

Improving
atftp{,d} and
-Package

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option

Windowsize

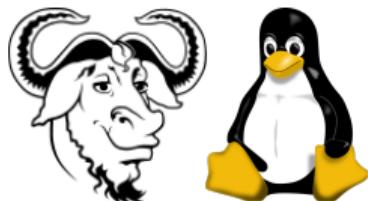
Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary



Improving atftp{,d} and -Package

Protocols, RFCs, CVEs, PCREs and a Sourcerer's Apprentice

Andreas B. Mundt
andi@debian.org

MiniDebConf Hamburg

29. May 2022



TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

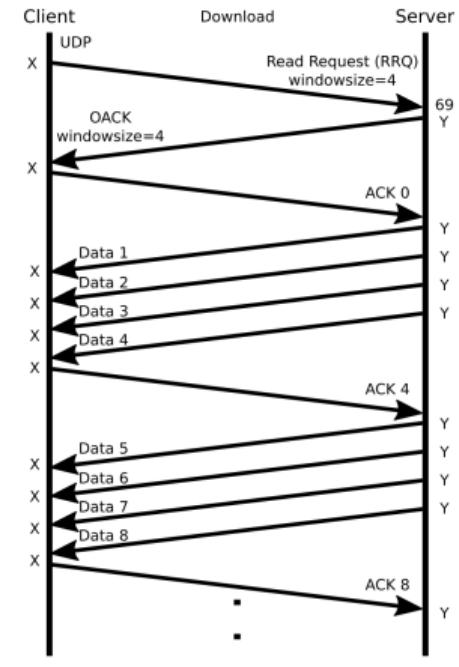
① TFTP Protocol

② atftp{,d}

③ TFTP Option Extension: Windowsize

④ Security Issues

⑤ PCRE2 Port



TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

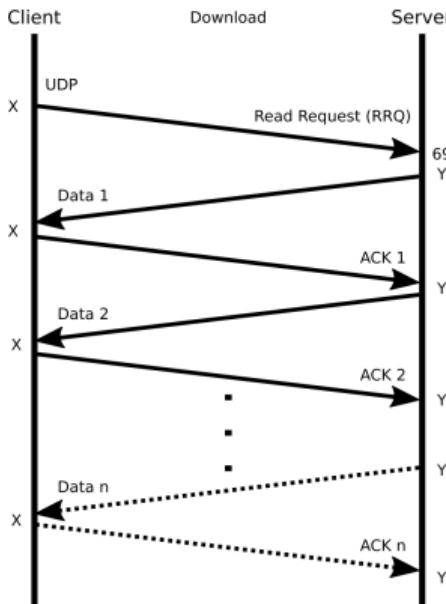
Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary



Trivial File Transfer Protocol

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
1	0.000000000	::1	41944	::1	69	TFTP	93	Read Request, File: d-i/n-
2	0.021296925	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 1
3	0.021366085	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 1
4	0.021398777	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 2
5	0.021429127	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 2
6	0.021469999	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 3
7	0.021498167	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 3
8	0.021527434	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 4
9	0.021556974	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 4
10	0.021573057	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 5
11	0.021604702	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 5
12	0.021619356	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 6
13	0.021631376	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 6
14	0.021644470	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 7
15	0.021656429	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 7
16	0.021669326	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 8
17	0.021681239	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 8
18	0.021697141	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 9
19	0.021744167	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 9
20	0.021758924	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 10
21	0.021772046	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 10
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
3645	0.061388936	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 1822
3646	0.061398571	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 1823
3647	0.061407236	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 1823
3648	0.061416838	::1	54995	::1	41944	TFTP	578	Data Packet, Block: 1824
3649	0.061425553	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 1824
3650	0.061437327	::1	54995	::1	41944	TFTP	418	Data Packet, Block: 1825 (last)
3651	0.061454647	::1	41944	::1	54995	TFTP	66	Acknowledgement, Block: 1825

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Request For Comments:

- RFC 783 (First Revision, 1981)
- RFC 1123 (1989): *Sorcerer's Apprentice Syndrome*¹
- RFC 1350 (Second Revision, 1992)
- RFC 2347 (TFTP Option Extension, 1998)
- RFC 2348 (TFTP Blocksize Option, 1998)
- RFC 2349 (TFTP Timeout Interval and Transfer Size Options, 1998)
- RFC 7440 (TFTP Windowsize Option, 2015)

