

NetBSD syslogd/IETF Syslog Protocols – Final Report

Martin Schütte



18 October 2008

Project Overview

Google Summer of Code project: Improve NetBSD's syslogd

Deliverables:

- TLS network transport
- New message format
- Digital Signatures

BSD Syslog
○
○○○○
○○

IETF
○

TLS
○○
○○○○
○○

Protocol & API
○○○
○○

Syslog-Sign
○
○○○
○○○○
○○
○○

Future
○○○
○

BSD Syslog

IETF

TLS

Protocol & API

Syslog-Sign

Future

Using Log Data

- Debugging
- Statistics/Planning
- Accountability for user actions
- Detect ongoing attacks
- Examine security incidents



BSD Syslog

- primarily designed for programming/debugging
- simple, uniform, easy to use and configure
- easy remote logging using UDP
- de facto standard for logging on Unix

Combination of:

- API
- message format
- daemon
- IPC protocol



API

SYSLOG(3)

NetBSD Library Functions Manual

SYSLOG(3)

NAME

syslog, vsyslog, openlog, closelog, setlogmask -- control system log

LIBRARY

Standard C Library (libc, -lc)

SYNOPSIS

```
#include <syslog.h>
```

```
void
syslog(int priority, const char *message, ...);
```

```
void
openlog(const char *ident, int logopt, int facility);
```

```
void
closelog(void);
```

```
int
setlogmask(int maskpri);
```



Syslog Message Format

```
<38>Mar 17 21:57:57 frodo sshd[701]: Connection from 211.74.5.81 port 5991
<52>Mar 17 13:54:30 192.168.0.42 printer: paper out
```

- Priority
- Header
 - Timestamp
 - Hostname
- Message
 - Tag
 - Content

By convention:

- Priority not written to logfile
- only printable ASCII
- up to 1024 characters



Syslog Message Format

```
<38>Mar 17 21:57:57 frodo sshd[701]: Connection from 211.74.5.81 port 5991
<52>Mar 17 13:54:30 192.168.0.42 printer: paper out
```

- Priority
- Header
 - Timestamp
 - Hostname
- Message
 - Tag
 - Content

By convention:

- Priority not written to logfile
- only printable ASCII
- up to 1024 characters



Syslog Message Format

```
<38>Mar 17 21:57:57 frodo sshd[701]: Connection from 211.74.5.81 port 5991
<52>Mar 17 13:54:30 192.168.0.42 printer: paper out
```

- Priority
- Header
 - Timestamp
 - Hostname
- Message
 - Tag
 - Content

By convention:

- Priority not written to logfile
- only printable ASCII
- up to 1024 characters

Syslog Message Format

```
<38>Mar 17 21:57:57 frodo sshd[701]: Connection from 211.74.5.81 port 5991
<52>Mar 17 13:54:30 192.168.0.42 printer: paper out
```

- Priority
- Header
 - Timestamp
 - Hostname
- Message
 - Tag
 - Content

By convention:

- Priority not written to logfile
- only printable ASCII
- up to 1024 characters



Syslog Message Format

```
<38>Mar 17 21:57:57 frodo sshd[701]: Connection from 211.74.5.81 port 5991
<52>Mar 17 13:54:30 192.168.0.42 printer: paper out
```

- Priority
- Header
 - Timestamp
 - Hostname
- Message
 - Tag
 - Content

By convention:

- Priority not written to logfile
- only printable ASCII
- up to 1024 characters



daemon: syslogd

- collects messages from kernel, applications, and network
- filters by priority
- writes to files, programs, terminals, or network (UDP)
- newer implementations/versions with additional features:
 - filter by host/program/regex
 - different message and timestamp formats
 - memory buffers, TCP, or SQL servers as destinations



“Transport Protocol“

Input from

- local applications: `socket(AF_UNIX, SOCK_DGRAM, 0);`
- network: `socket(AF_INET, SOCK_DGRAM, 0);`
- kernel: `open("/dev/klog", O_RDONLY, 0);`
(file interface to ring buffer)

⇒ One message per `recvfrom()/read()`.



Problems with UDP

Advantage:

- simple and efficient (usable for embedded devices)

Problems:

- possible packet loss
- no sender authentication

from `man syslogd`:

The ability to log messages received in UDP packets is equivalent to an unauthenticated remote disk-filling service. . .

⇒ move to TCP transport, optionally tunneled over SSL/TLS

IETF Working Group

“Security Issues in Network Event Logging”

- RFC 3164: The BSD Syslog Protocol (informational)
- RFC 3195: Reliable Delivery for Syslog
- current Drafts:
 - The Syslog Protocol
 - UDP transport mapping for Syslog
 - TLS transport mapping for Syslog
 - Signed Syslog Messages
 - Syslog Management Information Base

Current status:

syslog-protocol, transport-udp, transport-tls in RFC-Editor's Queue,
syslog-sign in IESG/AD evaluation, next draft in preparation

TLS Overview

Internet Draft

- point-to-point encryption, integrity, and authentication
- requires server and client certificates
- authenticate by CA or certificate/subject/fingerprint
- datagram encapsulation with length prefix, is transparent but not self-synchronizing:

```
APPLICATION-DATA = 1*SYSLOG-FRAME  
SYSLOG-FRAME = MSG-LEN SP SYSLOG-MSG  
MSG-LEN = NONZERO-DIGIT *DIGIT
```

