FTP: The Forgotten Cloud

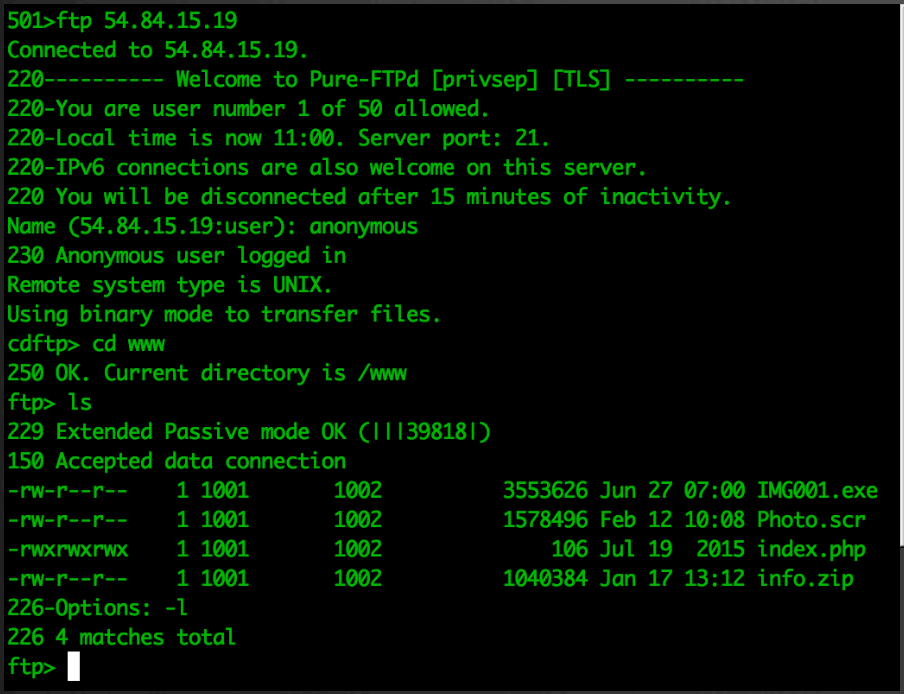
Drew Springall, Zakir Durumeric, and J. Alex Halderman
University of Michigan

FTP – File Transfer Protocol

- Simple text-based protocol
- View and traverse directory structure
- Upload and download files

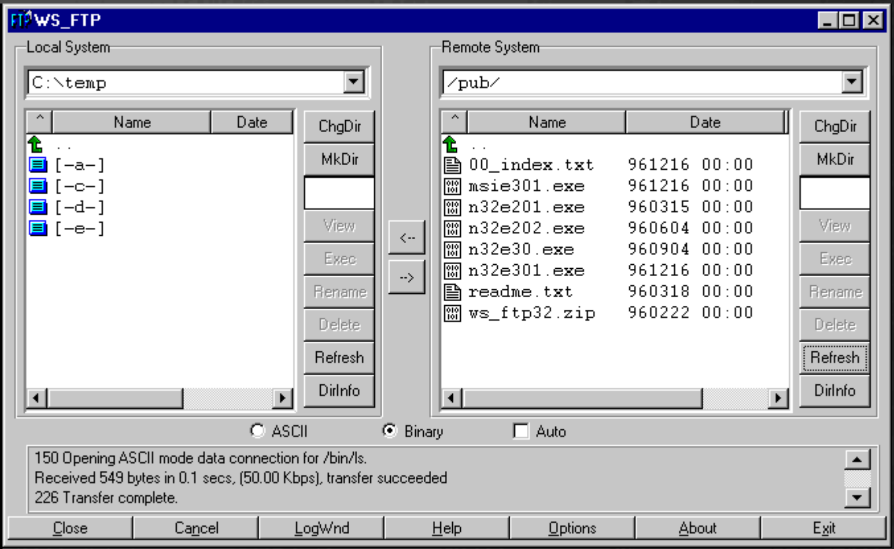
FTP Implementations

Terminal Client



```
501>ftp 54.84.15.19
Connected to 54.84.15.19.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 50 allowed.
220-Local time is now 11:00. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (54.84.15.19:user): anonymous
230 Anonymous user logged in
Remote system type is UNIX.
Using binary mode to transfer files.
cdftp> cd www
250 OK. Current directory is /www
ftp> ls
229 Extended Passive mode OK (|||39818|)
150 Accepted data connection
-rw-r--r--    1 1001       1002          3553626 Jun 27 07:00 IMG001.exe
-rw-r--r--    1 1001       1002          1578496 Feb 12 10:08 Photo.scr
-rwxrwxrwx    1 1001       1002              106 Jul 19  2015 index.php
-rw-r--r--    1 1001       1002          1040384 Jan 17 13:12 info.zip
226-Options: -l
226 4 matches total
ftp> █
```

GUI Client



WS_FTP

Local System: C:\temp

Name	Date
..	
[-a-]	
[-c-]	
[-d-]	
[-e-]	

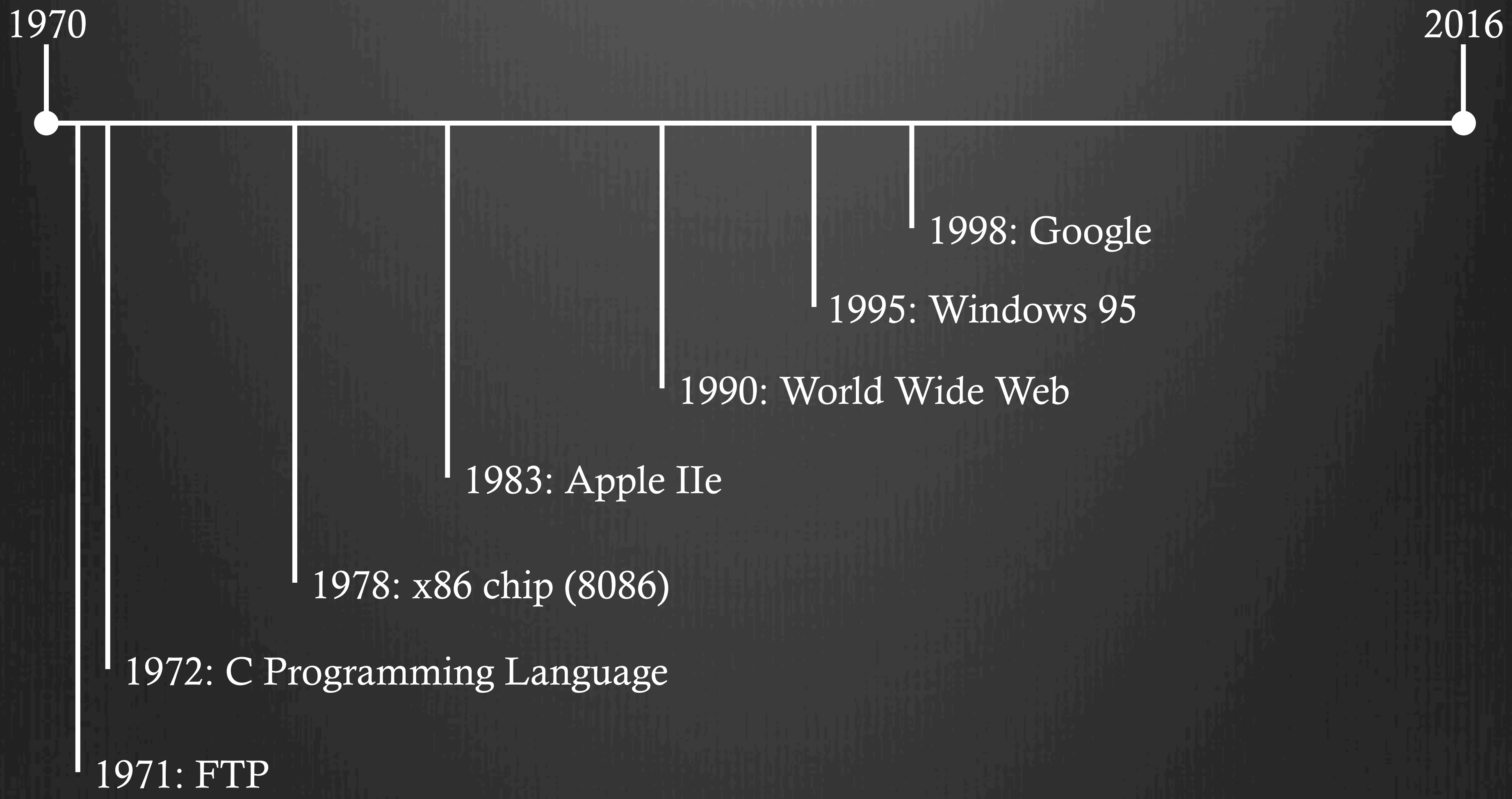
Remote System: /pub/

Name	Date
..	
00_index.txt	961216 00:00
msie301.exe	961216 00:00
n32e201.exe	960315 00:00
n32e202.exe	960604 00:00
n32e30.exe	960904 00:00
n32e301.exe	961216 00:00
readme.txt	960318 00:00
ws_ftp32.zip	960222 00:00

○ ASCII ● Binary □ Auto

```
150 Opening ASCII mode data connection for /bin/ls.
Received 549 bytes in 0.1 secs, (50.00 Kbps), transfer succeeded
226 Transfer complete.
```

FTP is Old



1970

2016

1971: FTP

1972: C Programming Language

1978: x86 chip (8086)

