UNC CHARLOTTE
College of Computing and Informatics

# Developing Methods to Infiltrate Samba Servers and Replace Legitimate Data with Malware

Mukund Ramakrishnan
REU Research Fellow
Rutgers University

Md Rabbi Alam
Doctoral Student Mentor
UNC Charlotte

Dr. Jinpeng Wei
Associate Professor
UNC Charlotte

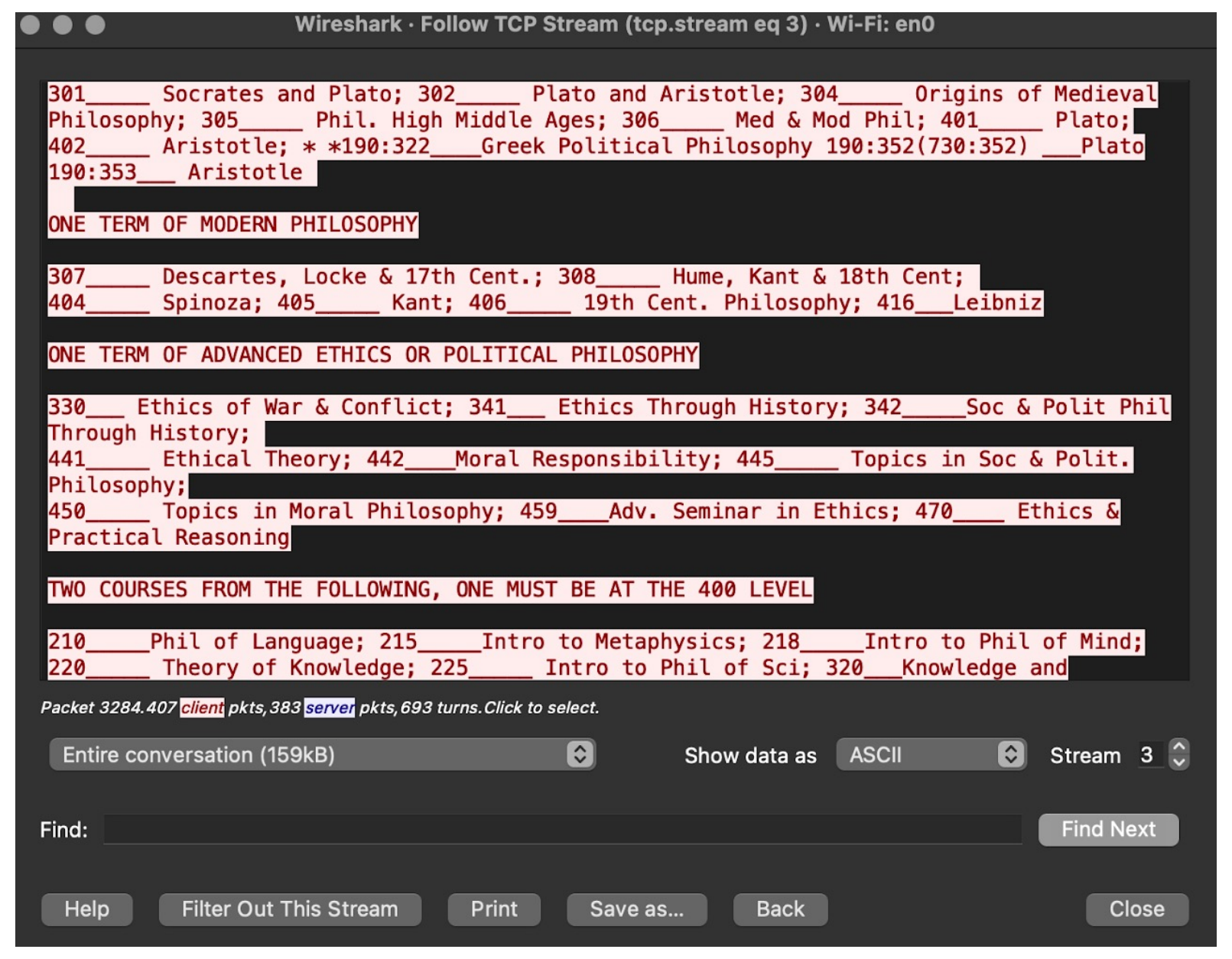
UNC CHARLOTTE
College of Computing and Informatics

## Introduction

- Samba is a widely-used networking protocol that allows computers on a local-area network to send and receive files with each other.
- Our study aims to determine if the Samba protocol is secure for file transfer on an infrastructure network.
- Our study also aims to fabricate packets similar to legitimate packets sent to a Samba server, and "trick" the server into receiving our illegitimate packets.
- Inter-process communications, or IPCs, often take place between system processes during a file transfer. Our study aims to evaluate the extent to which these communications are secure.
- macOS creates separate system user accounts for disparate system processes. This enhances the security of file transfers.
- Windows uses a more traditional pipe system for inter-process communications. This may make the system easier to exploit.

