SwitchMan: An Easy-to-Use Approach to Secure User Input and Output

Shengbao Zheng[1], Zhenyu Zhou[1], Heyi Tang[*] and Xiaowei Yang[1]

[1]Duke University, [*]Tsinghua University

Duke

Background

Sensitive user input/output data are vulnerable to data stealing attacks by keyloggers and screen scrapers

- e.g. Carbanak malware [1] in 2015 infects bank computers
- Stole almost one billion dollars from around 100 financial institutions

Challenging because OS provides user-level APIs for sharing the I/Os

- e.g. XGrabKeyboard() in X11
- Allow any malware to steal the keyboard input and screen output

Limitations of Existing Solutions

- All require significant user management
  - VM solution: which VM handles sensitive data
  - Using trusted device (e.g. mobile phone) input/output sensitive data
- Challenging for a non-expert user to manage these tasks
- Need automatically manage the switching to sensitive data input/output without user involvement

Contribution

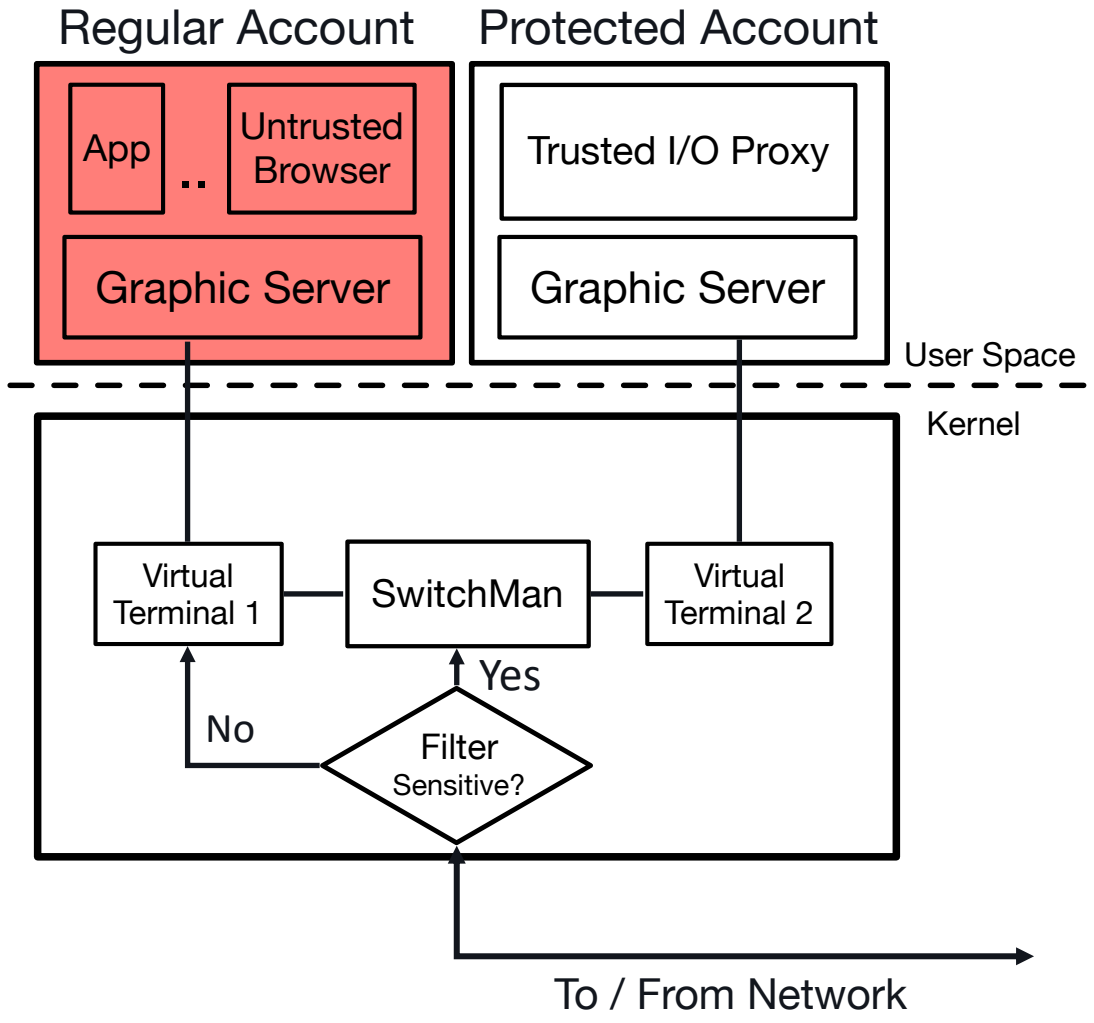
- SwitchMan architecture
  - A secure terminal for handling sensitive input/output data
  - Server initiated switching
  - Defending data stealing attacks by keylogger & screen scraper malware
- SwitchMan Network Protocol (SNP)
  - Enables a server to invoke a secure terminal for sensitive data
  - Works even if the client's software (e.g. a browser) is untrusted
  - Resistant to MITM attack
- Implement a SwitchMan prototype using Linux
  - Evaluate its performance

