ShadowMove: A Stealthy Lateral Movement Strategy

Amirreza Niakanlahiji, University of Illinois Springfield

Jinpeng Wei, UNC Charlotte

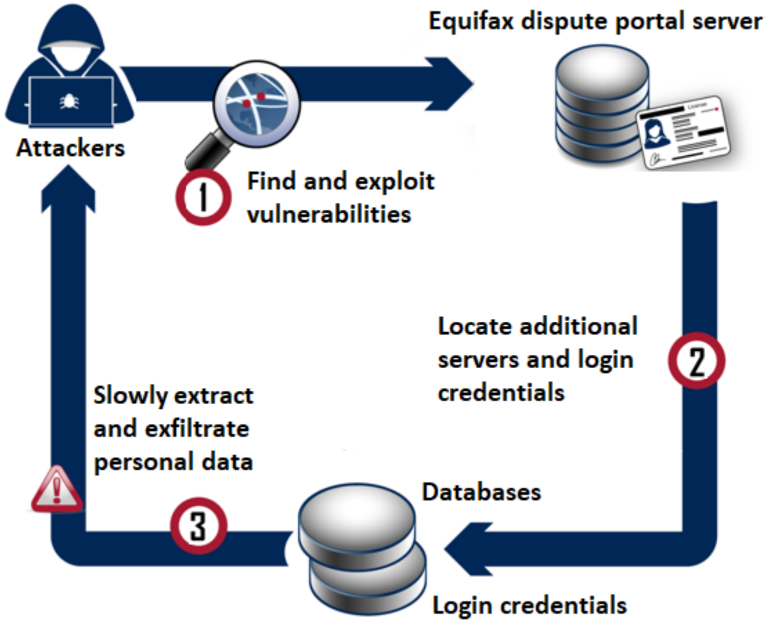
Md Rabbi Alam, UNC Charlotte

Qingyang Wang, Louisiana State University

Bei-Tseng Chu, UNC Charlotte

Lateral Movement Techniques

- Advanced Persistent Threat (APT) attackers use various lateral movement techniques
- Real world example: Equifax breach
- Features of lateral movement during APT attacks
  - Find a foothold within target networks
  - Use the compromised systems as stepping stones to reach critical systems



* Based on ZDNet article (https://zd.net/32Aqfol)

