New Threat Based Chinese P2P Network

Jun_Xie@McAfee

Agenda

- Who am I
- Background
- Thunder Network Architecture
- Security Issue
- Exploit
- Demo
- Questions

Who am I

- Security researcher @McAfee IDT team
- Network Intrusion Prevention System signature development
- Focus on vulnerability research
- P2P application protocol analysis
- Botnet detection
- Malware research
- Reverse engineering
- Mobile system security research

Background

- Background in China

  420 million internet users in china (From CNNIC 2010)

- Popular Application

  Online video, game, B2C, B2B,etc.

- P2P business market

  Xunlei (A.K.A Thunder network)

  QQDownload

  Flashget

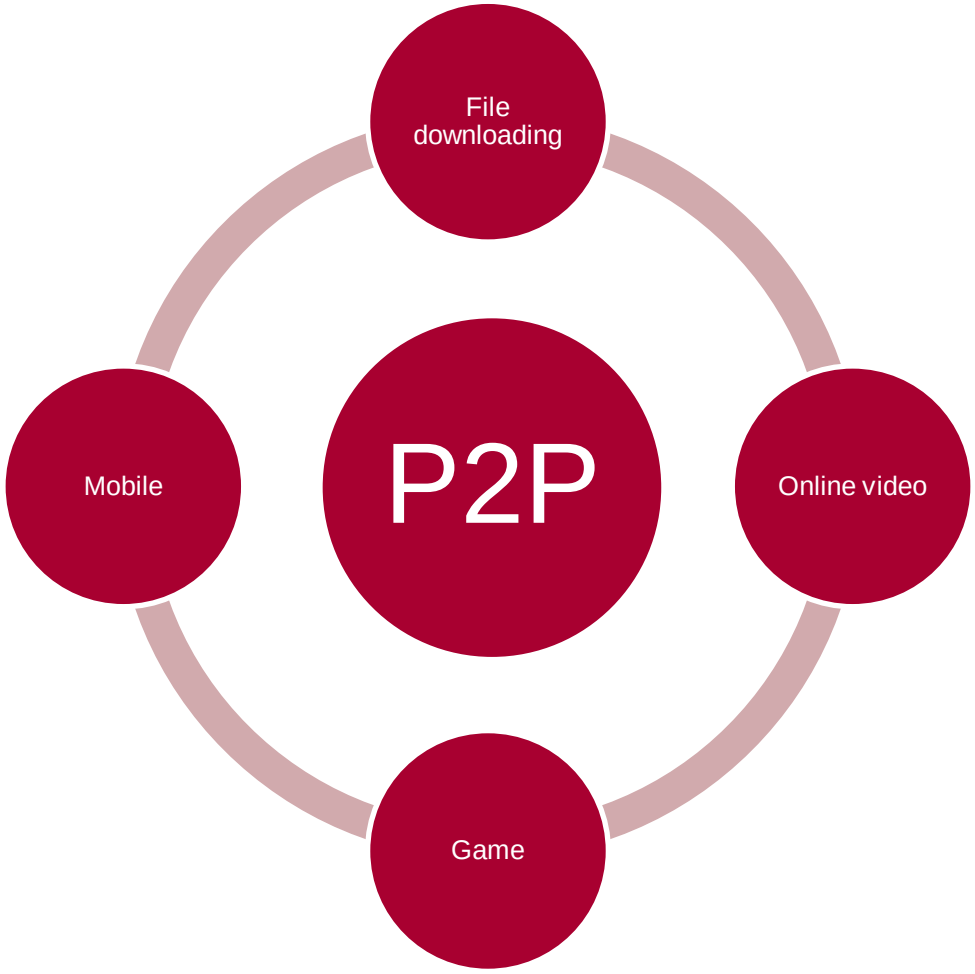
  PPTV

  PPS

  etc.

Background

- Why choose Thunder Network



Thunder Network Architecture

What is it?

- A downloading software like (Bittorent, emule, etc)
- downloading and uploading data through multi-protocols