Outline

- Design goals, assumptions, adversary model
- SwitchMan Design
  - SwitchMan Architecture
  - Trusted Input/Output Proxy (TIOP)
  - SwitchMan Network Protocol (SNP)
- Evaluation

- Goals
  - Protect sensitive input/output data against user-level malware
  - Easy to use
  - Efficient
- Assumptions
  - Trusting OS and its vendor
  - Secure storage & network transmission
- Adversary model
  - No physical access
  - Malicious Man-in-the-Middle (MITM)

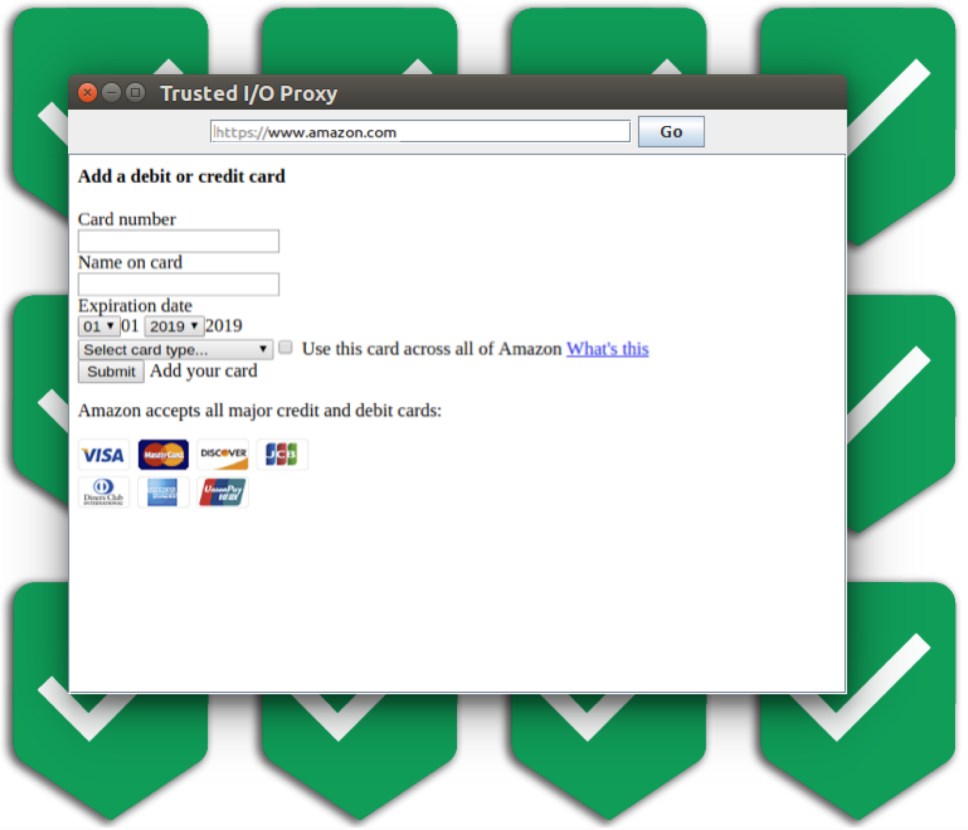
SwitchMan Architecture



Duke

Trusted Input/Output Proxy (TIOP)

- A simple web browser
  - Displays the sensitive output
  - Takes a user's input
- The only application
  - Connects to the graphic server running under the protected account
- Attacker may mimic a TIOP
  - Choose a secret background image
  - Encrypted and stored with a user's other login credentials



Duke

SwitchMan Network Protocol (SNP)