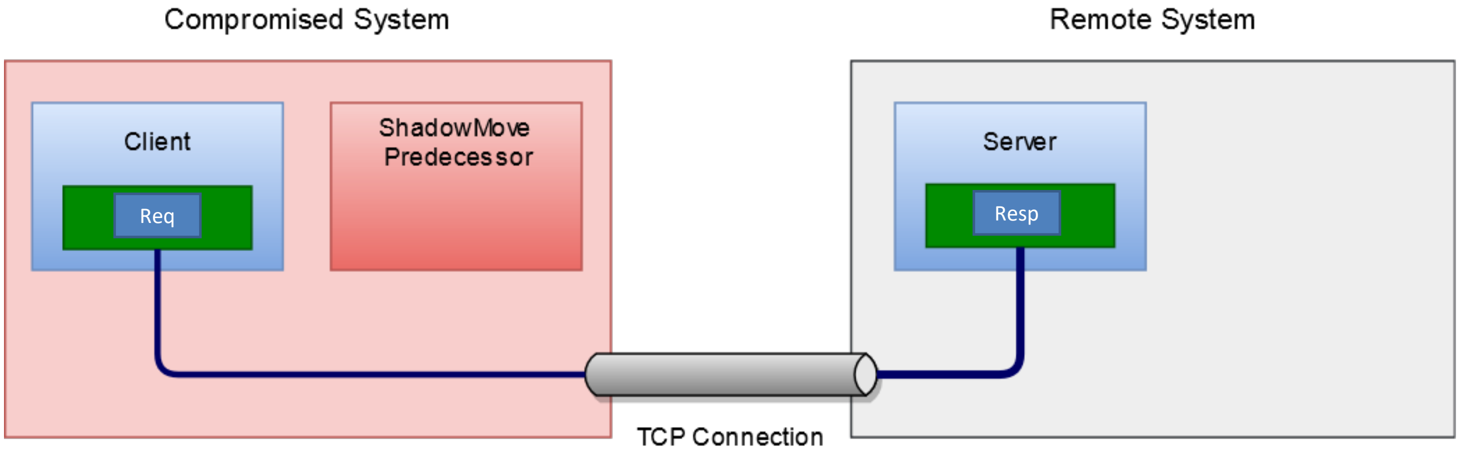
Existing Lateral Movement Techniques

Techniques	Limitations
Exploit vulnerabilities in network services	Increasingly hard due to advances in defense mechanisms
Harvest and abuse user credentials (e.g., passwords by Equifax breach)	Requires new network connections, which can be detected as anomaly
Inject application- and protocol-specific code into legitimate clients to reuse thier connections	Complex and can be detected by existing defensive solutions (e.g., Windows Defender ATP)

Novelty of ShadowMove Attacks

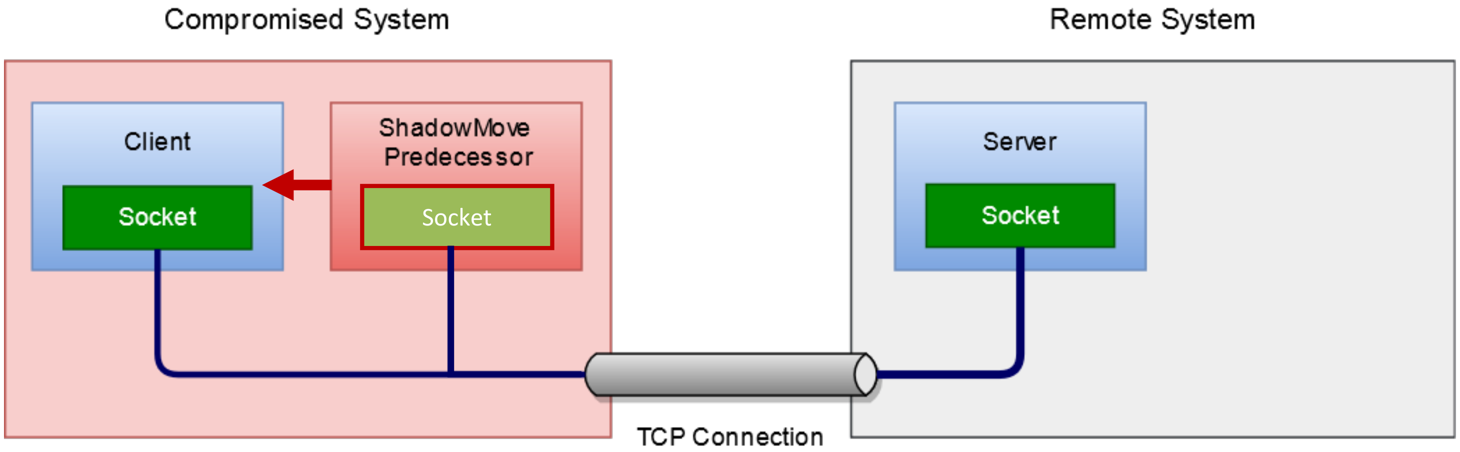
- No new connection, no extra authentication: the attack process secretly reuses authenticated connections and injects commands through such connections
- No privilege elevation: the attack is against client processes run by normal users
- No process injection (on Windows): the attack process secretly duplicates sockets owned by legitimate client processes without injecting code
- Application agnostic: No prior knowledge about the target process is needed