- message length: 2048 octets **MUST**, 8192 octets **SHOULD** be supported, no upper limit

TLS Overview

Implementation

- uses OpenSSL library
- accepts arbitrary message sizes
- buffers messages on connection loss
- implements draft-ietf-syslog-transport-tls-13
- still misses draft-14 requirements:
internationalized hostnames and wildcard matching
in subjectAltName/dNSName

Problems introduced with TLS

- many new settings in `syslog.conf`
⇒ keyword=value configuration
- a send can fail
⇒ message buffers
- concurrency from non-blocking sockets, events, timeouts
⇒ connection states

syslog.conf: extended options for TLS

```

tls_ca="/etc/my.cacert"
tls_cadir="/etc/openssl/CA"
tls_cert="/etc/localhost.crt"
tls_key="/etc/localhost.key"
tls_gen_cert=on
tls_verify=off

tls_server=on
tls_bindhost="192.168.1.2"
tls_bindport="syslog-tls"
tls_allow_fingerprints=sha-1:E4:E1:A6:1C:...
tls_allow_clientcerts="/etc/somehost.crt"

```

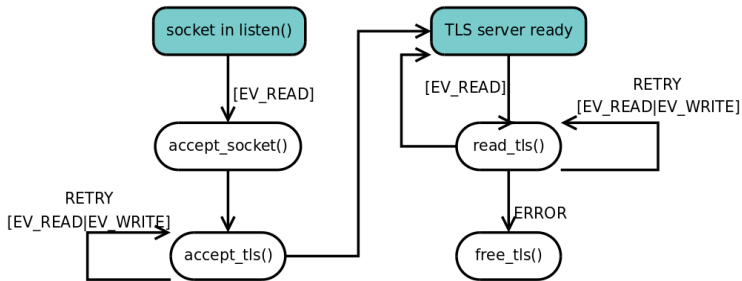
syslog.conf: TLS destinations

```
mark ,*.*    @[somehost](↵
                cert="/etc/somehost.crt")
mail.*      @[logserver]:1514(↵
                fingerprint="MD5:00:A2:....:27")
user.*      @[fe80::211:9ff:fe41:be53]:1234(↵
                verify="off")
*.alert     @[10.1.2.3]:syslog-tls(↵
                subject="logserver.example.org")
```

Buffer Queue

- every message is passed as a struct `buf_msg`
- every destination has a STAILQ of unsent buffers
- only one instance for every message, counts references
- unreliable transports: send a buffer and forget it
- reliable transports: append, send, then remove from STAILQ
- count number and size of messages per queue to control memory usage

Incoming Connection States



Draft: The Syslog Protocol

New Message Format

- keeps plain text format
- full ISO timestamps and FQDNs
- message IDs (like Windows Eventlog)
- structured data fields with namespaces (derived from SNMP Private Enterprise Codes)
- allows UTF-8 for data fields and messages
- message length:
MUST accept 480 octets, SHOULD accept 2048 octets, MAY receive larger messages (if larger: SHOULD truncate the payload, MAY discard the message)

Syslog-protocol message format

```
<165>1 2003-10-11T22:14:15.003Z frodo.example.com prog - ID47 ←
[exampleSDID@17660 iut="3" eventID="1011" eventSource="Application"] ←
BOMUne entré du journal des événements ...
```

- Header
 - Priority
 - Version (*new*)
 - Timestamp (*extended*)
 - Hostname
 - Application Name
 - Process ID
 - Message ID (*new*)
- Structured Data (*new*)
- Message text (*UTF-8*)

Syslog-protocol message format

```
<165>1 2003-10-11T22:14:15.003Z frodo.example.com prog - ID47 ←  
[exampleSDID@17660 iut="3" eventID="1011" eventSource="Application"] ←  
BOMUne entré du journal des événements ...
```

- Header
 - Priority
 - Version (*new*)
 - Timestamp (*extended*)
 - Hostname
 - Application Name
 - Process ID
 - Message ID (*new*)
- Structured Data (*new*)
- Message text (*UTF-8*)

Syslog-protocol message format

```
<165>1 2003-10-11T22:14:15.003Z frodo.example.com prog - ID47↵  
[exampleSDID@17660 iut="3" eventID="1011" eventSource="Application"]↵  
BOMUne entré du journal des événements ...
```

- Header
 - Priority
 - Version (*new*)
 - Timestamp (*extended*)
 - Hostname
 - Application Name
 - Process ID
 - Message ID (*new*)
- Structured Data (*new*)
- Message text (*UTF-8*)

Syslog-protocol message format

```
<165>1 2003-10-11T22:14:15.003Z frodo.example.com prog - ID47 ←
[exampleSDID@17660 iut="3" eventID="1011" eventSource="Application"] ←
BOMUne entré du journal des événements ...
```

- Header
 - Priority
 - Version (*new*)
 - Timestamp (*extended*)
 - Hostname
 - Application Name
 - Process ID
 - Message ID (*new*)
- Structured Data (*new*)
- Message text (*UTF-8*)