## Method

Packet capture utilities such as Wireshark and IO Monitor were used to isolate packets being transferred.


Wireshark · Follow TCP Stream (tcp.stream eq 3) · Wi-Fi: en0

```
301_____ Socrates and Plato; 302_____ Plato and Aristotle; 304_____ Origins of Medieval
Philosophy; 305_____ Phil. High Middle Ages; 306_____ Med & Mod Phil; 401_____ Plato;
402_____ Aristotle; * *190:322____Greek Political Philosophy 190:352(730:352) ___Plato
190:353___ Aristotle

ONE TERM OF MODERN PHILOSOPHY

307_____ Descartes, Locke & 17th Cent.; 308_____ Hume, Kant & 18th Cent;
404_____ Spinoza; 405_____ Kant; 406_____ 19th Cent. Philosophy; 416___Leibniz

ONE TERM OF ADVANCED ETHICS OR POLITICAL PHILOSOPHY

330___ Ethics of War & Conflict; 341___ Ethics Through History; 342_____Soc & Polit Phil
Through History;
441_____ Ethical Theory; 442____Moral Responsibility; 445_____ Topics in Soc & Polit.
Philosophy;
450_____ Topics in Moral Philosophy; 459____Adv. Seminar in Ethics; 470____ Ethics &
Practical Reasoning

TWO COURSES FROM THE FOLLOWING, ONE MUST BE AT THE 400 LEVEL

210_____Phil of Language; 215_____Intro to Metaphysics; 218_____Intro to Phil of Mind;
220_____ Theory of Knowledge; 225_____ Intro to Phil of Sci; 320___Knowledge and
```

Packet 3284. 407 client pkts, 383 server pkts, 693 turns. Click to select.

Entire conversation (159kB) | Show data as: ASCII | Stream: 3

*Figure B.* Unencrypted data being transferred from the Mac to the Time Capsule (sniffed by Wireshark).