Overview



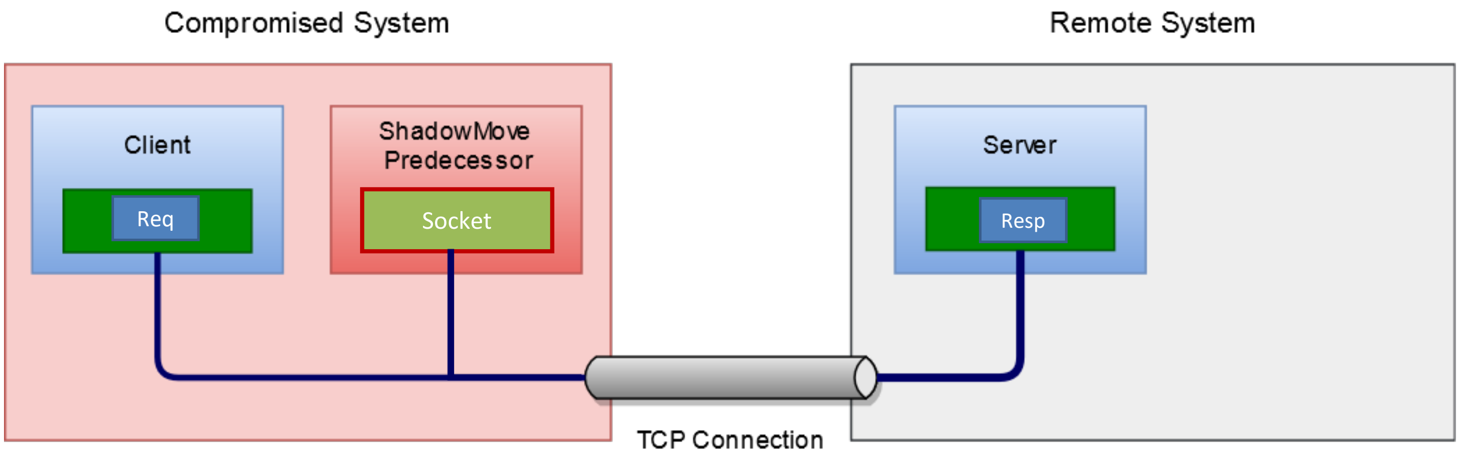
Client sends a request to the remote server
Client receives the response from the server

Overview



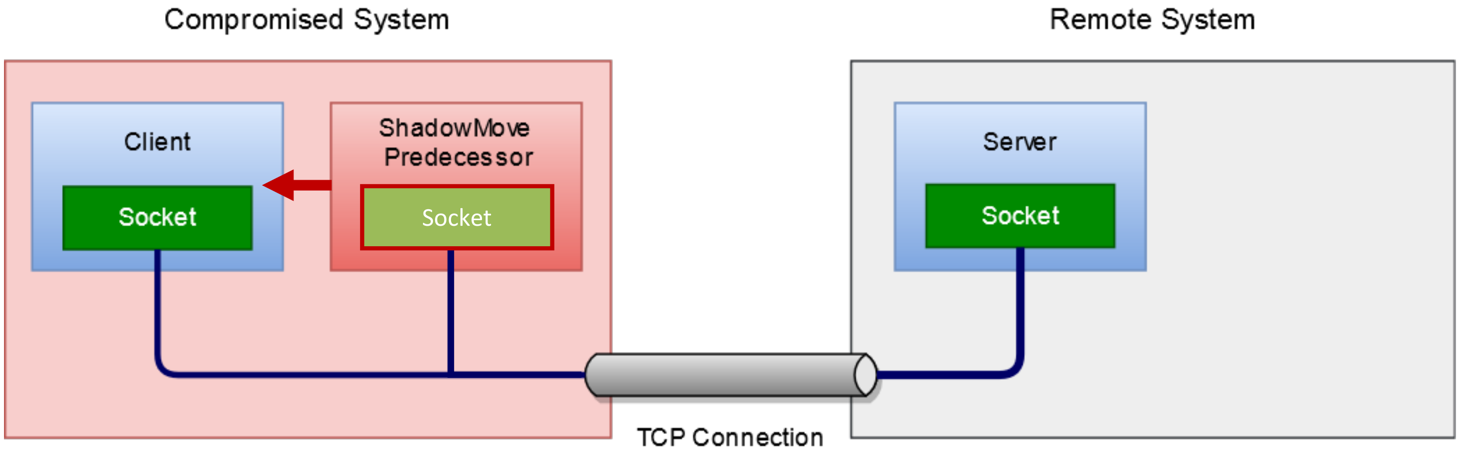
ShadowMove duplicates the socket created by the client