¹Cf. J.W. von Goethe, „Der Zauberlehrling“: „Die ich rief, die Geister werd ich nun nicht los.“ (1797)
„The spirits that I summoned / I now cannot rid myself of again“

Trivial File Transfer Protocol

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Request For Comments:

- RFC 783 (First Revision, 1981)
- RFC 1123 (1989): *Sorcerer's Apprentice Syndrome*¹
- RFC 1350 (Second Revision, 1992)
- RFC 2347 (TFTP Option Extension, 1998)
- RFC 2348 (TFTP Blocksize Option, 1998)
- RFC 2349 (TFTP Timeout Interval and Transfer Size Options, 1998)
- RFC 7440 (TFTP Windowsize Option, 2015)



¹Cf. J.W. von Goethe, „Der Zauberlehrling“: „Die ich rief, die Geister werd ich nun nicht los.“ (1797)
„The spirits that I summoned / I now cannot rid myself of again“

Trivial File Transfer Protocol

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Request For Comments:

- RFC 783 (First Revision, 1981)
- RFC 1123 (1989): *Sorcerer's Apprentice Syndrome*¹
- RFC 1350 (Second Revision, 1992)
- RFC 2347 (TFTP Option Extension, 1998)
- RFC 2348 (TFTP Blocksize Option, 1998)
- RFC 2349 (TFTP Timeout Interval and Transfer Size Options, 1998)
- RFC 7440 (TFTP Windowsize Option, 2015)



¹Cf. J.W. von Goethe, „Der Zauberlehrling“: „Die ich rief, die Geister werd ich nun nicht los.“ (1797)
„The spirits that I summoned / I now cannot rid myself of again“

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Request For Comments:

- RFC 783 (First Revision, 1981)
- RFC 1123 (1989): *Sorcerer's Apprentice Syndrome*¹
- RFC 1350 (Second Revision, 1992)
- RFC 2347 (TFTP Option Extension, 1998)
- RFC 2348 (TFTP Blocksize Option, 1998)
- RFC 2349 (TFTP Timeout Interval and Transfer Size Options, 1998)
- RFC 7440 (TFTP Windowsize Option, 2015)

¹Cf. J.W. von Goethe, „Der Zauberlehrling“: „Die ich rief, die Geister werd ich nun nicht los.“ (1797)
„The spirits that I summoned / I now cannot rid myself of again“

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Request For Comments:

- RFC 783 (First Revision, 1981)
- RFC 1123 (1989): *Sorcerer's Apprentice Syndrome*¹
- RFC 1350 (Second Revision, 1992)
- RFC 2347 (TFTP Option Extension, 1998)
- RFC 2348 (TFTP Blocksize Option, 1998)
- RFC 2349 (TFTP Timeout Interval and Transfer Size Options, 1998)
- RFC 7440 (TFTP Windowsize Option, 2015)

¹Cf. J.W. von Goethe, „Der Zauberlehrling“: „Die ich rief, die Geister werd ich nun nicht los.“ (1797)
„The spirits that I summoned / I now cannot rid myself of again“

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Request For Comments:

- RFC 783 (First Revision, 1981)
- RFC 1123 (1989): *Sorcerer's Apprentice Syndrome*¹
- RFC 1350 (Second Revision, 1992)
- RFC 2347 (TFTP Option Extension, 1998)
- RFC 2348 (TFTP Blocksize Option, 1998)
- RFC 2349 (TFTP Timeout Interval and Transfer Size Options, 1998)
- RFC 7440 (TFTP Windowsize Option, 2015)

¹Cf. J.W. von Goethe, „Der Zauberlehrling“: „Die ich rief, die Geister werd ich nun nicht los.“ (1797)
„The spirits that I summoned / I now cannot rid myself of again“

Trivial File Transfer Protocol

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Request For Comments:

- RFC 783 (First Revision, 1981)
- RFC 1123 (1989): *Sorcerer's Apprentice Syndrome*¹
- RFC 1350 (Second Revision, 1992)
- RFC 2347 (TFTP Option Extension, 1998)
- RFC 2348 (TFTP Blocksize Option, 1998)
- RFC 2349 (TFTP Timeout Interval and Transfer Size Options, 1998)
- RFC 7440 (TFTP Windowsize Option, 2015)



¹Cf. J.W. von Goethe, „Der Zauberlehrling“: „Die ich rief, die Geister werd ich nun nicht los.“ (1797)
„The spirits that I summoned / I now cannot rid myself of again“

FLOSS Implementations and Use Cases

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

TFTP-Server:

- `tftpd-hpa`: HPA's tftp server
- `atftpd`: advanced TFTP server
- `dnsmasq`: small caching DNS proxy and DHCP/TFTP server
- ...

