CERIAS
The Center for Education and Research in Information Assurance and Security

Cyber Analysis of OT Through Rehosting

Xander Lewis, Dan Joshwa, Lia Branstetter, Logan Manthey

Advisors: Zachary Estrada, Dave Henthorn, Chris Miller

Abstract: Rehosting is the process of porting a physical device to run in software. By rehosting operational technology (OT) devices, we are able to perform cyber analysis on critical infrastructure to protect from cyber attacks. Building upon MIT Lincoln Lab's existing rehosting infrastructure, we were able to demonstrate the feasibility of cyber analysis on two Programmable Logic Controllers (PLCs) to uncover existing and new vulnerabilities.

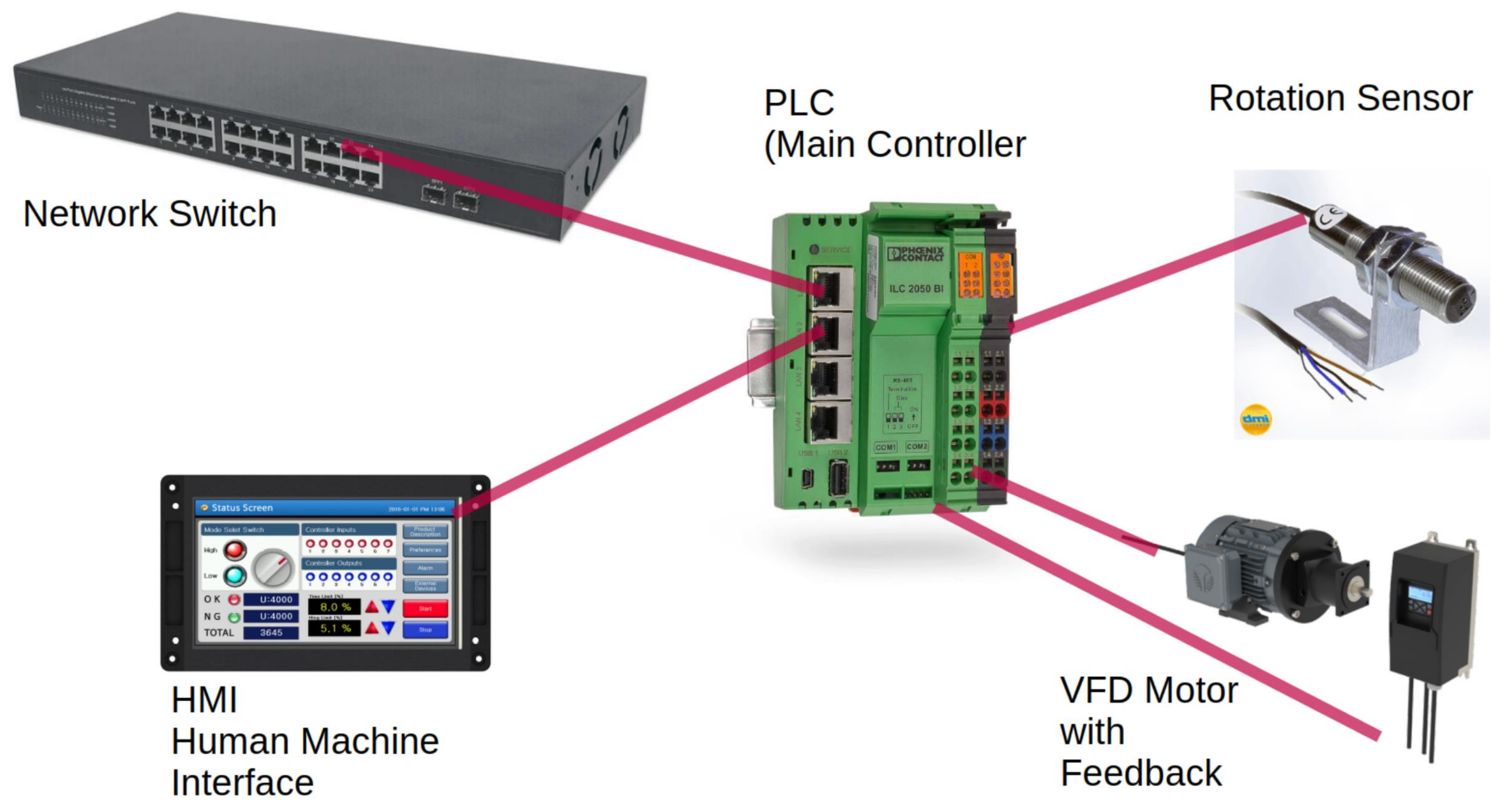


Figure 1: Problem Space of Rehosting a PLC

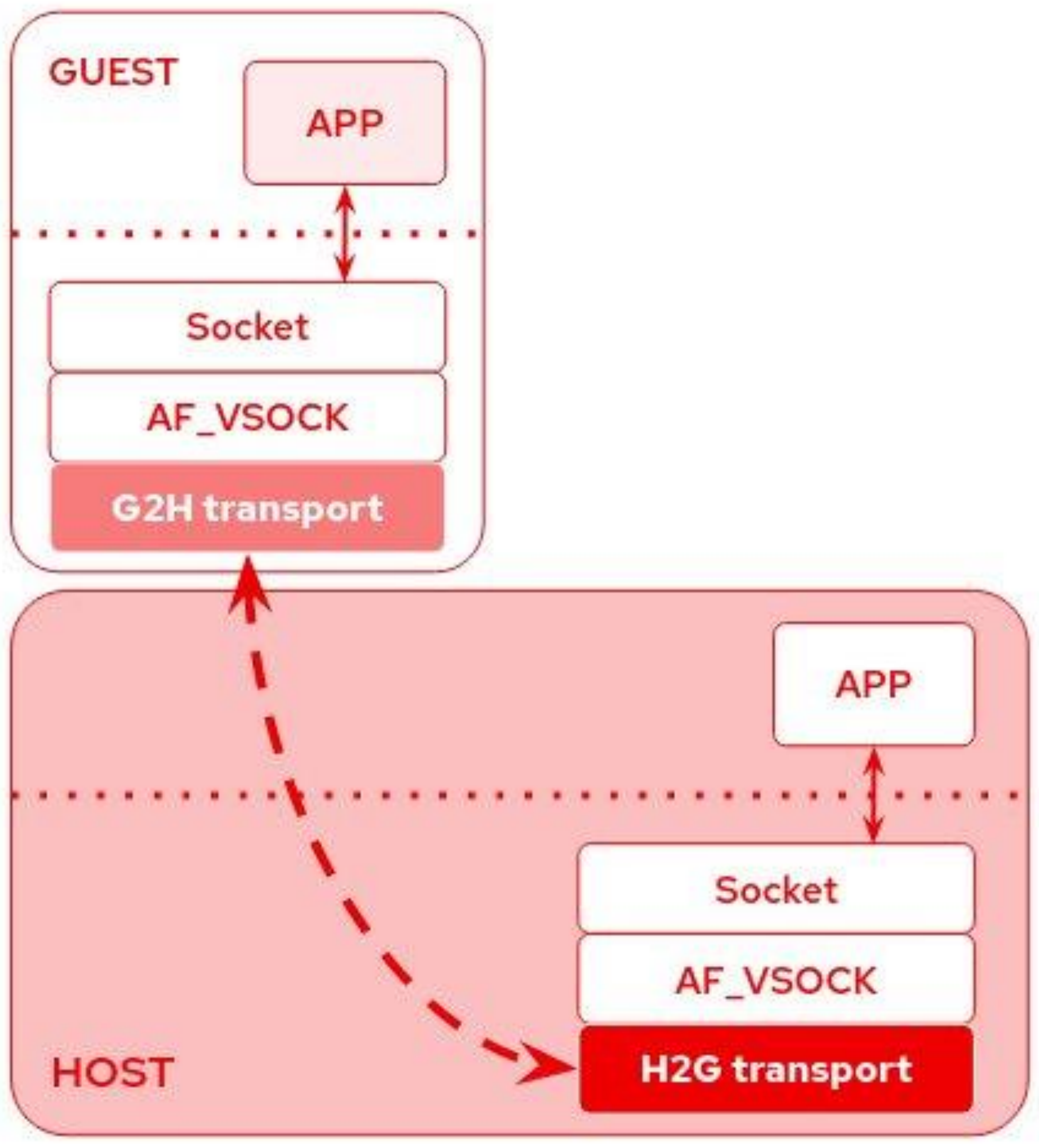
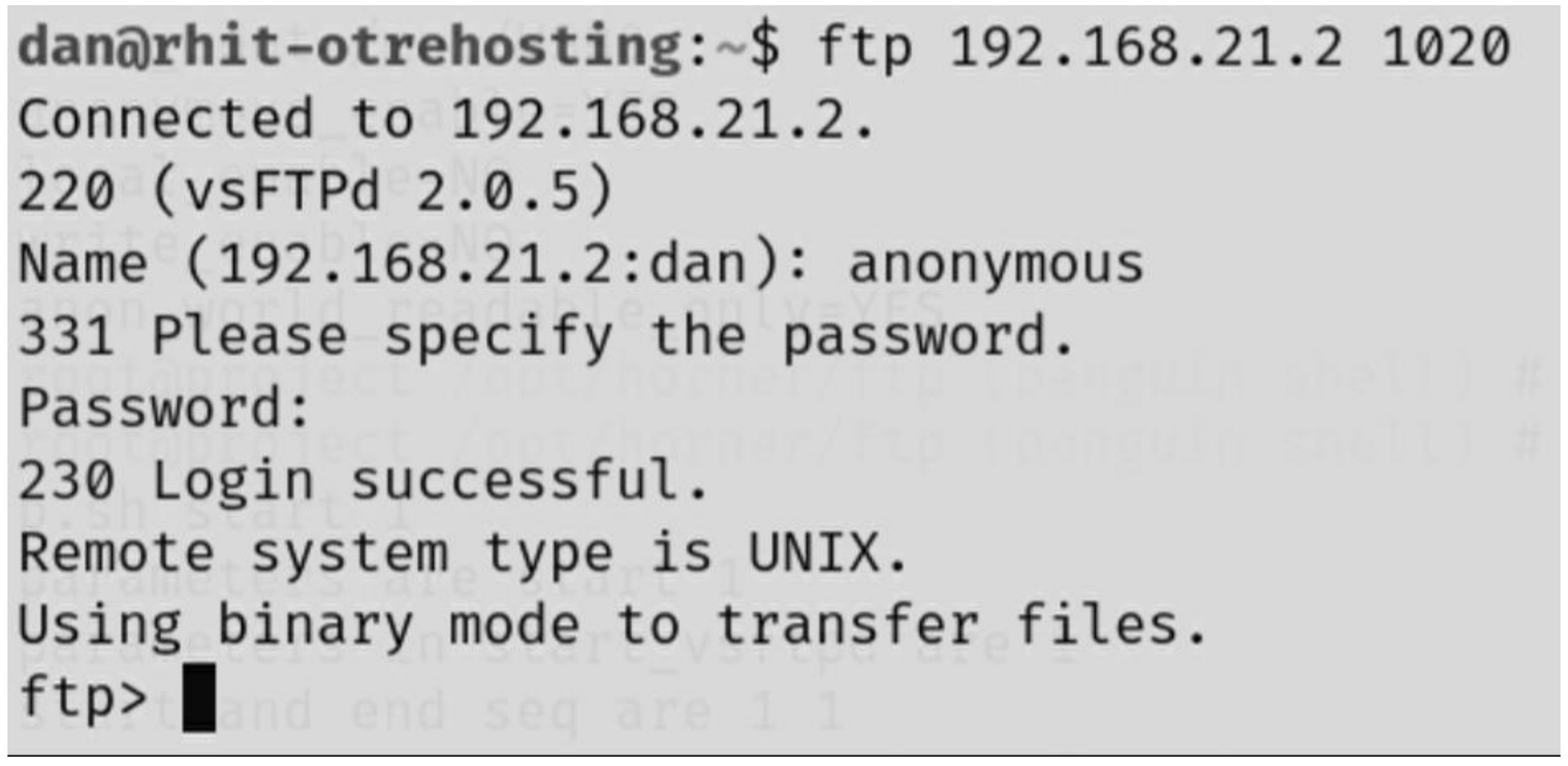