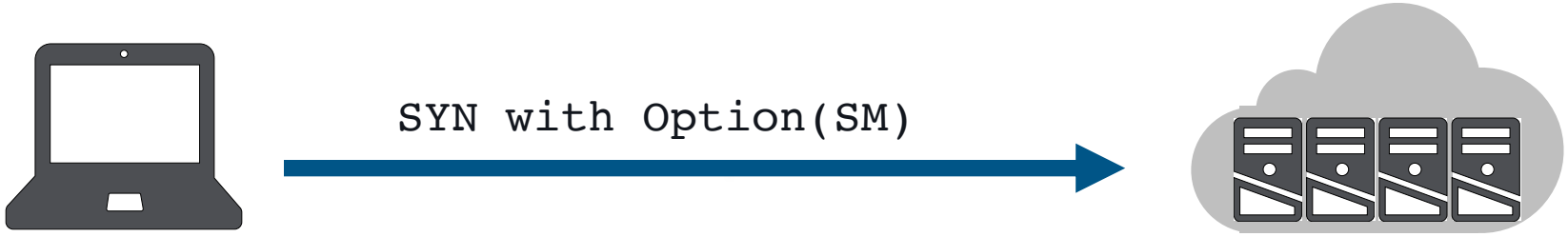
- Protocol to support server initiated switching
- Establish a separate secure connection with the server for sensitive data

Challenges:

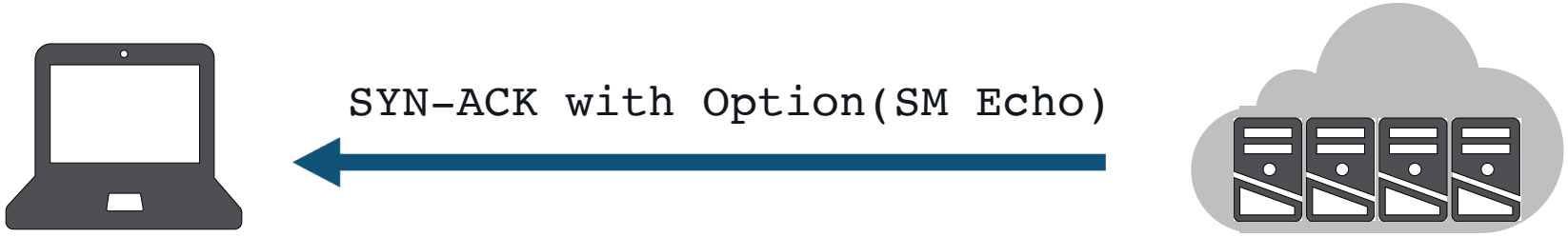
1. Support non-SwitchMan-upgraded client
   Negotiation during TCP Handshake
2. MITM attacks & malicious browser
   Separate the secrets for establishing secure connection into two parts:
   TCP Option + HTTPS