Use cases:

- because of triviality: only local area network (LAN)
- network boot, preboot execution environment (PXE)
- embedded systems: flashing firmware images on devices like routers, firewalls, IP phones, ...

FLOSS Implementations and Use Cases

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

TFTP-Server:

- tftpd-hpa: HPA's tftp server
- atftpd: advanced TFTP server
- dnsmasq: small caching DNS proxy and DHCP/TFTP server
- ...

Use cases:

- because of triviality: only local area network (LAN)
- network boot, preboot execution environment (PXE)
- embedded systems: flashing firmware images on devices like routers, firewalls, IP phones, ...

1 TFTP Protocol

2 atftp{,d}

3 TFTP Option Extension: Windowsize

Implementation in atftp{,d}

Open Questions and Tests

4 Security Issues

5 PCRE2 Port

atftpd Upstream

atftp is a client/server implementation of the TFTP protocol that implements RFCs 1350, 2090, 2347, 2348, 2349 and 7440. The server is multi-threaded and the client presents a friendly interface using libreadline.

Author: Jean-Pierre Lefebvre <helix@step.polymtl.ca> August, 2000

Contributions:

Jeff Miller <jeff.miller@transact.com.au>
Leif Lindholm <leif.lindholm@i3micro.com>
Jens Schmidt <Jens.A.Schmidt@dxd.ericsson.se>
Svend Odgaard <Svend.Odgaard@dxd.ericsson.se>
Joshua Aune <jluken@linuxnetworx.com>
Mario Lorenz <Mario.Lorenz@km3.de>
Allen Reese <areese@lnxi.com>
Thayne Harbaugh <tharbaugh@lnxi.com>
Thomas Anders <thomas.anders@blue-cable.de>
Michał Rzechonek <m.rzechonek@kelvatek.com>

Florian Fainelli <f.fainelli@gmail.com>
Denis Andzakovic <denis.andzakovic@pulsesecurity.co.nz>
Rosen Penev <rosenp@gmail.com>
Peter Kaestle <peter.kaestle@nokia.com>
Grant Edwards
Ryan Barnett <ryan.barnett@rockwellcollins.com>
Peter Seiderer <ps.report@gmx.net>
Simon Rettberg <simon.rettberg@rz.uni-freiburg.de>
...

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Debian Bug report logs - #69486

ITP: atftp -- advanced TFTP client/server

Package: [wnpp](#); Maintainer for [wnpp](#) is wnpp@debian.org;

Reported by: [Remi Lefebvre <remi@debian.org>](#)

Date: Sun, 20 Aug 2000 18:03:27 UTC

Severity: wishlist

Fixed in version atftp/0.1

Done: Remi Lefebvre <remi@debian.org>

Bug is archived. No further changes may be made.

Further Maintenance:

<https://tracker.debian.org/pkg/atftp/news/>

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Debian Bug report logs - #69486

ITP: atftp -- advanced TFTP client/server

Package: [wnpp](#); Maintainer for [wnpp](#) is wnpp@debian.org;

Reported by: [Remi Lefebvre <remi@debian.org>](#)

Date: Sun, 20 Aug 2000 18:03:27 UTC

Severity: wishlist

Fixed in version atftp/0.1

Done: Remi Lefebvre <remi@debian.org>

Bug is archived. No further changes may be made.

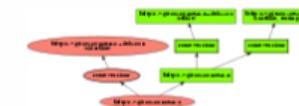
Further Maintenance:

<https://tracker.debian.org/pkg/atftp/news/>

Debian Bug report logs - #988456

Installation inconsistent, missing dependency, not up-to-date

Package: [atftpd](#); Maintainer for [atftpd](#) is [Ludovic Drolez <ldrolez@debian.org>](mailto:Ludovic_Drolez<ldrolez@debian.org); Source for [atftpd](#) is [src:atftp](#) ([PTS](#), [buildd](#), [popcon](#)).