P2SP

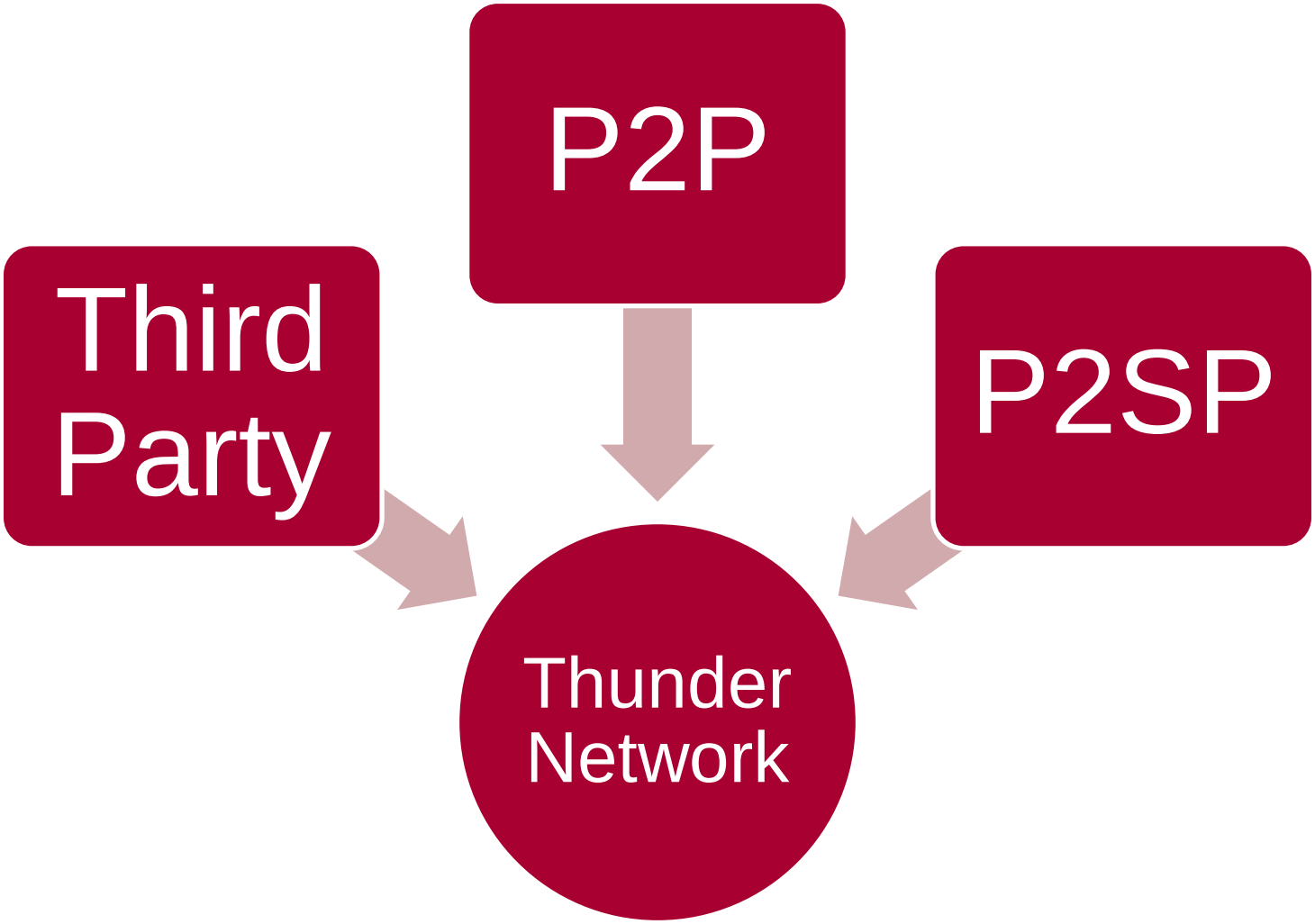
P2P

Integrated Bittorent, emule network

Clouding service

Thunder Network Architecture

Abstract architecture



Thunder Network Architecture

How is it work?