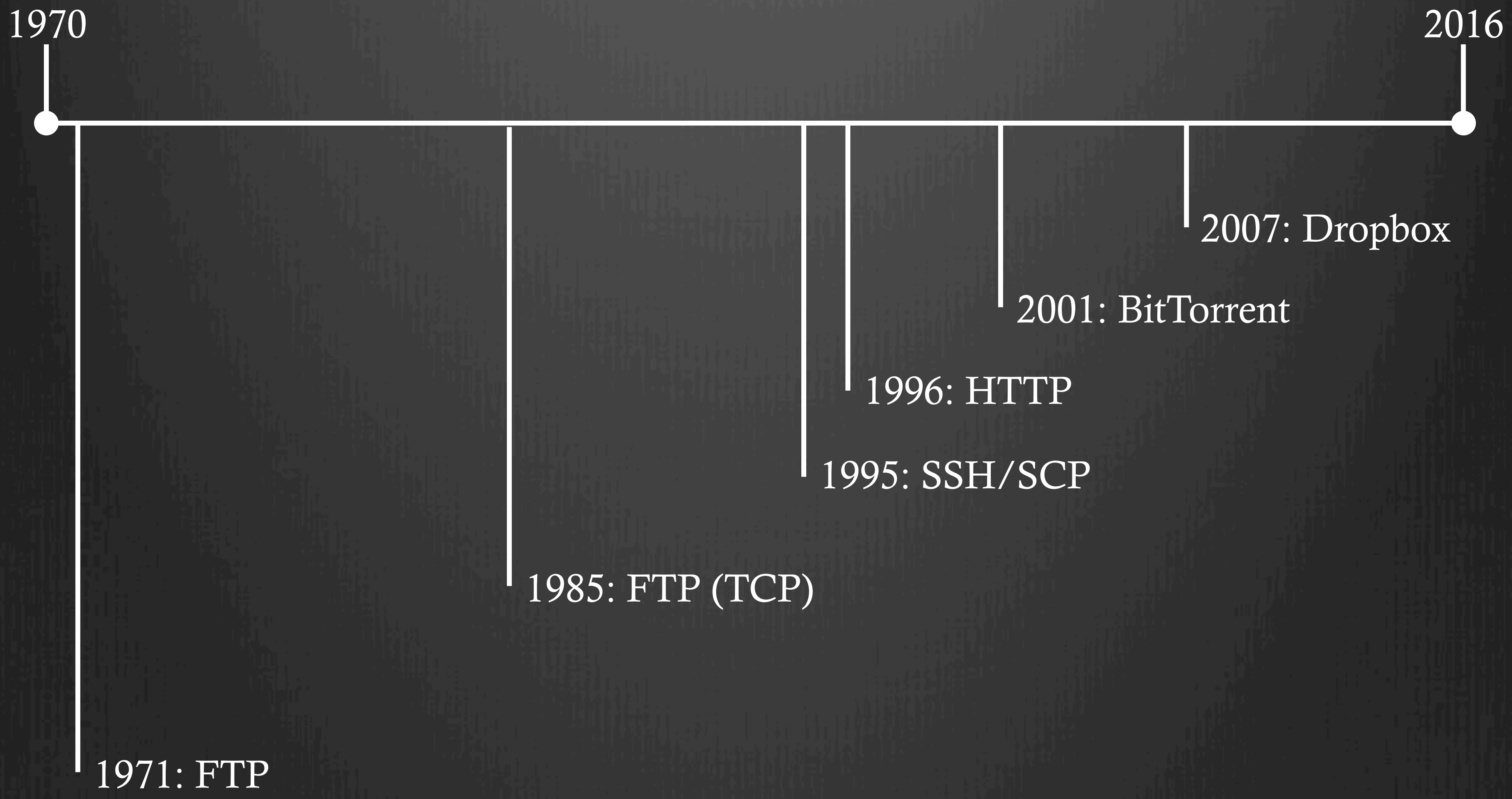
1983: Apple IIe

1990: World Wide Web

1995: Windows 95

1998: Google

FTP Replacements



1970

2016

2007: Dropbox

2001: BitTorrent

1996: HTTP

1995: SSH/SCP

1985: FTP (TCP)

1971: FTP

It’s Still Here

- 13.8M FTP Servers
- 1.1M publically-accessible FTP servers
- 600M visible files/directories

Questions

- What is the state of FTP in 2015?
- Is sensitive data being shared on FTP?
- Is FTP being used by malicious actors?
- What vulnerabilities still exist in FTP?

◆FTP Protocol

- ◆ Methodology
- ◆ What is the state of FTP in 2015?
- ◆ Is sensitive data being shared on FTP?
- ◆ Is FTP being used by malicious actors?
- ◆ What vulnerabilities still exist in FTP?
- ◆ Conclusions

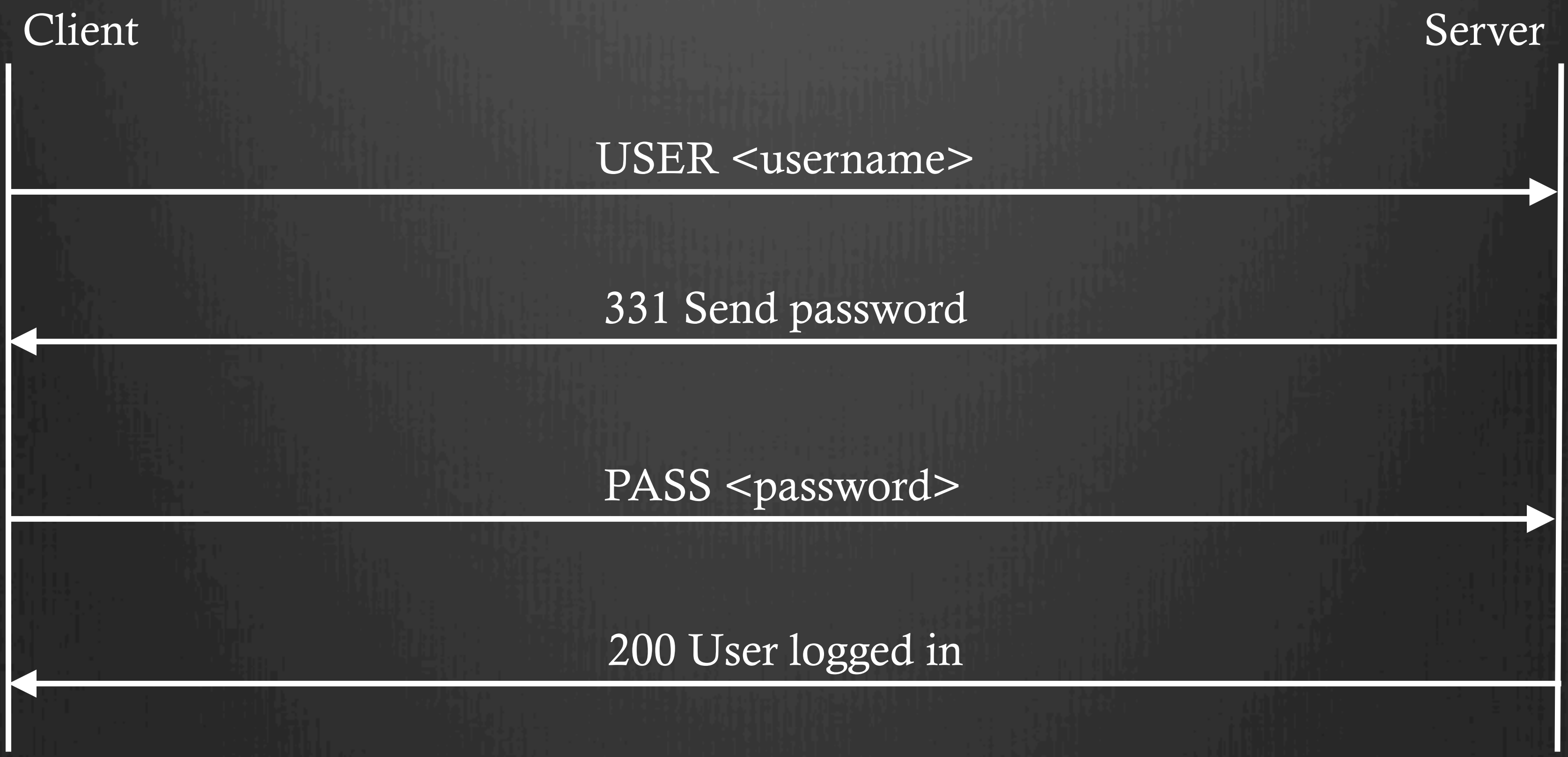
FTP Commands

- USER – Send username
- PASS – Send password
- CWD – Change Working Directory
- PWD – Present Working Directory
- PORT/PASV – Create secondary TCP connection
- LIST – Display directory contents
- RETR – Retrieve file

FTP Replies

- 3-digit response codes + optional text message
- 200 – OK
- 331 – User OK, send password
- 5XX -- Error