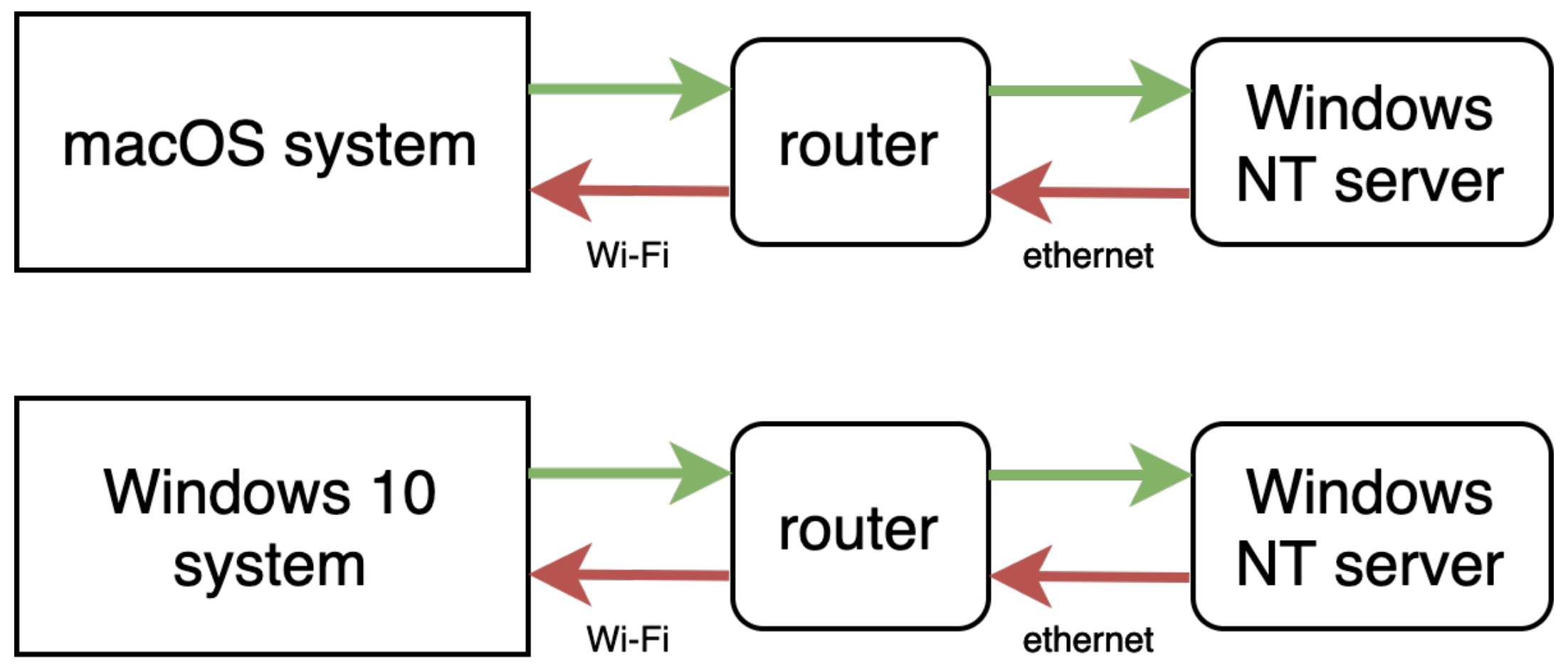
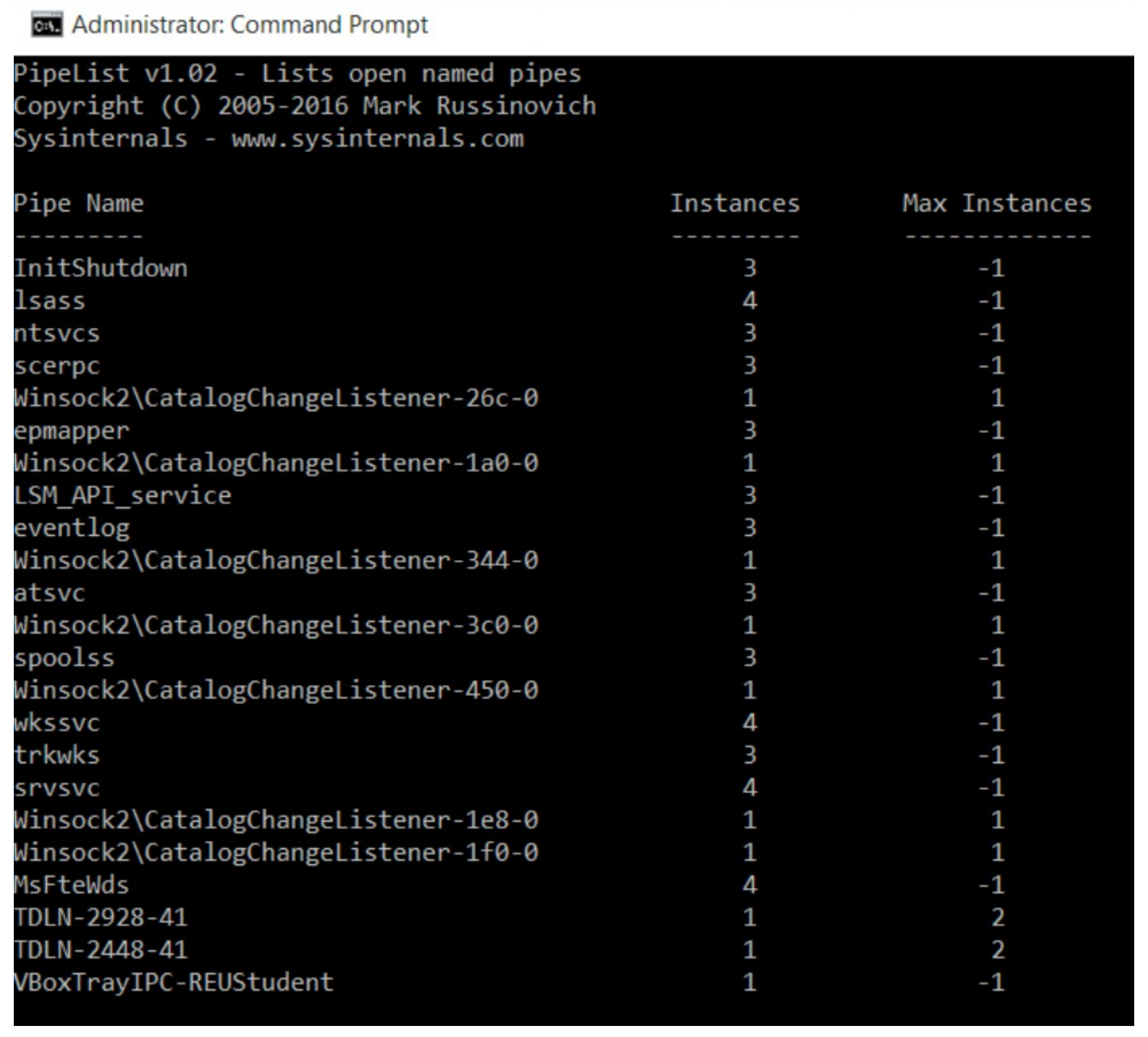