Server side

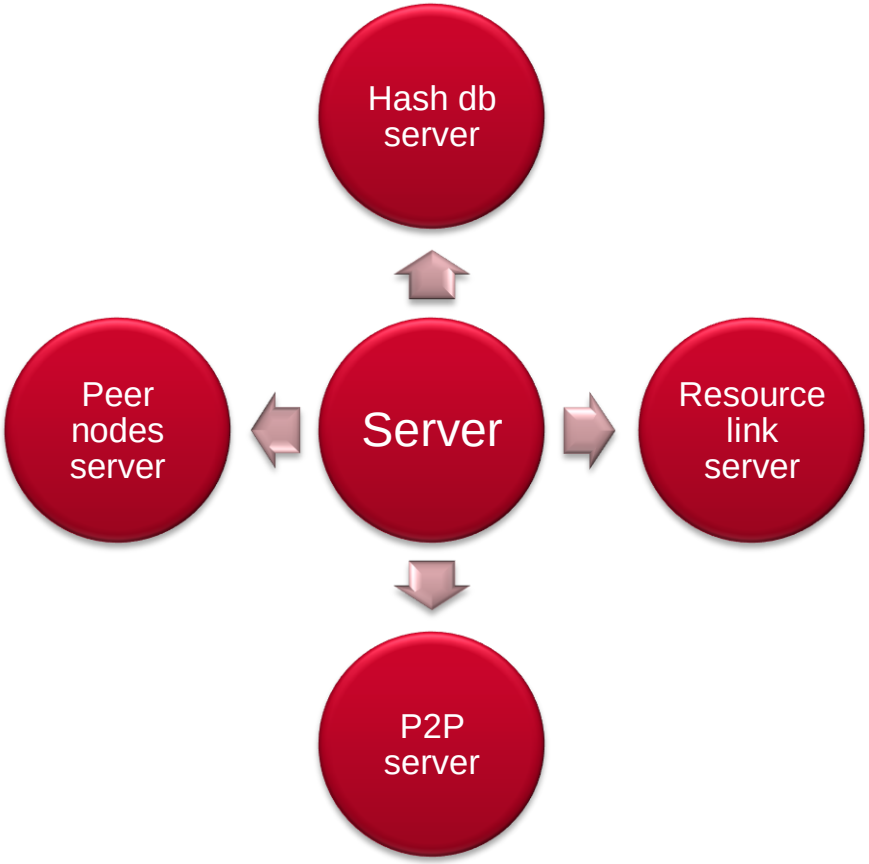
- Hash information query service
- Multi-downloading link query service
- Multi-Peer nodes query service
- High speed download channel query service (For VIP users)
- Clouding service & offline downloading (For VIP users)

Client side

- downloading data
- Assembling data
- Calculate Hash
- Uploading data for sharing

Thunder Network Architecture

- Server side



Thunder Network Architecture

- Server side

➢ Hash db server

Every single file have a unique file SHA1 hash(not hash all of data), and depends on it's file data length, split to multi-pieces data segment, every piece of data length 0x40000/0x100000/0x200000 bytes.

keyword: Unique HASH = every single file's SHA1 hash
File segment HASH= every single file segment SHA1 hash
Hash 's Hash =All of File segment HASH's SHA1 hash

DEMO show

Thunder Network Architecture

- Server side

➢ Resource link db server

This table maintained for every single file with multi-links mapping relationship [1=>N].

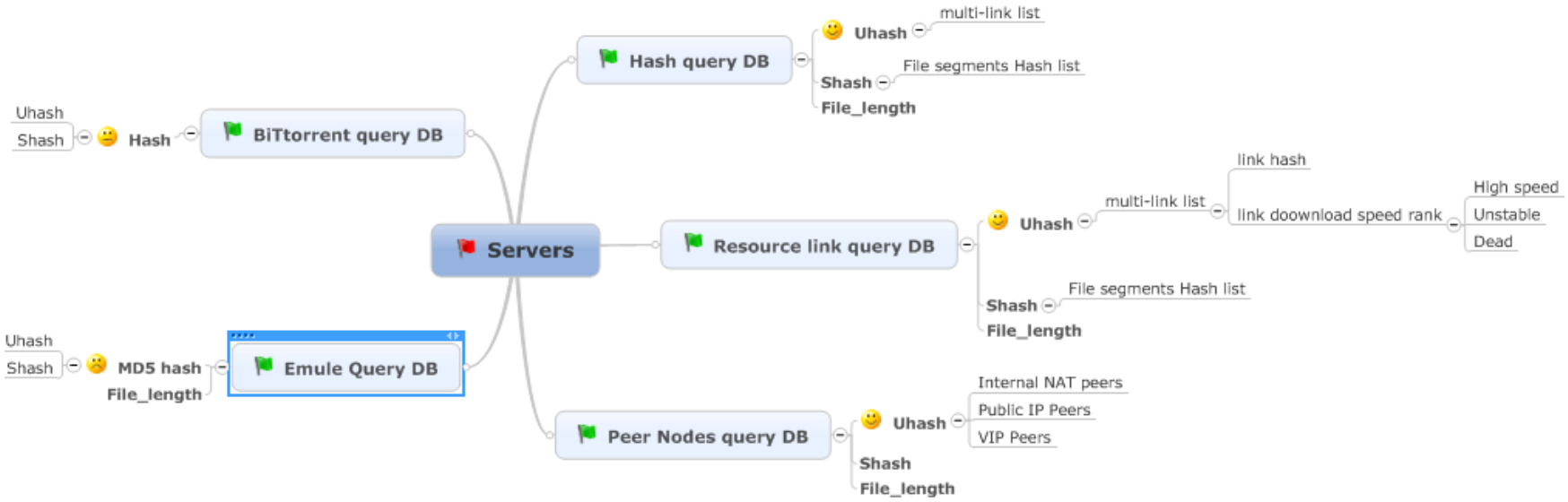
➢ Peer nodes db server

This table maintained for every single file with multi-nodes mapping relationship [1=>N].