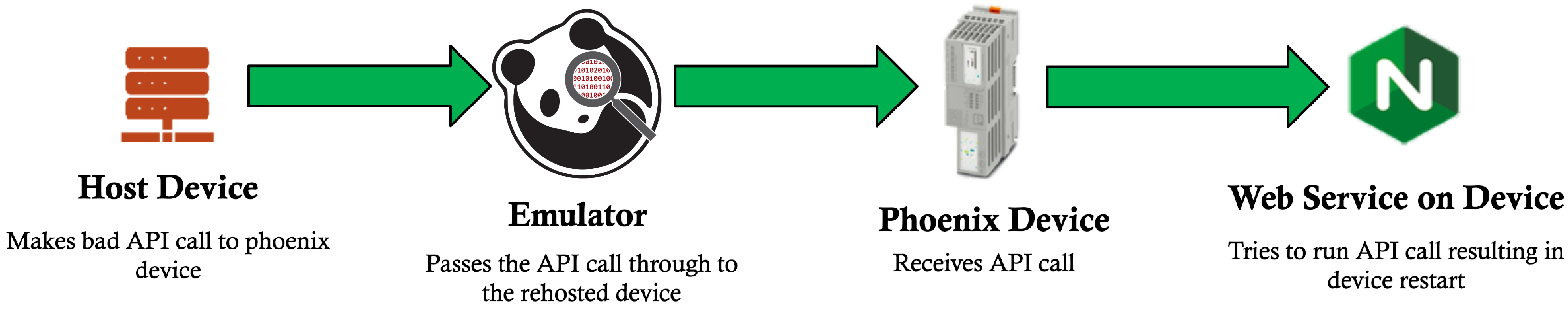
Figure 2: Virtual Socket Networking

Rehosting OT systems is possible through dynamic filesystem analysis. When emulation of a desired OT system is initialized, MITLL's emulator dynamically organizes itself based on the provided system to create the highest fidelity rehosted system.



```
dan@rhit-otrehosting:~$ ftp 192.168.21.2 1020
Connected to 192.168.21.2.
220 (vsFTPd 2.0.5)
Name (192.168.21.2:dan): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Figure 3: FTP Default Anonymous Login Vulnerability Demonstration



Host Device

Makes bad API call to phoenix device

Emulator

Passes the API call through to the rehosted device

Phoenix Device

Receives API call

Web Service on Device

Tries to run API call resulting in device restart

Figure 4: Denial of Service Attack Demonstration Pathway