*Figure C.* Details of the testbed.

## Objectives

We aim to discover a way to infiltrate a Samba server and insert data of our choosing without knowing the authentication data of the server, such as a username or password. We also aim to understand the inter-process communication involved when a Samba file transfer takes place (such as pipes used in Windows to carry out a file transfer), which can then be exploited to transport malware.

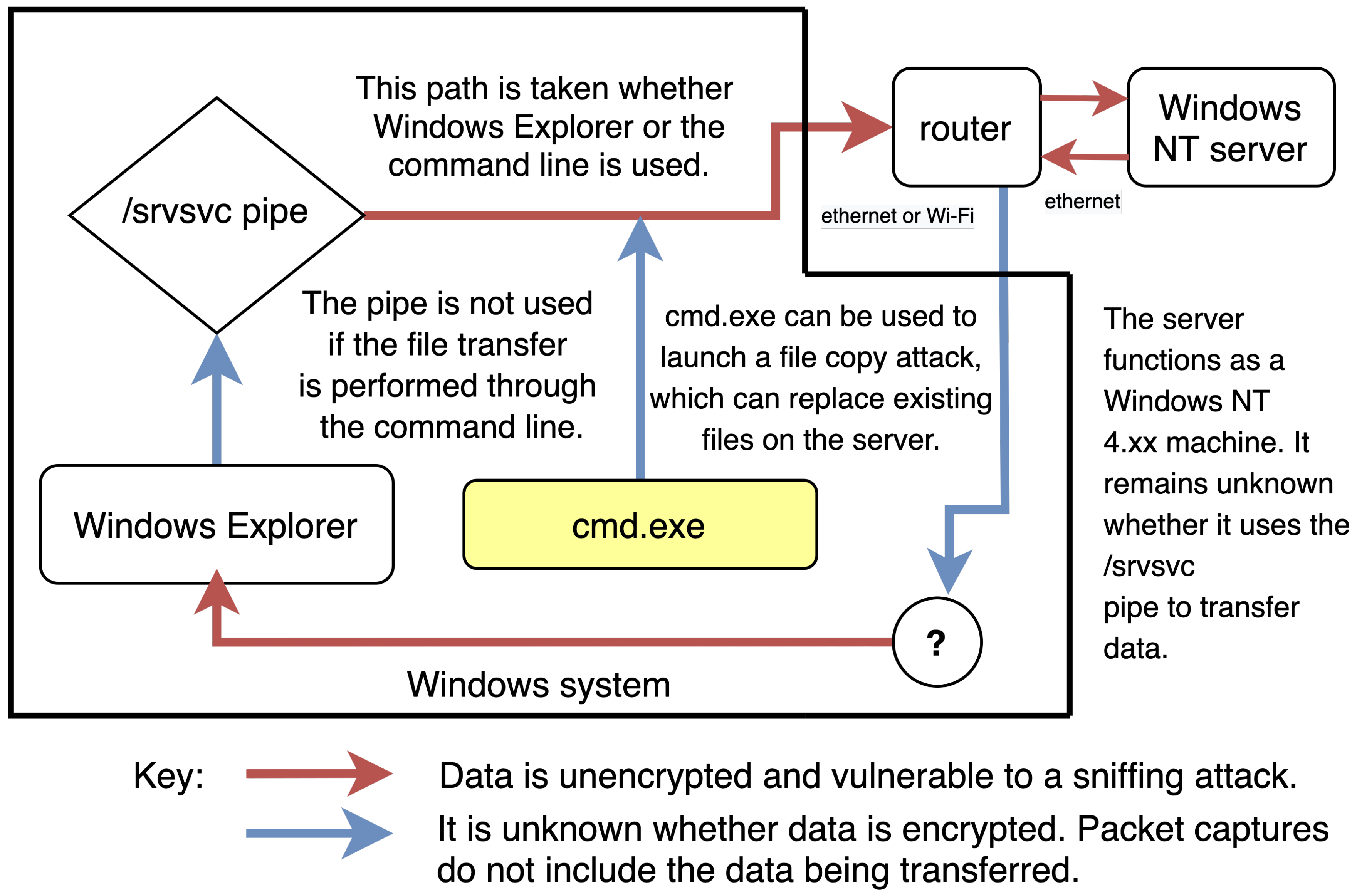


```
PipeList v1.02 - Lists open named pipes
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Pipe Name                                          Instances       Max Instances
---------                                          ---------       -------------
InitShutdown                                           3                -1
lsass                                                  4                -1
ntsvcs                                                 3                -1
scerpc                                                 3                -1
Winsock2\CatalogChangeListener-26c-0                   1                 1
epmapper                                               3                -1
Winsock2\CatalogChangeListener-1a0-0                   1                 1
LSM_API_service                                        3                -1
eventlog                                               3                -1
Winsock2\CatalogChangeListener-344-0                   1                 1
atsvc                                                  3                -1
Winsock2\CatalogChangeListener-3c0-0                   1                 1
spoolss                                                3                -1
Winsock2\CatalogChangeListener-450-0                   1                 1
wkssvc                                                 4                -1
trkwks                                                 3                -1
srvsvc                                                 4                -1
Winsock2\CatalogChangeListener-1e8-0                   1                 1
Winsock2\CatalogChangeListener-1f0-0                   1                 1
MsFteWds                                               4                -1
TDLN-2928-41                                           1                 2
TDLN-2448-41                                           1                 2
VBoxTrayIPC-REUStudent                                 1                -1
```

