Gerald Pfeifer

Managing Network Services

- 181.063 VU 2.0 AKIK3
  181.085 SE 2.0 Seminar aus Informatik
  181.101 SE 2.0 Informations− und Komm.sys
- Keywords:
  Domainsregistrierung, cfengine, logging (syslog, access_log,...), monitoring hosts and services, Name Services, NFS (network file system), NIS, offene Mailserver/abuse handling, rdist, rsync, scheduled tasks (cron), Security, Spam(−Bekämpfung), SSH, Webserver (Apache), whois, ...
- Vorbesprechung:
  Donnerstag, 8.3.2001, 17:00
  Seminarraum 184/2 (Favoritenstraße, 3. Stock)

Ablauf

- Vorlesung/Übung
  - Vorlesung (geblockt) + ggf. einige Vorträge aus dem Seminar
  - kleine Beispiele in Einzelausarbeitung (Studentenaccount)
  - Micro−Projekt in Kleingruppen auf einem Rechner am Institut (gruppenweise geblockt)
- Proseminar/Seminar
  - Gruppen von ein bis zwei TeilnehmerInnen
  - Einlesen in ein Thema
  - Ausarbeiten eines Vortrages (~25 min pro Person)
  - Review eines anderen Vortrages
  - Besuch der Vorträge

Seminarthemen

- NIS / LDAP
- NFS
- Server Monitoring
- Firewalls
- cfengine
- SSH
- rdist/rsync
- IDS (Intrusion Dections Systems)

Next lecture(s)

- RFCs, Standards Bodies and Procedures
- DNS and assorted tools, an overview
- Domain Registration/Administration
- …

RFCs & Standards Bodies

- "Underlying theory" of the Internet
- Internet Architecture Board (IAB)
  - http://www.iab.org/
  - Oversight, Appeals,...
- Internet Engineering Task Force (IETF)
  - http://www.ietf.org/
  - "Managed" by Internet Engineering Steering Group (IESG)

RFC Procedures

- Formal Guidelines and Overview
  - RFC 2026
    The Internet Standards Process
  - STD 1 (currently RFC 2500)
    Internet Official Protocol Standards
- Standards Track
  - Proposed Standard
  - Draft Standard
    2+ independent and interoperable implementations
  - Internet Standard (STD)

RFC Procedures /2

- Also "off−track" maturity levels
  - Not Internet Standards in any sense
  - Experimental − research or development effort
  - Informational − general information
  - Historic
- Best Current Practice (BCP) RFCs
  - somewhat similar to STDs
  - not purely technical

RFCs, some examples

- RFC 822
  Standard for the Format of ARPA Internet Text Messages
- RFC 1178 (FYI 5)
  Choosing a Name for Your Computer
- RFC 1855
  Netiquette Guidelines

RFCs, some examples /2

- RFC 1034 (STD 13)
  Domain Names−−Concepts and Facilities
- RFC 1035 (STD 13)
  Domain Names−−Implementation and Specification
  - **update**d by RFCs 1101, 1122, 1183, 1706, 1876, 1982, 1995, 1996, 2052, 2136, 2137, 2181, 2308 and 2535; **obsolete**s RFCs 882, 883 and 973

DNS Basics

- Relate symbolic names and IP addresses
  - IP addresses are used for the actual network transport (OSI network/transport layers).
    - IPv4 addresses: 32 bits
      X4.X3.X2.X1 (Xi ∈ [0..255])
    - IPv6 addresses: 128 bits
      X16:X15:...:X1 (Xi ∈ [0..ff])
  - Symbolic names (hostnames) are used by humans, but also as a level of abstraction.

