

# Mercury: Bandwidth-Effective Prevention of Rollback Attacks against Community Repositories

## 一、实验思路说明

本论文中的 Mercury 系统用于社区仓库管理，通过对仓库中软件元数据、快照文件、时间戳文件等的版本控制，达到社区仓库的安全需求。论文重点研究了社区仓库中的回滚攻击问题，作者提出 Mercury 系统可以很容易地防止这种攻击，并且是带宽高效的。

Mercury 系统是由作者团队开发的另一个系统 TUF 改良而来的，由于 TUF 已经在较多的社区仓库如 Haskell, OCaml, RubyGems 等开始使用，所以作者把 Mercury 的优势整合到了 TUF 中，论文中作者提供了 TUF 的开源代码地址。

我们的实验思路是，在本地搭建 TUF 环境，模拟建立社区仓库以及客户端，通过回滚软件版本号的行为查看客户端是否会被拒绝下载，从而判断 TUF 是否能够准确防止回滚攻击。论文中作者是将 Mercury 及其他用于对比的系统部署到 PyPI，得到大量真实用户下载日志数据，根据数据对比分析 Mercury 的性能，由于我们不具备部署其他系统和产生大量数据的条件，故通过再现和分析其防止回滚攻击的过程来验证其是否符合理论上的带宽高效。

## 二、实验过程

### 1. 现有条件

环境：Ubuntu-16.04-desktop

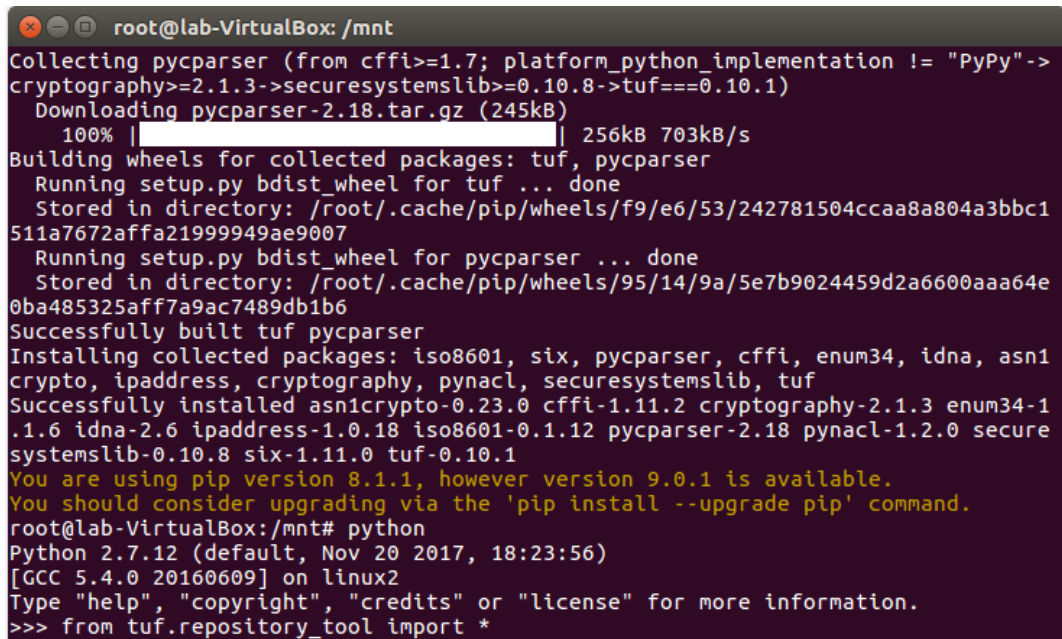
Python 2.7.12

源码：<https://github.com/theupdateframework/tuf>

### 2. TUF 搭建和部署

安装 TUF:

