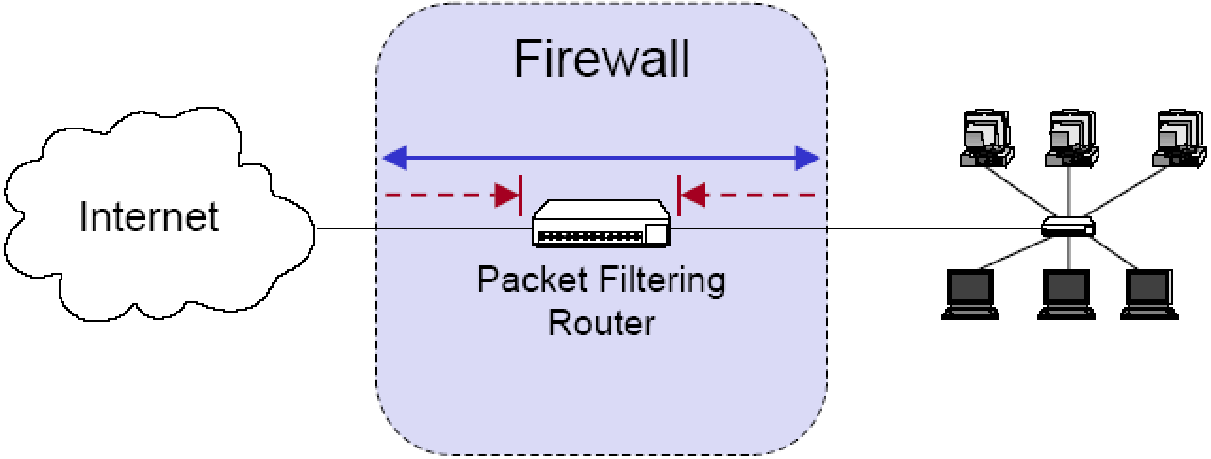


Verbindungstabelle der NAT

sIP	dIP	sNATIP	sPort	dPort	sNATPort
10.0.0.1	2.3.4.5	1.2.3.4	1220	80	1538

Architectures (1)