DNS Basics /2

- Tree structured name space
  - www.ibm.com, gcc.gnu.org, internic.net, vexpert.dbai.tuwien.ac.at, www.boku.ac.at,...
  - from right to left, "." separates nodes
  - root is "null string"
- Distributed, hierarchical database
- Caching at all levels

DNS Components

- Domain Name Space
  - Queries
  - Resource Records (RRs): returned for queries
- Name Servers
  - authoritative for "their" subtree (zones)
  - **lame server**: assumed to be authoritative, though it is not.
    - Usually maintainance/communications problem.
- Resolver: local, at the client

DNS: Zone Cuts

- DNS tree is divided into "zones".
  - Collections of domains that are treated as a unit.
- "Zone cuts" separates child zone from parent.
  - Indicated in the parent zone by the existence of NS records specifying the origin of the child zone.
  - Each zone resides between two cuts/the root of tree/a leaf of tree.
- Domain name at the top of a zone (just below the cut is called the zone’s "origin".
  - Name of zone = name of origin

DNS: cASe, absolutely

- Currently case−insensitive
- Implementations should be case−preserving!
- Absolute vs Relative Names
  - nunki.dbai% ssh www
  - www.dbai.tuwien.ac.at**.** (Note the trailing dot!)
- Everything starts at the root, in the end.

DNS Querytypes/RRs

- Querytypes / Resource Records (RRs)
  - Lookup
    - name −> address (A)
    - name −> name (CNAME, MX, NS)
    - name −> text (TXT, SOA)
  - Reverse lookup
    - address −> name (PTR)

DNS RRs

- A (Address)
  - Relate Name to IP address(es)
- NS (NameServer)
  - Obtain authoritative Nameserver(s)
- CNAME (Canonical Name)
  - Relate Name to Name
- MX (Mail eXchanger)
  - Which mail servers are responsible for a hostname?

DNS RRs /2

- SOA
  - Start of a zone of authority
    - zone = subtree, where some server is authoritative
  - Lists primary nameserver for the zone
  - and hostmaster mail address in domain notation
    - hosts.pfeifer.at –> hosts@pfeifer.at
  - plus serial number (time stamp), TTL (time to live),...
- TXT
  - For informational purposes, not used very often.
- Tons of experimental and obsolete RRs!

DNS examples

- nunki% host −t ns leitgeb.priv.at
  leitgeb.priv.at NS ns3.superb.net
  leitgeb.priv.at NS ns1.superb.net
  leitgeb.priv.at NS ns2.superb.net
- nunki% host −t mx leitgeb.priv.at ns1.superb.net
  leitgeb.priv.at MX 10 leitgeb.priv.at
- nunki% host −t a leitgeb.priv.at ns1.superb.net
  leitgeb.priv.at A 209.40.107.44
- markab[67]:~% host −t soa leitgeb.priv.at ns3.superb.net
  leitgeb.priv.at SOA ns1.superb.net hostmaster.superb.net (
  1999122714 ;serial (version)
  10800 ;refresh period (3 hours)
  3600 ;retry interval (1 hour)
  604800 ;expire time (1 week)
  172800 ;default ttl (2 days)
)

DNS examples /2

- Refer to another server (beyond your DNS control)
- nunki% host −t cname www.usenet.at
  www.usenet.at CNAME www.dbai.tuwien.ac.at
- Multiple Mail Servers
- nunki% host −t mx kpnqwest.at
  kpnqwest.at MX 100 smtp.austria.eu.net
  kpnqwest.at MX 150 mail−relay.eu.net
  kpnqwest.at MX 10 melone.austria.eu.net
  - Hosts with lower weights are preferred.
  - Backup MX servers.