Duke

Step 1: TCP handshake



Step 1: TCP handshake



Step 1: TCP handshake

Step 2: Server Initiated Switching

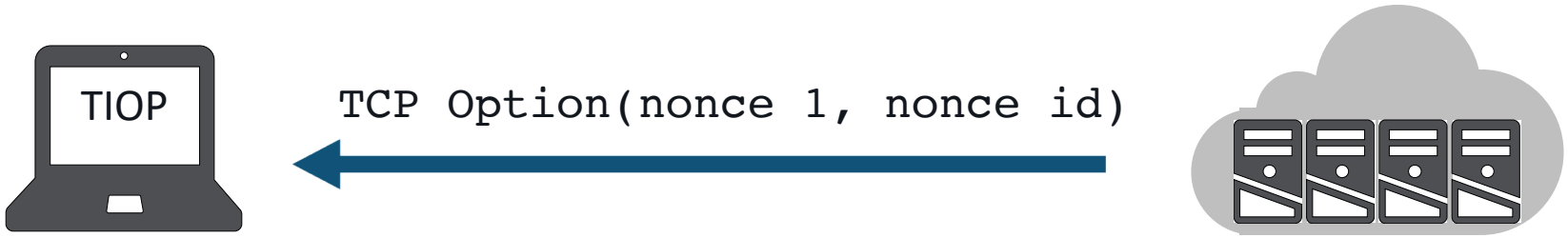
Duke

Step 2: Server Initiated Switching

Duke

Step 2: Server Initiated Switching

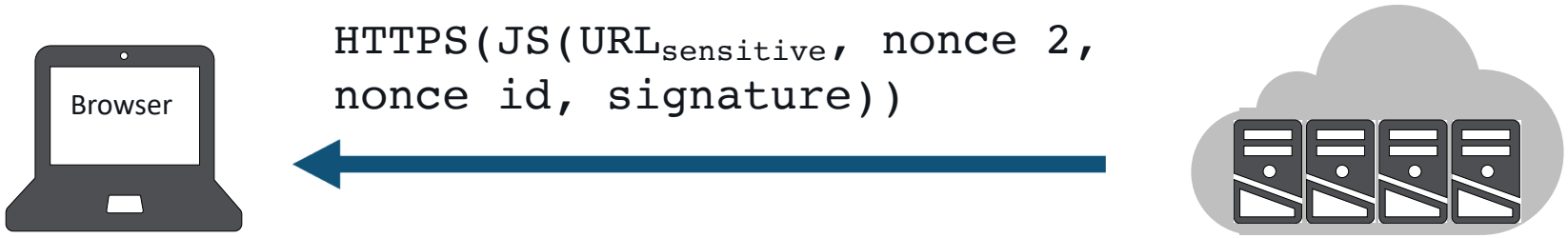
```
// First half of the secret
```



Duke

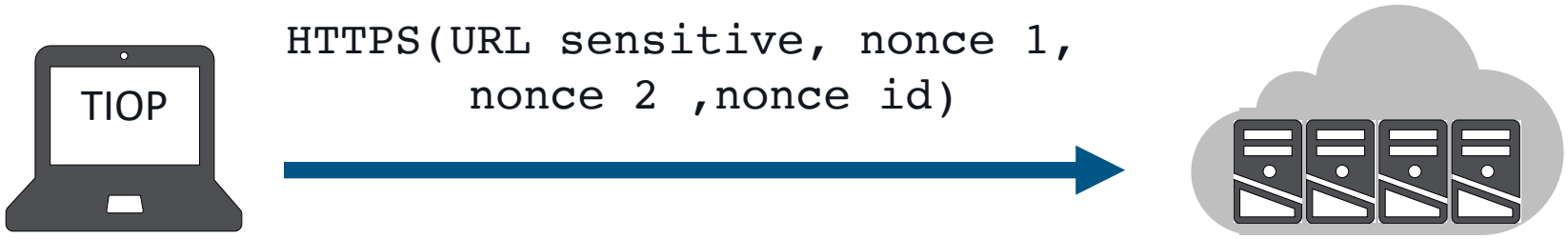
Step 2: Server Initiated Switching

```
// Second half of the secret
```



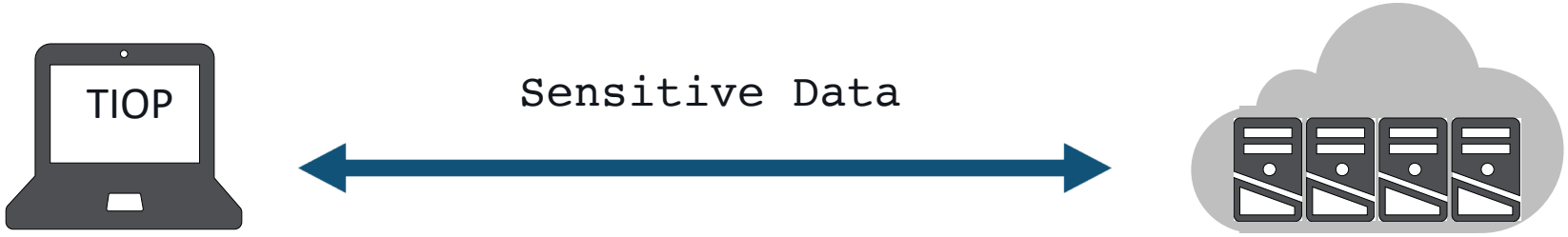
Duke

Step 3: TIOP Connects to the Server



Duke

Step 3: TIOP Connects to the Server



Duke

Step 4: Switching back to the regular account

Duke

Evaluation

- Compare SwitchMan with three other systems
  - Qubes OS, CloudTerminal, BitE
  - Usability
  - Security
- Performance
  - Implement a SwitchMan Prototype
  - Measure the latency of Alexa Top 10 financial websites
  - Compare the original response time vs. extra latency

Factor	Qubes	CloudTerminal	BitE	SwitchMan
		USABILITY		

Duke

Factor	Qubes	CloudTerminal	BitE	SwitchMan
		USABILITY		
Nothing-to-carry	✓	✓	✗	✓

Duke

Factor	Qubes	CloudTerminal	BitE	SwitchMan
USABILITY				
Nothing-to-carry	✓	✓	✗	✓
No user management effort	✗	✗	✗	✓

Duke

Factor	Qubes	CloudTerminal	BitE	SwitchMan
USABILITY				
Nothing-to-carry	✓	✓	✗	✓
No user management effort	✗	✗	✗	✓
No noticeable performance degradation	✗	✓	✓	✓