Authentication



Client

Server

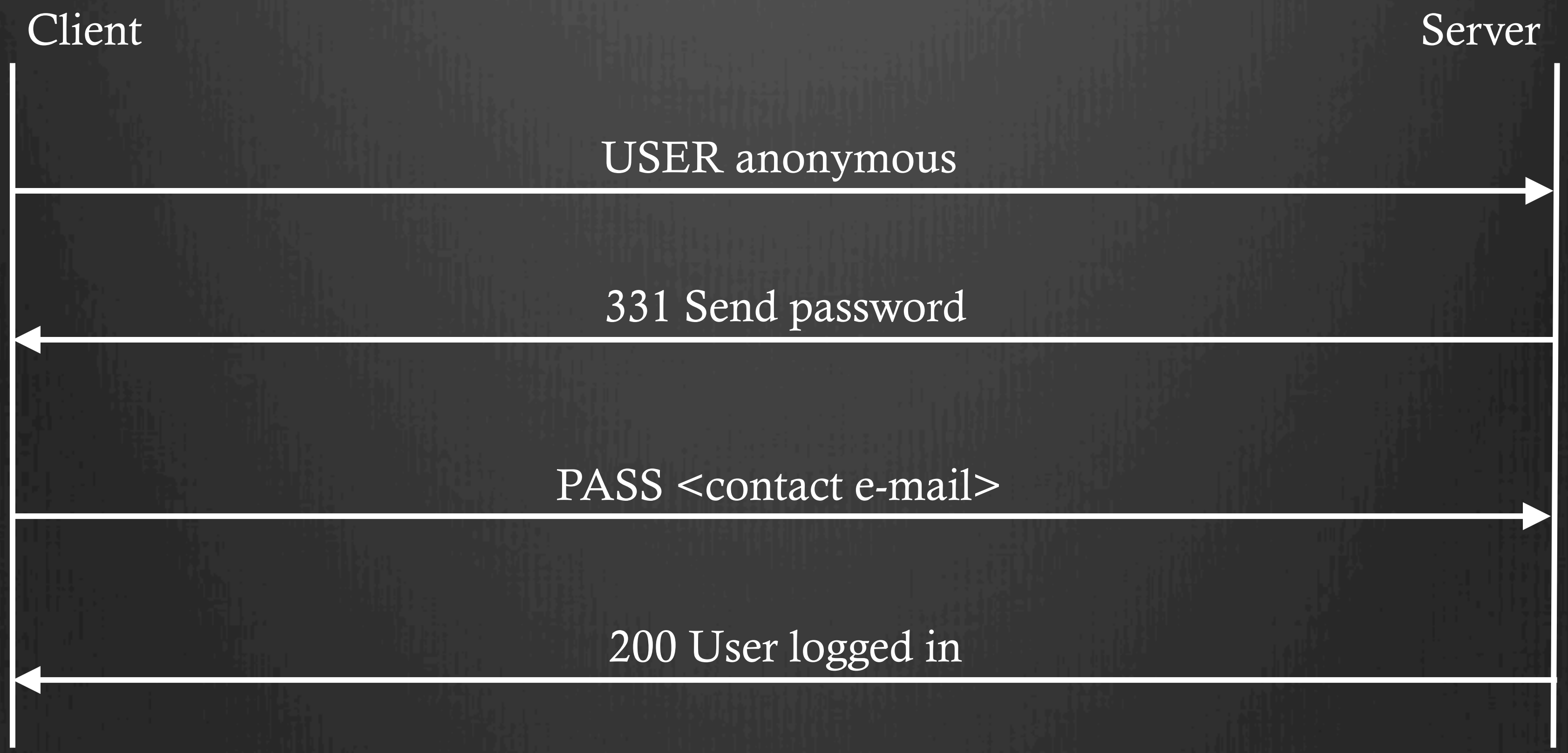
USER <username>

331 Send password

PASS <password>

200 User logged in

Anonymous Authentication



Client

Server

USER anonymous

331 Send password

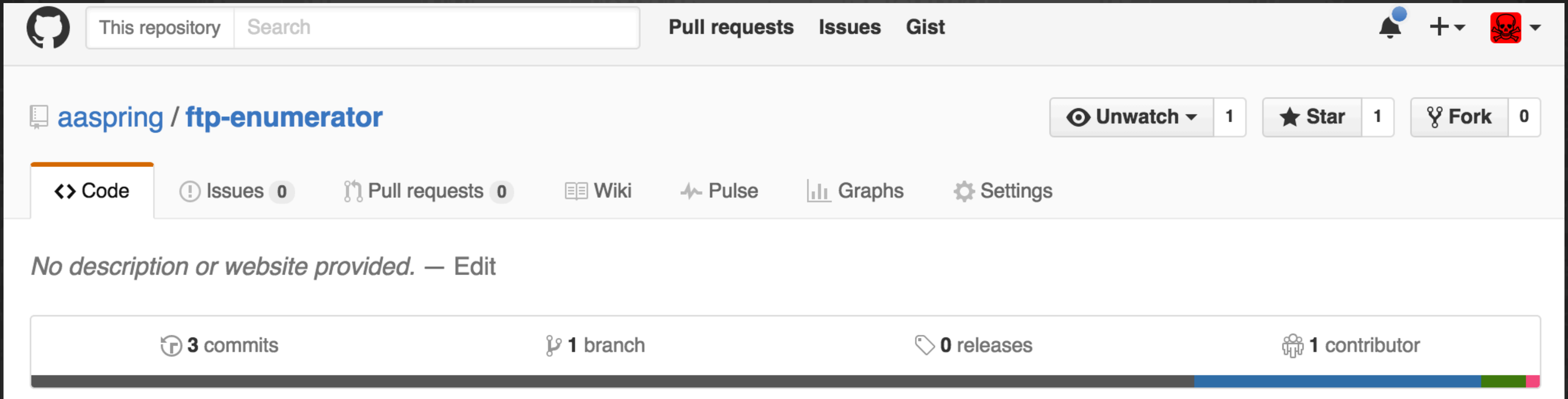
PASS <contact e-mail>

200 User logged in

- FTP Protocol
- **Methodology**
- What is the state of FTP in 2015?
- Is sensitive data being shared on FTP?
- Is FTP being used by malicious actors?
- What vulnerabilities still exist in FTP?
- Conclusions

Scanning & Enumeration

- ZMap Tool chain
- Custom protocol scanner
  - Available at github.com/aaspring/ftp-enumerator



No description or website provided. — Edit

Data Collection

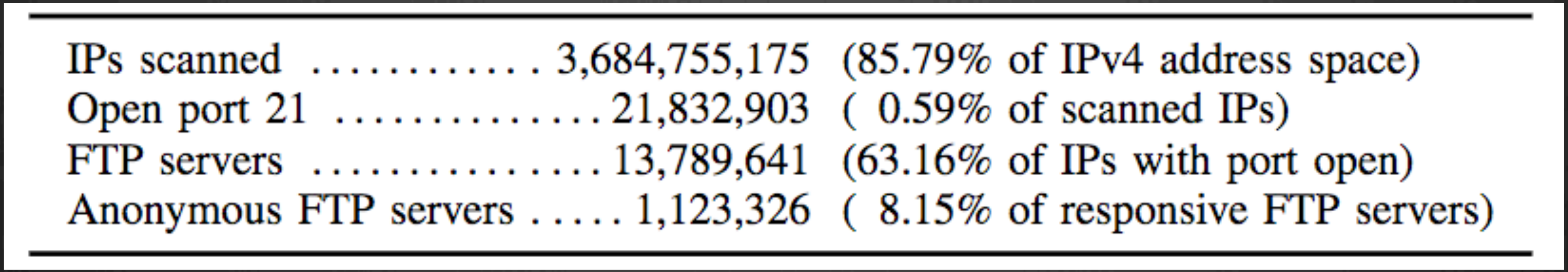
- Parse banner
- Login via the anonymous user
- Parse robots.txt
- Traverse the directory structure
- Collect Features, Help, Status
- Collect FTPS certificate if available

Ethical Considerations

- Scanning best practices
- Limited number and frequency of commands to each server
- Not trying to guess usernames/passwords
- Not downloading files en masse

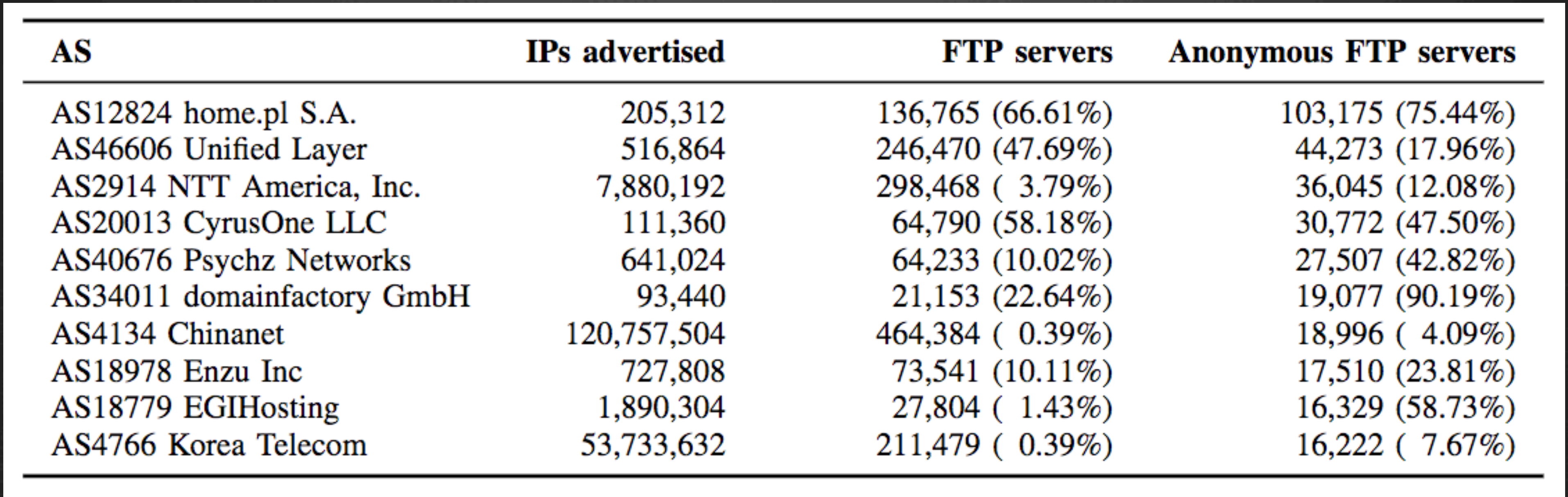
- FTP Protocol
- Methodology
- **What is the state of the FTP in 2015?**
- Is sensitive data being shared on FTP?
- Is FTP being used by malicious actors?
- What vulnerabilities still exist in FTP?
- Conclusions

How prevalent is FTP?



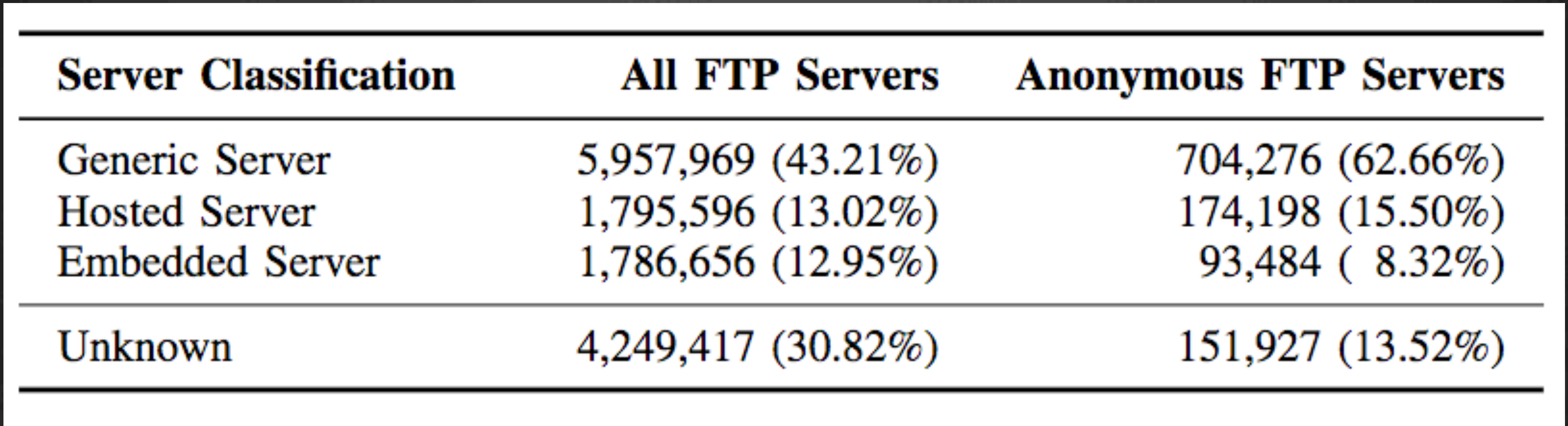
IPs scanned	3,684,755,175	(85.79% of IPv4 address space)
Open port 21	21,832,903	(0.59% of scanned IPs)
FTP servers	13,789,641	(63.16% of IPs with port open)
Anonymous FTP servers	1,123,326	(8.15% of responsive FTP servers)

Who has the most anonymous?



