Internet Technology & Web Engineering

Usenet

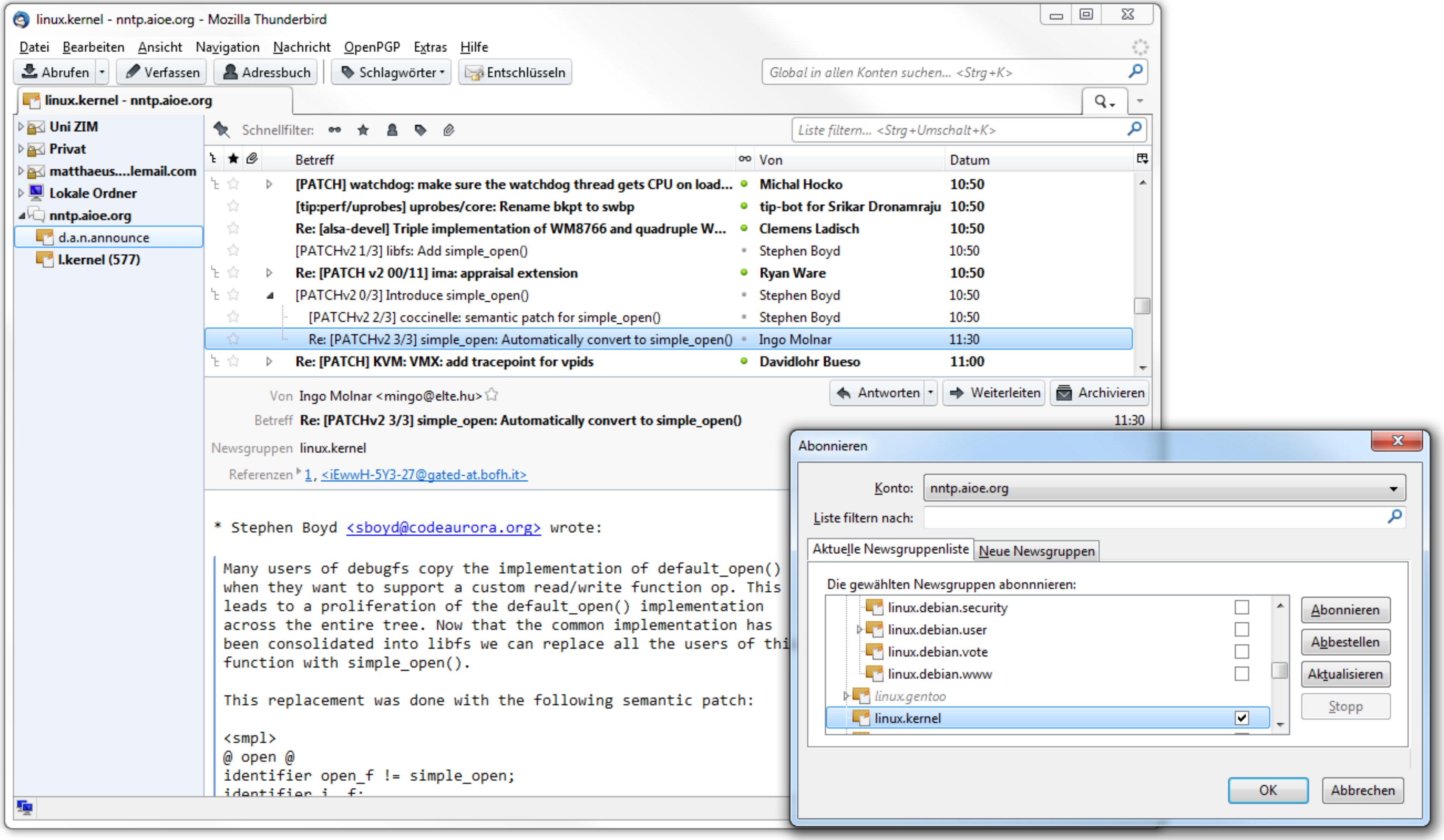
Dipl.-Inform. Matthäus Wander

Universität Duisburg-Essen

Overview

- Distributed system for discussion boards
- Articles posted in newsgroups
- Newsgroups structured by topic in hierarchies
- Unstructured network of newsservers
- Servers disseminate data with flooding algorithm
- Clients connect to server with newsreader software
- Originally specified in 1983 (RFC 850)
  - Unix-to-Unix Copy Protocol (UUCP) for data transfer
- Current specification: Netnews (RFCs 5536-5538)
  - Network News Transfer Protocol (NNTP) for data transfer

Newsreader


linux.kernel - nntp.aioe.org - Mozilla Thunderbird
Datei Bearbeiten Ansicht Navigation Nachricht OpenPGP Extras Hilfe
Abrufen
Verfassen
Adressbuch
Schlagwörter
Entschlüsseln
Global in allen Konten suchen... <Strg+K>
linux.kernel - nntp.aioe.org
Uni ZIM
Privat
matthaeus....lemail.com
Lokale Ordner
nntp.aioe.org
d.a.n.announce
l.kernel (577)
Schnellfilter:
Liste filtern... <Strg+Umschalt+K>
Antworten
Weiterleiten
Archivieren

Betreff	Von	Datum
[PATCH] watchdog: make sure the watchdog thread gets CPU on load...	Michal Hocko	10:50
[tip:perf/uprobes] uprobes/core: Rename bkpt to swbp	tip-bot for Srikar Dronamraju	10:50
Re: [alsa-devel] Triple implementation of WM8766 and quadruple W...	Clemens Ladisch	10:50
[PATCHv2 1/3] libfs: Add simple_open()	Stephen Boyd	10:50
Re: [PATCH v2 00/11] ima: appraisal extension	Ryan Ware	10:50
[PATCHv2 0/3] Introduce simple_open()	Stephen Boyd	10:50
[PATCHv2 2/3] coccinelle: semantic patch for simple_open()	Stephen Boyd	10:50
Re: [PATCHv2 3/3] simple_open: Automatically convert to simple_open()	Ingo Molnar	11:30
Re: [PATCH] KVM: VMX: add tracepoint for vpids	Davidlohr Bueso	11:00

Von Ingo Molnar <mingo@elte.hu>

Betreff **Re: [PATCHv2 3/3] simple_open: Automatically convert to simple_open()** 11:30

Newsgruppen linux.kernel

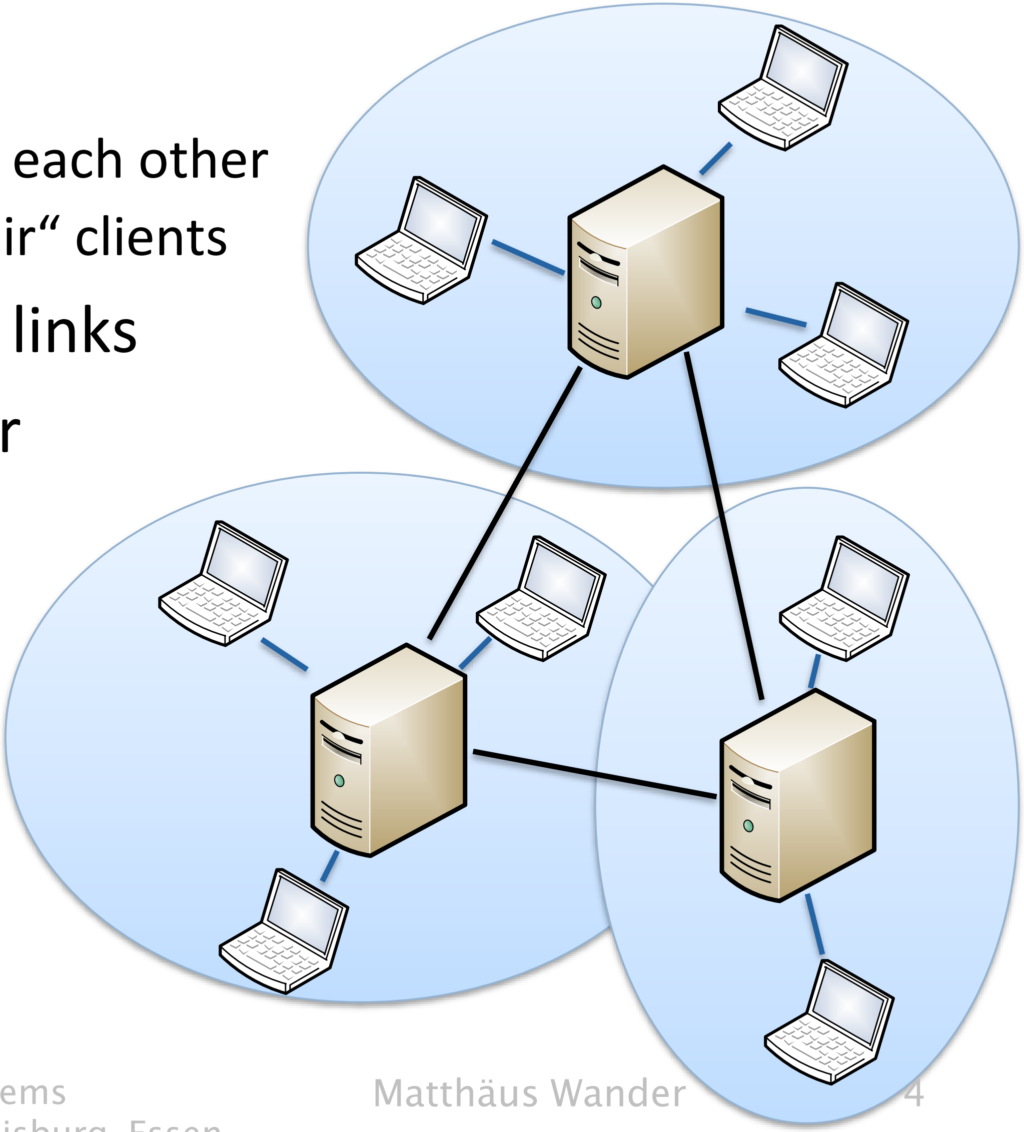
Referenzen 1, <iEwwH-5Y3-27@gated-at.bofh.it>

```
* Stephen Boyd <sboyd@codeaurora.org> wrote:

Many users of debugfs copy the implementation of default_open()
when they want to support a custom read/write function op. This
leads to a proliferation of the default_open() implementation
across the entire tree. Now that the common implementation has
been consolidated into libfs we can replace all the users of thi
function with simple_open().

This replacement was done with the following semantic patch:

<smpl>
@ open @
identifier open_f != simple_open;
identifier i, f;
```

- linux.debian.security ☐
- linux.debian.user ☐
- linux.debian.vote ☐
- linux.debian.www ☐
- linux.gentoo
- linux.kernel ☑

Architecture

- Client/Server
  - Servers share data among each other
  - Servers share data to „their“ clients
- Manual setup of allowed links
- Text-based NNTP transfer
  - Client-to-Server
  - Server-to-Server
- TCP connections



Network News Transfer Protocol

- Specified in 1986 (RFC 977), currently RFC 3977
- Text-based protocol
  - Originally 7-bit ASCII only
  - Today 8-bit possible (with constraints)
- Stateful session
  - Context does matter
  - E.g. NEXT command works only after GROUP command
- Authentication optional (though required mostly)
  - Plaintext login/password
  - SASL (generic authentication framework)
- SSL/TLS optional

NNTP Example Session

```
200 nntp.aioe.org InterNetNews NNRP server INN 2.5.2 ready (posting ok)
LIST
215 Newsgroups in form "group high low status"
linux.kernel 0000474808 0000450551 m
linux.redhat 0000000981 0000000980 y
.
GROUP linux.kernel
211 23844 450414 474258 linux.kernel
OVER 474243-474258
224 Overview information for 474243-474258 follows
474243  Re: [PATCH v2] block: fix ioc leak in put_io_context    Jens Axboe <axbo [...]
474258  Re: [patch 0/7] Add TRIM support for raid linear/0/1/10 Roberto Spadi    [...]
.
NEXT
223 474051 <imlzI-5Yh-11@gated-at.bofh.it> Article retrieved; request text separately
NEXT
223 474087 <iEwwI-5Y3-35@gated-at.bofh.it> Article retrieved; request text separately
ARTICLE
220 474087 <iEwwI-5Y3-35@gated-at.bofh.it> article
[...article...]
.
QUIT
205 Bye!
```

NNTP Commands (selection)

- LIST: Get list of all newsgroups
- NEWGROUPS: Get list of new groups since some date
- NEWNEWS: Get list of new messages since some date
- GROUP: Enter newsgroup and get summary
- NEXT: Set cursor to next article in newsgroup
- LAST: Set cursor to previous article in newsgroup
- ARTICLE: Retrieve article
- HEAD/BODY/HDR: Retrieve part of article
- OVER: Get overview of articles (subject, sender, …)
- POST: Submit new article

Article Format

```
Path: aioe.org!bofh.it!news.nic.it!robomod
From: Stephen Boyd <sboyd@codeaurora.org>
Newsgroups: linux.kernel
Subject: [PATCHv2 1/3] libfs: Add simple_open()
Date: Tue, 13 Mar 2012 10:50:04 +0100
Message-ID: <iEwwI-5Y3-35@gated-at.bofh.it>
Sender: robomod@news.nic.it
Approved: robomod@news.nic.it
Lines: 65
Xref: aioe.org linux.kernel:474087

This is the body of the article
[...]
```

Servers traveled
Email-like From
Destination newsgroup(s)

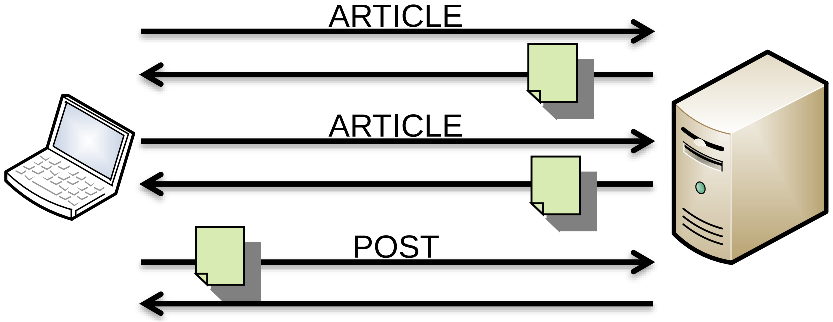
Unique global ID

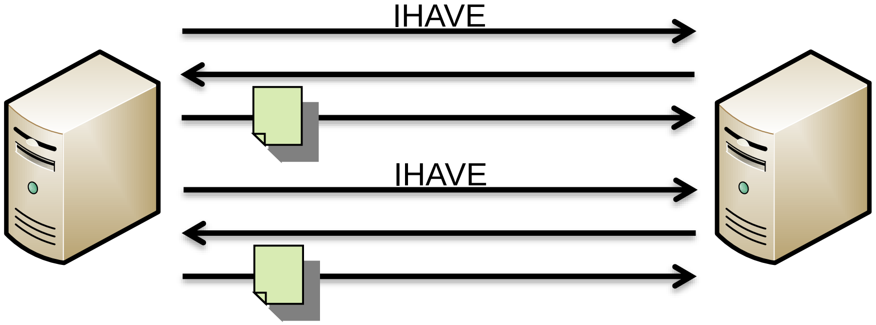
Server-local ID

Data Transfer with NNTP

- Newsreader
- Pulls data from server
  - Iterates over newsgroups and requests articles
  - Requests overview of changes since some date
- Posts article to server

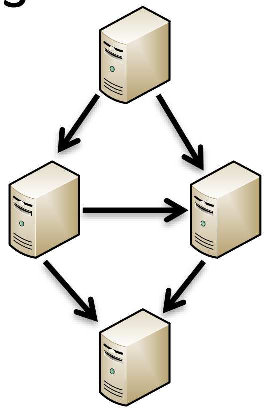
- Newsserver
- Pushes notifications of new articles to servers
  - Responds with „not interested“
  - Responds with „please send“



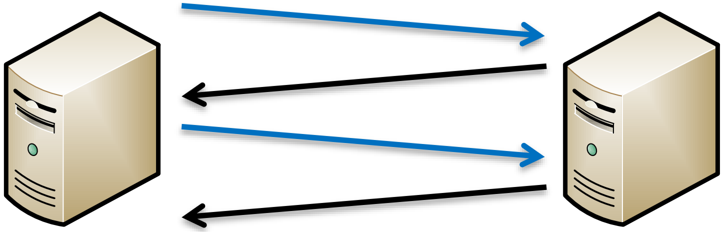


NNTP Article Propagation

- Newsservers forward new articles to known servers
  - Articles propagate through whole Usenet
- IHAVE command avoids transmission of duplicates
  - Stop-and-wait mechanism
  - Inefficient when many messages are transfered



```
IHAVE <some.message.id@example.net>
335 Go ahead
Path: pathost!demo!somewhere!not-for-mail
From: "Demo User" <nobody@example.com>
Newsgroups: misc.test
Subject: I am just a test article
Date: 6 Oct 1998 04:38:40 -0500
Message-ID: <some.message.id@example.net>

This is just a test article.
.
235 Article transferred OK
```



NNTP Streaming Extension

- IHAVE separated into two commands
  - CHECK: offer article
  - TAKETHIS: send requested article
- Pipelining: Send requests without waiting for responses

```
CHECK <some.message.id@example.net>
238 <some.message.id@example.net>
TAKETHIS <some.message.id@example.net>
[...article...]
.
239 <some.message.id@example.net>
CHECK <another.message.id@example.net>
238 <another.message.id@example.net>
TAKETHIS <another.message.id@example.net>
[...article...]
.
239 <another.message.id@example.net>
CHECK <duplicate-message@example.net>
438 <duplicate-message@example.net>
```

NNTP Streaming Extension

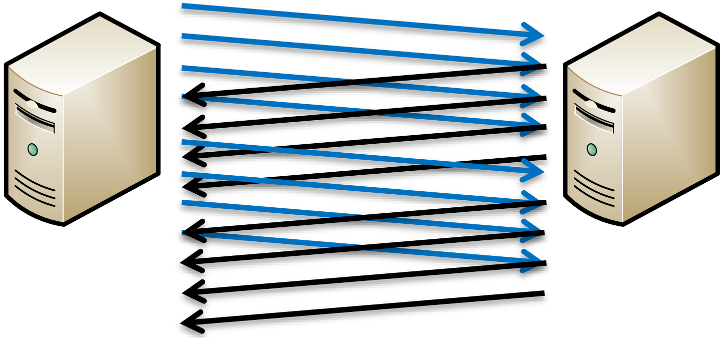
- IHAVE separated into two commands
  - CHECK: offer article
  - TAKETHIS: send requested article
- Pipelining: Send requests without waiting for responses

```
CHECK <some.message.id@example.net>
238 <some.message.id@example.net>
CHECK <another.message.id@example.net>
238 <another.message.id@example.net>
CHECK <duplicate-message@example.net>
438 <duplicate-message@example.net>
TAKETHIS <some.message.id@example.net>
[...article...]
.
239 <some.message.id@example.net>
TAKETHIS <another.message.id@example.net>
[...article...]
.
239 <another.message.id@example.net>
```

NNTP Streaming Extension

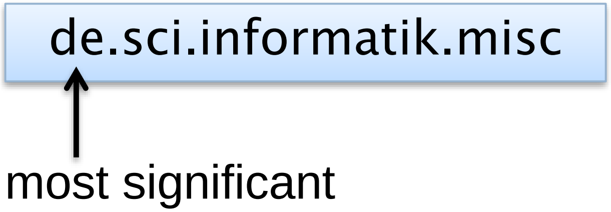
- IHAVE separated into two commands
  - CHECK: offer article
  - TAKETHIS: send requested article
- Pipelining: Send requests without waiting for responses

```
CHECK <some.message.id@example.net>
CHECK <another.message.id@example.net>
CHECK <duplicate-message@example.net>
238 <some.message.id@example.net>
238 <another.message.id@example.net>
438 <duplicate-message@example.net>
TAKETHIS <some.message.id@example.net>
[...article...]
.
TAKETHIS <another.message.id@example.net>
[...article...]
.
239 <some.message.id@example.net>
239 <another.message.id@example.net>
```



Newsgroup Organization

- Newsgroup name
  - Consists of components delimited by dot
  - A..Z, a..z, 0..9, +, -, _
  - Case insensitive



de.sci.informatik.misc

most significant

- Grouped into hierarchies
  - No root level: each hierarchy is independent from another
  - Example hierachies: alt.*, comp.*, de.*, rec.*, sci.*, soc.*
- Operator configures list of hierarchies to be shared on newsserver
  - Not all hierarchies shared on all servers

Moderated Newsgroups

- Purpose: moderator approves articles before publication
- All articles POSTed to moderated group is relayed via mail
  - misc.example → misc-example@moderators.isc.org
  - Moderator mailbox/domain configured per hierarchy
- Moderator POSTs article with „Approved“ field
  - Approved: Jane <jane@example.net>
- Newsservers do not forward article without Approved
  - No global address directory – any „Approved“ address is ok
  - No standardized verification – address can be forged
- Honest newsservers disallow „Approved“ POSTs
  - Except when user has been authorized as newsgroup moderator

Group Control Messages

- Purpose: Create or remove newsgroups
- Mechanism: Meta articles with „Control“ header
- Moderator „Approved“ required
- Many hierarchies use PGP verification

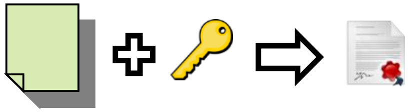
```
Path: aioe.org!news.snarked.org!newsfeed.news.ucla.edu![...]
From: group-admin@isc.org
Newsgroups: sci.psychology.journals.psycoloquy
Subject: cmsg rmgroup sci.psychology.journals.psycoloquy
Control: rmgroup sci.psychology.journals.psycoloquy
Approved: group-admin@isc.org
Date: Sun, 04 Sep 2011 13:02:03 -0700
Message-ID: <cmsg-20110904200203$49d7@isc.org>
X-PGP-Sig: 2.6.3a Subject,Control,Message-ID,Date,From,Sender
    iQCVAwUBTmPZO8JdOtO4janBAQE/3gP/YiPhLGXEYKxxdJngvtWEZO6pmfvch1Wo
    4CR+CR70Je9mFY6NHjqlj5RJzBomqgTRfTGZNEzsLHvArFuROUKtzcn/OB5rMkrx
    m7hpK2vak8xC+QzLXPRBTisM9RRD/HOsDzfOAEnP0Lm8FXpYsTba/WoKNk71zpP7
    y6XLoce6r8w=
    =taqh
Xref: aioe.org control.rmgroup:2138
```

Interlude: Public Key Cryptography

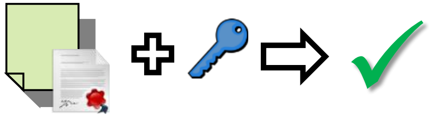
- Pair of two keys
  - Private Key 🔑: keep it secret
  - Public key 🔑: share with the world
- Use private key to sign data
  - Only you can sign with your private key 🔑
  - Everybody can verify with public key 🔑
- Use public key to encrypt data
  - Everybody can encrypt data for you with public key 🔑
  - Only you can decrypt with private key 🔑
- Algorithms: RSA, ElGamal, DSA, ECDSA, …
- Used as part of PGP, GnuPG, SSH, HTTPS, Bitcoin, …

Message Signing with Pretty Good Privacy (PGP)

- Sign control message with private key



- Post control message with signature
- Newsservers can verify signature with public key



- Public key must be delivered over trusted channel

```
## DE (German language)
# Contact: moderator@dana.de
# URL: http://www.dana.de/mod/
# Admin group: de.admin.news.announce
# Key URL: http://www.dana.de/mod/pgp/dana.asc
# Key fingerprint: 5B B0 52 88 BF 55 19 4F  66 7D C2 AE 16 26 28 25
# *PGP*   See comment at top of file.
checkgroups:moderator@dana.de:de.*:verify-de.admin.news.announce
newgroup:moderator@dana.de:de.*:verify-de.admin.news.announce
rmgroup:moderator@dana.de:de.*:verify-de.admin.news.announce
```

Cancelling Messages

- Purpose: Remove posted article from Usenet
  - Withdraw own article from public, delete spam, …
- Mechanism: Cancel control message with message ID
- Basically anyone can cancel any message
  - Moderator „Approved“ **not** required
- Newsserver honoring a cancel …
  - … removes cancelled article from newsgroup
  - … propagates cancel message
- Each newsserver handles cancel messages on its own, e.g.
  - Ignore all cancel messages
  - Filter obvious rogue cancels by checking headers („Path“)
  - Require PGP verification from trusted canceller

Interlude: Cryptographic Hash Function

- Hash Function: map arbitrary data to hash value
  - H(„foobar“) = 8843d7f92
  - Input data can be any size
  - Hash value is fixed size, e.g. 20 bytes (SHA-1)
- Deterministic: same input → same output
- Can‘t change data without changing hash value
  - H(„foobär“) = bcf2243b9
- Can‘t find data for a given hash value
  - e8636ea013e682faf61f56ce1cb1ab5c = H(???)
- Can‘t find different data with same hash value
  - H(„foobar“) = 8843d7f92 = H(???)

Cancel-Lock

- Purpose: protect from rogue cancels
- Mechanism: Cancel-Lock and Cancel-Key headers
  - Cancel-Key = Base64(Hash(message-id, password))
  - Cancel-Lock = Base64(Hash(Cancel-Key))
- Add public Cancel-Lock to article

```
Cancel-Lock: sha1:g04LZTIkiTKVkWgofM8UqkjjK8M=
```

- Cancel message must contain matching secret Cancel-Key
  - No Cancel-Key → ignore cancel
  - Base64(Hash(Cancel-Key)) ≠ Cancel-Lock → ignore cancel
- Secret password required to generate secret Cancel-Key

Conclusion

- Historically relevant with decreasing usage today
  - Replaced by web-based discussion platforms
- Originally text only
  - Binary data possible e.g. with MIME
- Still used for file sharing with commercial newsservers
- Unstructured network with flood-based data propagation
- Predecessor of peer-to-peer networks
- Not designed with strong security in mind
  - Security mechanisms added later have flaws