Overview



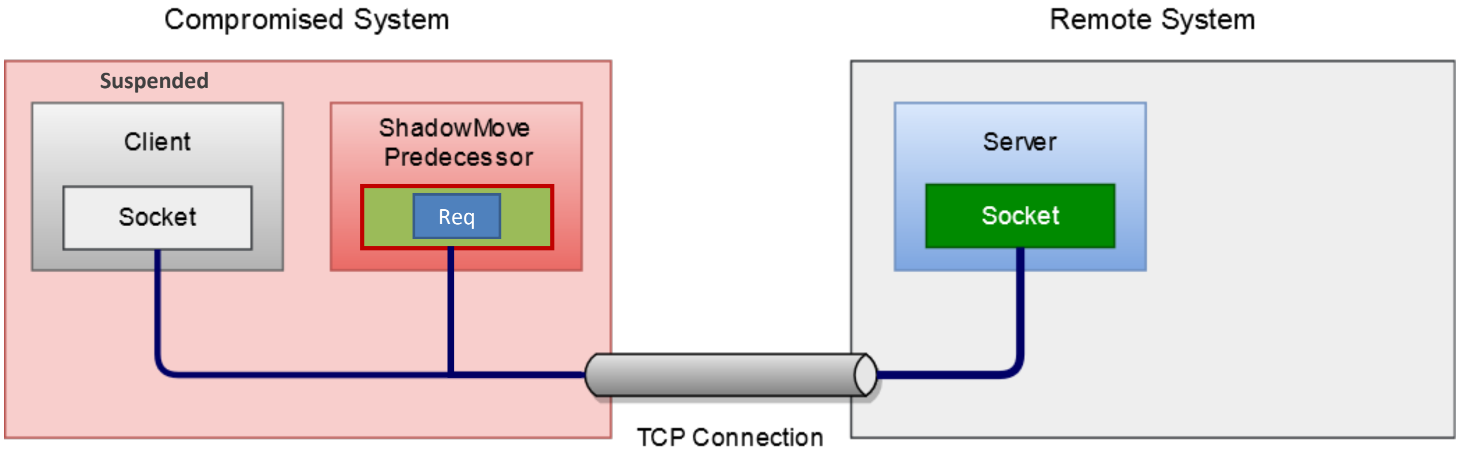
ShadowMove sniffs responses by peeking from the duplicated socket