AS	IPs advertised	FTP servers	Anonymous FTP servers
AS12824 home.pl S.A.	205,312	136,765 (66.61%)	103,175 (75.44%)
AS46606 Unified Layer	516,864	246,470 (47.69%)	44,273 (17.96%)
AS2914 NTT America, Inc.	7,880,192	298,468 (3.79%)	36,045 (12.08%)
AS20013 CyrusOne LLC	111,360	64,790 (58.18%)	30,772 (47.50%)
AS40676 Psychz Networks	641,024	64,233 (10.02%)	27,507 (42.82%)
AS34011 domainfactory GmbH	93,440	21,153 (22.64%)	19,077 (90.19%)
AS4134 Chinanet	120,757,504	464,384 (0.39%)	18,996 (4.09%)
AS18978 Enzu Inc	727,808	73,541 (10.11%)	17,510 (23.81%)
AS18779 EGIHosting	1,890,304	27,804 (1.43%)	16,329 (58.73%)
AS4766 Korea Telecom	53,733,632	211,479 (0.39%)	16,222 (7.67%)

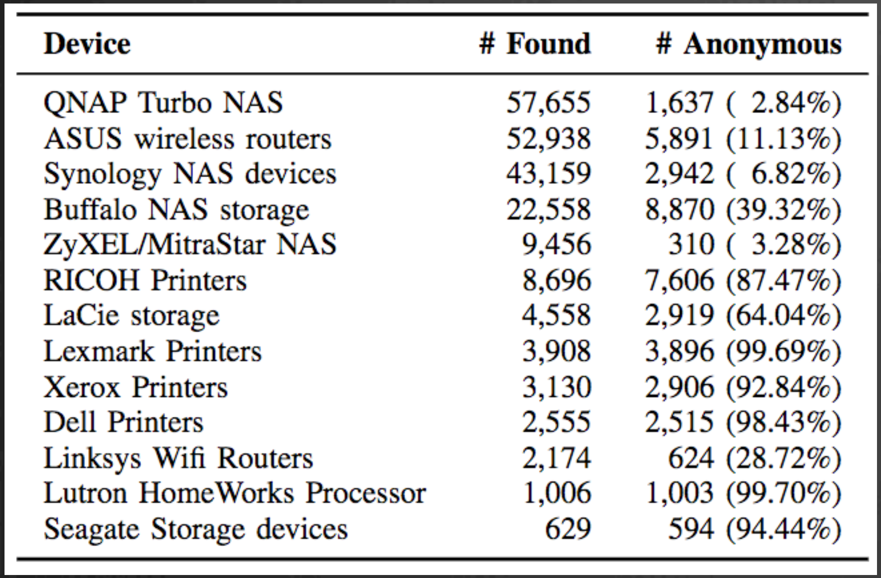
What kind of devices use FTP?



Server Classification	All FTP Servers	Anonymous FTP Servers
Generic Server	5,957,969 (43.21%)	704,276 (62.66%)
Hosted Server	1,795,596 (13.02%)	174,198 (15.50%)
Embedded Server	1,786,656 (12.95%)	93,484 (8.32%)
Unknown	4,249,417 (30.82%)	151,927 (13.52%)

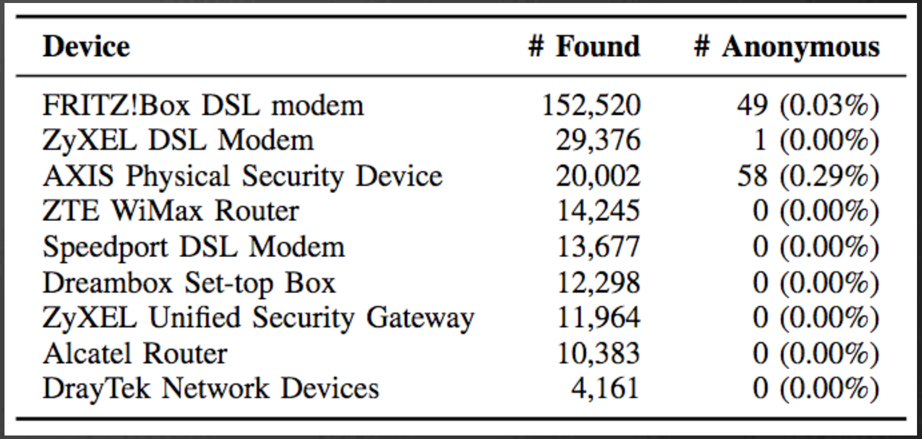
What embedded devices use FTP?

Consumer-deployed



Device	# Found	# Anonymous
QNAP Turbo NAS	57,655	1,637 (2.84%)
ASUS wireless routers	52,938	5,891 (11.13%)
Synology NAS devices	43,159	2,942 (6.82%)
Buffalo NAS storage	22,558	8,870 (39.32%)
ZyXEL/MitraStar NAS	9,456	310 (3.28%)
RICOH Printers	8,696	7,606 (87.47%)
LaCie storage	4,558	2,919 (64.04%)
Lexmark Printers	3,908	3,896 (99.69%)
Xerox Printers	3,130	2,906 (92.84%)
Dell Printers	2,555	2,515 (98.43%)
Linksys Wifi Routers	2,174	624 (28.72%)
Lutron HomeWorks Processor	1,006	1,003 (99.70%)
Seagate Storage devices	629	594 (94.44%)

Provider-deployed



Device	# Found	# Anonymous
FRITZ!Box DSL modem	152,520	49 (0.03%)
ZyXEL DSL Modem	29,376	1 (0.00%)
AXIS Physical Security Device	20,002	58 (0.29%)
ZTE WiMax Router	14,245	0 (0.00%)
Speedport DSL Modem	13,677	0 (0.00%)
Dreambox Set-top Box	12,298	0 (0.00%)
ZyXEL Unified Security Gateway	11,964	0 (0.00%)
Alcatel Router	10,383	0 (0.00%)
DrayTek Network Devices	4,161	0 (0.00%)

- FTP Protocol
- Methodology
- What is the state of FTP in 2015?
- **Is sensitive data being shared on FTP?**
- Is FTP being used by malicious actors?
- What vulnerabilities still exist in FTP?
- Conclusions

Obvious Examples

```
-SSL_certificate_backup/
   |
   |- SSL_certificate.pem
   |- SSL_priv_key.pem
   |- password.txt
```

Non-Obvious Examples

Ambiguous

```
-backup/

   |

   |- June-Dec.der

   |- key4.txt
```

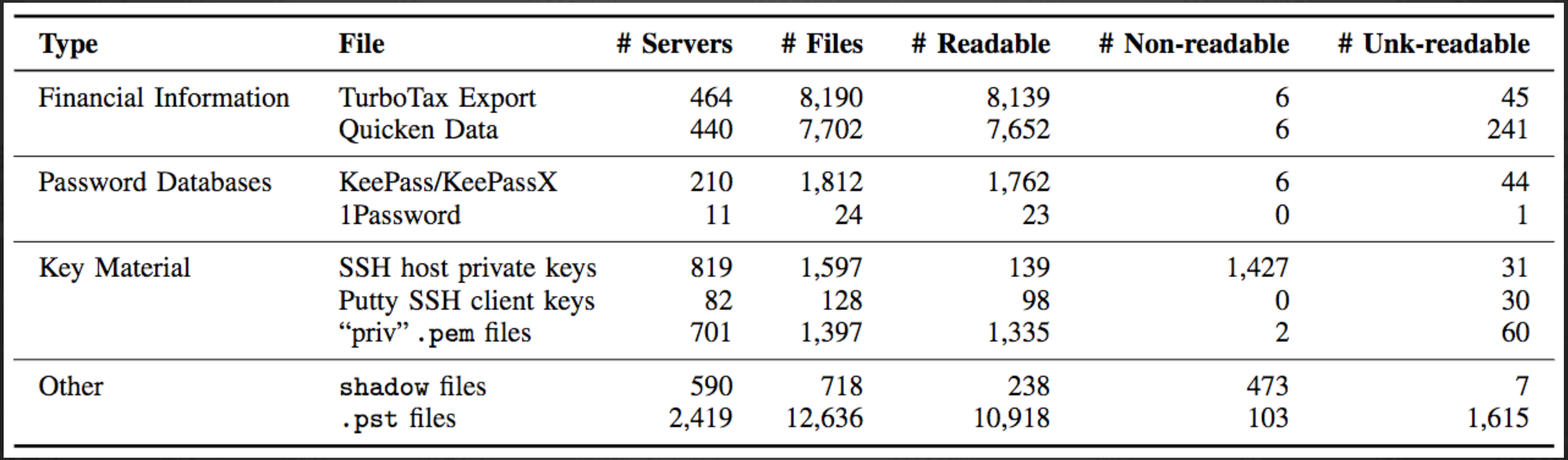
Non-English

```
-備份工作/

   |

   |-公證書.cer

   |-私鑰.pem
```

Difficulties

- Personalized naming
- Mix of languages
- What to look for
- How to measure

What data is being exposed?