Reverse DNS: IN-ADDR.ARPA

- IN-ADDR.ARPA Domain for reverse lookups
- PTR RR
- ```
  nunki% host -t a vexpert.dbai.tuwien.ac.at
  vexpert.dbai.tuwien.ac.at       A       128.130.111.12
  ```
- ```
  nunki% host -a 12.111.130.128.IN-ADDR.ARPA
  12.111.130.128.IN-ADDR.ARPA   PTR   vexpert.dbai.tuwien.ac.at
  12.111.130.128.IN-ADDR.ARPA   PTR   dbai.tuwien.ac.at
  ```
- ```
  nunki% host -t PTR 240.142.154.193.IN-ADDR.ARPA
  240.142.154.193.IN-ADDR.ARPA    PTR     melone.austria.eu.net
  240.142.154.193.IN-ADDR.ARPA    PTR     p240.austria.eu.net
  ```
- Observe the inversion of the address!
  ```

Reserved Top Level DNS Names

- RFC 2606 (BCP 32)
  - .test … testing DNS related code
  - .example … use in documentation, examples
  - .invalid … evidently invalid
  - .localhost … points back to local host
- Reserved by IANA, as well as
  - example.com, example.net, example.org

Assorted DNS Tools

- nslookup
  - Part of most operating systems (/usr/sbin/nslookup)
- dig
  - More general than nslookup
- host
  - By Eric Wassenaar
  - ftp://ftp.nikhef.nl/pub/network/
- ping
  - In the absence of *anything* else.

DNS References

- DNS Resources Directory
  - http://www.dns.net/dnsrd/
- RFC 1034+1035 (Standard: STD 13): Domain Names−−Concepts and Facilities
- RFC 1536: Common DNS Implementation Errors and Suggested Fixes
- RFC 1713: Tools for DNS debugging
- RFC 2181: Clarifications to the DNS Specification

Top Level Domains (TLDs)

- Generic Domains (gTLDs)
  - .com (Commercial)
  - .org (Organisations)
  - .net (Network Providers)
  - .edu (Educational, North America − in principle!)
  - .gov (US Government Agencies)
  - .mil (US military)
  - .int (International, Example: nato.int)
  - Originally, strict checks for appropriatness were performed. No longer for .com, .org, and .net!

Top Level Domains /2

- Country Code Domains (ccTLDs)
  - .at, .us, .jp, .cc (Cocos Islands),...
  - Some have a second level structure
    - .ac.uk, .co.uk,...
  - Some have a flat structure
    - uni−marburg.de, enst−bretagne.fr,...
  - Some have a mixed structure
    - .ac.at, .co.at, .gv.at, .or.at, .priv.at, as well as pfeifer.at,...

Registries

- (Prospective) Owners of domains have to register these with a registry:
  - NIC.AT (http://www.nic.at)Op
    - erated by ISPA − Internet Service Providers Austria.
    - Originally .at was handled by Universität Wien.
  - RIPE.NET (http://www.ripe.net)
    - Central registry for most/all of Europe.
    - Receives data from national registries.
  - InterNIC (http://www.internic.net)

Registries /2

- Historically: One registrar "owns" a TLD/TLDs.
  - Network Solutions: .com, .org, .net until 1999.
  - Still the case for .at!
- Current trend
  - One central registry; several registrars have access.
  - Alternately: Several registries for one TLD, together with a Meta−Registry

Technically Speaking

- Registry contains billing information, information on the domain itself, and contact handles
  - ADMIN−C, TECH−C, ZONE−C (<−> SOA RR)
- Plus data for the DNS servers for a domain.
  - Has to up−to−date, as…
  - …it is used as input for the DNS zone databases for the TLD (resp. Domains like .co.at).

whois

- Query registries for administrative information
  - Domains, Contact Handles, IP address assignments,...
- Distributed Database (once more!)
  - hierarchical and scaleable
- Standardized
  - RFC 2167: "Referral Whois (RWhois) Protocol V1.5"
- Syntax
  - % whois −h some.whois.server example.com
  - % whois −h another.whois.server HANDLE

Whois in Action

```
% whois −h whois.internic.net pfeifer.com
Domain Name: PFEIFER.COM
   Registrar: NETWORK SOLUTIONS, INC.
   Whois Server: whois.networksolutions.com
   Referral URL: www.networksolutions.com
   Name Server: NS1.SUPERB.NET
   Name Server: NS2.SUPERB.NET
   Updated Date: 13−jan−2000

>>> Last update of whois database: Tue, 9
May 00 04:36:57 EDT <<<
```

```
% whois −h whois.networksolutions.com pfeifer.com
Registrant:
Gerald Pfeifer (PFEIFER−DOM)
   Mondweg 64
   1140 Wien,
   AT

   Domain Name: PFEIFER.COM

   Administrative Contact, Billing Contact:
      Pfeifer, Gerald (GP383)
pfeifer@DBAI.TUWIEN.AC.AT
      Mondweg 64
      :
   Technical Contact, Zone Contact:
      Hostmaster, Superb Internet  (SIH2)
      :
      (604) 638−2525 (FAX) (604) 608−2953