Overview



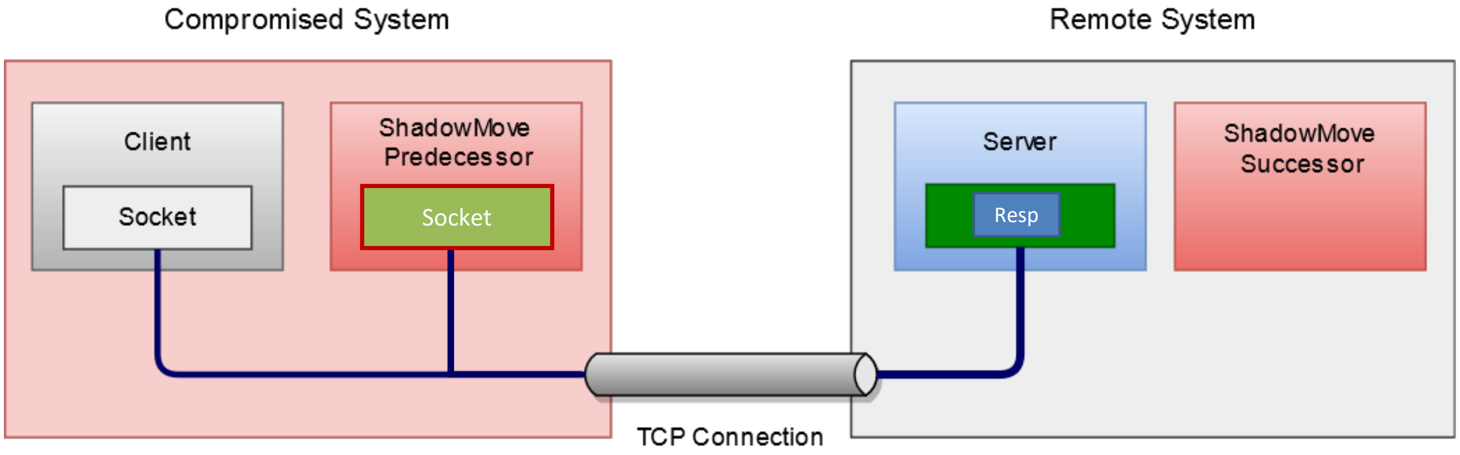
ShadowMove suspends the client, before sending requests to the remote server

Overview



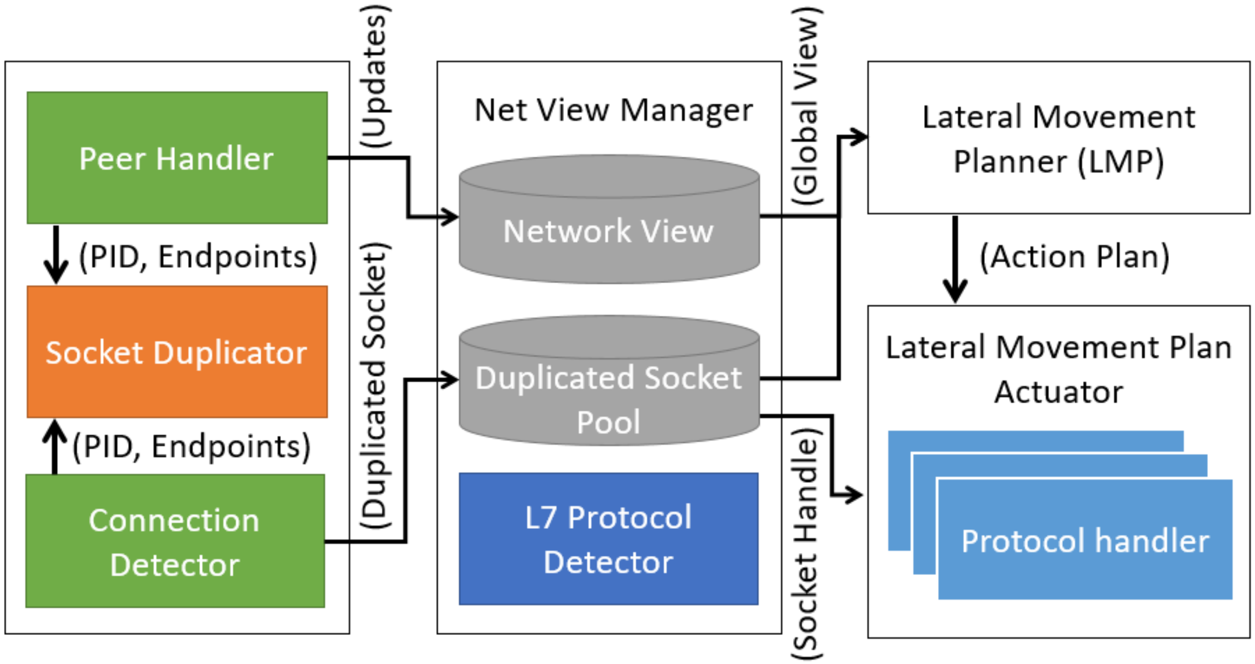
ShadowMove sends a set of requests to perform an action
Example of an action: Upload, Download, or Execute a file