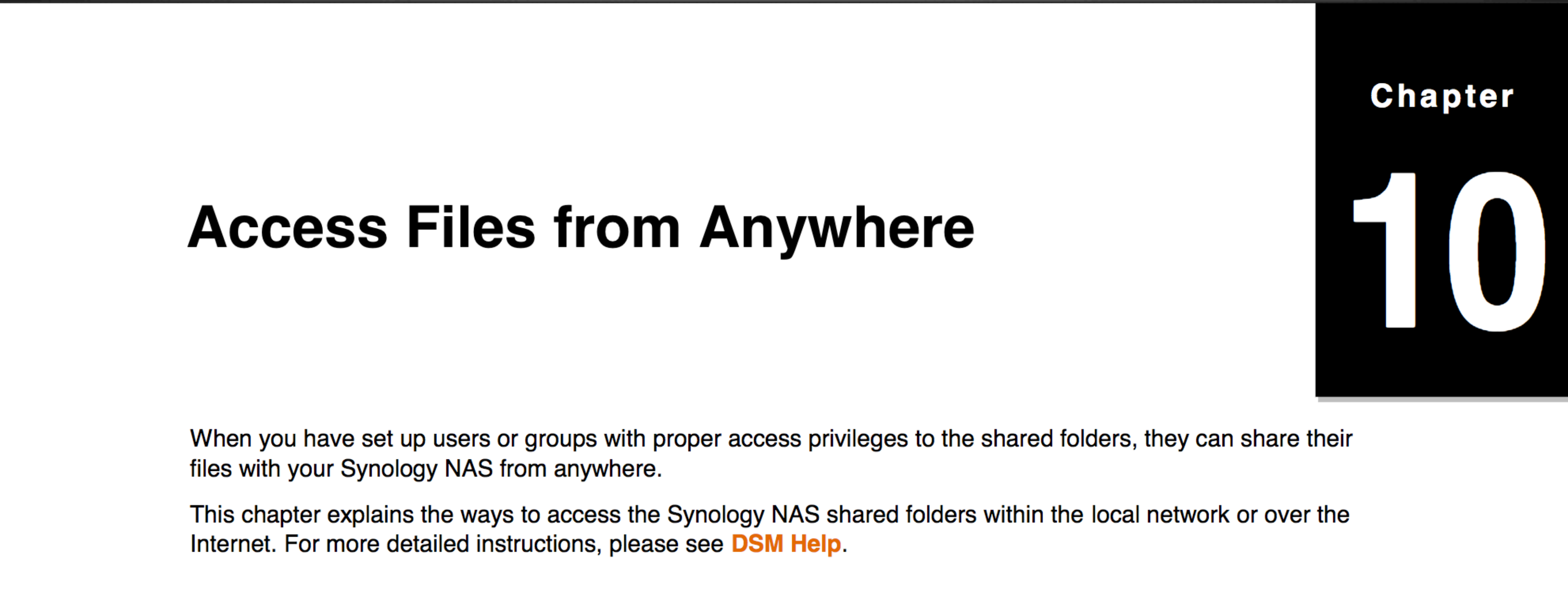
Type	File	# Servers	# Files	# Readable	# Non-readable	# Unk-readable
Financial Information	TurboTax Export	464	8,190	8,139	6	45
	Quicken Data	440	7,702	7,652	6	241
Password Databases	KeePass/KeePassX	210	1,812	1,762	6	44
	1Password	11	24	23	0	1
Key Material	SSH host private keys	819	1,597	139	1,427	31
	Putty SSH client keys	82	128	98	0	30
	"priv" `.pem` files	701	1,397	1,335	2	60
Other	`shadow` files	590	718	238	473	7
	`.pst` files	2,419	12,636	10,918	103	1,615

Irresponsible Devices

Wireless Routers

NAS Systems

Responsible Devices



Chapter 10

Access Files from Anywhere

When you have set up users or groups with proper access privileges to the shared folders, they can share their files with your Synology NAS from anywhere.

This chapter explains the ways to access the Synology NAS shared folders within the local network or over the Internet. For more detailed instructions, please see **DSM Help**.

- FTP Protocol
- Methodology
- What is the state of FTP in 2015?
- Is sensitive data being shared on FTP?
- **Is FTP being used by malicious actors?**
- What vulnerabilities still exist in FTP?
- Conclusions

World-Writable FTP

- Anonymous user can upload file
- Indicated by presence of a known file
  - w0000000t.[txt/php], sjutd.txt, hello.world.txt
- 19.4K world-writable server (lower bound)

Server-side Scripting

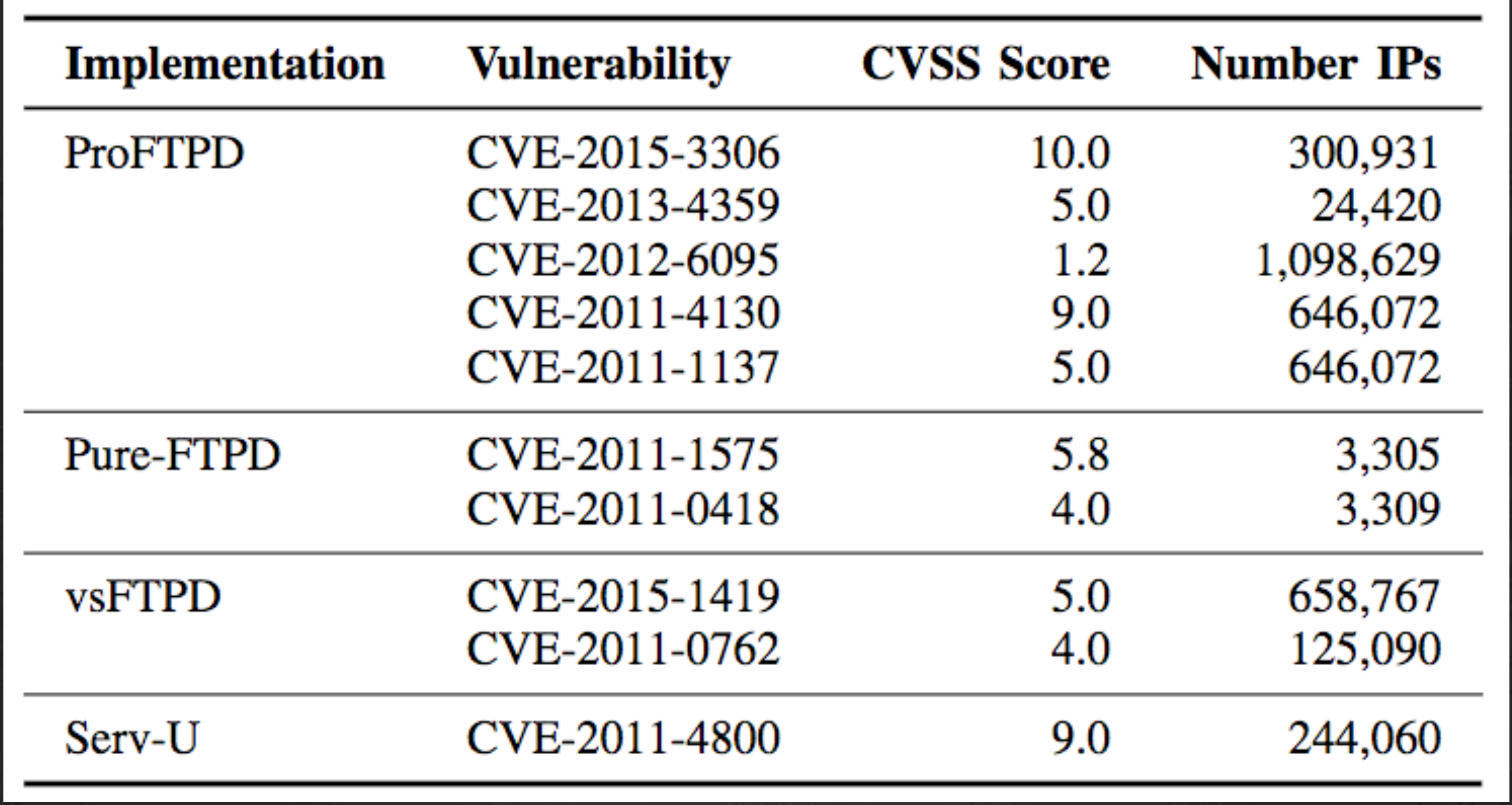
- 9M IPs have both FTP and HTTP server
  - 2.1M explicitly indicate PHP/ASP.NET engine
- Remote Access Tools
  - 724 servers
- UDP DDoS infrastructure
  - 1,792 servers
- `ftpchk3` multi-stage campaign
  - 1,264 servers

Other Assorted Campaigns

- ``really cool software cracking'' advertisement
  - 2,095 servers
- Candy-dropping malware
- WaReZ
  - [year][month][day][time]p/
  - 4,868 servers

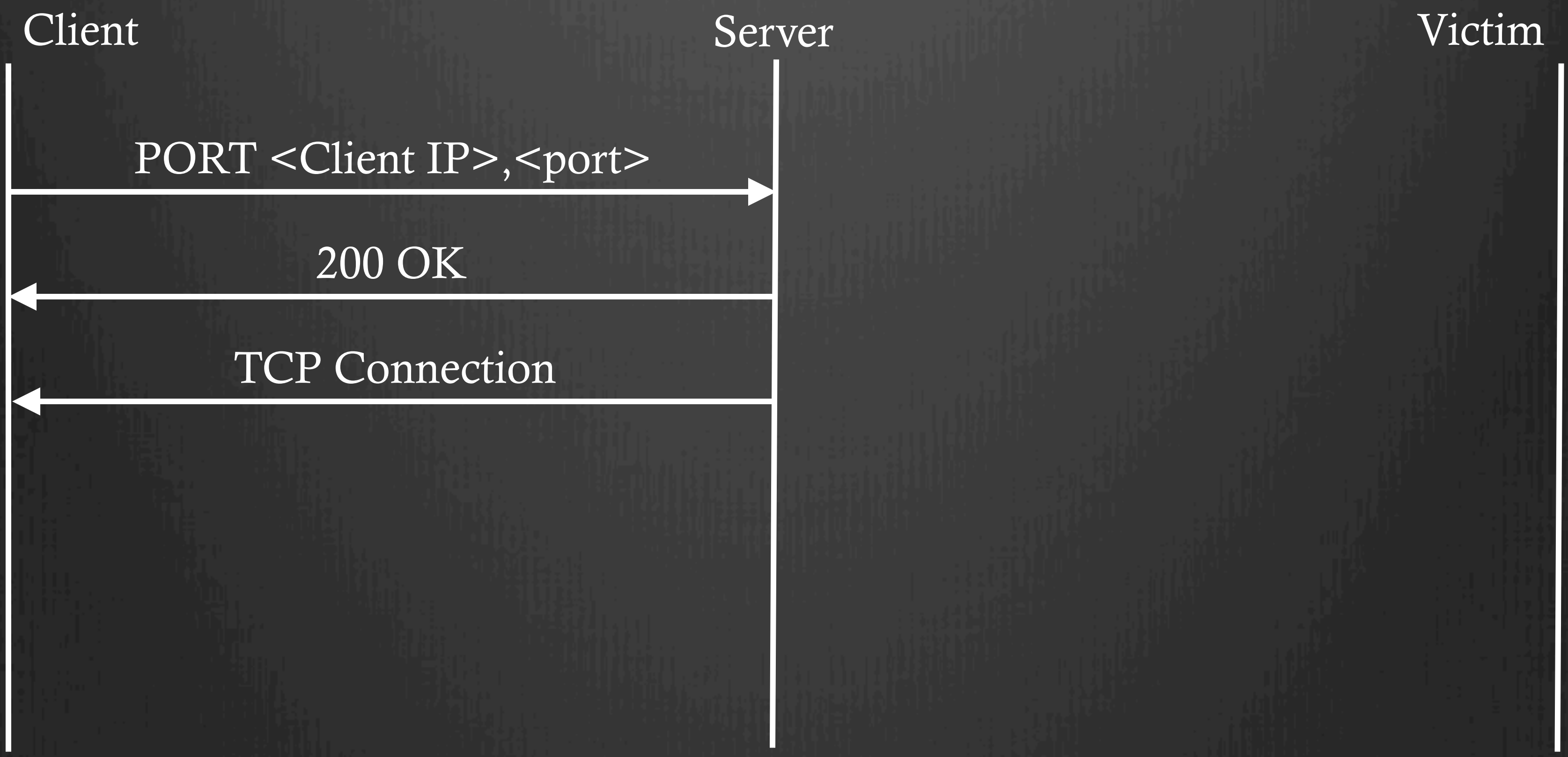
- FTP Protocol
- Methodology
- What is the state of FTP in 2015?
- Is sensitive data being shared on FTP?
- Is FTP being used by malicious actors?
- **What vulnerabilities still exist in FTP?**
- Conclusions