➢ P2P servers

These servers help peer node communication with other nodes, like(join Thunder P2P network, leave P2P network, P2P punch NAT hole , etc.

Thunder Network Architecture



Thunder Network Architecture

- Client side

  Every single Thunder Client have a Unique ID---CID(16 bytes string) “00E04C042121XTH4”, first 12 bytes indicated Client MAC address “00:E0:4C:04:21”, “XTH” random bytes, the last byte is a special flag. “Q” indicate normal users, “I” indicated VIP users, etc.

- downloading data

  downloading data from HTTP/FTP servers or thunder peers, emule or BiTtorrent nodes.

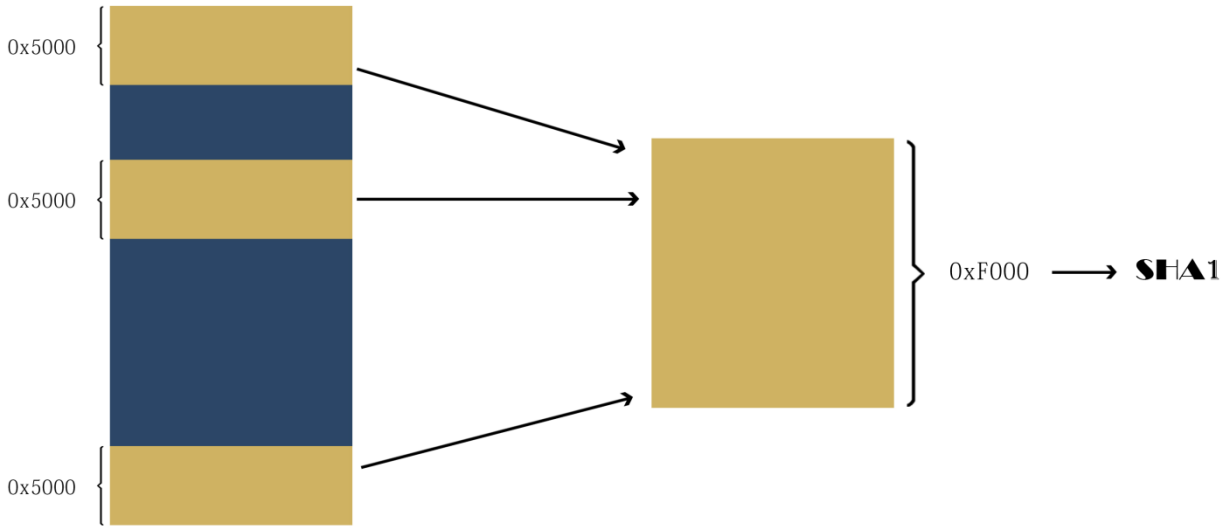
- Assembling data

  Client get hash block list from Hash DB server, then verify the downloaded data, check that correct or not.