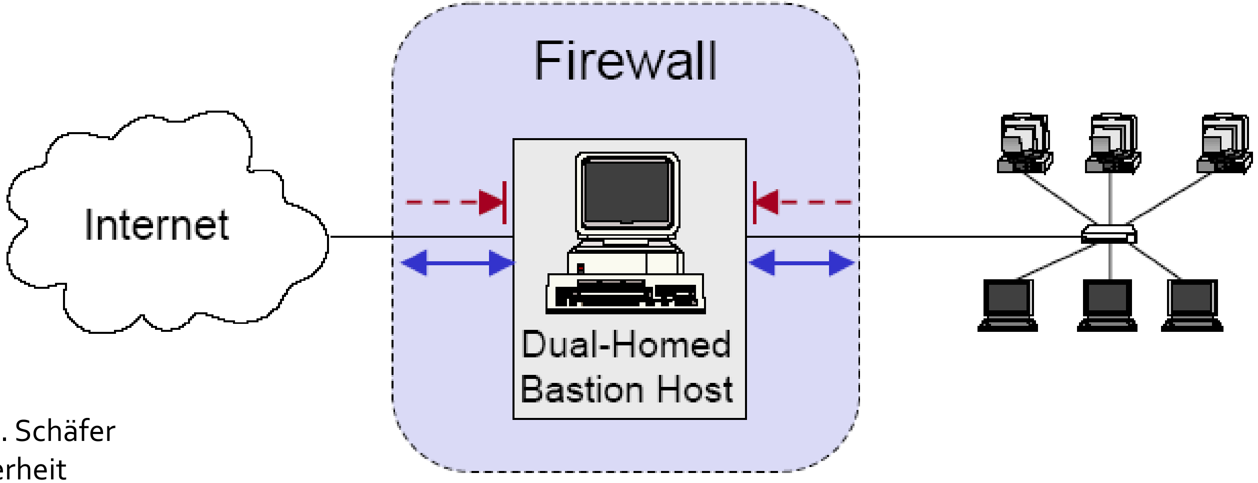
Screening Router Architecture



- - - -▸| Denied Traffic

◂——▸ Permitted Traffic

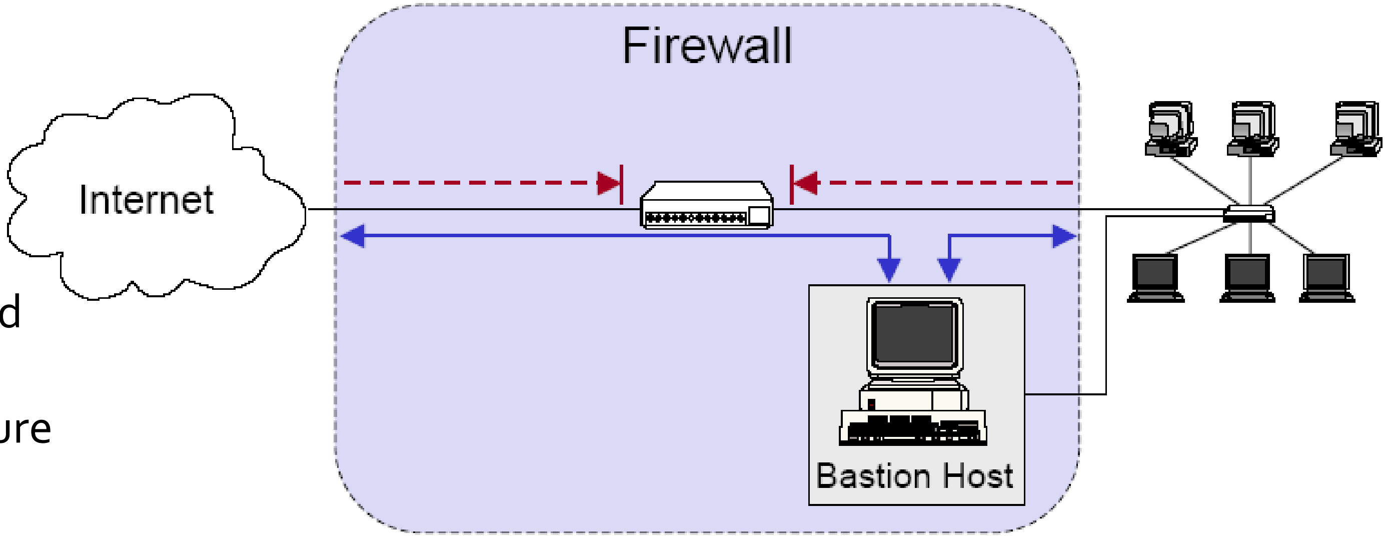
Homed-Host Architecture



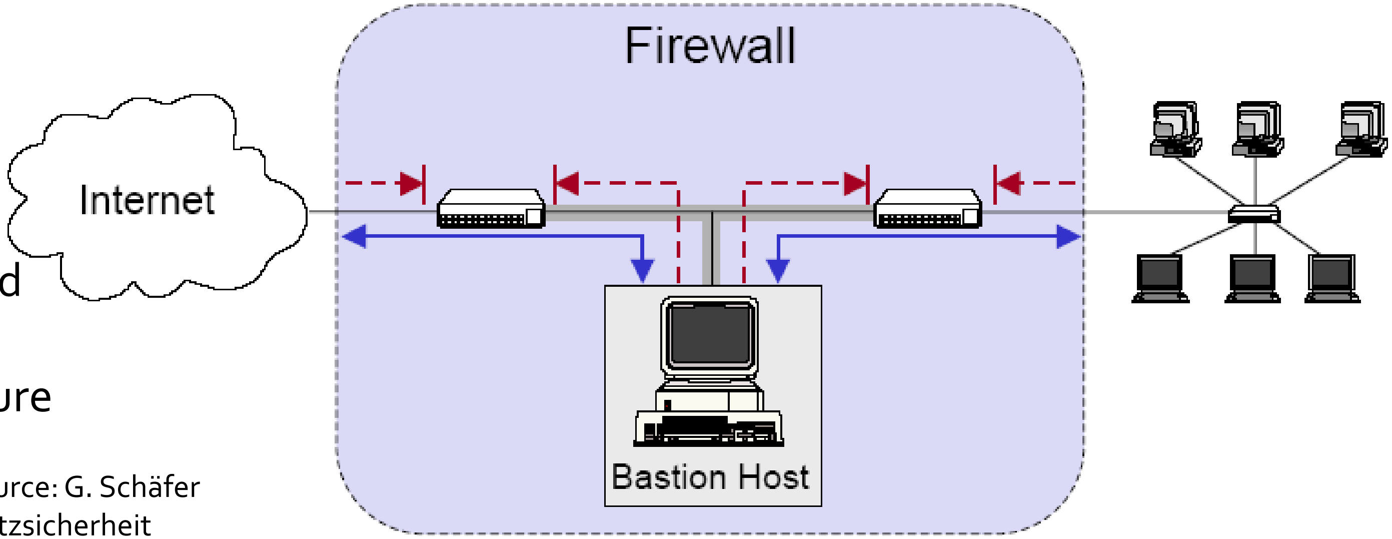
Source: G. Schäfer Netzsicherheit

Architectures (2)