Reported by: **Frank Winkler <debian@f.winkler-ka.de>**

Date: Thu, 13 May 2021 10:54:02 UTC

Severity: *serious*

Found in versions atftp/0.7.git20120829-3.2, atftp/0.7.git20120829-3.2~deb10u1

Fixed in version atftp/0.7.git20120829-3.3

Done: Andreas B. Mundt <andi@debian.org>

Bug is archived. No further changes may be made.

<https://bugs.debian.org/988456>

Team Maintenance of atftpd

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

- Fix #988456 (missing dependency) durch NMU (Non-Maintainer-Upload)²
- Salsa Repository: <https://salsa.debian.org/debian/atftp>
- Debian ← Upstream Sources: 0.7.git20120829 → 0.7.git20210202
- Clean-up and bookwork³
- BTS (Bug Tracking System): *Sorcerer's Apprentice Syndrome*⁴

² <https://tracker.debian.org/news/1244996/accepted-atftp-07git20120829-33-source-into-unstable/>

³ <https://tracker.debian.org/news/1245138/accepted-atftp-07git20210202-1-source-into-experimental/>

⁴ (original) patch from 2011: <https://bugs.debian.org/275056>

Improving atftp{,d} and -Package

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Upstream . . .

Updated:	Created:	Creator:	Private:
2021-09-13	2021-05-25	Ferdinand T.	No

Use Vladimir Nadvornik's heuristic for packet retransmission by default, the RFC1350 compliant behaviour stays optional.

This patch (by vcizek@suse.com) is used by SUSE / openSUSE for some years, so I think it should be upstreamed.

1 Attachments

[atftp-0.7-ack_heuristic.patch](#)

Updated:	Created:	Creator:	Private:
2021-09-13	2021-05-25	Ferdinand T.	No

Fix a race condition where two server threads pick up a single client, which causes the transported file being overwritten.

This patch is used by SUSE / openSUSE for some years, not sure why it is not upstreamed.
I think it should be.

1 Attachments

[atftp-0.7-server_receive_race.patch](#)

Updated:	Created:	Creator:	Private:
2021-09-13	2021-05-26	Ferdinand T.	No

Add a option to prevent the Sorcerer's Apprentice Syndrome

See https://en.wikipedia.org/wiki/Sorcerer%27s_Apprentice_Syndrome

This patch is used on SUSE / openSUSE for some years, time to upstream it.

1 Attachments

[atftp-0.7-sorcerers_apprentice.patch](#)

① TFTP Protocol

② atftp{,d}

③ TFTP Option Extension: Windowsize

Implementation in atftp{,d}

Open Questions and Tests

④ Security Issues

⑤ PCRE2 Port

RFC 2347 (TFTP Option Extension, 1998)

The client can suggest parameters to the server:

- **tsize** → transfer size
- **blksize** → block size
- **timeout** → timeout :-)
- **windowsize** → number of blocks sent without waiting for an ACK

```
132 Read Request, File: d-1/n-a/menu.ipxe, Transfer type: octet, tsize=0, timeout=1, blksize=1434, windowsize=8
111 Option Acknowledgement, tsize=3593, timeout=1, blksize=1434, windowsize=8
   66 Acknowledgement, Block: 0
1500 Data Packet, Block: 1
1500 Data Packet, Block: 2
  791 Data Packet, Block: 3 (last)
   66 Acknowledgement, Block: 3
```

Improving atftp{,d} and -Package

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

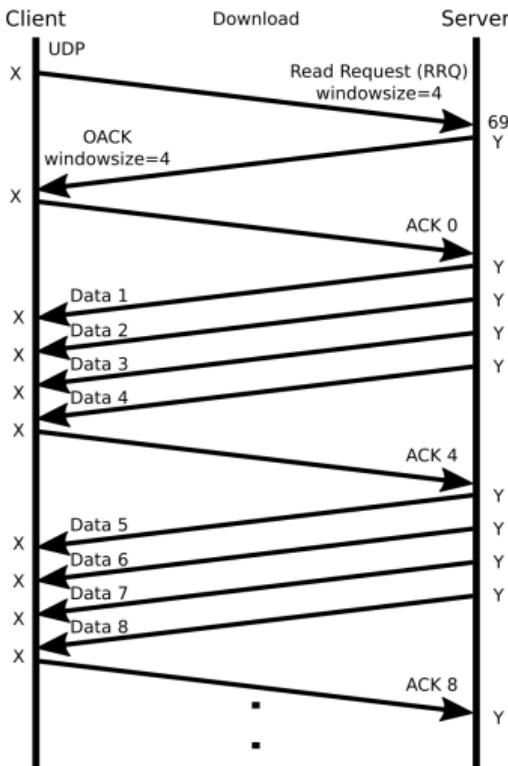
Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary



TFTP Windowsize Option

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
1	0.000000000	::1	57394	::1	69	TFTP	101	Read Request, File: d-i/n-a/menu.ipxe
2	0.019275714	::1	60556	::1	57394	TFTP	77	Option Acknowledgement, windowsize=4
3	0.019335292	::1	57394	::1	60556	TFTP	66	Acknowledgement, Block: 0
4	0.019597917	::1	60556	::1	57394	TFTP	578	Data Packet, Block: 1
5	0.019614407	::1	60556	::1	57394	TFTP	578	Data Packet, Block: 2
6	0.019622339	::1	60556	::1	57394	TFTP	578	Data Packet, Block: 3
7	0.019629666	::1	60556	::1	57394	TFTP	578	Data Packet, Block: 4
8	0.019651267	::1	57394	::1	60556	TFTP	66	Acknowledgement, Block: 4
9	0.019692844	::1	60556	::1	57394	TFTP	578	Data Packet, Block: 5
10	0.019707647	::1	60556	::1	57394	TFTP	578	Data Packet, Block: 6
11	0.019715360	::1	60556	::1	57394	TFTP	578	Data Packet, Block: 7
12	0.019724429	::1	60556	::1	57394	TFTP	75	Data Packet, Block: 8 (last)
13	0.019743221	::1	57394	::1	60556	TFTP	66	Acknowledgement, Block: 8
64	97.686022677	::1	54834	::1	69	TFTP	105	Read Request, File: d-i/n-a/grub/grub
65	97.703660307	::1	57246	::1	54834	TFTP	77	Option Acknowledgement, windowsize=4
66	97.703115588	::1	54834	::1	57246	TFTP	66	Acknowledgement, Block: 0
67	97.703368319	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 1
68	97.703383131	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 2
69	97.703392627	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 3
70	97.703396619	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 4
71	97.703415088	::1	54834	::1	57246	TFTP	66	Acknowledgement, Block: 4
72	97.703451215	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 5
73	97.703471905	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 6
74	97.703487414	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 7
75	97.703493439	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 8
76	97.703511357	::1	54834	::1	57246	TFTP	66	Acknowledgement, Block: 8
77	97.703545040	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 9
78	97.703558124	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 10
79	97.703563936	::1	57246	::1	54834	TFTP	578	Data Packet, Block: 11
80	97.703579999	::1	57246	::1	54834	TFTP	173	Data Packet, Block: 12 (last)
81	97.703646128	::1	54834	::1	57246	TFTP	66	Acknowledgement, Block: 12

```
Frame 1: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface lo, id 0
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 6, Src: ::1, Dst: ::1
User Datagram Protocol, Src Port: 57394, Dst Port: 69
Trivial File Transfer Protocol
  Opcode: Read Request (1)
  Source File: d-i/n-a/menu.ipxe
  Type: octet
  ▾ Option: windowsize = 4
    Option name: windowsize
    Option value: 4
```