Overview



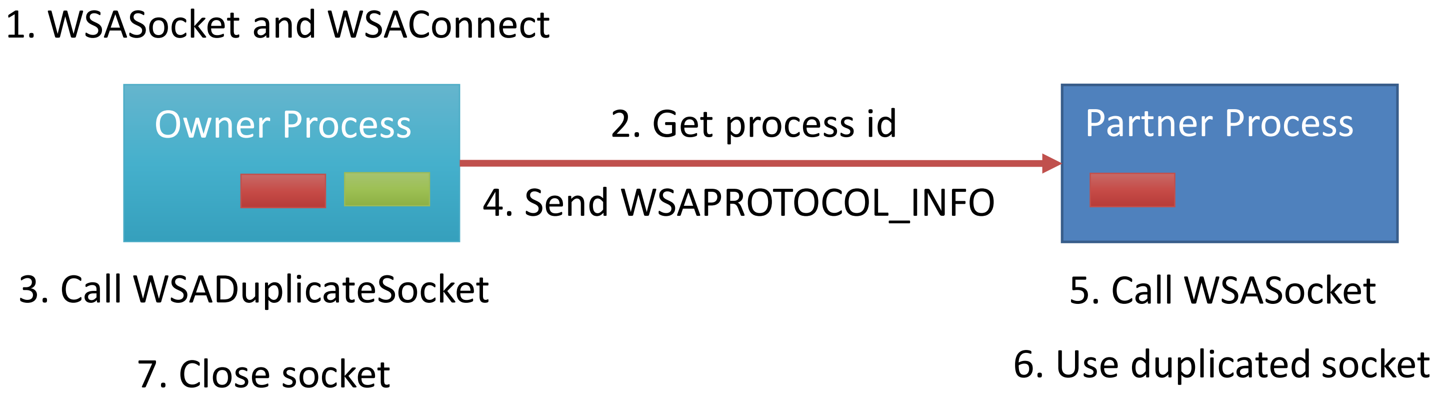
ShadowMove sends a set of requests to perform an action
Example of an action: Upload, Download, or Execute a file

Architecture



Socket Duplicator

- Socket duplication requires cooperation of socket owner



Socket Duplicator

- In ShadowMove, no co-operation is required

Step	Description	kernel/ntdll functions
1	Open the owner process with PROCESS_DUP_HANDLE	OpenProcess(PROCESS_DUP_HANDLE, , pid)
2	Foreach handle with type 0x24 (file)	NtQuerySystemInformation(SystemHandleInformation, ...)
3	Duplicate the handle	NtDuplicateObject
4	Retrieve its names	NtQueryObject(ObjectNameInformation)
5	Skip if the name is not \device\afd	
6	Obtain remote IP and remote port number	getpeername(handle, ...)
7	Skip if remote IP and port do not match the input parameters	
8	Call WSADuplicateSocketW to get a special WSAPROTOCOL_INFO structure	WSADuplicateSocketW(handle, ...)
9	Create a duplicate socket	WSASocketW(WSAPROTOCOL_INFO, ...)
10	Use the socket	recv(), send()

Connection Detector

Detects newly created sockets suitable for duplication

- Periodically gets a list of TCP connections
  - E.g. by calling GetTcpTable2 and GetTcp6Table2
- Identifies new connections
- Filters out the ones owned by a process that cannot be accessed
- Calls socket duplicator to duplicate the new ones

Peer Handler

Helps to construct a global view of the compromised network by synchronizing its current view with neighboring ShadowMove instances