- Uploading data for sharing
- Update client current state

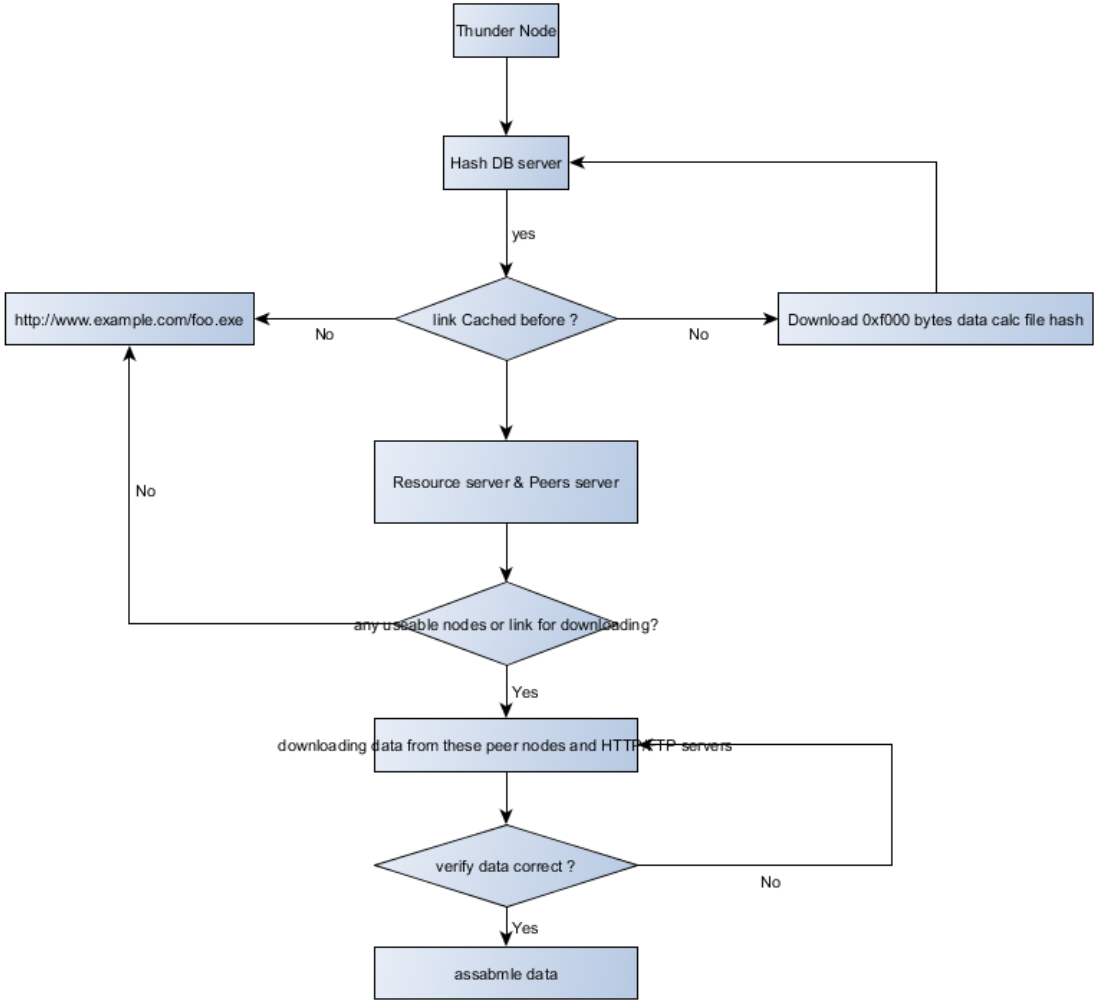
Thunder Network Architecture

- Client side
  how to let Thunder resource server know what you want to download?
  Unique file hash construct



