Package Management Over Tor

Alexander Nasonov
alnsn@NetBSD.org

\textsuperscript{1}The NetBSD Project

\textsuperscript{2}XMM Swap Ltd

February 2018, FOSDEM, Brussels
About Myself

Member of the NetBSD project

- Author of bpfjit and aes-xts disk encryption
About Myself

Member of the NetBSD project

- Author of bpfjit and aes-xts disk encryption
- Maintainer of a dozen of packages in pkgsrc
About Myself

Member of the NetBSD project

- Author of bpfjit and aes-xts disk encryption
- Maintainer of a dozen of packages in pkgsrc
- Run non-official mirror pkgsrcbadj4vrrrr.onion
About Myself

Member of the NetBSD project
  ▶ Author of bpfjit and aes-xts disk encryption
  ▶ Maintainer of a dozen of packages in pkgsrc
  ▶ Run non-official mirror pkgsrcbadj4vrrrr.onion

Director of XMM Swap Ltd
  ▶ Low-latency high performance software
About Myself

Member of the NetBSD project

- Author of `bpfjit` and `aes-xts` disk encryption
- Maintainer of a dozen of packages in `pkgsrc`
- Run non-official mirror `pkgsrcbadj4vrrrr.onion`

Director of XMM Swap Ltd

- Low-latency high performance software
- C++, x86 assembler and LuaJIT
About Myself

Member of the NetBSD project

- Author of bpfjit and aes-xts disk encryption
- Maintainer of a dozen of packages in pkgsrc
- Run non-official mirror pkgsrcbadj4vrrrr.onion

Director of XMM Swap Ltd

- Low-latency high performance software
- C++, x86 assembler and LuaJIT
- Mini compilers and DSL
Why? (thread model)

What’s wrong with downloading packages over clearnet?
Why? (thread model)

What’s wrong with downloading packages over clearnet?

- Easily observable (e.g. vulnerable version of software)
Why? (thread model)

What’s wrong with downloading packages over clearnet?

- Easily observable (e.g. vulnerable version of software)
- Plain http is clearly bad
Why? (thread model)

What’s wrong with downloading packages over clearnet?

- Easily observable (e.g. vulnerable version of software)
- Plain http is clearly bad
- https is better but think about middle-boxes
Why? (thread model)

What’s wrong with downloading packages over clearnet?

- Easily observable (e.g. vulnerable version of software)
- Plain http is clearly bad
- https is better but think about middle-boxes
- MitM (man in the middle) attack
Why? (thread model)

What’s wrong with downloading packages over clearnet?

- Easily observable (e.g. vulnerable version of software)
- Plain http is clearly bad
- https is better but think about middle-boxes
- MitM (man in the middle) attack
- Sizes are observable
Why? (thread model)

What’s wrong with downloading packages over clearnet?

- Easily observable (e.g. vulnerable version of software)
- Plain http is clearly bad
- https is better but think about middle-boxes
- MitM (man in the middle) attack
- Sizes are observable

What Tor gives you?

- Three tor nodes make it hard to track endpoints
Why? (thread model)

What’s wrong with downloading packages over clearnet?

- Easily observable (e.g. vulnerable version of software)
- Plain http is clearly bad
- https is better but think about middle-boxes
- MitM (man in the middle) attack
- Sizes are observable

What Tor gives you?

- Three tor nodes make it hard to track endpoints
- Hidden service name is a proof of identity
Why? (thread model)

What’s wrong with downloading packages over clearnet?

- Easily observable (e.g. vulnerable version of software)
- Plain http is clearly bad
- https is better but think about middle-boxes
- MitM (man in the middle) attack
- Sizes are observable

What Tor gives you?

- Three tor nodes make it hard to track endpoints
- Hidden service name is a proof of identity
Torified Debian

On Debian and some derivative distros, `apt-transport-tor` package can be installed.
On Debian and some derivative distros, `apt-transport-tor` package can be installed.

```bash
# /etc/apt/sources.list
deb tor+http://vwakviie2ienjx6t.onion/debian jessie main
deb tor+http://vwakviie2ienjx6t.onion/debian jessie-updates main
deb tor+http://sgvtcaew4bxjd7ln.onion/debian-security jessie
```
Torified Debian