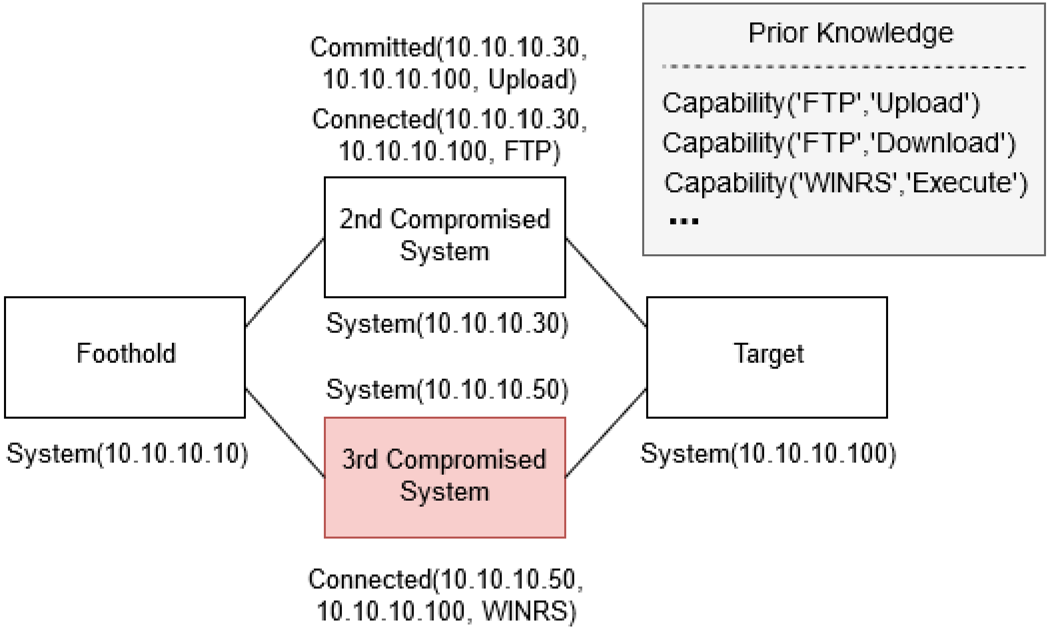
- Receives network views from neighboring nodes
  - Peeks from duplicated sockets
  - waits for synchronization signal
- Sends synchronization signal periodically to its predecessor/successor nodes

Lateral Movement Planner

- Formulates the next lateral movement action plan
  - Current network view
  - History of action plans performed by all ShadowMove instances

An action plan describes the action that must be performed on a specific end point

Lateral Movement Planner



commitExecuteOperation(X, Y) :-
connected(X, Y, Z), capability(Z,
execute), origin(I),
remoteOperation(I, Y, upload, _R),
committed(_K, Y, upload).

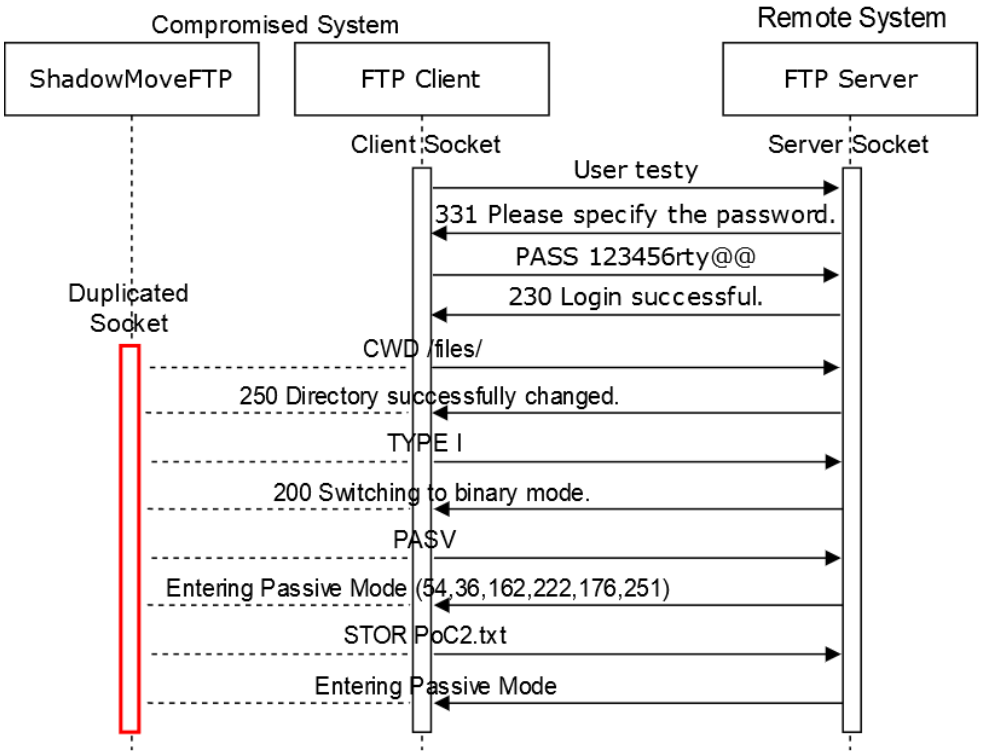
remoteOperation(X, Y, Action, Route):-
connected(X, Z, Service),
capability(Service, Action),
remoteOperation(Z, Y, Action, R),
Route=[X| R].