CVEs

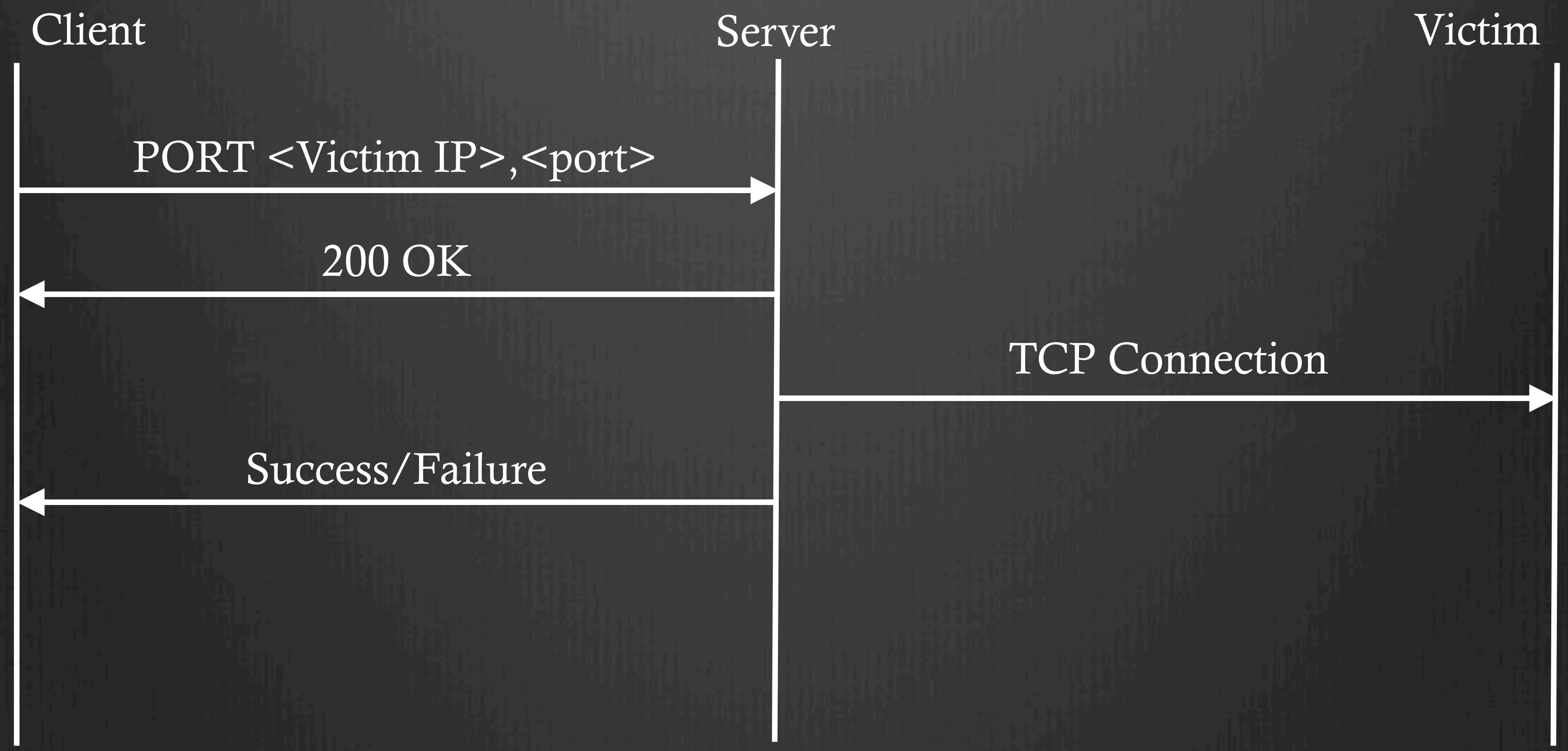


Implementation	Vulnerability	CVSS Score	Number IPs
ProFTPD	CVE-2015-3306	10.0	300,931
	CVE-2013-4359	5.0	24,420
	CVE-2012-6095	1.2	1,098,629
	CVE-2011-4130	9.0	646,072
	CVE-2011-1137	5.0	646,072
Pure-FTPD	CVE-2011-1575	5.8	3,305
	CVE-2011-0418	4.0	3,309
vsFTPD	CVE-2015-1419	5.0	658,767
	CVE-2011-0762	4.0	125,090
Serv-U	CVE-2011-4800	9.0	244,060

PORT Bounce

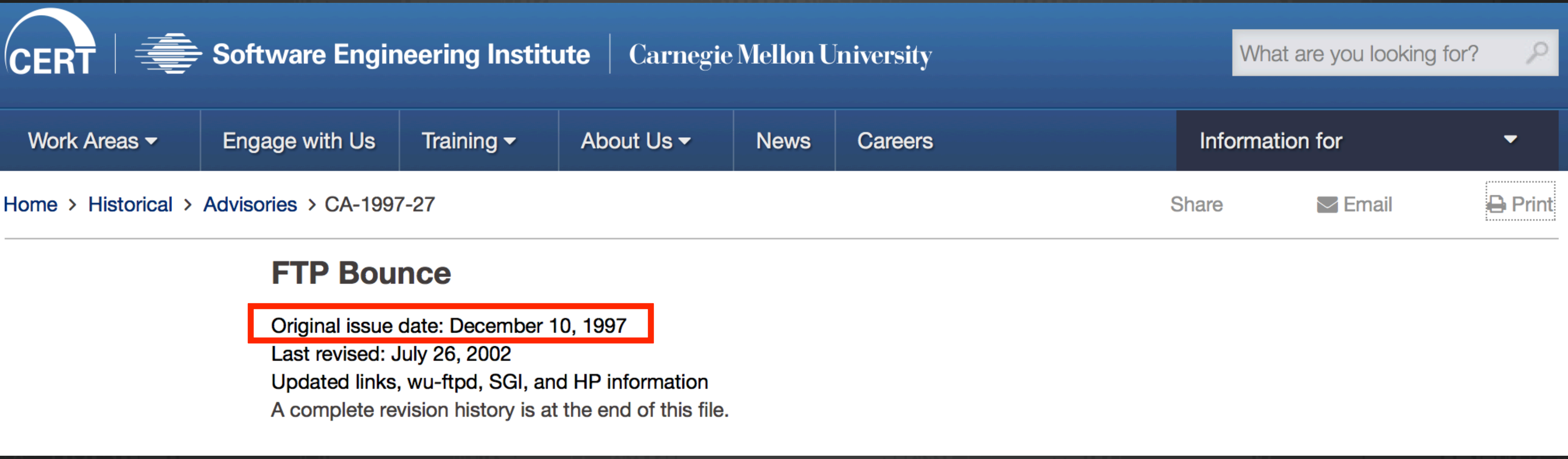


PORT Bounce


Client
Server
Victim
PORT <Victim IP>,<port>
200 OK
TCP Connection
Success/Failure

PORT Bounce

- 143K servers vulnerable
  - Including inside NAT/Firewall


CERT
Software Engineering Institute
Carnegie Mellon University
What are you looking for?
Work Areas
Engage with Us
Training
About Us
News
Careers
Information for
Home > Historical > Advisories > CA-1997-27
Share
Email
Print

FTP Bounce

Original issue date: December 10, 1997
Last revised: July 26, 2002
Updated links, wu-ftpd, SGI, and HP information
A complete revision history is at the end of this file.

- ◆ FTP Protocol
- ◆ Methodology
- ◆ What is the state of FTP in 2015?
- ◆ Is sensitive data being shared on FTP?
- ◆ Is FTP being used by malicious actors?
- ◆ What vulnerabilities still exist in FTP?
- ◆ **Conclusions**

Conclusions

- Documentation and interfaces for consumer products need re-evaluation
- Malicious actors are aware of and actively exploiting FTP access
- FTP is still around, still exposes information, and still puts users at risk

FTP: The Forgotten Cloud

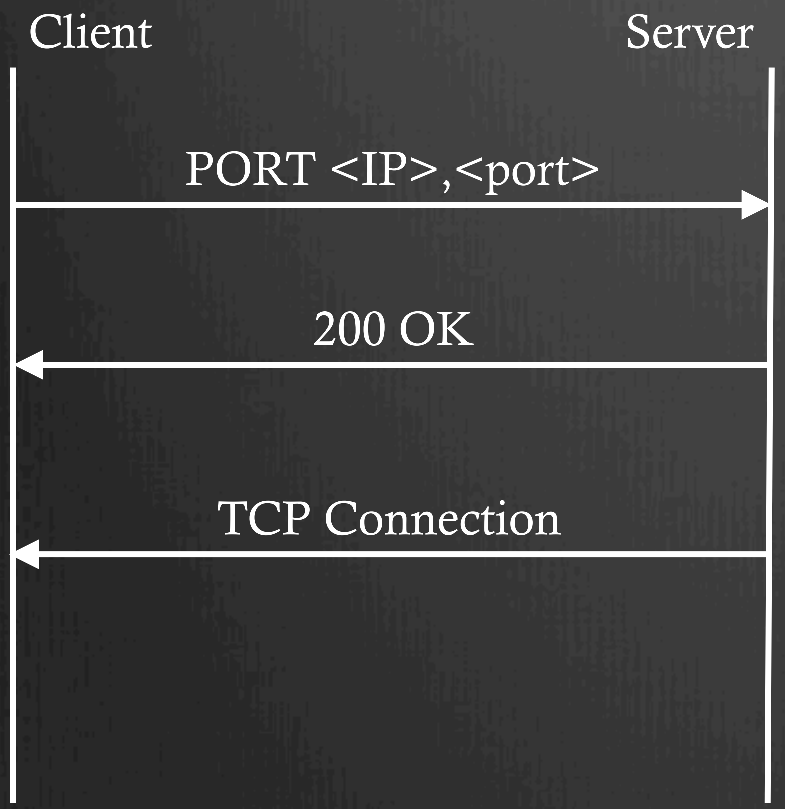
Drew Springall, Zakir Durumeric, and J. Alex Halderman
University of Michigan