*Figure A.* The pipes that are open during a Samba file transfer on Windows 10.

## Results



This path is taken whether Windows Explorer or the command line is used.

The pipe is not used if the file transfer is performed through the command line.

cmd.exe can be used to launch a file copy attack, which can replace existing files on the server.

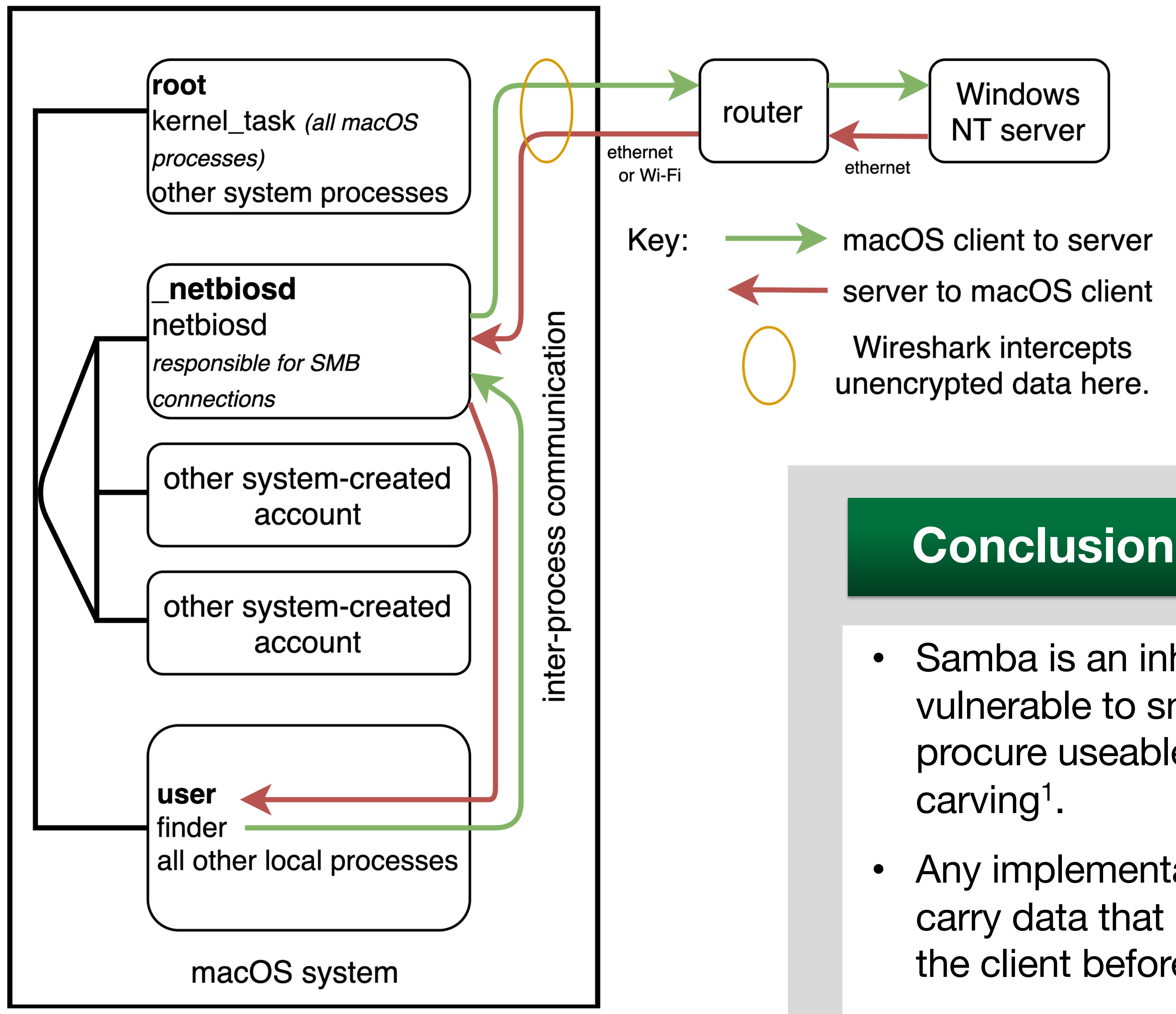
The server functions as a Windows NT 4.xx machine. It remains unknown whether it uses the /srvsvc pipe to transfer data.