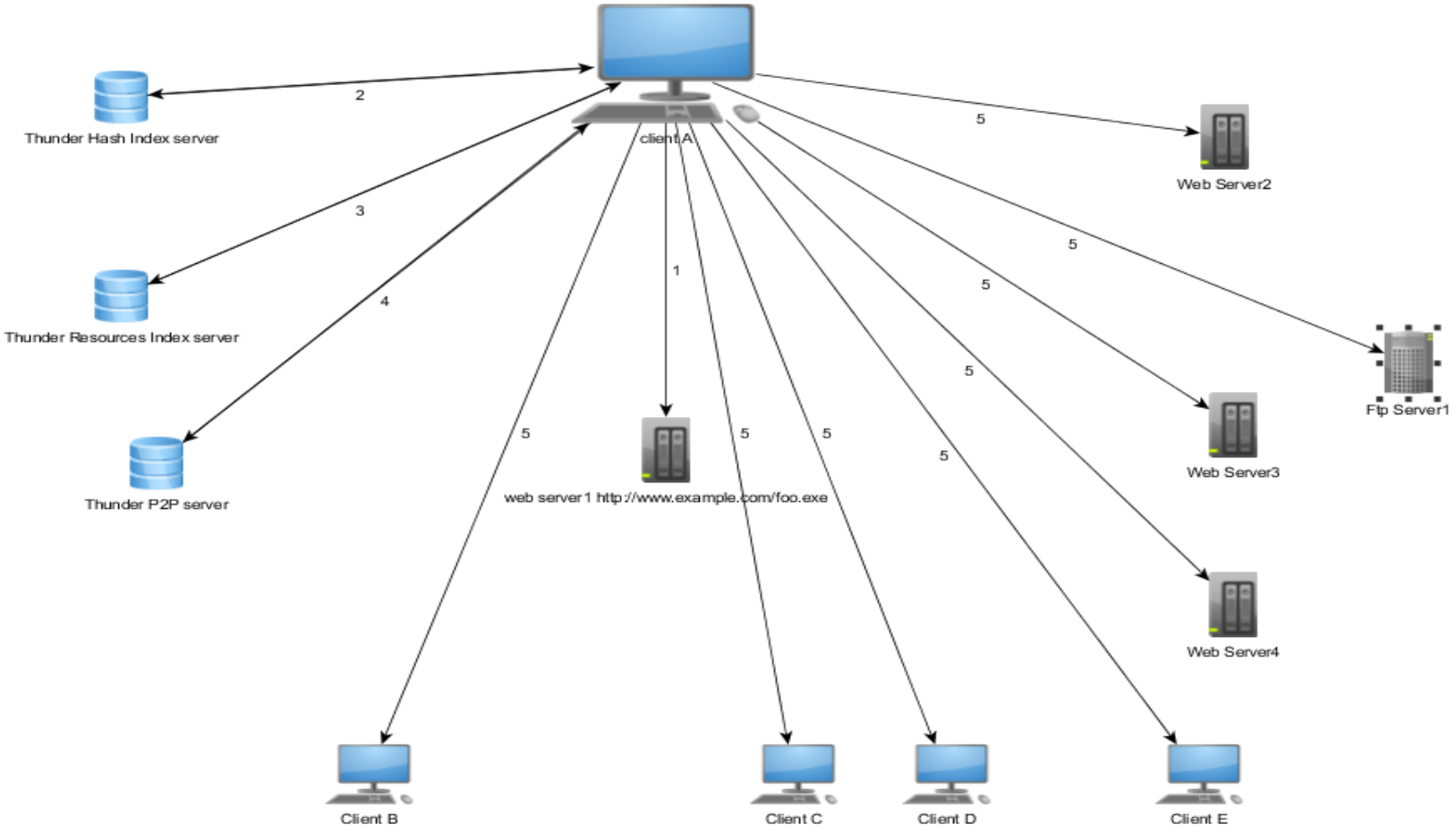
Thunder Network Architecture

- Client side
  download flowchart



Thunder Network Architecture

File downloading whole flow



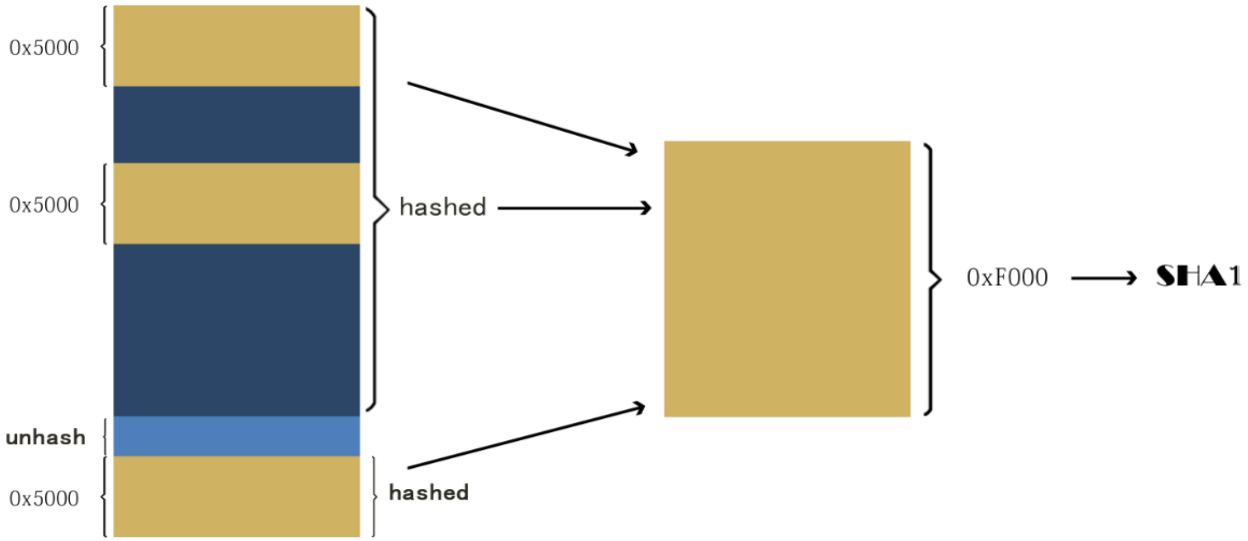
Security Issue

- Client side
  - File integrity check

    every data block length is 0x40000/0x100000/0x200000

    if last data block length less than 0x40000/0x100000/0x200000

    data of length (0<length<block_len-0x5000) haven't hashed



Security Issue

- Server side
  - haven’t check client submit download information
    download link(HTTP/FTP)
    download link’s rank(speed)
    so in the client side, we can fake these information.

Exploit

- Launch passive DDOS attack

➢ Thunder Client feature

➢ Thunder server haven't check client submitted information

SO

➢ we can submit fake HTTP/FTP link

like we can fake http://www.example.com/foo.exe, actually in this site haven't foo.exe

➢ we can submit fake HTTP/FTP link rank

like we can fake download speed of foo.exe from http://www.example.com.

Exploit

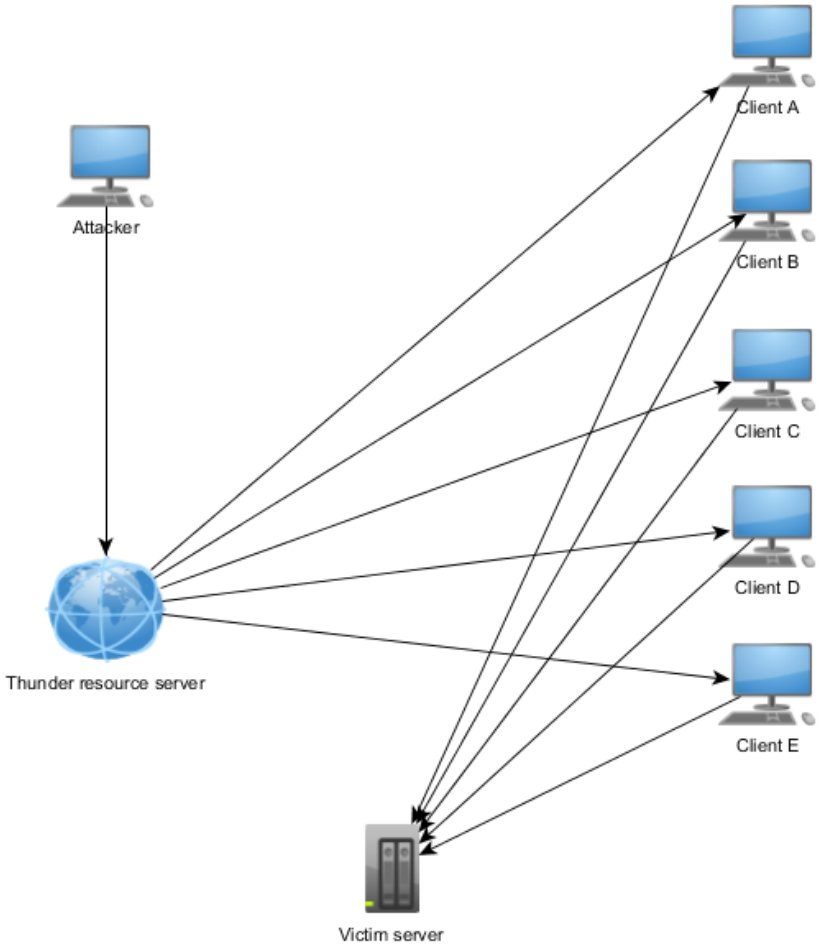
- Launch passive DDOS attack

How to fake resource link?(HTTP/FTP link)

Attacker can commit many file information with http link relationship.

Others users query resource server find victim server can download file what they wanted.