\$pip install <path/TUF>



```
root@lab-VirtualBox: /mnt
Collecting pycparser (from cffi>=1.7; platform_python_implementation != "PyPy"->
cryptography>=2.1.3->securesystemslib>=0.10.8->tuf==0.10.1)
  Downloading pycparser-2.18.tar.gz (245kB)
    100% |#####| 256kB 703kB/s
Building wheels for collected packages: tuf, pycparser
  Running setup.py bdist_wheel for tuf ... done
  Stored in directory: /root/.cache/pip/wheels/f9/e6/53/242781504ccaa8a804a3bbc1
511a7672affa21999949ae9007
  Running setup.py bdist_wheel for pycparser ... done
  Stored in directory: /root/.cache/pip/wheels/95/14/9a/5e7b9024459d2a6600aaa64e
0ba485325aff7a9ac7489db1b6
Successfully built tuf pycparser
Installing collected packages: iso8601, six, pycparser, cffi, enum34, idna, asn1
crypto, ipaddress, cryptography, pynacl, securesystemslib, tuf
Successfully installed asn1crypto-0.23.0 cffi-1.11.2 cryptography-2.1.3 enum34-1
.6 idna-2.6 ipaddress-1.0.18 iso8601-0.1.12 pycparser-2.18 pynacl-1.2.0 secure
systemslib-0.10.8 six-1.11.0 tuf-0.10.1
You are using pip version 8.1.1, however version 9.0.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
root@lab-VirtualBox:/mnt# python
Python 2.7.12 (default, Nov 20 2017, 18:23:56)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from tuf.repository_tool import *
```

创建和导入 RSA 密钥:

```
root@lab-VirtualBox: /home/lab/下载/tuf-develop
File "tuf/repository_lib.py", line 586, in _load_top_level_metadata
    'root file: ' + repr(root_filename))
securesystemslib.exceptions.RepositoryError: Cannot load the required root file:
u'/home/lab/\u4e0b\u8f7d/tuf-develop/path/to/repository/metadata.staged/root.js
on'
>>> repository = load_repository("tests/repository_data/repository")
>>> from tuf.repository_tool import *
>>> generate_and_write_rsa_keypair("keystore/root_key", bits=2048, password="pas
sword")
>>> generate_and_write_rsa_keypair("keystore/root_key2")
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
TypeError: generate_and_write_rsa_keypair() takes exactly 3 arguments (1 given)
>>> generate_and_write_rsa_keypair("keystore/root_key2")
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
TypeError: generate_and_write_rsa_keypair() takes exactly 3 arguments (1 given)
>>> generate_and_write_rsa_keypair("keystore/root_key2",password="password")
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
TypeError: generate_and_write_rsa_keypair() takes exactly 3 arguments (2 given)
>>> generate_and_write_rsa_keypair("keystore/root_key2",bits=3072,password="pass
word")
>>> □
```

已生成的密钥:

```
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/keystore
drwxr-xr-x 3 root root 4096 11月 28 04:51 ./
drwxr-xr-x 3 root root 4096 11月 28 04:51 client/
-rwxr-xr-x 1 root root 3757 11月 28 04:51 generate_project_data.py*
-rwxr-xr-x 1 root root 6988 11月 28 04:51 generate.py*
drwxr-xr-x 2 root root 4096 11月 28 04:51 keystore/
drwxr-xr-x 4 root root 4096 11月 28 04:51 project/
drwxr-xr-x 5 root root 4096 11月 28 04:51 repository/
drwxr-xr-x 2 root root 4096 11月 30 10:49 tmp/
-rw-r--r-- 1 root root 4462 11月 30 12:24 tuf.log
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data# cd keystore/
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/keystore# ll
总用量 48
drwxr-xr-x 2 root root 4096 11月 28 04:51 ./
drwxr-xr-x 7 root root 4096 11月 30 10:50 ../
-rw-r--r-- 1 root root 822 11月 28 04:51 delegation_key
-rw-r--r-- 1 root root 180 11月 28 04:51 delegation_key.pub
-rw-r--r-- 1 root root 2654 11月 28 04:51 root_key
-rw-r--r-- 1 root root 625 11月 28 04:51 root_key.pub
-rw-r--r-- 1 root root 822 11月 28 04:51 snapshot_key
-rw-r--r-- 1 root root 180 11月 28 04:51 snapshot_key.pub
-rw-r--r-- 1 root root 822 11月 28 04:51 targets_key
-rw-r--r-- 1 root root 180 11月 28 04:51 targets_key.pub
-rw-r--r-- 1 root root 1766 11月 30 11:01 timestamp_key
-rw-r--r-- 1 root root 451 11月 30 11:01 timestamp_key.pub
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/keystore# □
```