STOP

STOP

Data Transfer

Active



Client

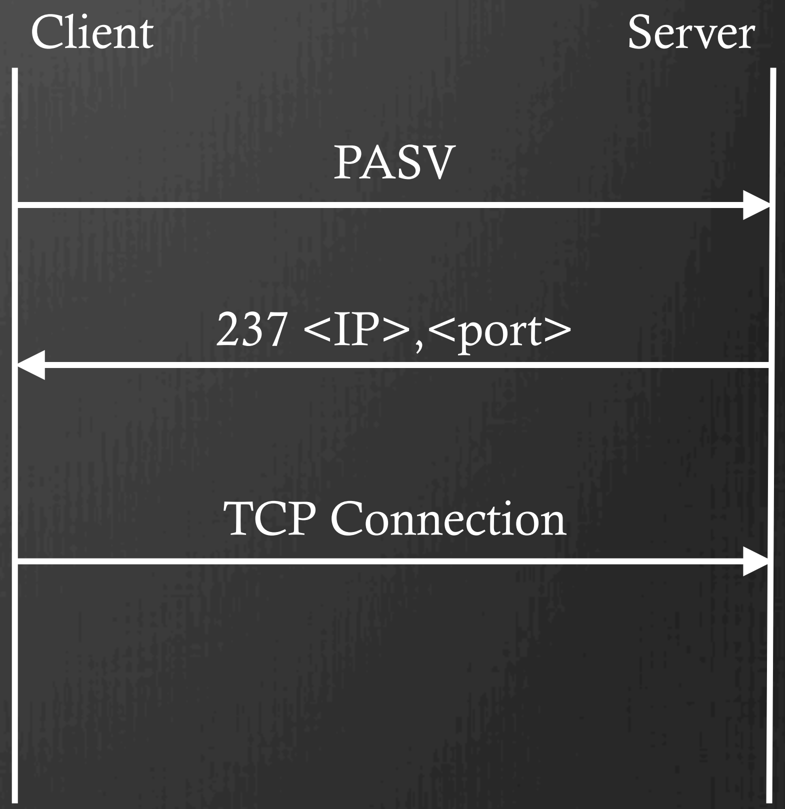
Server

PORT <IP>,<port>

200 OK

TCP Connection

Passive



Client

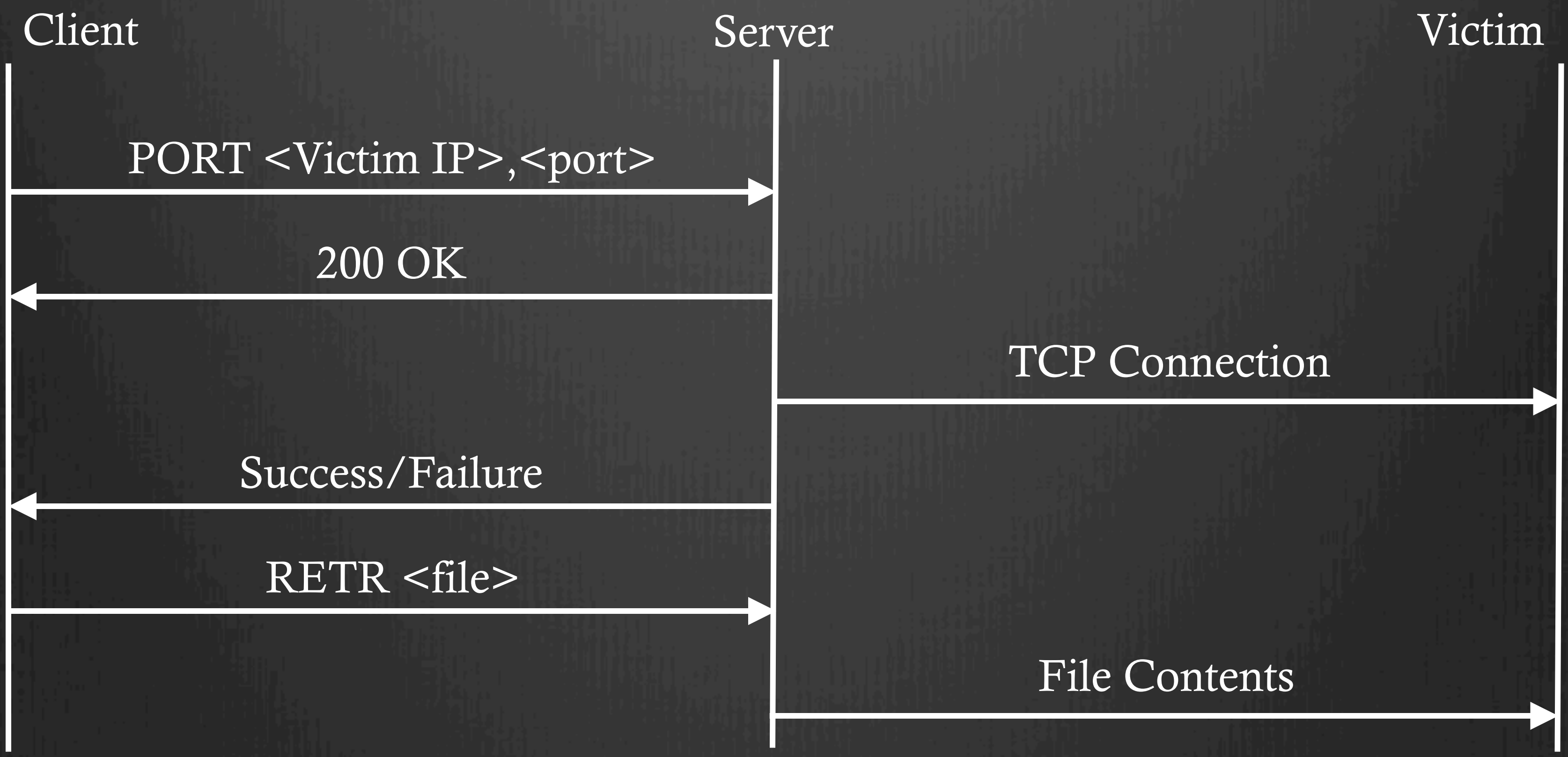
Server

PASV

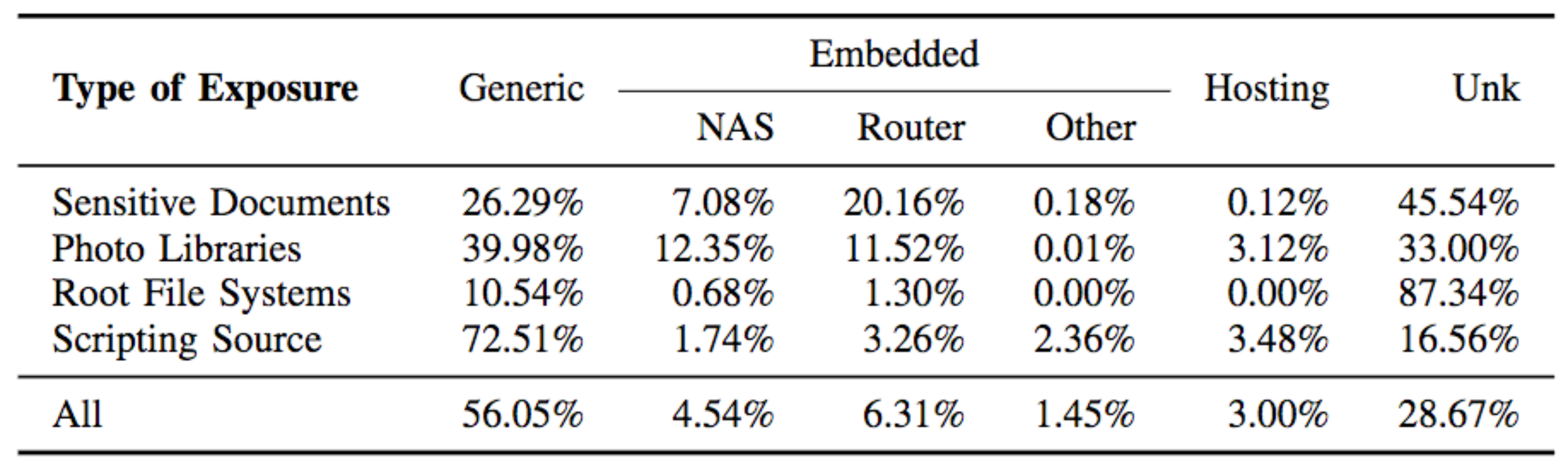
237 <IP>,<port>

TCP Connection

PORT Bounce

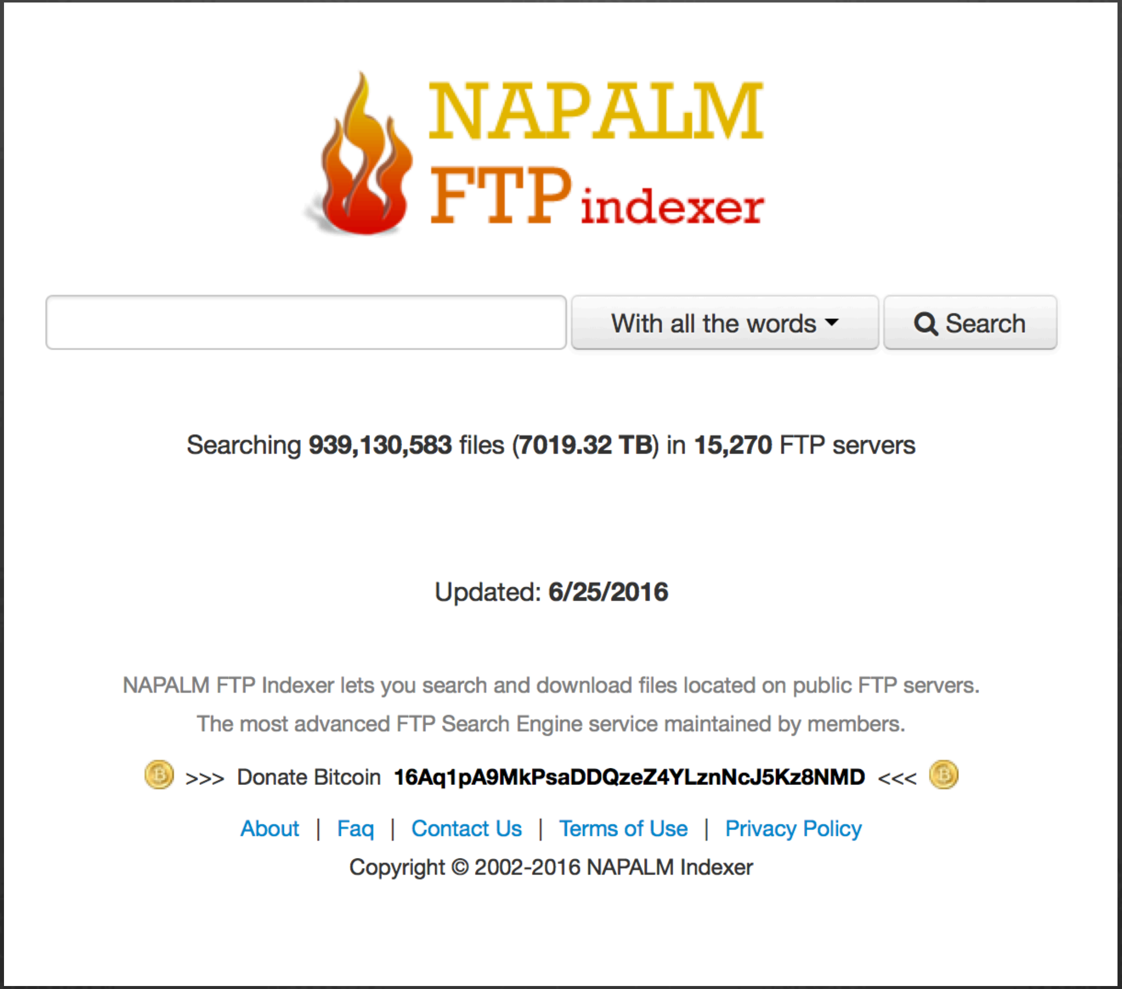

Client
Server
Victim
PORT <Victim IP>,<port>
200 OK
TCP Connection
Success/Failure
RETR <file>
File Contents

Responsible Devices



Type of Exposure	Generic	Embedded			Hosting	Unk
		NAS	Router	Other		
Sensitive Documents	26.29%	7.08%	20.16%	0.18%	0.12%	45.54%
Photo Libraries	39.98%	12.35%	11.52%	0.01%	3.12%	33.00%
Root File Systems	10.54%	0.68%	1.30%	0.00%	0.00%	87.34%
Scripting Source	72.51%	1.74%	3.26%	2.36%	3.48%	16.56%
All	56.05%	4.54%	6.31%	1.45%	3.00%	28.67%

Non-Academic Enumeration