Finally many Thunder users request victim server for downloading

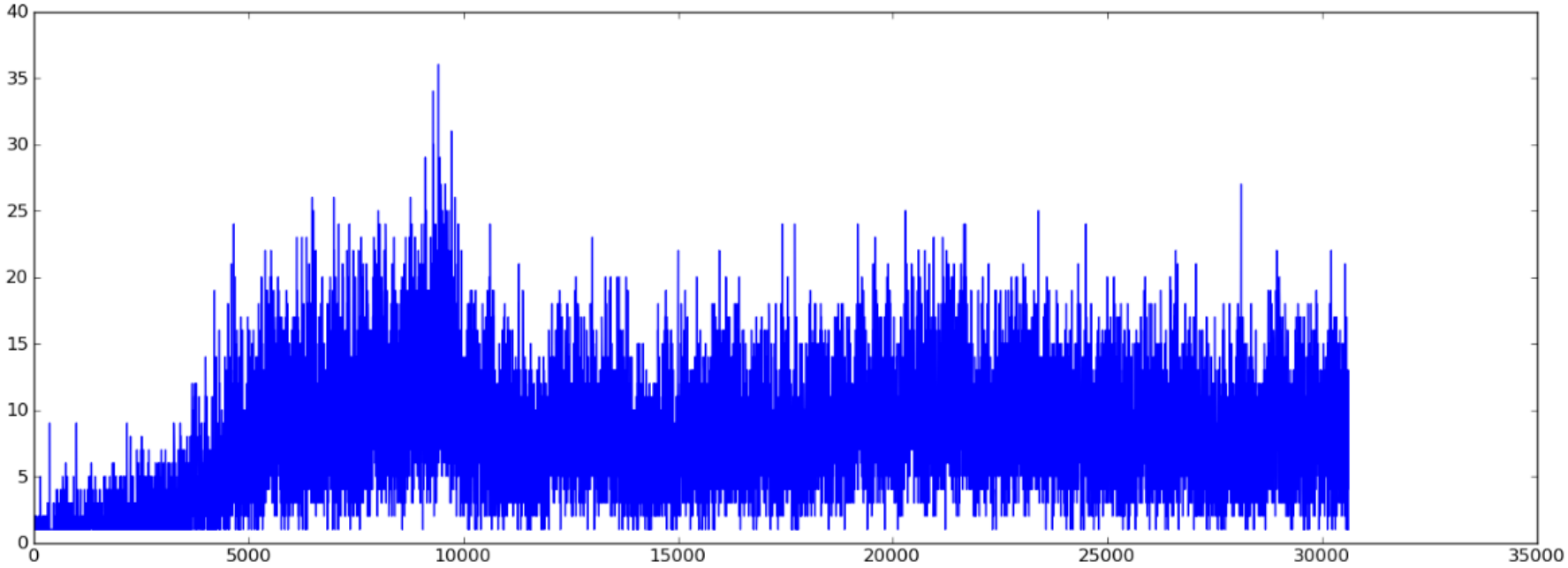


Exploit

- Launch passive DDOS attack

Real-world testing

2011 May 21 http://www.mamushi.tk http request log, haven't launch http flood from Thunder network

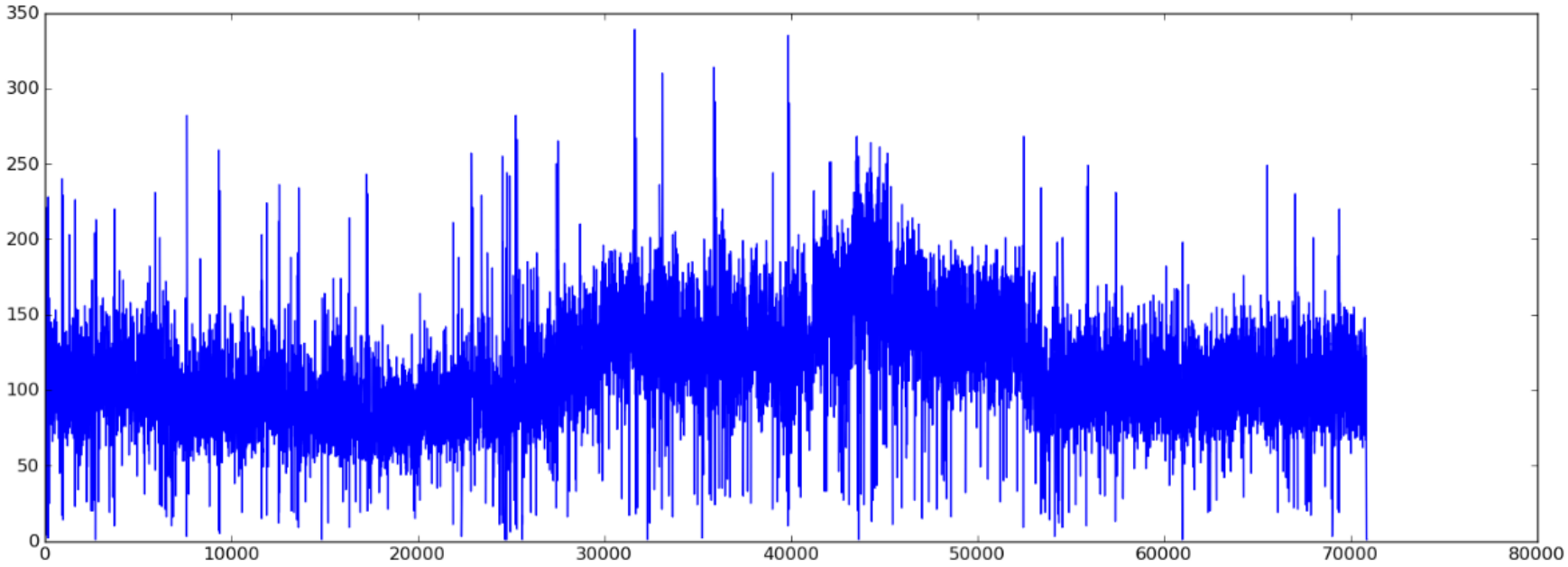


Exploit

- Launch passive DDOS attack

Real-world testing

Fake 10000 file information with victim server relationship



Exploit

- Compare with BitTorrent P2P attack

	BitTorrent	Thunder
Fake resource info	fake .torrent file and publish in online channel	Fake file info commit in resource server directly
Flexibility	Difficult to launch an attack	easy
Effectiveness	Need much more time	About one or two hours

Exploit

- Attack Thunder Client

Mechanism

- client share file feature
  client will share it's history of downloaded file
- every single client have a unique ID
  you need know target CID, and fake downloaded file info with CID relationship.

Not verify it, still work on it, maybe next year ☺

Demo

- Thunder Client query demo
- Insert fake resource information to resource server
- Join Thunder P2P demo

Future work

Expect next year we would like to share☺

- About P2P emulator
- The New Generation of Botnet Based on Thunder P2P

Questions

Thanks!