创建添加时间戳、快照、目标文件：

```
root@lab-VirtualBox: /home/lab/download/tuf-develop
File "<stdin>", line 1, in <module>
TypeError: generate_and_write_rsa_keypair() takes exactly 3 arguments (2 given)
>>> generate_and_write_rsa_keypair("keystore/targets_key", bits=2048, password="password")
>>> generate_and_write_rsa_keypair("keystore/snapshot_key", bits=2048, password="password")
>>> generate_and_write_rsa_keypair("keystore/timestamp_key", bits=2048, password="password")
>>> repository.targets.add_verification_key(import_rsa_publickey_from_file("keystore/targets_key.pub"))
>>> repository.snapshot.add_verification_key(import_rsa_publickey_from_file("keystore/snapshot_key.pub"))
>>> repository.timestamp.add_verification_key(import_rsa_publickey_from_file("keystore/timestamp_key.pub"))
>>> private_targets_key = import_rsa_privatekey_from_file("keystore/targets_key")
Traceback (most recent call last):
File "<stdin>", line 1, in <module>
TypeError: import_rsa_privatekey_from_file() takes exactly 2 arguments (1 given)
>>> private_targets_key = import_rsa_privatekey_from_file("keystore/targets_key", "password")
>>> private_snapshot_key = import_rsa_privatekey_from_file("keystore/snapshot_key", "password")
>>> private_timestamp_key = import_rsa_privatekey_from_file("keystore/timestamp_key", "password")
>>> repository.targets.load_signing_key(private_targets_key)
>>> repository.snapshot.load_signing_key(private_snapshot_key)
>>> repository.timestamp.load_signing_key(private_timestamp_key)
>>> repository.timestamp.expiration = datetime.datetime(2080, 10, 28, 12, 8)
>>> repository.writeall()
>>>
```

已创建的时间戳、快照、目标文件：

```
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/repository/metadata
data# cd ../
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/repository# ll
总用量 20
drwxr-xr-x 5 root root 4096 11月 28 04:51 ./
drwxr-xr-x 7 root root 4096 11月 30 10:50 ../
drwxr-xr-x 2 root root 4096 11月 30 12:21 metadata/
drwxr-xr-x 2 root root 4096 11月 30 12:24 metadata.staged/
drwxr-xr-x 2 root root 4096 11月 28 04:51 targets/
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/repository# cd metadata.staged/
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/repository/metadata.staged# ll
总用量 36
drwxr-xr-x 2 root root 4096 11月 30 12:24 ./
drwxr-xr-x 5 root root 4096 11月 28 04:51 ../
-rw-r--r-- 1 root root 3394 11月 28 04:51 1.root.json
-rw-r--r-- 1 root root 1251 11月 28 04:51 role1.json
-rw-r--r-- 1 root root 439 11月 28 04:51 role2.json
-rw-r--r-- 1 root root 3394 11月 28 04:51 root.json
-rw-r--r-- 1 root root 554 11月 28 04:51 snapshot.json
-rw-r--r-- 1 root root 1624 11月 28 04:51 targets.json
-rw-r--r-- 1 root root 940 11月 30 12:24 timestamp.json
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/repository/metadata.staged#
```

运行本地 TUF 存储服务器:

```
root@lab-VirtualBox: /home/lab/download/tuf-develop/tests/repository_data
-rwxr-xr-x 1 lab lab 8494 11月 28 04:51 test_root_versioning_integration.py*
-rwxr-xr-x 1 lab lab 15495 11月 28 04:51 test_sig.py*
-rwxr-xr-x 1 lab lab 12059 11月 28 04:51 test_slow_retrieval_attack.py*
-rwxr-xr-x 1 lab lab 1292 11月 28 04:51 test_unittest_toolbox.py*
-rw-rw-r-- 1 lab lab 75219 11月 28 04:51 test_updater.py
-rwxr-xr-x 1 lab lab 15176 11月 28 04:51 test_updater_root_rotation_integration.py*
-rw-r--r-- 1 root root 692029 11月 29 19:14 tuf.log
root@lab-VirtualBox:/home/lab/download/tuf-develop/tests# cd repository_data/
root@lab-VirtualBox:/home/lab/download/tuf-develop/tests/repository_data# ll
总用量 36
drwxrwxr-x 6 lab lab 4096 11月 28 04:51 ./
drwxrwxr-x 4 lab lab 4096 11月 29 19:14 ../
drwxrwxr-x 3 lab lab 4096 11月 28 04:51 client/
-rwxr-xr-x 1 lab lab 3757 11月 28 04:51 generate_project_data.py*
-rwxr-xr-x 1 lab lab 6988 11月 28 04:51 generate.py*
drwxrwxr-x 2 lab lab 4096 11月 28 04:51 keystore/
drwxrwxr-x 4 lab lab 4096 11月 28 04:51 project/
drwxrwxr-x 5 lab lab 4096 11月 28 04:51 repository/
root@lab-VirtualBox:/home/lab/download/tuf-develop/tests/repository_data# cd "repository/"; python -m SimpleHTTPServer 8001
Serving HTTP on 0.0.0.0 port 8001 ...
```

客户端正常请求数据:

```
root@lab-VirtualBox: /home/lab/download/tuf-develop/tests/repository_data/repository
httpd.server_forever()
File "/usr/lib/python2.7/SocketServer.py", line 231, in serve_forever
    poll interval)
File "/usr/lib/python2.7/SocketServer.py", line 150, in _eintr_retry
    return func(*args)
KeyboardInterrupt
root@lab-VirtualBox:/home/lab/download/tuf-develop/tests/repository_data# cd repository/
root@lab-VirtualBox:/home/lab/download/tuf-develop/tests/repository_data/repository# ll
总用量 20
drwxrwxr-x 5 lab lab 4096 11月 28 04:51 ./
drwxrwxr-x 6 lab lab 4096 11月 28 04:51 ../
drwxrwxr-x 2 lab lab 4096 11月 28 04:51 metadata/
drwxrwxr-x 2 lab lab 4096 11月 28 04:51 metadata.staged/
drwxrwxr-x 2 lab lab 4096 11月 28 04:51 targets/
root@lab-VirtualBox:/home/lab/download/tuf-develop/tests/repository_data/repository# python -m SimpleHTTPServer 8001
Serving HTTP on 0.0.0.0 port 8001 ...

127.0.0.1 - - [30/Nov/2017 10:10:09] "GET /metadata/root.json HTTP/1.1" 200 -
127.0.0.1 - - [30/Nov/2017 10:10:12] "GET /metadata/timestamp.json HTTP/1.1" 200 -
127.0.0.1 - - [30/Nov/2017 10:10:15] "GET /targets/file1.txt HTTP/1.1" 200 -
127.0.0.1 - - [30/Nov/2017 10:10:15] "GET /targets/file2.txt HTTP/1.1" 200 -
127.0.0.1 - - [30/Nov/2017 10:10:15] "GET /targets/file3.txt HTTP/1.1" 200 -
```



客户端数据请求成功:

```
root@lab-VirtualBox: /home/lab/download/tuf-develop/tests/repository_data/client/test_repository# python basic_client.py --repo http://localhost:8001
Error: No working mirror was found:
  u'localhost:8001': HTTPError()
root@lab-VirtualBox: /home/lab/download/tuf-develop/tests/repository_data/client/test_repository# python basic_client.py --repo http://localhost:8001
root@lab-VirtualBox: /home/lab/download/tuf-develop/tests/repository_data/client/test_repository# ll
总用量 36
drwxrwxr-x 4 lab lab 4096 11月 30 10:10 ./
drwxrwxr-x 3 lab lab 4096 11月 30 09:57 ../
-rwxr-xr-x 1 root root 7658 11月 30 09:54 basic_client.py*
drwxrwxr-x 4 lab lab 4096 11月 30 09:59 metadata/
drwxr-xr-x 2 root root 4096 11月 30 10:10 targets/
-rw-r--r-- 1 root root 11726 11月 30 10:10 tuf.log
root@lab-VirtualBox: /home/lab/download/tuf-develop/tests/repository_data/client/test_repository# cd targets/
root@lab-VirtualBox: /home/lab/download/tuf-develop/tests/repository_data/client/repository/targets# ll
总用量 20
drwxr-xr-x 2 root root 4096 11月 30 10:10 ./
drwxrwxr-x 4 lab lab 4096 11月 30 10:10 ../
-rw-r--r-- 1 root root 31 11月 30 10:10 file1.txt
-rw-r--r-- 1 root root 39 11月 30 10:10 file2.txt
-rw-r--r-- 1 root root 28 11月 30 10:10 file3.txt
root@lab-VirtualBox: /home/lab/download/tuf-develop/tests/repository_data/client/repository/targets#
```

客户端元数据时间戳版本:

```
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/client/test_repository/metadata
{"signatures": [
  {
    "keyid": "8a1c4a3ac2d515dec982ba9910c5fd79b91ae57f625b9cff25d06bf0a61c1758",
    "sig": "7dddbfe94d6d80253433551700ea6dfe4171a33f1227a07830e951900b8325d67c3dce6410b9cf55abefa3dfca0b57814a4965c2d6ee60bb0336755cd0557e03"
  }
],
"signed": {
  "_type": "timestamp",
  "expires": "2030-01-01T00:00:00Z",
  "meta": {
    "snapshot.json": {
      "hashes": {
        "sha256": "6990b6586ed545387c6a51db62173b903a5dff46b17b1bc3fe1e6ca0d0844f2f"
      },
      "length": 554,
      "version": 1
    }
  },
  "spec_version": "1.0",
  "version": 1
}
```

### 3. TUF 搭建和部署

备份存储库当前版本为 1 的时间戳文件：

```
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/tmp
drwxr-xr-x 5 root root 4096 11月 28 04:51 repository/
-rw-r--r-- 1 root root 555 11月 30 10:48 tmp
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data# rm tmp
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data# mkdir tmp
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data# cp repository/metada
ta/timestamp.json ./tmp/
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data# ll
总用量 40
drwxr-xr-x 7 root root 4096 11月 30 10:49 ./
drwxr-xr-x 3 root root 4096 11月 28 04:51 ../
drwxr-xr-x 3 root root 4096 11月 28 04:51 client/
-rwxr-xr-x 1 root root 3757 11月 28 04:51 generate_project_data.py*
-rwxr-xr-x 1 root root 6988 11月 28 04:51 generate.py*
drwxr-xr-x 2 root root 4096 11月 28 04:51 keystore/
drwxr-xr-x 4 root root 4096 11月 28 04:51 project/
drwxr-xr-x 5 root root 4096 11月 28 04:51 repository/
drwxr-xr-x 2 root root 4096 11月 30 10:49 tmp/
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data# cd tmp/
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/tmp# ll
总用量 12
drwxr-xr-x 2 root root 4096 11月 30 10:49 ./
drwxr-xr-x 7 root root 4096 11月 30 10:49 ../
-rw-r--r-- 1 root root 555 11月 30 10:49 timestamp.json
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/tmp#
```

