Ensuring security on encrypted network connections

Chris Komoroski†
Nabil Schear*

University of Illinois at Urbana-Champaign

† Department of Electrical and Computer Engineering
* Department of Computer Science

{ckomoro2, nschea2}@illinois.edu
Introduction

• Goal: Implement additional defenses against traffic analysis attacks on the Tor network
• Nabil implemented the program to send false data and the encryption routines
• I implemented the proxy to send the data through the Tor network and to receive the data when it comes out of the network.
The Project

Encrypt or send false data program

Client
(the user)

Decrypt and remove false data program

Server
(google.com)

Tor Network

The red arrows represent my part of the project.
What I Learned

• Network programming in C
• How to work as a group on a programming project
• How the open-source Tor network operates
Aft Browser

Matt Dordal†

Nabil Schear*

University of Illinois at Urbana-Champaign

† Department of Electrical and Computer Engineering
* Department of Computer Science

{mdordal2, nschea2}@illinois.edu
Overview

- The Web is a dangerous place
  - More attack vectors
  - More info on web
    - Attacks are more commonplace, and more damaging
- Aft Solution:
  - Isolation
  - Redundancy
  - Fault Tolerance
  - Additional benefits:
    - Honeynet, collection
My Part

• VM Client Controller
  – Controls browsers
  – Communicates with external controller
    • Filesystem events, commands

• Filesystem Monitor
  – LoggedFS parsed into objects
VM Detection

Wenxun Huang†

Nabil Schear*

University of Illinois at Urbana-Champaign

† Department of Electrical and Computer Engineering
* Department of Computer Science

{huang55, nschear2}@illinois.edu
Brief

• What is the project about?
  – Survey on techniques to figure out whether a program is running inside a real machine or not.

• What’s so cool?
  – A movie <<The Matrix>> ---- Finding discrepancies between real and virtual world.

• Exploring possibilities of creating 100% undetectable malware.
About Virtual Machines

• Software that simulates a computer and let programs run in it.

• Advantages:
  – Utilize server resources better.
  – Easy to build and manage.
One way to detect VMware
--Through the “CommChannel”

- VMware implements many special ports to maintain communication between guest and VMM.

**Code segment:**

```assembly
...  
mov eax, 'VMXh'       // VMware magic value (0x564D5868)
mov ecx, 0Ah          // special version cmd (0x0a)
mov dx, 'VX'          // special VMware I/O port (0x5658)
in eax, dx             // load data from specified port with I/O cmd
...  
```

**Consequences:**

- If running inside VMware, the version of VMware will be stored in ECX.
- Otherwise, an exception occurs.
Thank you

Any questions?