Syslog-protocol message format

```
<165>1 2003-10-11T22:14:15.003Z frodo.example.com prog - ID47 ↵
 [exampleSDID@17660 iut="3" eventID="1011" eventSource="Application"] ↵
 BOMUne entré du journal des événements ...
```

- Header
 - Priority
 - Version (*new*)
 - Timestamp (*extended*)
 - Hostname
 - Application Name
 - Process ID
 - Message ID (*new*)
- Structured Data (*new*)
- Message text (*UTF-8*)

Syslog-protocol message format

```
<165>1 2003-10-11T22:14:15.003Z frodo.example.com prog - ID47 ←
[exampleSDID@17660 iut="3" eventId="1011" eventSource="Application"] ←
BOMUne entré du journal des événements ...
```

- Header
 - Priority
 - Version (*new*)
 - Timestamp (*extended*)
 - Hostname
 - Application Name
 - Process ID
 - Message ID (*new*)
- Structured Data (*new*)
- Message text (*UTF-8*)

Syslog-protocol message format

```
<165>1 2003-10-11T22:14:15.003Z frodo.example.com prog - ID47↵
[exampleSDID@17660 iut="3" eventID="1011" eventSource="Application"]↵
BOMUne entrée du journal des événements ...
```

- Header
 - Priority
 - Version (*new*)
 - Timestamp (*extended*)
 - Hostname
 - Application Name
 - Process ID
 - Message ID (*new*)
- Structured Data (*new*)
- Message text (*UTF-8*)

Format Conversion in syslogd

- on input detect and parse
 - message only (from kernel),
 - BSD Syslog (RFC3164), or
 - Syslog-Protocol
- work with struct `buf_msg`
- on output format as
 - BSD Syslog (`-o rfc3164`) or
 - Syslog-Protocol (`-o syslog`, default)

Changes to syslog(3)

- API unchanged
- Syslog-Protocol from library to syslogd:
 - ISO timestamp
 - FQDN
 - new fields (MSGID and SD) remain empty

new function: syslogp(3)

- minimal extension to include MSGID and SD

≈ syslog(3) with three format strings

```
void syslogp(int priority, const char *msgid, ←
             const char *sdfmt, const char *message, ...);
void vsyslogp(int priority, const char *msgid, ←
              const char *sdfmt, const char *message, va_list args);
```

```
syslog(LOG_INFO, "foobar error: %m");
syslog(LOG_INFO, NULL, NULL, "foobar error: %m");
```

```
syslogp(LOG_INFO, "ID%d", "[meta language=\"en-US\"]", ←
        "event: %s", 42, EventDescription);
```

Draft: Signed syslog Messages

Overview

- adds detached, in-band signatures
- end-to-end authentication, integrity, sequencing, and lost message detection
- design elements:
 - allow several "streams" with Signature Groups
 - send public key first
 - translate sequence of messages into enumerated sequence of hash values
 - sign all control messages with keys and hashes

Signature Groups

Problem

```

2008-10-03T03:16:06.453358+02:00 host.example.org /netbsd - - - wd1e: error reading
2008-10-03T03:16:07.006246+02:00 host.example.org /netbsd - - - wd1: soft error (corrected)
2008-10-03T03:30:00.719082+02:00 host.example.org cron 24634 - - (root) CMD START (atrun)
2008-10-03T03:30:01.033121+02:00 host.example.org cron 2613 - - (root) CMD FINISH (atrun)
2008-10-03T03:32:15.035432+02:00 host.example.org postfix/pickup 3251 - - EBE21FE99: ...
2008-10-03T03:32:15.228748+02:00 host.example.org postfix/local 23858 - - EBE21FE99: ...
2008-10-03T03:32:15.234989+02:00 host.example.org postfix/qmgr 666 - - EBE21FE99: removed
2008-10-03T03:40:00.977562+02:00 host.example.org cron 2289 - - (root) CMD START (atrun)

```

Signature Groups

Problem

```

2008-10-03T03:16:06.453358+02:00 host.example.org /netbsd - - - wdie: error reading
2008-10-03T03:16:07.006246+02:00 host.example.org /netbsd - - - wdl: soft error (corrected)
2008-10-03T03:30:00.719082+02:00 host.example.org cron 24634 - - (root) CMD START (atrun)
2008-10-03T03:30:01.033121+02:00 host.example.org cron 2613 - - (root) CMD FINISH (atrun)
2008-10-03T03:32:15.035432+02:00 host.example.org postfix/pickup 3251 - - EBE21FE99: ...
2008-10-03T03:32:15.228748+02:00 host.example.org postfix/local 23858 - - EBE21FE99: ...
2008-10-03T03:32:15.234989+02:00 host.example.org postfix/qmgr 666 - - EBE21FE99: removed
2008-10-03T03:40:00.977562+02:00 host.example.org cron 2289 - - (root) CMD START (atrun)