Lateral Movement Plan Actuator

Creates application-specific queries to carry out lateral movement plans

- Contains a set of Protocol Handlers
  - Application protocol specific
    - FTP, TDS (MS SQL), and WinRM
  - Performs different operations
    - Upload, Download, or Execute

Example Actuator Leveraging FTP



ShadowMove Implementation

- We implement prototypes of the ShadowMove design on Windows (2,501 lines in C/C++) and Linux (1,316 lines in C/C++)
- The lateral movement planner is based on SWI-Prolog
- A demo video of our ShadowMove prototype that leverages FTP is available[1]
- The prototype implementation is available upon request (aniak2@uis.edu)

[1] http://54.36.162.222/ShadowMoveDemo/ShadowmovePrototypeDemo.mp4

Why is ShadowMove Possible?

- The conflicting requirements between process isolation and resource sharing in commodity OS
  - allows the attack process to duplicate (share) sockets belonging to legitimate client processes.
- A lack of built-in message origin integrity validation in many networking protocols
  - allows malicious packets in existing connections that cannot be differentiated from legitimate packets.

Evaluation

- Not detected by off-the-shelf solutions

Type	Name	Version	Update time	FTP/MSSql/WinRM
AV	McAfee	16.0	03 Feb 2019	N/N/N
AV	Norton	22.16.2.22	03 Feb 2019	N/N/N
AV	Webroot	9.0.24.37	03 Feb 2019	N/N/N
AV	Bitdefender	6.6.7.106	03 Feb 2019	N/N/N
AV	Windows Defender	4.18.1901.7	03 Feb 2019	N/N/N
IDS	Snort (Windows and Linux)	2.9.12	07 Feb 2019	N/N/N
HIDS	OSSEC (Linux)	3.4.0	12 Oct 2019	N/--/--
HIDS	Osquery (Linux)	4.0.2	24 Oct 2019	N/--/--
HIDS	Wazuh (Linux)	3.10.2	24 Oct 2019	N/--/--
EDR	Cisco AMP	6.1.5.10729	14 Jun 2018	N/N/N
EDR	CrowdStrike Falcon Prevent	4.20.8305.0	11 Feb 2019	N/N/N

Limitations of ShadowMove Prototype

- It cannot hijack connections for which user-level encryption is applied to the payload

- It may not be able to get information such as the shellID in WinRM attack from the receiving buffer if the legitimate client consumes the buffer first

- Our design of ShadowMove on Linux relies on code injection

Thank you

Questions?

Amirreza Niakanlahiji, aniak2@uis.edu

Jinpeng Wei, jwei8@uncc.edu

Md Rabbi Alam, malam5@uncc.edu

Qingyang Wang, qywang@csc.lsu.edu

Bei-Tseng Chu, billchu@uncc.edu