Data is unencrypted and vulnerable to a sniffing attack.

It is unknown whether data is encrypted. Packet captures do not include the data being transferred.

The copy command, when executed through the Windows command line, can replace files on the server with data of our choosing. This is a gaping vulnerability in the Windows file transfer procedure – cmd.exe does not use the /srvsvc pipe, as observed in Pipe Monitor, whereas it is used when the Samba file transfer is completed through Windows Explorer.

*Figure E.* The process by which data is transferred through Samba on a Windows machine. Note that regardless of the method of data transfer, or whether the transfer takes place from the client to the server or the server to the client, there exists at least one point where a sniffing attack would be successful.


root
kernel_task (all macOS processes)
other system processes
_netbiosd
netbiosd
responsible for SMB connections
other system-created account
other system-created account
user
finder
all other local processes
macOS system
inter-process communication
router
Windows NT server
ethernet or Wi-Fi
ethernet
Key:
macOS client to server
server to macOS client
Wireshark intercepts unencrypted data here.

Transferring data through Samba on macOS is more secure than on Windows, as macOS creates separate user accounts which isolate the processes responsible for a given task (such as file transfer). Even with root access to the system, these processes cannot be sniffed.

*Figure D.* macOS uses the principle of least privilege[2] to assign processes to system-created accounts.

## Conclusions and Future Work

- Samba is an inherently insecure protocol vulnerable to sniffing attacks, which can procure useable data through packet carving[1].
- Any implementation of Samba must only carry data that is already encrypted by the client before being sent.
- In some operating systems such as Windows, inter-process communications can be intercepted as well.

Further work will focus on exploiting the unencrypted Windows pipe data transfer in order to send illegitimate data through the pipe, and thus to the server.

## References

1. Richard R, et. al. "Packet Carving with SMB and SMB2: Chris Sanders." *Chris Sanders | Information Security Analyst, Author, and Instructor*, 17 Dec. 2011, chrissanders.org/2011/11/packet-carving-with-smb-and-smb2/.

2. Gegick, Michael et. al. "Least Privilege." *US Cybersecurity and Infrastructure Security Agency*, United States Computer Emergency Readiness Team, 14 Sept. 2005, us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege.

This project was made possible through funding from the National Science Foundation. Thank you Professors Jinpeng Wei, David Wilson, and Katie Dunn, as well as doctoral students Md Rabbi Alam and Trevon Williams, and the faculty of UNC Charlotte for your guidance and support.