```

Problem: Different message destinations

Signature Groups

Problem

```

2008-10-03T03:16:06.453358+02:00 host.example.org /netbsd - - - wdie: error reading
2008-10-03T03:16:07.006246+02:00 host.example.org /netbsd - - - wdl: soft error (corrected)
2008-10-03T03:30:00.719082+02:00 host.example.org cron 24634 - - (root) CMD START (atrun)
2008-10-03T03:30:01.033121+02:00 host.example.org cron 2613 - - (root) CMD FINISH (atrun)
2008-10-03T03:32:15.035432+02:00 host.example.org postfix/pickup 3251 - - EBE21FE99: ...
2008-10-03T03:32:15.228748+02:00 host.example.org postfix/local 23858 - - EBE21FE99: ...
2008-10-03T03:32:15.234989+02:00 host.example.org postfix/qmgr 666 - - EBE21FE99: removed
2008-10-03T03:40:00.977562+02:00 host.example.org cron 2289 - - (root) CMD START (atrun)

```

Problem: Different message destinations

⇒ Signature Groups to partition messages

Signature Groups

Concepts

Signature Groups distinguished by message attributes.
Basic concepts and relations:

Originator := (HOSTNAME, APP-NAME, PROCID)

Reboot Session := (*Originator*, VER, RSID)

Signature Group := (*Reboot Session*, SG, SPRI)

Signature Groups

SG/SPRI and Schemata

three predefined schemata/SG values:

- one global Signature Group (SG="0" SPRI="0")
- 192 Signature Groups, one per PRI value (SG="1" SPRI="PRI")
- Signature Groups for ranges of sequential PRI values (SG="2" SPRI="X")

and one implementation-defined value:

- in syslogd: one Signature Group per destination (SG="3" SPRI="fd")

Payload Blocks

Send Public Key

```
<110>1 2008-08-02T01:09:27.773505+02:00 host.example.org syslogd - - ←  
[ssign-cert VER="0111" RSID="1217632162" SG="3" SPRI="0" TBPL="1059" ←  
INDEX="1" FLEN="1059" FRAG="2008-08-02T01:09:27.773464+02:00 C ←  
MIIC+jCCArmGAWIBAwIBA...YA==" SIGN="MCOCFFEHx8UX32vEW...k+o="]
```

sent on startup, contains:

- Signature Group (VER, RSID, SG, SPRI)
- fragmentation info (TBPL, INDEX, FLEN)
- Payload Block (FRAG) with
 - timestamp
 - key type
 - key blob (base64)
- DSA Signature (SIGN)

Payload Blocks

Send Public Key

```
<110>1 2008-08-02T01:09:27.773505+02:00 host.example.org syslogd - - ←  
[ssign-cert VER="0111" RSID="1217632162" SG="3" SPRI="0" TBPL="1059" ←  
INDEX="1" FLEN="1059" FRAG="2008-08-02T01:09:27.773464+02:00 C ←  
MIIC+jCCArmGAWIBAwIBA...YA==" SIGN="MCOCFFEHx8UX32vEW...k+o="]
```

sent on startup, contains:

- Signature Group (VER, RSID, SG, SPRI)
- fragmentation info (TBPL, INDEX, FLEN)
- Payload Block (FRAG) with
 - timestamp
 - key type
 - key blob (base64)
- DSA Signature (SIGN)

Payload Blocks

Send Public Key

```
<110>1 2008-08-02T01:09:27.773505+02:00 host.example.org syslogd - - ←  
[ssign-cert VER="0111" RSID="1217632162" SG="3" SPRI="0" TBPL="1059" ←  
INDEX="1" FLEN="1059" FRAG="2008-08-02T01:09:27.773464+02:00 C ←  
MIIC+jCCArmGAWIBAwIBA...YA==" SIGN="MCOCFFEHx8UX32vEW...k+o="]
```

sent on startup, contains:

- Signature Group (VER, RSID, SG, SPRI)
- fragmentation info (TBPL, INDEX, FLEN)
- Payload Block (FRAG) with
 - timestamp
 - key type
 - key blob (base64)
- DSA Signature (SIGN)

Payload Blocks

Send Public Key

```
<110>1 2008-08-02T01:09:27.773505+02:00 host.example.org syslogd - - ←  
[ssign-cert VER="0111" RSID="1217632162" SG="3" SPRI="0" TBPL="1059" ←  
INDEX="1" FLEN="1059" FRAG="2008-08-02T01:09:27.773464+02:00 C ←  
MIIC+jCCArmGAWIBAwIBA. . . YA==" SIGN="MCOCFFEHx8UX32vEW. . . k+o="]
```

sent on startup, contains:

- Signature Group (VER, RSID, SG, SPRI)
- fragmentation info (TBPL, INDEX, FLEN)
- Payload Block (FRAG) with
 - timestamp
 - key type
 - key blob (base64)
- DSA Signature (SIGN)

Payload Blocks

Send Public Key

```
<110>1 2008-08-02T01:09:27.773505+02:00 host.example.org syslogd - - ←  
[ssign-cert VER="0111" RSID="1217632162" SG="3" SPRI="0" TBPL="1059" ←  
INDEX="1" FLEN="1059" FRAG="2008-08-02T01:09:27.773464+02:00 C ←  
MIIC+jCCArmGAWIBAwIBA...YA==" SIGN="MCOCFFEHx8UX32vEW...k+o="]
```

sent on startup, contains:

- Signature Group (VER, RSID, SG, SPRI)
- fragmentation info (TBPL, INDEX, FLEN)
- Payload Block (FRAG) with
 - timestamp
 - key type
 - key blob (base64)
- DSA Signature (SIGN)

Signature Blocks

Collect SHA-1 Hashes

```
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg0
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg1
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg2
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg3
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg4
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg5
```

Signature Blocks

Collect SHA-1 Hashes

```
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg0
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg1
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg2
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg3
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg4
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg5
```

```
siUJM358eYFHOS2KOMTlveWeH/U=
```

Signature Blocks

Collect SHA-1 Hashes

```
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg0
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg1
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg2
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg3
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg4
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg5
```

```
siUJM358eYFHOS2KOMTlveWeH/U= zTxfthW8WqmtFhOG4k/+ZxkirTA=
```

Signature Blocks

Collect SHA-1 Hashes

```
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg0
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg1
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg2
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg3
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg4
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg5
```

```
siUJM358eYFHOS2KOMTlveWeH/U= zTxfthW8WqmtFhOG4k/+ZxkirTA=
j9dubU1GNVp7qWShwph/w32nD08=
```

Signature Blocks

Collect SHA-1 Hashes

```
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg0
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg1
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg2
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg3
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg4
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg5
```

```
siUJM358eYFHOS2KOMTlveWeH/U= zTxfthW8WqmtFhOG4k/+ZxkirTA=
j9dubU1GNVp7qWShwph/w32nD08= XQDLZ/NuwirmLdMORTm84r9kIW4=
```

Signature Blocks

Collect SHA-1 Hashes

```
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg0
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg1
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg2
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg3
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg4
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg5
```

```
siUJM358eYFHOS2KOMTlveWeH/U= zTxfthW8WqmtFhOG4k/+ZxkirTA=
j9dubU1GNVp7qWShwph/w32nD08= XQDLZ/NuwirmLdMORtm84r9kIW4=
RNDFNCo7hiCsK/EKumsPBbFHNZA=
```

Signature Blocks

Collect SHA-1 Hashes

```
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg0
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg1
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg2
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg3
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg4
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg5
. . .
```

```
siUJM358eYFHOS2KOMTlveWeH/U= zTxfthW8WqmtFhOG4k/+ZxkirTA=
j9dubU1GNVp7qWShwph/w32nD08= XQDLZ/NuwirmLdMORtm84r9kIW4=
RNDFNCo7hiCsK/EKumsPBbFHNZA= ANiE3KbY948J6cEB640fAtWXu04=
. . .
```



Signature Blocks

Collect SHA-1 Hashes

```
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg0
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg1
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg2
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg3
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg4
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg5
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg6
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg7
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg8
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg9
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg10
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg11
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg12
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg13
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg14
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg15
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg16
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - msg17
```

```
siUJM358eYFHOS2KOMTlveWeH/U= zTxfthW8WqmtFh0G4k/+ZxkirTA= j9dubU1GNVp7qWShwph/w32nD08=
XQDLZ/NuwirmLdMORtm84r9kIW4= RNDFNcO7hiCsK/EKumsPBbFHNZA= ANiE3KbY948J6cEB640fAtWxU04=
e2M/QqjHdfxLVUSPt1CsNJHm9wU= Y+racQst7F1gR8eEUh807o+M53s= JAMULRxjMPb005EhhKbsUkAwb10=
pd+N5kmlnyQ0BoItELd/KWQrcMg= dsMQSzPHIS6S3Vaa23/t7U8JAJ4= i4rE3x7N4qyQGTkmaWHSWDFP9SY=
qgTqV4EgFUFD3uZXNPvJ25erzBI= XWOYrME5kQEh+fxhg1fetrWxfIc= 7YPcRHsDwXWnQuGRWaJtFwW9hus=
PIvLm0mh+he5+PDihG1p7sQ1x8k= 1PzUvx0I1VwSGWV7yKF9W//Yb2U= X+PWYcx5AXnsDVSNAHLZUGk5ioY=
```

Signature Blocks

Send Signature Block Message

```
<110>1 2008-08-02T01:09:32.399406+02:00 host.example.org syslogd - - [ssign VER="0111"
RSID="1217632162" SG="3" SPRI="0" GBC="4" FMN="1" CNT="20" HB="siUJM358eYFHOS2KOMTlveWeH/U=
zTxfthW8WqmtFhOG4k/+ZxkirTA= j9dubU1GNVp7qWShwph/w32nD08= XQDLZ/NuwirmLdMORtm84r9kIW4=
RNDFNCo7hiCsK/EKumsPBbFHNZA= ANiE3KbY948J6cEB640fAtWXu04= e2M/0qjHDfxLVUSPt1CsNJHm9wU=
Y+racQst7F1gr8eEUh807o+M53s= JAMULRxjMPb005EhhKbsUkAwbl0= pd+N5kmlnyQ0BoItELd/KWQrcMg=
dsMQSszPHIS6S3Vaa23/t7U8JAJ4= i4rE3x7N4qyQGTkmaWHsWDFP9SY= qgTqV4EgfUFd3uZXPvJ25erzBI=
XW0YrME5kQEh+fxhg1fetnWxfIc= 7YPcRHsDwXWnQuGRWaJtFWw9hus= PIvLmOmh+he5+PDihG1p7sQ1x8k=
lPzUvxOI1VwSGWV7yKF9W//Yb2U= X+PWYcx5AXnsDVSNAHLZUGk5ioY= okXY88MGG4QybrYMf8HJN23W01Y=
HcaPyHfQ2s1SuSciTKw4woYwMg=" SIGN="MCWCFFr0i6taT1vWowR7yc5bEQxFfY7/Ah...IQ==" ]
```

sent as syslog message, contains:

- Signature Group (VER, RSID, SG, SPRI)
- Global Block Counter (GBC, counts syslog-sign messages)
- First Message Number (FMN, counts normal messages)
- CNT Hash Blocks (HB)
- DSA Signature (SIGN)

Signature Blocks

Send Signature Block Message

```
<110>1 2008-08-02T01:09:32.399406+02:00 host.example.org syslogd - - [ssign VER="0111"
RSID="1217632162" SG="3" SPRI="0" GBC="4" FMN="1" CNT="20" HB="siUJM358eYFHOS2KOMTlveWeH/U=
zTxfthW8WqmtFhOG4k/+ZxkirTA= j9dubU1GNVp7qWShwph/w32nD08= XQDLZ/NuwirmLdMORtm84r9kIW4=
RNDFNCo7hiCsK/EKumsPBbFHNZA= ANiE3KbY948J6cEB640fAtWXu04= e2M/0qjHDfxLVUSPt1CsNJHm9wU=
Y+racQst7F1gr8eEUh807o+M53s= JAMULRxjMPb005EhhKbsUkAwbl0= pd+N5kmlnyQ0BoItELd/KWQrcMg=
dsMQSzPHIS6S3Vaa23/t7U8JAJ4= i4rE3x7N4qyQGTkmaWHsWDFP9SY= qgTqV4EgfUFd3uZXPvJ25erzBI=
XW0YrME5kQEh+fxhg1fetnWxfIc= 7YPcRHsDwXWnQuGRWaJtFWw9hus= PIvLmOmh+he5+PDihG1p7sQ1x8k=
lPzUvxOI1VwSGWV7yKF9W//Yb2U= X+PWYcx5AXnsDVSNAHLZUGk5ioY= okXY88MGG4QybrYMf8HJN23W01Y=
HcaPyHfQ2s1SuSciTKw4woYwMg=" SIGN="MCWCFFr0i6taT1vWowR7yc5bEQxFfY7/Ah...IQ=="]
```

sent as syslog message, contains:

- Signature Group (VER, RSID, SG, SPRI)
- Global Block Counter (GBC, counts syslog-sign messages)
- First Message Number (FMN, counts normal messages)
- CNT Hash Blocks (HB)
- DSA Signature (SIGN)

Signature Blocks

Send Signature Block Message

```
<110>1 2008-08-02T01:09:32.399406+02:00 host.example.org syslogd - - [ssign VER="0111"  
RSID="1217632162" SG="3" SPRI="0" GBC="4" FMN="1" CNT="20" HB="siUJM358eYFHOS2KOMTlveWeH/U=  
zTxfthW8WqmtFhOG4k/+ZxkirTA= j9dubU1GNVp7qWShwph/w32nD08= XQDLZ/NuwirmLdMORtm84r9kIW4=  
RNDFNCo7hiCsK/EKumsPBbFHNZA= ANiE3KbY948J6cEB640fAtWXu04= e2M/0qjHDfxLVUSPt1CsNJHm9wU=  
Y+racQst7F1gr8eEUh807o+M53s= JAMULRxjMPb005EhhKbsUkAwbl0= pd+N5kmlnyQ0BoItELd/KWQrcMg=  
dsMQS3PHIS6S3Vaa23/t7U8JAJ4= i4rE3x7N4qyQGTkmaWHsWDFP9SY= qgTqV4EgfUFd3uZXNPvJ25erzBI=  
XW0YrME5kQEh+fxhg1fetnWxfIc= 7YPcRHsDwXWnQuGRWaJtFWw9hus= PIvLmOmh+he5+PDihG1p7sQ1x8k=  
lPzUvx0I1VwSGWV7yKF9W//Yb2U= X+PWYcx5AXnsDVSNAHLZUGk5ioY= okXY88MGG4QybrYMf8HJN23W01Y=  
HcaPyHfQ2s1SuSciTKw4woYwMg=" SIGN="MCwCFFr0i6taT1vWowR7yc5bEQxFfY7/Ah...IQ==" ]
```

sent as syslog message, contains:

- Signature Group (VER, RSID, SG, SPRI)
- Global Block Counter (GBC, counts syslog-sign messages)
- First Message Number (FMN, counts normal messages)
- CNT Hash Blocks (HB)
- DSA Signature (SIGN)

Signature Blocks

Send Signature Block Message

```
<110>1 2008-08-02T01:09:32.399406+02:00 host.example.org syslogd - - [ssign VER="0111"  
RSID="1217632162" SG="3" SPRI="0" GBC="4" FMN="1" CNT="20" HB="siUJM358eYFHOS2KOMTlveWeH/U=  
zTxfthW8WqmtFhOG4k/+ZxkirTA= j9dubU1GNVp7qWShwph/w32nD08= XQDLZ/NuwirmLdMORtm84r9kIW4=  
RNDFNCo7hiCsK/EKumsPBbFHNZA= ANiE3KbY948J6cEB640fAtWXu04= e2M/0qjHDfxLVUSPt1CsNJHm9wU=  
Y+racQst7F1gr8eEUh807o+M53s= JAMULRxjMPb005EhhKbsUkAwbl0= pd+N5kmlnyQ0BoItELd/KWQrcMg=  
dsMQSzPHIS6S3Vaa23/t7U8JAJ4= i4rE3x7N4qyQGTkmaWHsWDFP9SY= qgTqV4EgfUFd3uZXNPvJ25erzBI=  
XW0YrME5kQEh+fxhg1fetnWxfIc= 7YPcRHsDwXWnQuGRWaJtFWw9hus= PIvLmOmh+he5+PDihG1p7sQ1x8k=  
lPzUvx0I1VwSGWV7yKF9W//Yb2U= X+PWYcx5AXnsDVSNAHLZUGk5ioY= okXY88MGG4QybrYMf8HJN23W01Y=  
HcaPyHfQ2s1SuSciTKw4woYwMg=" SIGN="MCWCFFr0i6taT1vWowR7yc5bEQxPfY7/Ah...IQ==" ]
```

sent as syslog message, contains:

- Signature Group (VER, RSID, SG, SPRI)
- Global Block Counter (GBC, counts syslog-sign messages)
- First Message Number (FMN, counts normal messages)
- CNT Hash Blocks (HB)
- DSA Signature (SIGN)

Signature Blocks

Send Signature Block Message

```
<110>1 2008-08-02T01:09:32.399406+02:00 host.example.org syslogd - - [ssign VER="0111"  
RSID="1217632162" SG="3" SPRI="0" GBC="4" FMN="1" CNT="20" HB="siUJM358eYFHOS2KOMTLveWeH/U=  
zTxfthW8WqmtFhOG4k/+ZxkirTA= j9dubU1GNVp7qWShwph/w32nD08= XQDLZ/NuwirmLdMORtm84r9kIW4=  
RNDFNCo7hiCsK/EKumsPBbFHNZA= ANiE3KbY948J6cEB640fAtWXu04= e2M/OqjHDfxLVUSPt1CsNJHm9wU=  
Y+racQst7F1gr8eEUh807o+M53s= JAMULRxjMPb005EhhKbsUkAwbl0= pd+N5kmlnyQ0BoItELd/KWQrcMg=  
dsMQSszPHIS6S3Vaa23/t7U8JAJ4= i4rE3x7N4qyQGTkmaWHsWDFP9SY= qgTqV4EgfUFd3uZXNPvJ25erzBI=  
XWOYrME5kQEh+fxhg1fetnWxfIc= 7YPcRHsDwXWnQuGRWaJtFWw9hus= PIvLmOmh+he5+PDihG1p7sQ1x8k=  
lPzUvxOI1VwSGWV7yKF9W//Yb2U= X+PWYcx5AXnsDVSNAHLZUGk5ioY= okXY88MGG4QybrYMf8HJN23W01Y=  
HcaPyHfQ2s1SuSciTKw4woYwMg=" SIGN="MCwCFFr0i6taT1vWowR7yc5bEQxFfY7/Ah...IQ==" ]
```

sent as syslog message, contains:

- Signature Group (VER, RSID, SG, SPRI)
- Global Block Counter (GBC, counts syslog-sign messages)
- First Message Number (FMN, counts normal messages)
- CNT Hash Blocks (HB)
- DSA Signature (SIGN)

Signature Blocks

Send Signature Block Message

```
<110>1 2008-08-02T01:09:32.399406+02:00 host.example.org syslogd - - [ssign VER="0111"
RSID="1217632162" SG="3" SPRI="0" GBC="4" FMN="1" CNT="20" HB="siUJM358eYFHOS2KOMTlveWeH/U=
zTxfthW8WqmtFhOG4k/+ZxkirTA= j9dubU1GNVp7qWShwph/w32nD08= XQDLZ/NuwirmLdMORtm84r9kIW4=
RNDFNCo7hiCsK/EKumsPBbFHNZA= ANiE3KbY948J6cEB640fAtWXu04= e2M/0qjHDfxLVUSPt1CsNJHm9wU=
Y+racQst7F1gr8eEUh807o+M53s= JAMULRxjMPb005EhhKbsUkAwbl0= pd+N5kmlnyQ0BoItELd/KWQrcMg=
dsMQSzPHIS6S3Vaa23/t7U8JAJ4= i4rE3x7N4qyQGTkmaWHsWDFP9SY= qgTqV4EgfUFd3uZXNPvJ25erzBI=
XW0YrME5kQEh+fxhg1fetnWxfIc= 7YPcRHsDwXWnQuGRWaJtFWw9hus= PIvLmOmh+he5+PDihG1p7sQ1x8k=
lPzUvxOI1VwSGWV7yKF9W//Yb2U= X+PWYcx5AXnsDVSNAHLZUGk5ioY= okXY88MGG4QybrYMf8HJN23W01Y=
HcaPyHfQ2s1SuSciTKw4woYwMg=" SIGN="MCwCFFr0i6taT1vWowR7yc5bEQxFfY7/Ah...IQ==" ]
```

sent as syslog message, contains:

- Signature Group (VER, RSID, SG, SPRI)
- Global Block Counter (GBC, counts syslog-sign messages)
- First Message Number (FMN, counts normal messages)
- CNT Hash Blocks (HB)
- DSA Signature (SIGN)

Redundancy

Implementation-dependent

Syslog-Sign messages might be lost (with UDP), thus

- Certificate Blocks are repeated several times
- Hashes are sent using a sliding window:

```
ssign: FMN="12" HB="#12 #13 #14 #15 #16 #17 #18 #19 #20"
```

```
ssign: FMN="15" HB="#15 #16 #17 #18 #19 #20 #21 #22 #23"
```

```
ssign: FMN="18" HB="#18 #19 #20 #21 #22 #23 #24 #25 #26"
```

```
ssign: FMN="21" HB="#21 #22 #23 #24 #25 #26 #27 #28 #29"
```

```
ssign: FMN="24" HB="#24 #25 #26 #27 #28 #29 #30 #31 #32"
```

Redundancy

Implementation-dependent

Syslog-Sign messages might be lost (with UDP), thus

- Certificate Blocks are repeated several times
- Hashes are sent using a sliding window:

```
ssign: FMN="12" HB="#12 #13 #14 #15 #16 #17 #18 #19 #20"  
ssign: FMN="15" HB="#15 #16 #17 #18 #19 #20 #21 #22 #23"  
ssign: FMN="18" HB="#18 #19 #20 #21 #22 #23 #24 #25 #26"  
ssign: FMN="21" HB="#21 #22 #23 #24 #25 #26 #27 #28 #29"  
ssign: FMN="24" HB="#24 #25 #26 #27 #28 #29 #30 #31 #32"
```

Configuration

not variable

- not configurable: hash and key type
 - always VER="0111" (currently only SHA-1)
 - PKIX if TLS key is of type DSA,
otherwise public key (sent in DER encoding)
- at compile time: redundancy and message length
 - `#define SIGN_RESENDCOUNT_CERTBLOCK 2`
 - `#define SIGN_RESENDCOUNT_HASHES 3`
 - `#define SIGN_MAX_LENGTH 2048`

Configuration

syslog.conf

- configurable: Signature Groups
 - `sign_sg=2`
 - `sign_delim_sg=15 31`
- configurable: write priority and version

```

*.*          +/var/log/signed.log
mail.*      +-/var/log/signed-mail.log
*.alert     +|/usr/local/sbin/monitor

```

Offline Verification

1. split input into
Certificate Blocks, Signature Blocks, normal messages
2. index normal messages by hash value
3. sort Certificate Blocks and Signature Blocks
4. reassemble and verify Certificate Blocks
⇒ yields public keys for all Signature Groups
5. verify Signature Blocks
6. build enumerated sequence of hashes (with FMN)
7. match received messages against hashes
⇒ yields verified message sequence, including gaps

verify.pl

```

$ perl verify.pl -i test.log
reading input...
processing CBs...
decoding SGs...
got PKIX DSA key
verifying CBs...
verified CB and got key for SG: (host.example.org,1217632162,0111,3,0), ←
    start: 2008-08-02T01:09:27.773464+02:00
now process SBs
signed messages:
...
host.example.org,1217632162,0111,3,0,11 <15>1 ... test 6255 - - msg10
host.example.org,1217632162,0111,3,0,12 <15>1 ... test 6255 - - msg11
host.example.org,1217632162,0111,3,0,13 **** msg lost
host.example.org,1217632162,0111,3,0,14 <15>1 ... test 6255 - - msg13
host.example.org,1217632162,0111,3,0,15 <15>1 ... test 6255 - - msg14
host.example.org,1217632162,0111,3,0,16 <15>1 ... test 6255 - - msg15
...
messages without signature:
<15>1 2008-08-02T02:09:27+02:00 host.example.org test 6255 - - modified msg12

```

ToDo List

- implement missing parts of transport-tls-14
- implement online signature verification
- implement alternative configuration file format

- port to other systems
- agree on syslogp(3) (or similar)
- upgrade log infrastructure
- use structured data
- wait for RFCs

possible alternative syslog.conf

- too many new settings for old syslog.conf
- especially for per-destination settings
- new format wanted
- proposed:

```
*.info    /var/log/messages
```

```
mail.* {  tls
          host "server.example.net"
          port 1234
          fingerprint "SHA1:e4e1:a61c:d431:d7d4:9bb8:dcdcf:..."
        }
```

```
{ *.debug
  app-id postfix
} { udp
  host "host.example.net"
  port 1514
}
```

Portability

- uses OpenSSL
- uses libevent to hide kqueue(2)
- wallmsg() is system-dependend
- differences in libc/syslog(3)
- small differences in stdlibs

Conclusion

- working implementation of transport-tls
- receive/send syslog-protocol in syslogd(8)
- send syslog-protocol from syslog(3)
- add extended function syslogp(3)
- implement syslog-sign to sign in syslogd(8)
- “Proof of Concept” implementation to verify syslog-sign