TARdiss
packaging bugs in package manager

David Fifield & Nathan Malkin

INSTALL.SH

```
#!/bin/bash

pip install "$1" &
easy_install "$1" &
brew install "$1" &
npm install "$1" &
yum install "$1" & dnf install "$1" &
docker run "$1" &
pkg install "$1" &
apt-get install "$1" &
sudo apt-get install "$1" &
steamcmd +app_update "$1" validate &
git clone https://github.com/"$1"/"$1" &
cd "$1";./configure;make;make install &
curl "$1" | bash &
```

xkcd.com/1654

What’s in a package?

- Files
- More files
- Directories
  - with even more files
- Metadata
  - Signatures

What's in a package?

- Files
- More files
- Directories
  - with even more files
- Metadata
  - Signatures

tar
zip

Expected

– Writes limited to one directory

Unexpected

– Anything else

How can we escape a directory?

- Relative paths
  - × `../../../file`
- Shortcuts
  - × `~/file`
- Symlinks
  - × `packaged_file → /somewhere/cool`

How can we escape a directory?

- Relative paths
  - ✗ `../../../file`
- Shortcuts
  - ✗ `~/file`
- Symlinks
  - ✗ `packaged_file → /somewhere/cool`
  - ✓ `dir → /somewhere`
    `dir/cool ⇔ /somewhere/cool`

What this looks like

```
$ tar -tvf package.tar
-rw-r--r-- 0/0               1 2017-11-01 16:00 README
lrw-r--r-- 0/0               0 2017-11-01 16:00 link -> /tmp
-rw-r--r-- 0/0               6 2017-11-01 16:00 link/HACKED
```

How can we escalate this?

This bug was also in GNU tar!

CVE-[redacted]-1216

– Discovered in [redacted]

This bug was also in GNU tar!

CVE-2002-1216

– Discovered in 1998

Signature forgery

Packages can have digital signatures.

```
$ tar -tvf package.tar
-r--r--r-- 0/0       16908 2017-10-15 16:00 data.zip
-r--r--r-- 0/0         256 2017-10-15 16:00 data.zip.sig
```

You cannot change data.zip without failing the signature check.

But: tar archives can contain multiple entries with the same name.

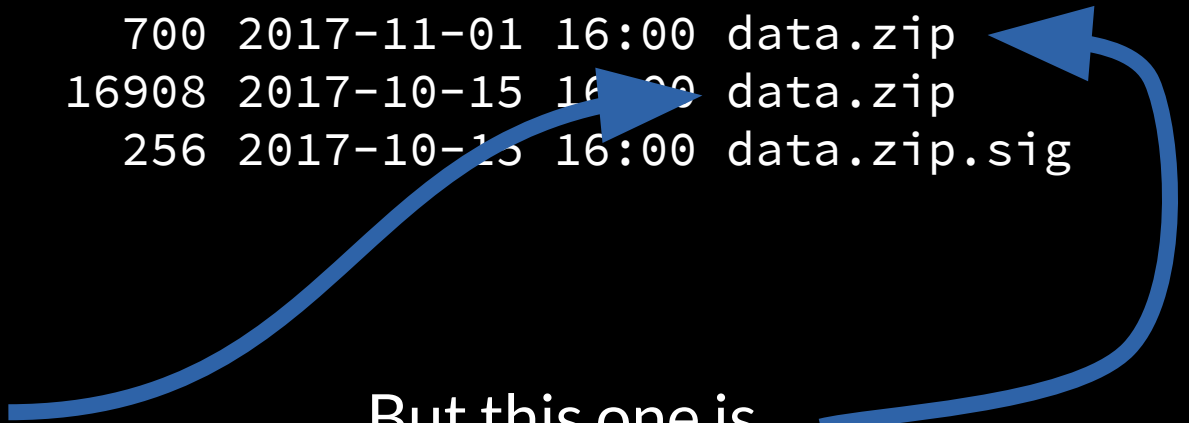
```
$ tar -tvf hello.tar
-rw-r--r-- 0/0   12 2017-11-01 07:55 README
-rw-r--r-- 0/0   37 2017-11-01 07:54 Makefile
-rw-r--r-- 0/0   96 2017-11-01 07:53 hello.c
-rw-r--r-- 0/0   28 2017-11-01 07:55 README
```

Step 1: download some else's signed package
Step 2: insert your own files at the beginning

Now you have a package with a valid signature but your own malicious contents.

```
$ tar -tvf package.tar
-r--r--r-- 0/0          700 2017-11-01 16:00 data.zip
-r--r--r-- 0/0        16908 2017-10-15 16:00 data.zip
-r--r--r-- 0/0          256 2017-10-15 16:00 data.zip.sig
```

```
$ tar -tvf package.tar
-r--r--r-- 0/0          700 2017-11-01 16:00 data.zip
-r--r--r-- 0/0        16908 2017-10-15 16:00 data.zip
-r--r--r-- 0/0          256 2017-10-15 16:00 data.zip.sig
```



This one has its signature checked

But this one is actually extracted