TFTP Windowsize Option

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

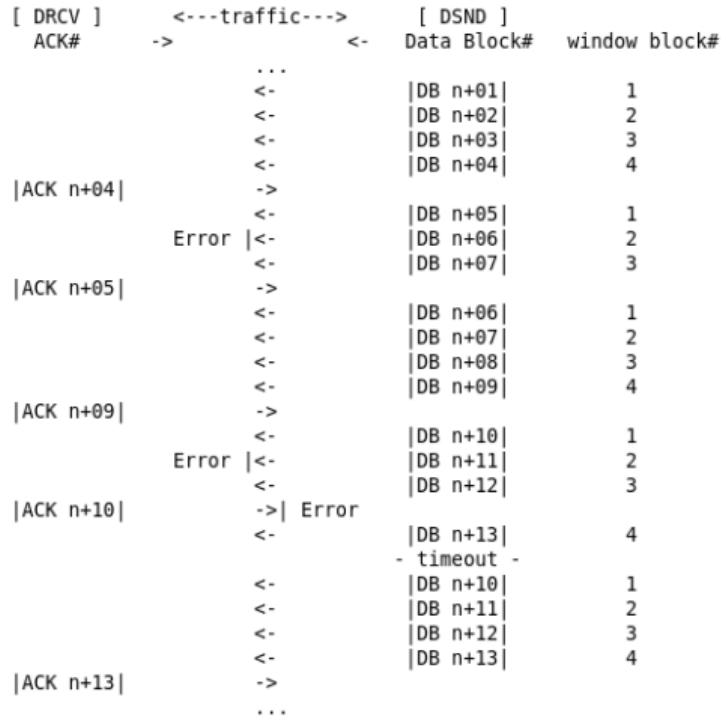
Open Questions and Tests

Security Issues

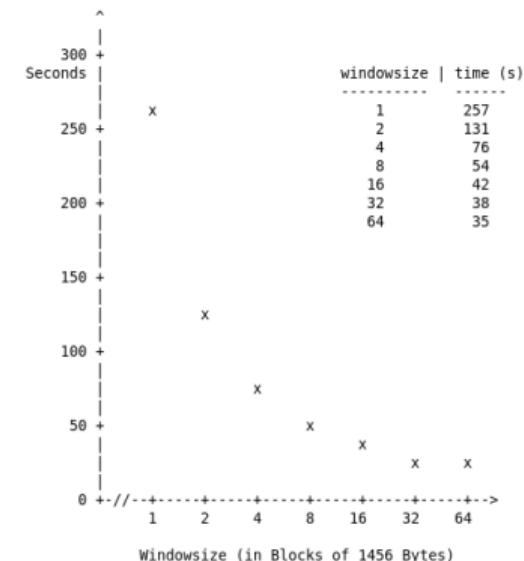
PCRE2 Port

Summary

RFC 7440 (2015)



Performance tests were run on the prototype implementation using a variety of windowsizes and a fixed blocksize of 1456 bytes. The tests were run on a lightly loaded Gigabit Ethernet, between two Toshiba Tecra Core 2 Duo 2.2 Ghz laptops, in "octet" mode, transferring a 180 MByte file.



windowsize option (RFC 7440, 2015)

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	::1	::1	TFTP	101	Read Request, File: d-i/n-a/menu.ipxe, Transfer type: octet, windowsize=3
2	0.016803443	::1	::1	TFTP	77	Option Acknowledgement, windowsize=3
3	0.016852472	::1	::1	TFTP	66	Acknowledgement, Block: 0
4	0.016898404	::1	::1	TFTP	578	Data Packet, Block: 1
5	0.016914065	::1	::1	TFTP	578	Data Packet, Block: 2
6	0.016922623	::1	::1	TFTP	578	Data Packet, Block: 3
7	0.016935795	::1	::1	TFTP	66	Acknowledgement, Block: 3
8	0.016949373	::1	::1	TFTP	578	Data Packet, Block: 4
9	0.016960107	::1	::1	TFTP	578	Data Packet, Block: 5
10	0.016969592	::1	::1	TFTP	578	Data Packet, Block: 6
11	0.016980340	::1	::1	TFTP	66	Acknowledgement, Block: 6
12	0.017003561	::1	::1	TFTP	578	Data Packet, Block: 7
13	0.017017159	::1	::1	TFTP	75	Data Packet, Block: 8 (last)
14	0.017028243	::1	::1	TFTP	66	Acknowledgement, Block: 8
15	14.047689367	::1	::1	TFTP	101	Read Request, File: d-i/n-a/menu.ipxe, Transfer type: octet, windowsize=5
16	14.048077016	::1	::1	TFTP	77	Option Acknowledgement, windowsize=5
17	14.048132049	::1	::1	TFTP	66	Acknowledgement, Block: 0
18	14.048231740	::1	::1	TFTP	578	Data Packet, Block: 1
19	14.048271914	::1	::1	TFTP	578	Data Packet, Block: 2
20	14.048300157	::1	::1	TFTP	578	Data Packet, Block: 3
21	14.048316349	::1	::1	TFTP	578	Data Packet, Block: 4
22	14.048331901	::1	::1	TFTP	578	Data Packet, Block: 5
23	14.048343989	::1	::1	TFTP	66	Acknowledgement, Block: 5
24	14.048358115	::1	::1	TFTP	578	Data Packet, Block: 6
25	14.048374024	::1	::1	TFTP	578	Data Packet, Block: 7
26	14.048391615	::1	::1	TFTP	75	Data Packet, Block: 8 (last)
27	14.048402887	::1	::1	TFTP	66	Acknowledgement, Block: 8

iPXE has windowsize option implemented:

Read Request, File: /d-i/n-a/menu.ipxe, Transfer type: octet, tsize=0, blksize=1468, windowsize=4

Windowsize Option in atftpd

Idea: Implement the Windowsize Option in atftpd (Server) and atftp (Client)

tftpd_file.c:

```
/* Send a file. It is implemented as a state machine using a while loop
 * and a switch statement. Function flow is as follow:
 *   - sanity check
 *   - check client's request
 *   - enter state machine
 *
 *   1) send a DATA or OACK
 *   2) wait replay
 *       - if ACK, goto 3
 *       - if ERROR abort
 *       - if TIMEOUT goto previous state
 *   3) send data, goto 2
 */

```

- Options already supported
 - Options tsize, blksize, timeout already implemented
- Add some code for windowsize and adapt algorithm → done!

Windowsize Option in atftpd

Idea: Implement the Windowsize Option in atftpd (Server) and atftp (Client)

tftpd_file.c:

```
/* Send a file. It is implemented as a state machine using a while loop
 * and a switch statement. Function flow is as follow:
 *   - sanity check
 *   - check client's request
 *   - enter state machine
 *
 *   1) send a DATA or OACK
 *   2) wait replay
 *       - if ACK, goto 3
 *       - if ERROR abort
 *       - if TIMEOUT goto previous state
 *   3) send data, goto 2
 */
```

- Options already supported
- Options tsize, blksize, timeout already implemented
- Add some code for windowsize and adapt algorithm → done!

Open Questions and Tests

- Best way to handle packet loss or delay?
- Best inter-packet delay within a window?
- Congestion-control?

Network Emulation⁵:

<https://wiki.linuxfoundation.org/networking/netem>

netem provides Network Emulation functionality for testing protocols by emulating the properties of **wide area networks**. The current version emulates variable delay, loss, duplication and re-ordering.

What is the (a?) realistic scenario ...

⁵ https://en.wikipedia.org/wiki/Network_emulation

Open Questions and Tests

- Best way to handle packet loss or delay?
- Best inter-packet delay within a window?
- Congestion-control?

Network Emulation⁵:

<https://wiki.linuxfoundation.org/networking/netem>

netem provides Network Emulation functionality for testing protocols by emulating the properties of **wide area networks**. The current version emulates variable delay, loss, duplication and re-ordering.

What is the (a?) realistic scenario ...

⁵ https://en.wikipedia.org/wiki/Network_emulation

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

① TFTP Protocol

② atftp{,d}

③ TFTP Option Extension: Windowsize

Implementation in atftp{,d}

Open Questions and Tests

④ Security Issues

⑤ PCRE2 Port

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Length Info

```
115 Read Request, File: d-i/n-a/grub/grub.cfg, Transfer type: octet, blksize=8, windowsize=4
103 Error Code, Code: Option negotiation failed, Message: Failure to negotiate RFC1782 options
116 Read Request, File: d-i/n-a/grub/grub.cfg, Transfer type: octet, blksize=16, windowsize=4
103 Error Code, Code: Option negotiation failed, Message: Failure to negotiate RFC1782 options
116 Read Request, File: d-i/n-a/grub/grub.cfg, Transfer type: octet, blksize=32, windowsize=4
88 Option Acknowledgement, blksize=32, windowsize=4
66 Acknowledgement, Block: 0
98 Data Packet, Block: 1
98 Data Packet, Block: 2
98 Data Packet, Block: 3
98 Data Packet, Block: 4
66 Acknowledgement, Block: 4
98 Data Packet, Block: 5
98 Data Packet, Block: 6
```

```
▶ Frame 24: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface lo, id 0
  Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Internet Protocol Version 6, Src: ::1, Dst: ::1
  User Datagram Protocol, Src Port: 53617, Dst Port: 60081
```

Opcode: Option Acknowledgement (6)
[Destination File: d-i/n-a/grub/grub.cfg]

[Read Request in frame 23]

Option name: blksize
Option value: 32

```
    ▼ Option: windowsize = 4
        Option name: windowsize
        Option value: 4
```