On Debian and some derivative distros, `apt-transport-tor` package can be installed.

```
# /etc/apt/sources.list
deb tor+http://vwakviie2ienjx6t.onion/debian jessie main
deb tor+http://vwakviie2ienjx6t.onion/debian jessie-updates main
deb tor+http://sgvtcaew4bxjd7ln.onion/debian-security jessie/updates main
```

Non-standard `tor+http` uri scheme.
pkgsrc

Cross-platform package management system
pkgsrc

Cross-platform package management system

» NetBSD
pkgsrc

Cross-platform package management system

- NetBSD
- Linux
Cross-platform package management system

- NetBSD
- Linux
- Darwin / Mac OS X / OS X / macOS
Cross-platform package management system

- NetBSD
- Linux
- Darwin / Mac OS X / OS X / macOS
- FreeBSD
pkgsrc

Cross-platform package management system

- NetBSD
- Linux
- Darwin / Mac OS X / OS X / macOS
- FreeBSD
- OpenBSD
pkgsrc

Cross-platform package management system

- NetBSD
- Linux
- Darwin / Mac OS X / OS X / macOS
- FreeBSD
- OpenBSD
- Solaris
pkgsrc

Cross-platform package management system

- NetBSD
- Linux
- Darwin / Mac OS X / OS X / macOS
- FreeBSD
- OpenBSD
- Solaris
- Windows (!!!)
Overview

Prerequisites

► Ubuntu on Windows or Tails Live CD
Overview

Prerequisites

- Ubuntu on Windows or Tails Live CD
- Tor Browser
Overview

Prerequisites

- Ubuntu on Windows or Tails Live CD
- Tor Browser
- Basics of pkgsrc and package management
Overview

Prerequisites

▶ Ubuntu on Windows or Tails Live CD
▶ Tor Browser
▶ Basics of pkgsrc and package management

Overview of the installation

▶ Prepare your host (toolchain, libs)
Overview

Prerequisites

- Ubuntu on Windows or Tails Live CD
- Tor Browser
- Basics of pkgsrc and package management

Overview of the installation

- Prepare your host (toolchain, libs)
- Clone pkgsrc
Overview

Prerequisites
- Ubuntu on Windows or Tails Live CD
- Tor Browser
- Basics of pkgsrc and package management

Overview of the installation
- Prepare your host (toolchain, libs)
- Clone pkgsrc
- Bootstrap pkgsrc
Overview

Prerequisites

▶ Ubuntu on Windows or Tails Live CD
▶ Tor Browser
▶ Basics of pkgsrc and package management

Overview of the installation

▶ Prepare your host (toolchain, libs)
▶ Clone pkgsrc
▶ Bootstrap pkgsrc
▶ Build essential packages
Overview

Prerequisites
- Ubuntu on Windows or Tails Live CD
- Tor Browser
- Basics of pkgsrc and package management

Overview of the installation
- Prepare your host (toolchain, libs)
- Clone pkgsrc
- Bootstrap pkgsrc
- Build essential packages
- Host your binary packages on a hidden service
Overview

Prerequisites
- Ubuntu on Windows or Tails Live CD
- Tor Browser
- Basics of pkgsrc and package management

Overview of the installation
- Prepare your host (toolchain, libs)
- Clone pkgsrc
- Bootstrap pkgsrc
- Build essential packages
- Host your binary packages on a hidden service
- Update binary packages
Prepare your host

- Update your host environment
  apt update
  apt upgrade
Prepare your host

- Update your host environment
  ```
  apt update
  apt upgrade
  ```
- Install dev packages for bootstrapping pkgsrc and building packages
  ```
  apt install gcc
  apt install g++
  apt install ncurses-dev
  apt install cvs
  ```
Prepare your host

- Update your host environment
  `apt update`
  `apt upgrade`

- Install dev packages for bootstrapping `pkgsrc` and building packages
  `apt install gcc`
  `apt install g++`
  `apt install ncurses-dev`
  `apt install cvs`

- Install packages for connecting over `tor`
  `apt install curl`
  `apt install socat`
Clone pkgsrc: connections over ssh

- Add ProxyCommand to your ssh_config file

  # ~/.ssh/config file
  Host *.NetBSD.org, *.onion
  ProxyCommand /usr/bin/socat STDIO \
    SOCKS4A:127.0.0.1:%h:%p,sockport=9150
Clone pkgsrc: connections over ssh

- Add ProxyCommand to you your `ssh_config` file
  ```
  Host *.NetBSD.org, *.onion
  ProxyCommand /usr/bin/socat STDIO \
  SOCKS4A:127.0.0.1:%h:%p,sockport=9150
  ```
- On Tails, you can use `netcat`
  ```
  Host *.NetBSD.org, *.onion
  ProxyCommand /usr/bin/nc -X 5 -x 127.0.0.1:9150 %h %p
  ```
Clone pkgsrc: CVS or Git

Official anon CVS:

```bash
export CVS_RSH=ssh
export CVSRoot=anонcvs@anонcvs.NetBSD.org:/cvsroot
cvs co pkgsrc
```
Clone pkgsrc: CVS or Git

Official anon CVS:

export CVS_RSH=ssh
export CVSRoot=anoncvs@anoncvs.NetBSD.org:/cvsroot
cvs co pkgsrc

Mirror on github:

# if you have a github account
git clone --depth 1 git@github.com:/NetBSD/pkgsrc.git
Bootstrap pkgsrc: mk-fragment

MAKE_JOBS=4
PREFER_PKGSRCDIR=yes
UPDATE_TARGET=package-install
DEPENDS_TARGET=package-install

PKGSRCDIR=${HOME}/pkgsrc

FETCH_USING=curl
FETCH_PROXY=socks4a://127.0.0.1:9150
#PREFER_NATIVE=curl

MASTER_SITE_OVERRIDE=\n  http://pkgsrcrcbadj4vrrrrr.onion/pub/pkgsrc/distfiles/
Bootstrap pkgsrc: optional hardening

Use only if you know what you’re doing.

PKGSRC_MKPIE=yes
PKGSRC_USE_RELRO=full
PKGSRC_USE_SSP=strong
PKGSRC_USE_FORTIFY=strong
Bootstrap pkgsrc

cd pkgsrc/bootstrap
env SH=/bin/bash \n./bootstrap --unprivileged \n    --prefix=${HOME:?}/pkg \n    --mk-fragment=/tmp/mk-fragment
Build essential packages

- **digest** - message digest (for checksums)
  
  `cd pkgsrc/pkgtools/digest
  ~/pkg/bin/bmake package-install

- **curl** - for downloading over the SOCKS protocol
  
  `cd pkgsrc/www/curl
  ~/pkg/bin/bmake package-install`
Build essential packages

- digest - message digest (for checksums)
  
cd pkgsrc/pkgtools/digest
  ~/pkg/bin/bmake package-install
Build essential packages

- digest - message digest (for checksums)
  cd pkgsrc/pkgtools/digest
  ~/pkg/bin/bmake package-install

- curl - for downloading over the SOCKS protocol
  cd pkgsrc/www/curl
  ~/pkg/bin/bmake package-install
Other packages

- www/privoxy - http proxy
Other packages

- www/privoxy - http proxy
- www/bozohttpd - simple web server
Other packages

- www/privoxy - http proxy
- www/bozohttpd - simple web server
- pkgtools/pkg_chk - to build or install a list of packages
Other packages

- www/privoxy - http proxy
- www/bozohttpd - simple web server
- pkgtools/pkg_chk - to build or install a list of packages
- pkgtools/pbulk - if you want build ALL packages
Other packages

- www/privoxy - http proxy
- www/bozohttpd - simple web server
- pkgtools/pkg_chk - to build or install a list of packages
- pkgtools/pbulk - if you want build ALL packages
- pkgtools/pkgin - apt-like package management tool
Other packages

▶ www/privoxy - http proxy
▶ www/bozohttpd - simple web server
▶ pkgtools/pkg_chk - to build or install a list of packages
▶ pkgtools/pbulk - if you want build ALL packages
▶ pkgtools/pkgin - apt-like package management tool
▶ pkgtools/pkgdepgraph - show dependency graphs
▶ graphics/graphviz - graphs in various formats (pdf, svg)
Demo
Demo

- Configure and start a new hidden service
Demo

- Configure and start a new hidden service
- Start a web server to host binary packages
Demo

- Configure and start a new hidden service
- Start a web server to host binary packages
- Remove some packages
Demo

- Configure and start a new hidden service
- Start a web server to host binary packages
- Remove some packages
- Install some new packages
References

Official project sites:

▶ https://www.pkgsrc.org
▶ https://www.NetBSD.org

My stuff:

▶ http://pkgsrccbadj4vrrrr.onion
▶ https://www.xmmmswap.com