   Record last updated on 29−Jan−1998.
   Record expires on 14−Jan−2001.
   :
   NS1.SUPERB.NET          207.228.225.5
   NS2.SUPERB.NET          216.23.151.5
```

Setting up a Domain

- Set up name server to carry domain (resp. changed data).
- Apply for domain (resp. submit change request).
- Wait for reply and possibly reload of nameservers operated by registry (once a day)
  - When changing nameservers, decommission old servers.
- Critical: Authentication when submitting changes.
  - Strong potential for abuse (hijacking,…)!

procmail

- Sort incoming mail: mailing lists,...
- Selectively forward mails
- Preprocess mail: PGP signature check,...
- Invoke programs; send automatic replies

- Powerful enough to implement mailing lists!

Why procmail?

- Independent of mail server software and client
  - Unix philosophy: Easily change/update one of the three without affecting any other!
- More powerful than any mail server/client alone!
- Extremely stable
  - Syntax errors, file locking, out of memory,...
- 24x7x52, immediate processing
- Why not?
  - Not always easy to use.

procmail Syntax /1

- Recipes

```
:0 [flags] [: [locallockfile] ]
«zero or more condition lines»
«exactly one action line»
```

- Condition lines
  - `* «regular expression»`
  - `* > «size»` (compare size of mail)
  - `* ? «command»` (use exit code of command)
  - `* var ?? ...` (match remainder of condition against value of environment variable var)
  - `* ! «condition»` (invert condition)

procmail Syntax /2

- Action lines
  - `! address (, address)*` (forward message)
  - `| program` (start program, pipe message to stdin)
  - { (start nested block)
    :
    } (close nested block)

procmail Syntax /3

- Assignments are allowed nearly everywhere
  - `MAILDIR=$HOME/MyIncomingMail/`
  - `LOGFILE=/var/mail/pfeifer.log`
  - `EXITCODE=67` ("user unknown")
- Include other files
  - `INCLUDERC=$HOME/.procmail-antispam`
- "Jump" to other files ("goto")
  - `SWITCHRC=$HOME/.procmail-antispam`
  - Turing complete!?

RegExps, a quick tour

- . Any character (except \n = newline)
- \. A dot
- ^, $ Start of line, end of line
- x? Zero or one occurrences of the expression x
- x* A sequence of zero or more occurrences of x
- x+ A sequence of one or more occurrences of x
- x|y Either one of x or y
- (xy❒) Aggregate sequence
- [abd9] Either one of a, b, d, or 9
- [^a−m] Any character apart from a,❒,m or newline

procmail: Filtering Lists

- :0
  * ^Sender: gcc−cvs−wwwdocs−owner@gcc.gnu.org
  INBOX.announce
- Filter duplicate messages via multiple lists by means of their Message−ID.

  :0 Wh: msgid.lock
  * ^Sender: gcc(−announce|−bugs|−patches)?−owner@gcc.gnu.org
  | formail −D 8192 msgid.cache

  :0
  * ^Sender: gcc(−announce|−bugs|−patches)?−owner@gcc.gnu.org
  INLIST.gcc

procmail Syntax /4

- Flags
  - D case sensitive
  - H / h grep header / feed header to pipe
  - B / b grep body / feed body to pipe
  - f consider pipe as a filter
  - W wait for filter (and ignore errors)
  - A / E AND/ELSE −− only execute if preceeding recipe was/was not executed.
  - c generate copy of the current message
- and any combination thereof!

procmail Syntax: Scoring

- Scoring Rules
  `* w^x «condition»`
  - Weight w and exponent x are real numbers.
  - The first time the regular expression is found, it will add w to the score; the second time, w*x will be added; the third time, w*x*x❐
  - Final score for the recipe must be positive for it to match.

procmail: Spam Filter

- ```
  :0
  * 100^0 ^Message−Id: <>
  * 100^0 ^Message−Id: <\.>
  * 100^0 ^Received:.*\[.*([3−9][0−9][0−9]|25[6−9]|[0−9]{4,})[\.\]]
  * 100^0 ^Subject: (AD:|\[AD\]|ADV:|ADV )
  * 100^0 ^TO.*@public.com
  * 100^0 ^X−Mailer: (Emailer Platinum|DiffondiCool)
  {
      EXITCODE=$EXIT_NOUSER

      :0
      $SPAM
  }
  ```
- Observe how the conditions are OR−ed!
  ```

formail & procmail: A Team

- Filter, Rewrite, Modify,… messages
- Options
  - −r Generate auto−reply header
  - −s Split mailbox file into messages − very handy!
  - −b Do not escape From−lines in the body
  - −D Detect duplicate messages (see example)
  - −A Append a header field
  - −I Insert (replace) header field
  - …and many more.

procmail: Another example

- Tag messages from a certain mailing list
- ```
  :0
  * ^Sender: owner−freebsd−emulation@FreeBSD.ORG
  {
        :0f
        * ^Subject: Re:\/.*
        | formail −b −I"Subject: Re: [emulation]$MATCH"

        :Ef
        * ^Subject:\/.*
        | formail −b −I"Subject: [emulation]$MATCH"|

    :0
    INLIST.freebsd
  }
  ```
  ```

Mail DOs and DON'Ts

- Do use your real name
- Do use a valid e−mail address (of yours)
- Do use a standard charset
  - US−ASCII, ISO−8859−1, ISO−8859−15 (Euro),...
  - Don't use Windows−1252, X−UNKNOWN,...
- Don't use HTML
- Don't use proprietary formats
  - MS TNEF,...

Standard Mailbox Names 1/2

- Mailbox Names for Common Services, Roles and Function (RFC 2142)
- Network Operations
  - "...experiencing difficulties with the organization's Internet service"
  - **ABUSE@...** Inappropriate public behaviour
  - NOC@... Network infrastructure
  - SECURITY@... Security bulletins or queries

Standard Mailbox Names 2/2

- DNS Administration Mailbox
  - HOSTMASTER@... or any other, specified in SOA Resource Record
- Specific Internet Services
  - POSTMASTER@... SMTP
  - USENET@... (or NEWS@...) NNTP
  - WEBMASTER@... (or WWW@...) HTTP
- Administrative Mailbox for Mailing Lists
  - LISTNAME−REQUEST@... Required for every list!

Spam, spam, spam...

- Luncheon meat in a can, made by Hormel
- Song by Monty Python’s "Spam−loving Vikings"
- Usenet
  - Excessive Multiple Posting (EMP)
  - Excessive Cross−Posting (ECP)
  - ...and combinations thereof
- Mail
  - Unsoliticed Commercial Email (UCE)
  - Unsoliticed Bulk Email (UBE)

Austrian Legalese 1/2

- Telekommunikationsgesetz TKG § 101
  - "Unerbetene Anrufe: Anrufe − einschließlich das Senden von Fernkopien − zu Werbezwecken ohne vorherige Einwilligung des Teilnehmers sind unzulässig. [...] Die erteilte Einwilligung kann jederzeit widerrufen werden [...]"
  - Seit 1999−07−15: "Die Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken bedarf der vorherigen ◆ jederzeit widerruflichen ◆ Zustimmung des Empfängers."

Austrian Legalese 2/2

- TKG § 104 (3) 23. "Eine Verwaltungsübertretung begeht und ist mit einer Geldstrafe bis zu 500.000 Schilling zu bestrafen, wer [...] entgegen § 101 unerbetene Anrufe oder die Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken tätigt.
- Anzeige persönlich oder anonym, brieflich oder per E−mail, mit vollem Body und sämtlichen Headern der Mail an ein Fernmeldebüro:
  - http://www.bmv.gv.at/tk/2ofb/sektion4main.htm

Open Mail Relays 1/3

- What is it?
  - Mail Server, accepting and delivering mail from third parties to third parties
  - Neither sender nor recipients are legitimate users
- Quite common in the "early" days
- Now responsible for 50+% of UCE/UBE!
  - (Dial−up) Spammer sends his messages to an open relay very quickly (one message, many recipients), only delivery is expensive

Open Mail Relays 2/3

- Per se useful for testing and users on the road
- Possibility of abuse outweighs these advantages
  - Server operator has to pay traffic−based fees
  - Server may run out−of−disk, out−of−bandwidth, experience significant delays
  - □and appear on blacklists!
- Mobile Users
  - SMTP−after−POP/IMAP
  - SMTP Authentication

Open Mail Relays 3/3

- How to fix?
  - Most current version of mail servers have been fixed
  - MAPS Transport Security Initiative http://www.mail−abuse.org/tsi/
- Inappropriate fix
  - Only accept mail from IPs with an MX−Record
  - This is not RFC−conformant and stupid!
  - Also breaks in cases where ingoing and outgoing servers are different!

Filtering/Blocking Spam

- Heuristics
  - Subject: (\[AD\]|ADV:|ADV)
    To: friend@public.com
    :
  - Hard to maintain
  - False positives (Mail classified as Spam, but is not)
  - Feasible for end users, but usually takes place after the mail has been delivered.

Filtering/Blocking Spam 2/2

- DNS−based lists of "spamming" IPs
  - Mostly for system administrators / mail server configurations
  - Easy to maintain
  - Blocks Ips (Servers), not Users (Spammers)
  - Reliance on external sources and decisions
  - May slow down delivery and increase server load (open connection!)
    - affects large servers
    - local DNS server / secondary DNS server?

MAPS RBL

- Mail Abuse Prevention System Realtime Blackhole List
- http://www.mail−abuse.org/rbl/
- List of networks which are known to be friendly, or at least neutral, to spammers who use these networks either to originate or relay spam.
- It’s hard to get listed by MAPS RBL
  - => Mostly die−hard spammers and providers
  - few false positives, but not very effective

ORBS

- Validated database of open mail relays and open mail relay output points
- http://www.orbs.org/
- Also lists multi−level relays
  - Example: Customer has an open relay and does not deliver outgoing mail directly, but uses a mail server provided by the ISP.
- Easy nominations, by e−mail or web
  - To: relays@orbs.org
    :
    Relay: 128.130.111.12 (in the body)

MAPS RSS

- MAPS Relay Spam Stopper
- http://www.mail−abuse.org/rss/
- Similiar to ORBS, but
  - does not list multi−level relays
  - only lists servers that have been already (ab)used
  - => not as effective, but fewer false positives
- Nominations by e−mail
  - To: relays@mail−abuse.org
  - Must include sample of relayed spam!

MAPS DUL

- Prevent trespass spam
  - Mass e−mailers who offload UCE/UBE using direct connections to their victims' mail servers without using their ISP's mail server as a relay or gateway
  - Received: from segasolution.com (mx4−22.contact.net [209.104.110.150])
    by vexpert.dbai.tuwien.ac.at (8.9.3/8.9.3) with SMTP id AAA29928
    for <pfeifer@dbai.tuwien.ac.at>; Tue, 13 Jun 2000 00:52:29 +0200 (MET DST)
    From: a____67@hotmail.com
    Message−Id: <200006122252.AAA29928@vexpert.dbai.tuwien.ac.at>
    Subject: $25.00 USD for Gerald Pfeifer
- http://www.mail−abuse.org/dul/
- Nominations by e−mail
  - must include sample of spam

Querying RBLs

- Reverse the octets of the IP address and check for a DNS A RR for that under rbl.maps.vix.com, relays.orbs.org,...
  - % host −a 12.111.130.128.rbl.maps.vix.com
    ❒does not exist (authoritative answer)
    => Server OK!
  - % host −a 50.162.58.195.relays.orbs.org
    50.162.58.195.relays.orbs.org A 127.0.0.3
    => Server NOT OK!
    - (usually matches produce 127.0.0.2, but this is a special case where apparently the entry was added manually.)

What to do as a provider?

- Secure open relays
- Regularily check for open relays
  - your servers and those of your customers
  - telnet mail−abuse.org (from the mail server)
- Subscribe to MAPS RBL, ORBS,…
  - …but let the customers/users choose if possible
- Provide customers/users with AUP (Acceptable Usage Policy)
- Reply to and act upon complaints!!!

Good luck...

…for the final example(s) and the exam!

(It shouldn’t be hard ;–))