Duke

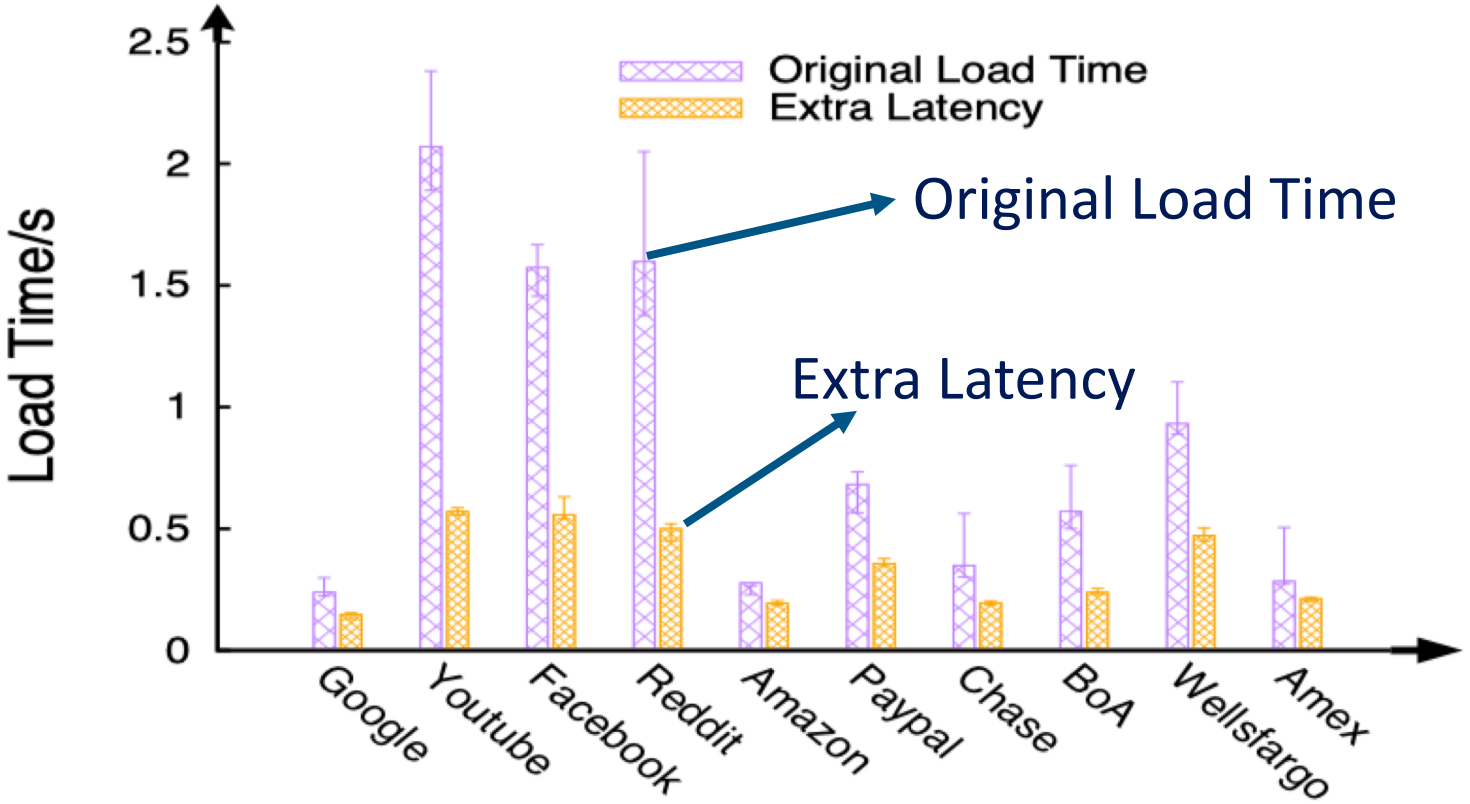
Factor	Qubes	CloudTerminal	BitE	SwitchMan
USABILITY				
Nothing-to-carry	✓	✓	✗	✓
No user management effort	✗	✗	✗	✓
No noticeable performance degradation	✗	✓	✓	✓
SECURITY				

Duke

Factor	Qubes	CloudTerminal	BitE	SwitchMan
USABILITY				
Nothing-to-carry	✓	✓	✗	✓
No user management effort	✗	✗	✗	✓
No noticeable performance degradation	✗	✓	✓	✓
SECURITY				
TCB size	VMM + guest OS kernel + graphic system	kernel modules + hypervisor + cloud	kernel + mobile OS	kernel + graphic system

Duke

SwitchMan Latency



Duke

Conclusion

- SwitchMan
  - an architecture that enables a server to automatically switch a user to a secure terminal for sensitive user input/output
- Lightweight and easy to use
- A valuable design alternative for the real-world to adopt

Duke

Thanks

Duke