创建新的时间戳文件并将版本号从 1 提升至 2，替换原仓库中的时间戳数据文件：

```
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data
drwxr-xr-x 2 root root 4096 11月 30 10:49 tmp/
-rw-r--r-- 1 root root 3927 11月 30 12:22 tuf.log
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data# python
Python 2.7.12 (default, Nov 20 2017, 18:23:56)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from tuf.repository_tool import *
>>> repository = load_repository('repository')
>>> repository.timestamp.version
1
>>> repository.timestamp.version = 2
>>> repository.dirty_roles()
Dirty roles: [u'timestamp']
>>> private_timestamp_key = import_rsa_privatekey_from_file("keystore/timestam
p_key", "password")
>>> repository.timestamp.load_signing_key(private_timestamp_key)
>>> repository.write('timestamp')
>>>
KeyboardInterrupt
>>>
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data# cp repository/meta
data.staged/* repository/metadata
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data#
```

客户端发起新一次的请求，客户端成功 get 新版本：

```
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/client/test_repository/
basic_client.py metadata/ targets/ tuf.log
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repository# cp -r /home/lab/download/tuf-develop/tests/repository_data/client/test_repository/basic_client.py ./
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repository# ll
未找到 'll' 命令，您要输入的是否是：
命令 'dll' 来自于包 'brickos' (universe)
命令 'llc' 来自于包 'llvm' (universe)
命令 'lli' 来自于包 'llvm-runtime' (universe)
命令 'llt' 来自于包 'storebackup' (universe)
ll: 未找到命令
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repository# ll
总用量 20
drwxr-xr-x 3 root root 4096 11月 30 11:19 ./
drwxr-xr-x 3 root root 4096 11月 28 04:51 ../
-rwxr-xr-x 1 root root 7658 11月 30 11:19 basic_client.py*
drwxr-xr-x 4 root root 4096 11月 28 04:51 metadata/
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repository# python basic_client.py --repo http://localhost:8001
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repository# python basic_client.py --repo http://localhost:8001
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repository# python basic_client.py --repo http://localhost:8001
```

服务端传输数据：

```
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/repository
^CTraceback (most recent call last):
  File "/usr/lib/python2.7/runpy.py", line 174, in _run_module_as_main
    "__main__", fname, loader, pkg_name)
  File "/usr/lib/python2.7/runpy.py", line 72, in _run_code
    exec code in run_globals
  File "/usr/lib/python2.7/SimpleHTTPServer.py", line 235, in <module>
    test()
  File "/usr/lib/python2.7/SimpleHTTPServer.py", line 231, in test
    BaseHTTPServer.test(HandlerClass, ServerClass)
  File "/usr/lib/python2.7/BaseHTTPServer.py", line 610, in test
    httpd.serve_forever()
  File "/usr/lib/python2.7/SocketServer.py", line 231, in serve_forever
    poll_interval)
  File "/usr/lib/python2.7/SocketServer.py", line 150, in _eintr_retry
    return func(*args)
KeyboardInterrupt
root@lab-VirtualBox:/home/lab/download/tuf-develop/tests/repository_data/repository# python -m SimpleHTTPServer 8001
Serving HTTP on 0.0.0.0 port 8001 ...
127.0.0.1 - - [30/Nov/2017 11:06:56] "GET /metadata/root.json HTTP/1.1" 200 -
127.0.0.1 - - [30/Nov/2017 11:06:59] "GET /metadata/timestamp.json HTTP/1.1" 200 -
127.0.0.1 - - [30/Nov/2017 11:19:40] "GET /metadata/root.json HTTP/1.1" 200 -
127.0.0.1 - - [30/Nov/2017 11:19:43] "GET /metadata/timestamp.json HTTP/1.1" 200 -
```

客户端获得的新版本时间戳文件，显示版本号为 2：



```

root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/client/test_repository/mc
{"signatures": [
  {
    "keyid": "8a1c4a3ac2d515dec982ba9910c5fd79b91ae57f625b9cff25d06bf0a61c1758",
    "sig": "7dddbfe94d6d80253433551700ea6dfe4171a33f1227a07830e951900b8325d67c3dce6410b9cf55abefa3dfca0b57814a4965c2d6ee60bb0336755cd0557e03"
  }
],
"signed": {
  "_type": "timestamp",
  "expires": "2030-01-01T00:00:00Z",
  "meta": {
    "snapshot.json": {
      "hashes": {
        "sha256": "6990b6586ed545387c6a51db62173b903a5dff46b17b1bc3fe1e6ca0d0844f2
f"
      },
      "length": 554,
      "version": 1
    }
  },
  "spec_version": "1.0",
  "version": 2
}
}
~

```

将备份的版本号为 1 的版本替换到当前存储库：

```

root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data
总用量 48
drwxr-xr-x 7 root root 4096 11月 30 10:50 ./
drwxr-xr-x 3 root root 4096 11月 28 04:51 ../
drwxr-xr-x 3 root root 4096 11月 28 04:51 client/
-rwxr-xr-x 1 root root 3757 11月 28 04:51 generate_project_data.py*
-rwxr-xr-x 1 root root 6988 11月 28 04:51 generate.py*
drwxr-xr-x 2 root root 4096 11月 28 04:51 keystore/
drwxr-xr-x 4 root root 4096 11月 28 04:51 project/
drwxr-xr-x 5 root root 4096 11月 28 04:51 repository/
drwxr-xr-x 2 root root 4096 11月 30 10:49 tmp/
-rw-r--r-- 1 root root 5011 11月 30 13:23 tuf.log
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data# cd repository/
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/repository# ll
总用量 20
drwxr-xr-x 5 root root 4096 11月 28 04:51 ./
drwxr-xr-x 7 root root 4096 11月 30 10:50 ../
drwxr-xr-x 2 root root 4096 11月 30 12:21 metadata/
drwxr-xr-x 2 root root 4096 11月 30 12:24 metadata.staged/
drwxr-xr-x 2 root root 4096 11月 28 04:51 targets/
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/repository# cd ../
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data# cp /tmp/timestamp.
json repository/metadata/
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data#

```

重启服务端，客户端发起新一次请求，显示请求数据未找到，报  
ReplayedMetadataError，表面请求版本低于当前拥有版本：

```
root@lab-VirtualBox: /mnt/tuf-develop/tests/repository_data/client/test_repository
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repositor
y# python basic_client.py --repo http://localhost:8001

Error: No working mirror was found:
  u'localhost:8001': BadSignatureError()
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repositor
y#
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repositor
y# ll
总用量 32
drwxr-xr-x 4 root root 4096 11月 30 11:19 ./
drwxr-xr-x 3 root root 4096 11月 28 04:51 ../
-rwxr-xr-x 1 root root 7658 11月 30 11:19 basic_client.py*
drwxr-xr-x 4 root root 4096 11月 28 04:51 metadata/
drwxr-xr-x 2 root root 4096 11月 30 11:19 targets/
-rw-r--r-- 1 root root 6411 11月 30 11:26 tuf.log
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repositor
y# gedit basic_client.py

** (gedit:2430): WARNING **: Set document metadata failed: 不支持设置属性 metada
ta::gedit-position
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repositor
y# python basic_client.py --repo http://localhost:8001
Error: No working mirror was found:
  u'localhost:8001': ReplayedMetadataError()
root@lab-VirtualBox:/mnt/tuf-develop/tests/repository_data/client/test_repositor
y#
```

### 三、 实验结论

实验中我们可以看到，客户端在请求更新时，首先只会请求 `root.json` 和 `timestamp.json` 文件，这就是论文中所描述的，第一步，下载快照元数据，然后对比新旧快照元数据版本号，第二步，下载需安装的项目的 `Project metadata`，将 `Project metadata` 中的版本号与最新的 `Snapshot metadata` 中的版本号进行对比，本次实验我们回滚了项目版本号，TUF 客户端只下载了论文中所描述的较少的文件便拒绝了项目数据请求，说明其在单例客户端请求时展现了其带宽高效的优势，在大量项目大量客户端的请求下，相对应该有更明显的优势。