Screened Host Architecture

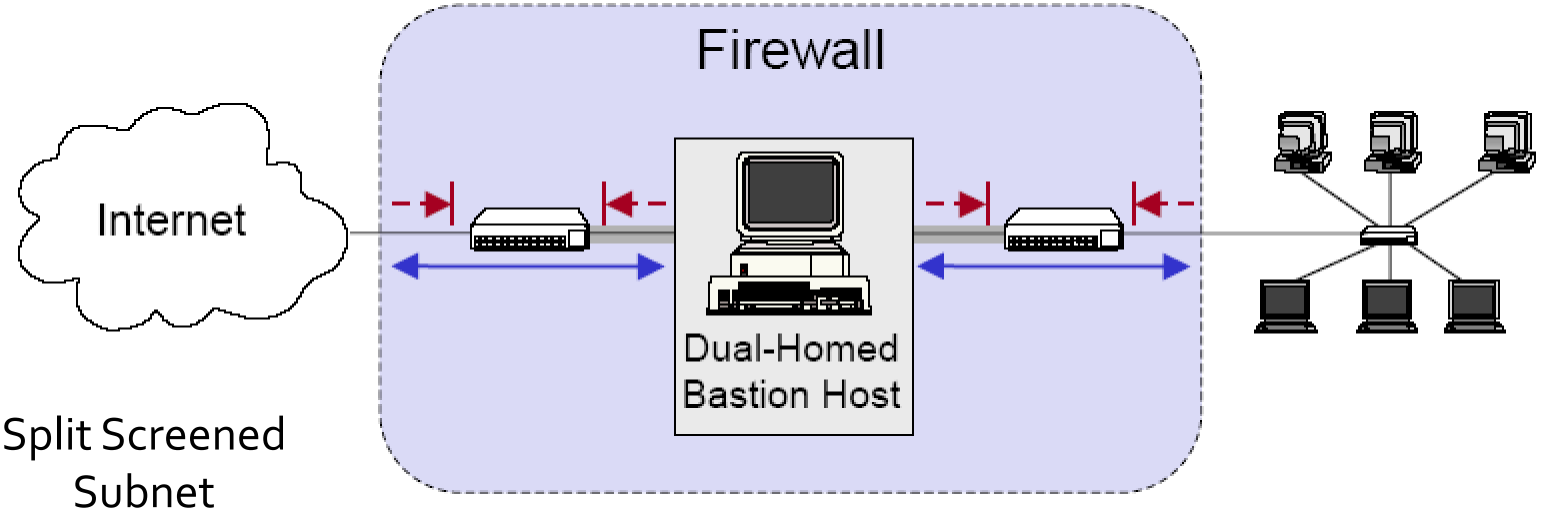


Screened Subnet Architecture



Source: G. Schäfer Netzsicherheit

Architectures (3)



Split Screened Subnet Architecture

Perimeter Network

Demilitarized Zone (DMZ)

Source: G. Schäfer
Netzsicherheit

Disappearing Perimeter

- Mobile devices
- Peer-to-Peer systems
- Ubiquitous computing
- Ad-Hoc networks
- Sensor networks
- …

- No clearly defined "perimeter network" available anymore

IT-Security Management Aspects

- Determination of the required security level
- Firewall placement and coordination
  - Clear transition point between ‘internal‘ and ‘external‘?
  - Select entrance architecture (dual homed, screened subnet, ...)
  - Should the subnets be protected from one another?
  - Do devices require ‘personal firewalls‘?
  - How can the three stages (entrance, subnet, end-system) be kept consistent and checked for errors?
- Analysis of open communication channels
  - Dependencies on the first point
  - Administration concept: who gets to issue which rules?
- Firewall management requires security policy support

Used Literature and Links

- Matthew Strebe and Charles Perkins, *Firewalls 24Seven*, 2nd ed., Sybex, 2002
- IP Accounting, Arbeitsbericht BelWü Koordination, 2002
- Günter Schäfer, *Netzsicherheit*, dpunkt.verlag, 2003
- Claudia Eckert, *IT-Sicherheit*, 3. Auflage, Oldenbourg Verlag, 2004; Chapter 12

Chapter 7

INTRUSION DETECTION SYSTEMS

Intrusion Detection

Motivation:

- Computer has been compromized and is used for (illegal) data distribution
- Network operator performs IP accounting and finds out that a computer, which has previously generated next to no load, is suddenly generating a high amount of it
- Goal: Attack detection and intrusion detection alarm

IDS:

- Find and report suspicious activity in systems and networks
- Intrusion prevention: Initiation of control measures
  - Intrusion response

Intrusion Detection: Classification

Location:

- Host-based
  - System breach and misuse detection
  - Examination of log files
  - Integrity checks by checksums
  - Inspection of “Privilege Escalation“
- Network-based
  - Monitoring and verification of network traffic, which can take place at various network locations
- Hybrid

Detection:

- Signature-based
- Anomaly-based

Signature-based Detection

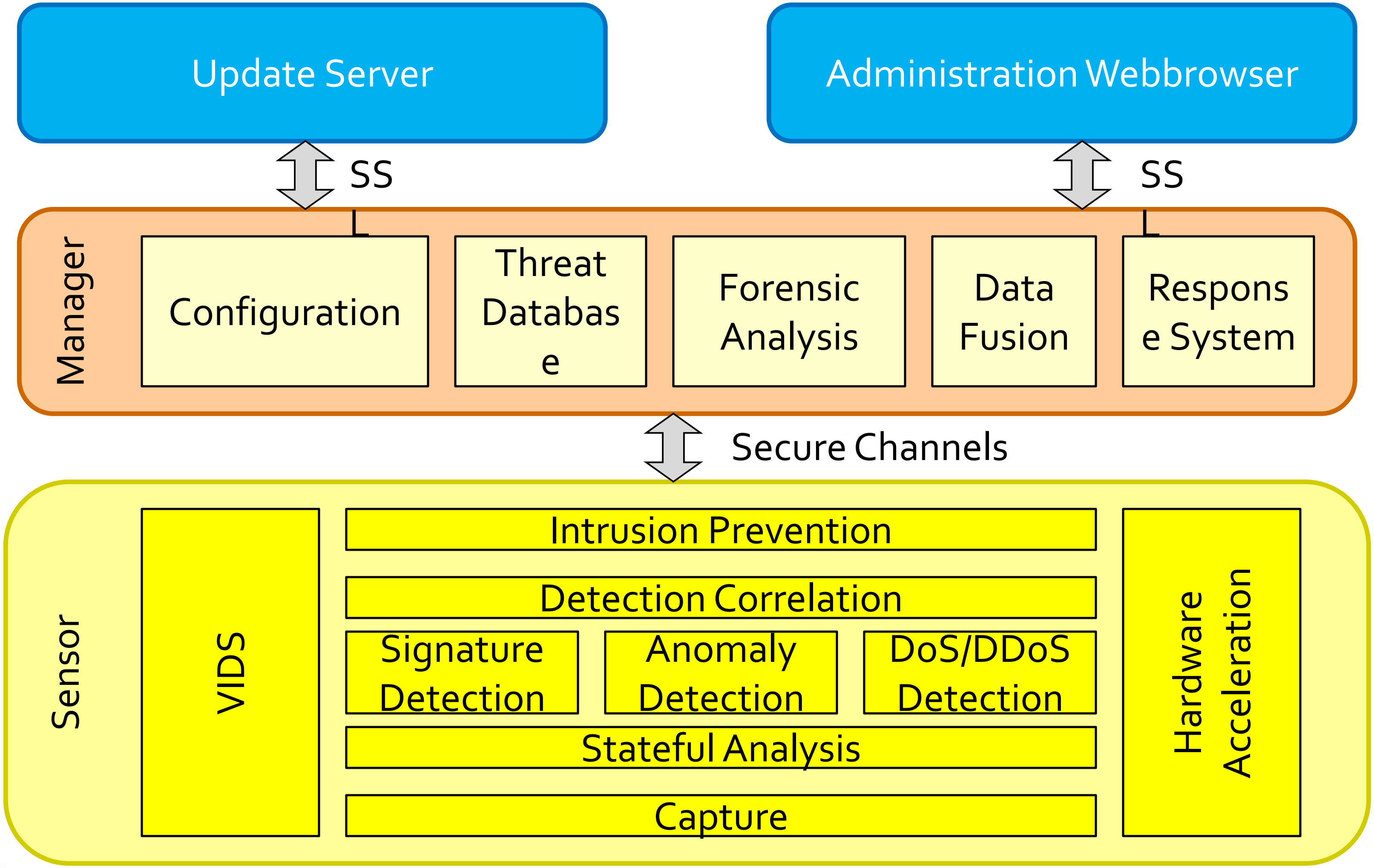
- Break-in (attempt) detection based on known procedures
  - For example, the known Buffer Overflow attack
  - For example, implies *default.ida* within a URL in an HTTP packet together with a certain pattern in the URL Argument Name Field is a Code Red attack
- Signatures must (same holds for the virus scanner) be kept up-to-date
- Challenges:
  - Register the attacks
  - Describe the attacks
  - Errors of type 1. and 2. (classification problem)

Anomaly-based Detection

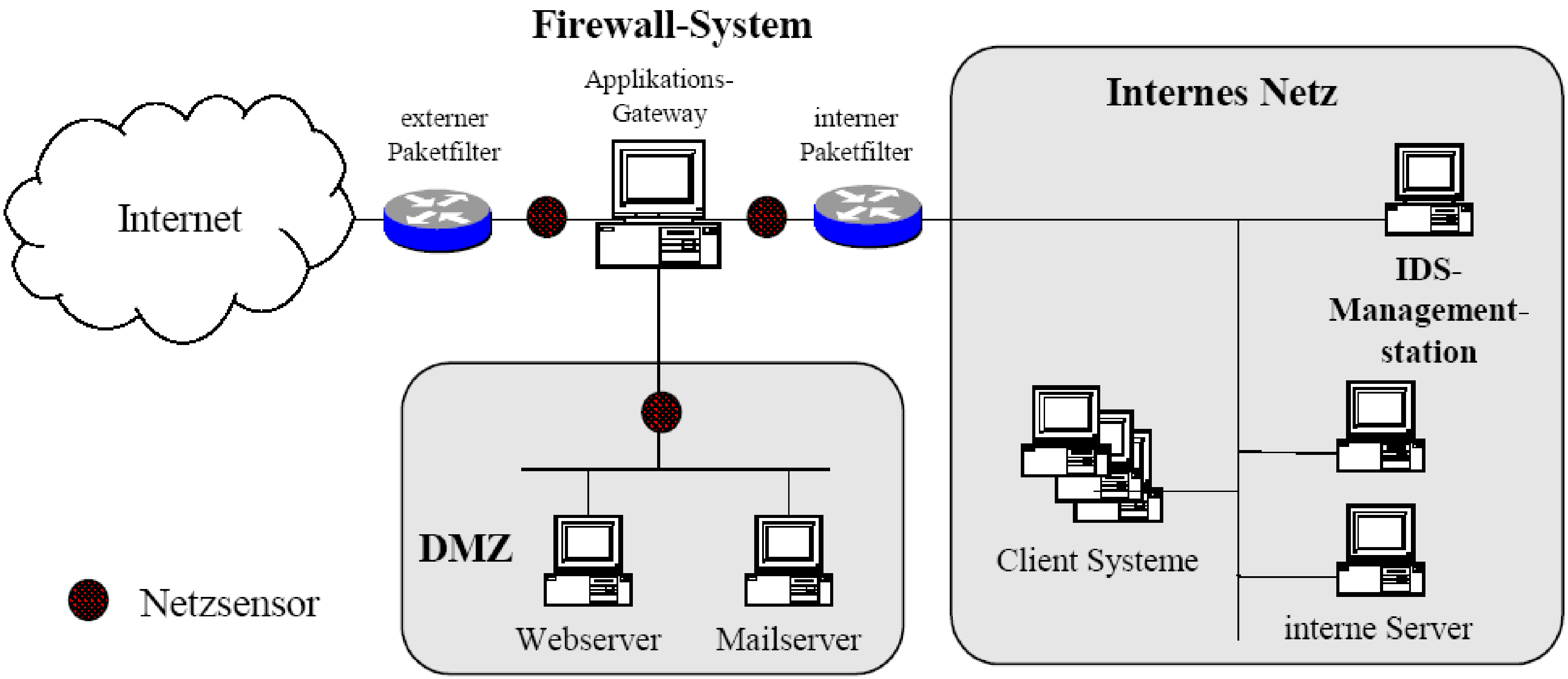
- Detection of ‘normal‘ user behaviour devitations
- Nomal behaviour has to be statically describable
- Classification problem
- Normal behaviour should be determined through learning

- Very effective attacks not deviating much from normal user behaviour might remain undetected

Case Study: McAfee IntruShield™



Example: Securing Gateways



Honeypots

Approach:

- Place unsecured server/service („Honeypots“) in the network
- Monitor Honeypots
- Analyse attacks and compromises
  - Identify tools, tactics and intruder motives

Typical objectives:

- Detect Botnet attacks
  - Botnet: Network of compromized computers that can be remotely orchestrated by the attacker
- Detect phishing attacks

IT-Security Management: IDS / IPS

- Intrusion Detection is a reactive IT-security approach
  - Complements preventive measures, such as firewalls
- Data protection legal requirements must be met
- Intrusion prevention (response): given automatic reactions, one has to make sure they can not be used as an attack themselves (such as Denial-of-Service)
- Integration with network management is appropriate and necessary

Used Literature and Links

- Günter Schäfer, *Netzsicherheit*, dpunkt.verlag, 2003
- Claudia Eckert, *IT-Sicherheit*, 3. Auflage, Oldenbourg Verlag, 2004
- Hartmut König, *IntrusionDetection - Möglichkeiten und Probleme einer wirksamen Erkennung sicherheitsgefährdender Aktionen im Internet*, KuVS Summer School 2004, http://www-rnks.informatik.tu-cottbus.de/~forschung
- BSI, Einführung von Intrusion-Detection-Systemen, Grundlagen, Version 1, Oktober 2002
- McAfee, IntruShield Technical Workshop, 2004

Chapter 8

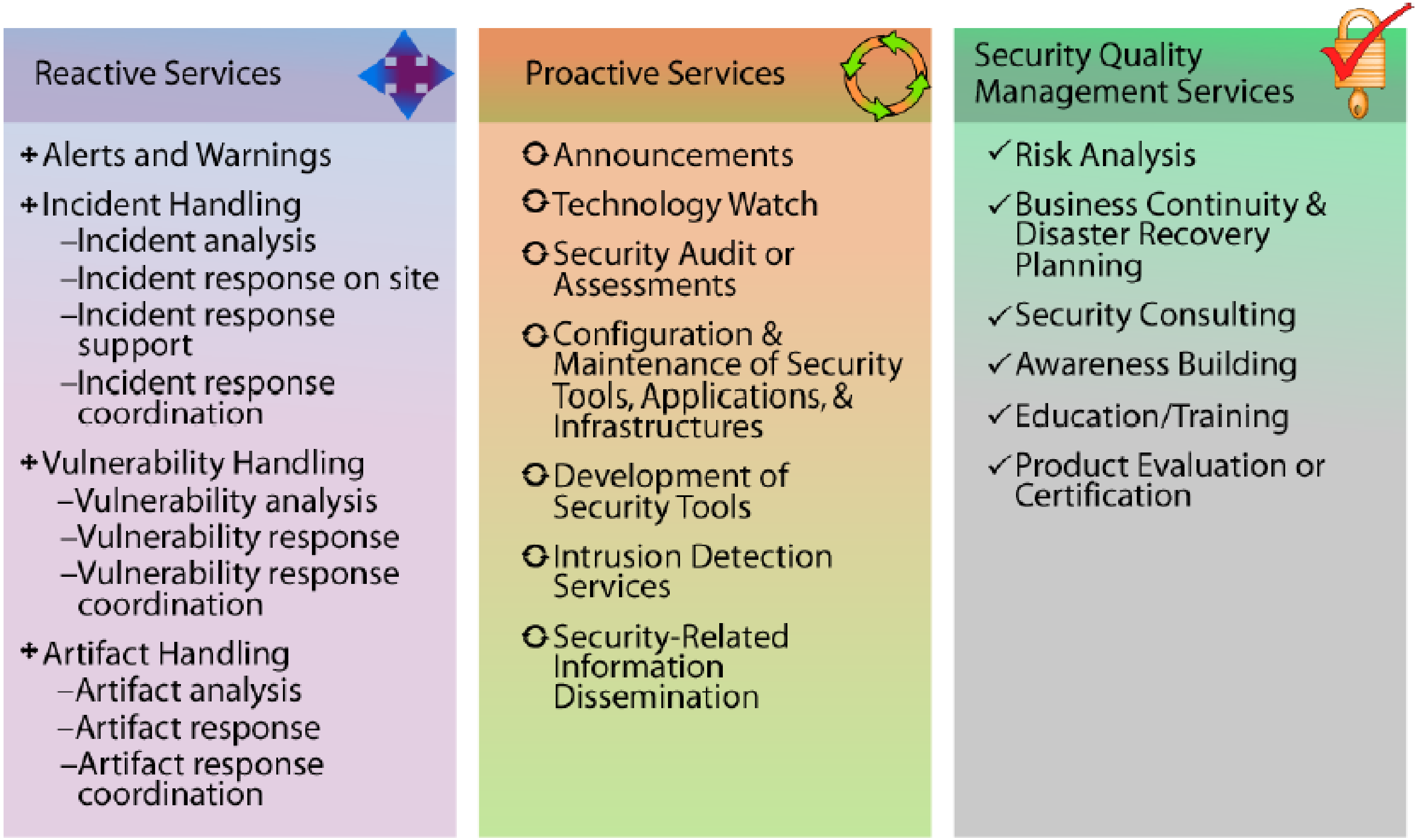
INCIDENT MANAGEMENT

History of CERTs / CSIRTs

- Trigger: Internet worm 1988
- Need of an IT-security ‘fire brigade‘ became evident
- CERT/CC ‚Computer Emergency Response Team / Coordination Center‘ was founded by DARPA and located at CMU

- Today:
  - Not just ‘Response‘, but, generally, ‘Incident Handling‘
  - Many CERTs and CSIRTs (Computer Security Incident Response Team) in the world, z.B. DFN-CERT, M-CERT, CERT-Bund, ...
  - In Germany: CERT-network
  - International network: FIRST
    (Forum of Incident Response and Security Teams)

CSIRTs Tasks



Reactive Services

- + Alerts and Warnings
- + Incident Handling
  - –Incident analysis
  - –Incident response on site
  - –Incident response support
  - –Incident response coordination
- + Vulnerability Handling
  - –Vulnerability analysis
  - –Vulnerability response
  - –Vulnerability response coordination
- + Artifact Handling
  - –Artifact analysis
  - –Artifact response
  - –Artifact response coordination

Proactive Services

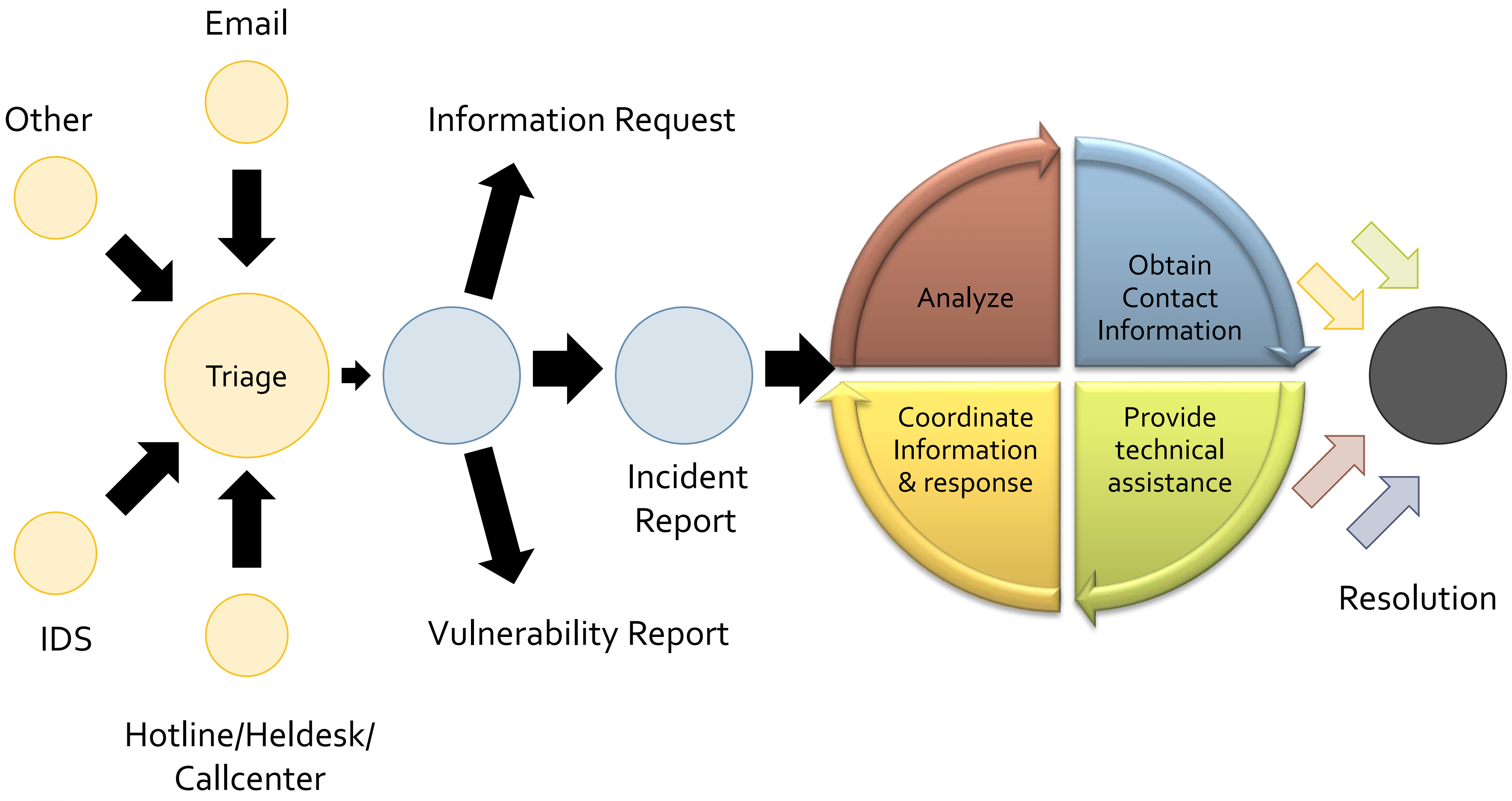
- ○ Announcements
- ○ Technology Watch
- ○ Security Audit or Assessments
- ○ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- ○ Development of Security Tools
- ○ Intrusion Detection Services
- ○ Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

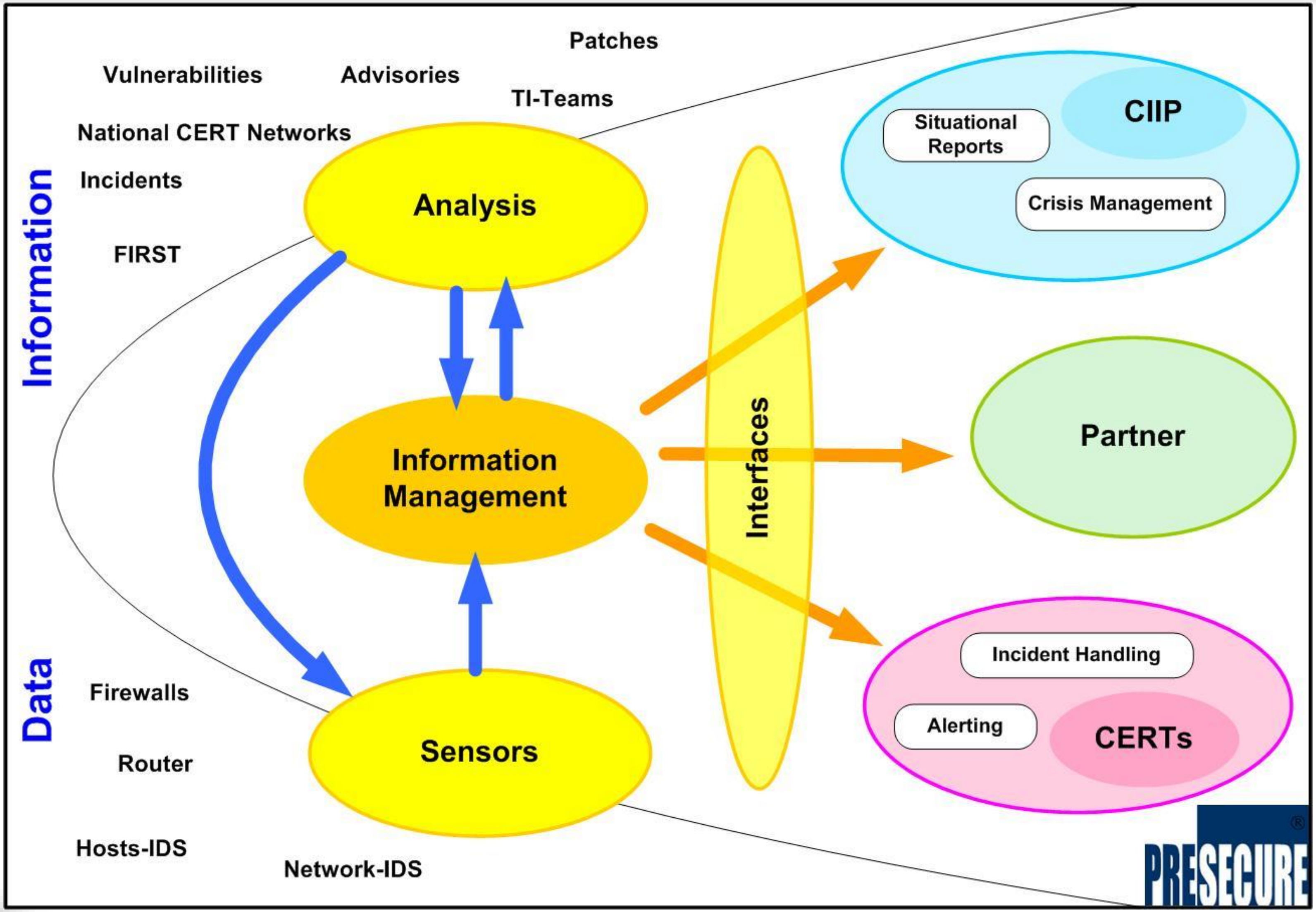
Handbook for Computer Security, Incident ResponseTeams (CSIRTs), 2nd ed., 2003

Incident Handling


Email
Other
Information Request
Analyze
Obtain Contact Information
Triage
Coordinate Information & response
Provide technical assistance
Incident Report
Resolution
IDS
Vulnerability Report
Hotline/Heldesk/ Callcenter

Handbook for Computer Security Incident ResponseTeams (CSIRTs), 2nd ed., 2003

Coordination: Early Warning System



Naming Example

- Naming requires standardization
  - Otherwise, cooperation and coordination become complex
- Standard: Common Vulnerabilities and Exposures
  - Managed by The Mitre Corporation

Name: CVE-2004-0309

Description:

Stack-based buffer overflow in the SMTP service support in vsmon.exe in Zone Labs ZoneAlarm before 4.5.538.001, ZoneLabs Integrity client 4.0 before 4.0.146.046, and 4.5 before 4.5.085, allows remote attackers to execute arbitrary code via a long RCPT TO argument.

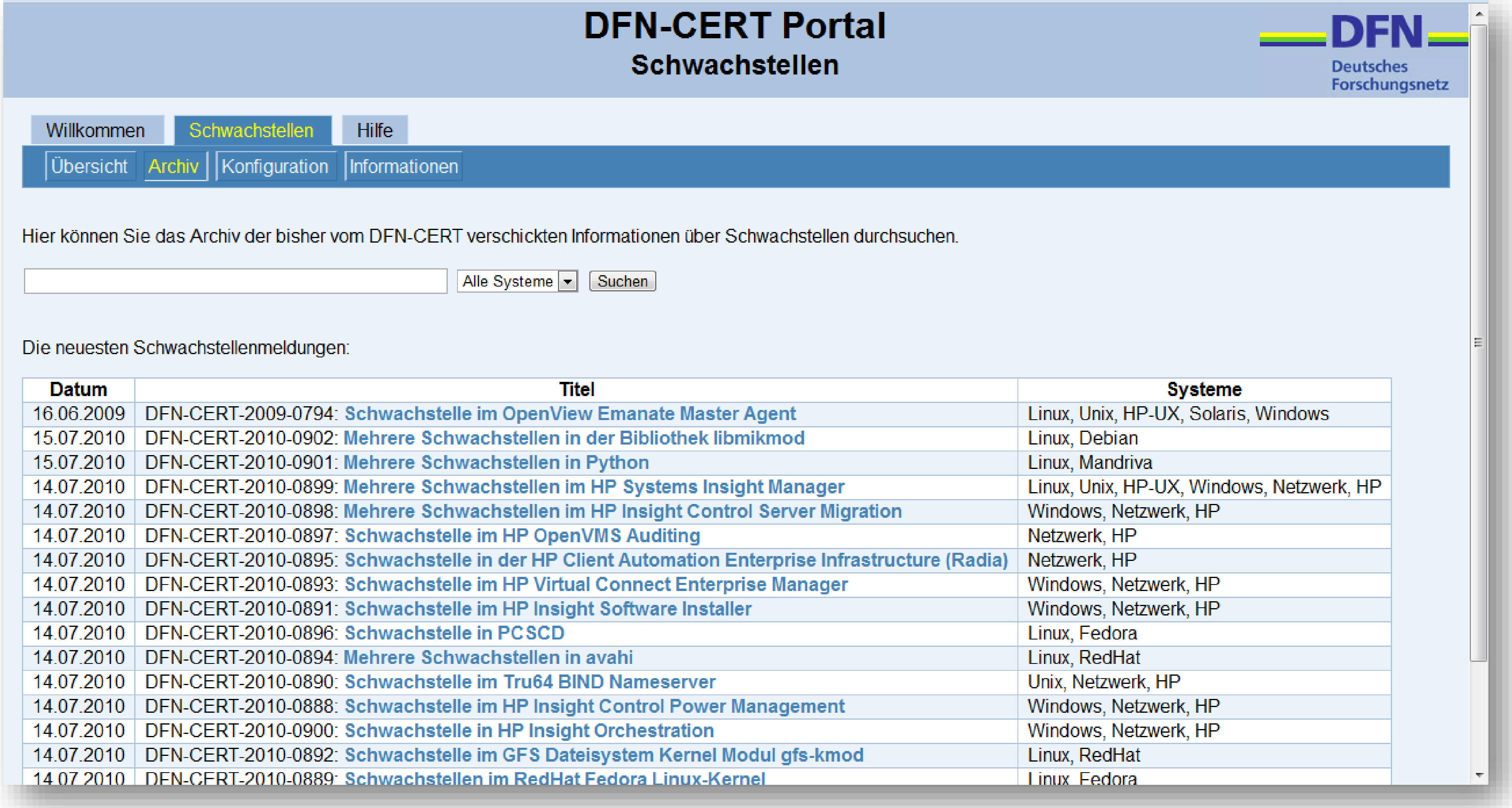
Status: Entry

Reference: BUGTRAQ:20040219 EEYE: ZoneLabs SMTP Processing Buffer Overflow

Reference: CERT-VN:VU#619982

…

DFN-CERT



DFN-CERT Portal

Schwachstellen

Hier können Sie das Archiv der bisher vom DFN-CERT verschickten Informationen über Schwachstellen durchsuchen.

Die neuesten Schwachstellenmeldungen:

Datum	Titel	Systeme
16.06.2009	DFN-CERT-2009-0794: Schwachstelle im OpenView Emanate Master Agent	Linux, Unix, HP-UX, Solaris, Windows
15.07.2010	DFN-CERT-2010-0902: Mehrere Schwachstellen in der Bibliothek libmikmod	Linux, Debian
15.07.2010	DFN-CERT-2010-0901: Mehrere Schwachstellen in Python	Linux, Mandriva
14.07.2010	DFN-CERT-2010-0899: Mehrere Schwachstellen im HP Systems Insight Manager	Linux, Unix, HP-UX, Windows, Netzwerk, HP
14.07.2010	DFN-CERT-2010-0898: Mehrere Schwachstellen im HP Insight Control Server Migration	Windows, Netzwerk, HP
14.07.2010	DFN-CERT-2010-0897: Schwachstelle im HP OpenVMS Auditing	Netzwerk, HP
14.07.2010	DFN-CERT-2010-0895: Schwachstelle in der HP Client Automation Enterprise Infrastructure (Radia)	Netzwerk, HP
14.07.2010	DFN-CERT-2010-0893: Schwachstelle im HP Virtual Connect Enterprise Manager	Windows, Netzwerk, HP
14.07.2010	DFN-CERT-2010-0891: Schwachstelle im HP Insight Software Installer	Windows, Netzwerk, HP
14.07.2010	DFN-CERT-2010-0896: Schwachstelle in PCSCD	Linux, Fedora
14.07.2010	DFN-CERT-2010-0894: Mehrere Schwachstellen in avahi	Linux, RedHat
14.07.2010	DFN-CERT-2010-0890: Schwachstelle im Tru64 BIND Nameserver	Unix, Netzwerk, HP
14.07.2010	DFN-CERT-2010-0888: Schwachstelle im HP Insight Control Power Management	Windows, Netzwerk, HP
14.07.2010	DFN-CERT-2010-0900: Schwachstelle in HP Insight Orchestration	Windows, Netzwerk, HP
14.07.2010	DFN-CERT-2010-0892: Schwachstelle im GFS Dateisystem Kernel Modul gfs-kmod	Linux, RedHat
14.07.2010	DFN-CERT-2010-0889: Schwachstellen im RedHat Fedora Linux-Kernel	Linux, Fedora

Used Literature and Links

- Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle. Mark Zajicek, *Handbook for Computer Security Incident Response Teams (CSIRTs)*, 2nd ed. April 2004

- Check out Common Vulnerabilities and Exposures (CVE) at https://nvd.nist.gov