0000	00	00	00	00	00	00	00	00	00	00	00	00	86	dd	60	09
0010	49	ec	00	22	11	40	00	00	00	00	00	00	00	00	00	00
0020	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00
0030	00	00	00	00	00	01	d1	71	ea	b1	00	22	00	35	00	06
0040	62	6c	6b	73	69	7a	65	00	33	32	00	77	69	6e	64	6f
0050	77	73	69	7a	65	00	34	00								

```
I .." @  
..... q ..." 5.  
blksize 32 wind  
wsize 4.
```

Common Vulnerabilities and Exposures (CVE)

Andreas B. Mundt

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

- Debian-Security⁶ → CVE-2021-41054⁷
- Debian Security Tracker⁸
- Debian LTS Advisory DLA-2820-1⁹
- Letzte Aktion: CVE-2021-46671¹⁰

⁶ <https://www.debian.org/security/faq>

⁷ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41054>

⁸ <https://security-tracker.debian.org/tracker/source-package/atftp>

⁹ <https://lists.debian.org/debian-lts-announce/2021/11/msg00014.html>

¹⁰ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46671>

① TFTP Protocol

② atftp{,d}

③ TFTP Option Extension: Windowsize

Implementation in atftp{,d}

Open Questions and Tests

④ Security Issues

⑤ PCRE2 Port

TFTP Protocol

atftp{,d}

TFTP Option
Windowsize

Implementation in
atftp{,d}

Open Questions and Tests

Security Issues

PCRE2 Port

Summary

Debian Bug #1000071

Dear maintainer,

Your package still depends on the old, obsolete PCRE3[0] libraries (i.e. libpcre3-dev). This has been end of life for a while now, and upstream do not intend to fix any further bugs in it. Accordingly, I would like to remove the pcre3 libraries from Debian, preferably in time for the release of Bookworm.

The newer PCRE2 library was first released in 2015, and has been in Debian since stretch. Upstream's documentation for PCRE2 is available here:

<https://pcre.org/current/doc/html/>

Many large projects that use PCRE have made the switch now (e.g. git, php); **it does involve some work**, but we are now at the stage where PCRE3 should not be used, particularly if it might ever be exposed to untrusted input.

...

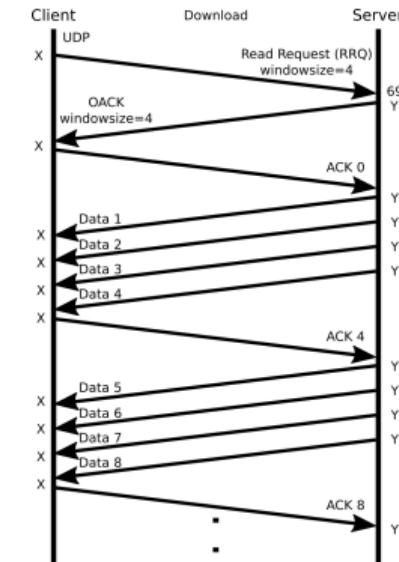
¹¹ <https://sourceforge.net/p/atftp/support-requests/11/>



Keep the sourcerer alive!

Summary

- ① TFTP Protocol
 - ② atftp{,d}
 - ③ TFTP Option Extension: Windowsize
 - Implementation in atftp{,d}
 - Open Questions and Tests
 - ④ Security Issues
 - ⑤ PCRE2 Port

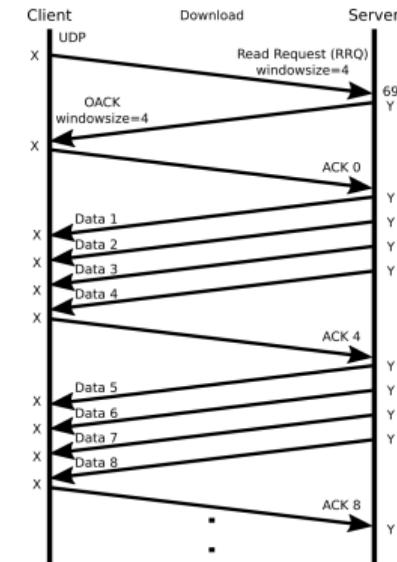




Keep the sourcerer alive!

Summary

- ① TFTP Protocol
- ② atftp{,d}
- ③ TFTP Option Extension: Windowsize
 - Implementation in atftp{,d}
 - Open Questions and Tests
- ④ Security Issues
- ⑤ PCRE2 Port



Thanks!