NAPALM FTP indexer

Searching **939,130,583** files (**7019.32 TB**) in **15,270** FTP servers

Updated: **6/25/2016**

NAPALM FTP Indexer lets you search and download files located on public FTP servers.
The most advanced FTP Search Engine service maintained by members.

>>> Donate Bitcoin **16Aq1pA9MkPsaDDQzeZ4YLznNcJ5Kz8NMD** <<<

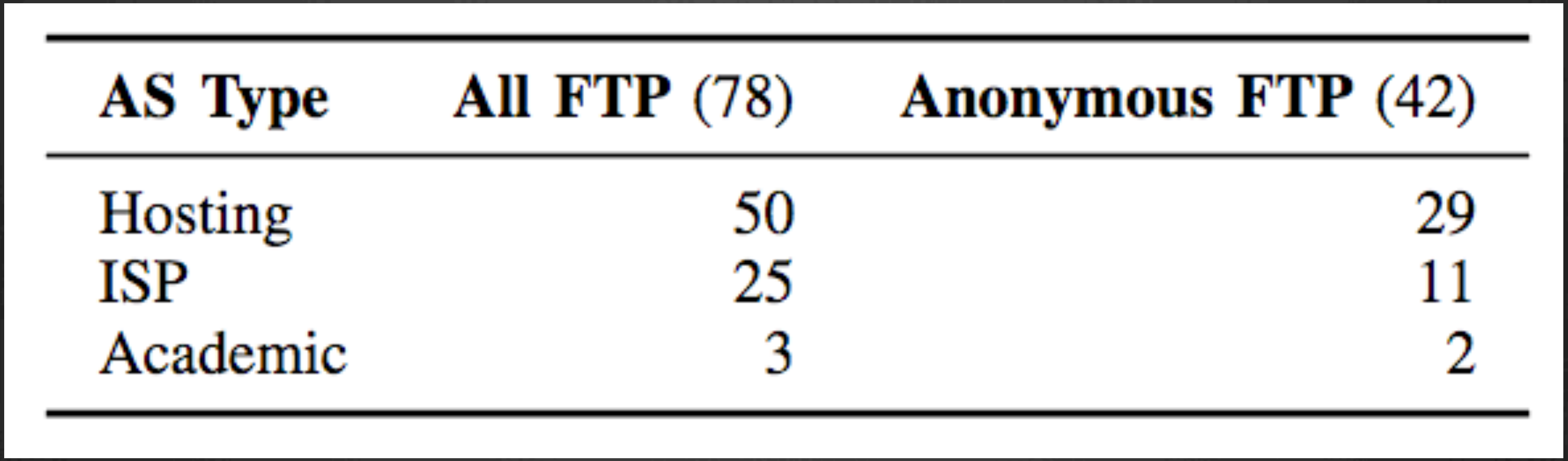
About | Faq | Contact Us | Terms of Use | Privacy Policy

Copyright © 2002-2016 NAPALM Indexer

FTPS

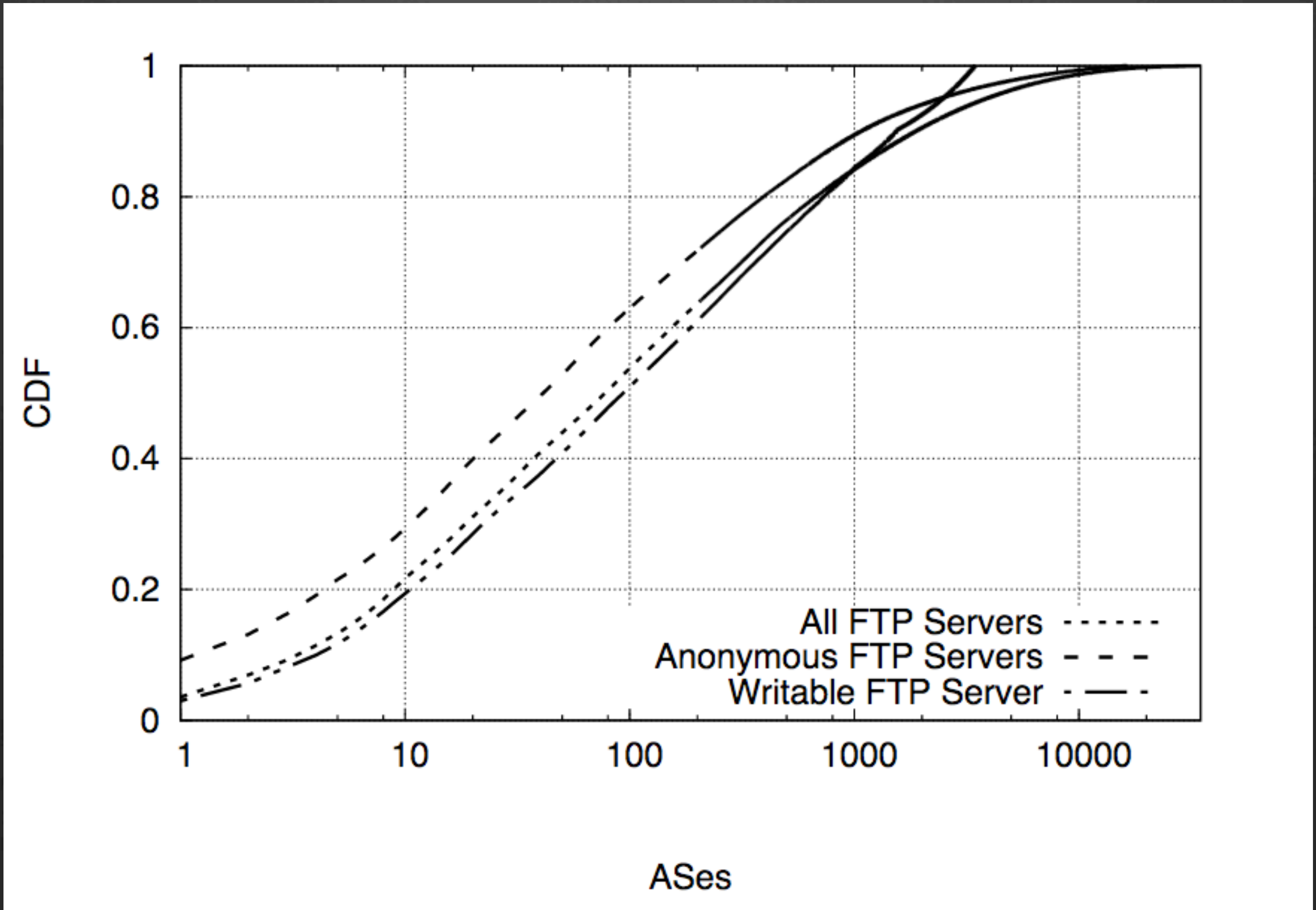
- STARTTLS-like encapsulation
- AUTH SSL or AUTH TLS command
- Control channel and Data channel

Classifying AS



AS Type	All FTP (78)	Anonymous FTP (42)
Hosting	50	29
ISP	25	11
Academic	3	2

AS Distribution



STOP #2

Seriously though…

STOP

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu