MUD Extension

Fast Response to New Vulnerabilities

Sávyo Morais

HotRFC - IETF 106
Singapore
November 2019

LabNet

IETF®

The problem

- Manufacturer Usage Description (MUD) [RFC 8520] is not efficient against new vulnerabilities:
  - Exploits can use whitelisted traffic.
- Firmware or MUD updates depends on the manufacturer:
  - May take a long time to be done;
  - The manufacturer may exist no more;
  - The manufacturer may have no interest in doing so.

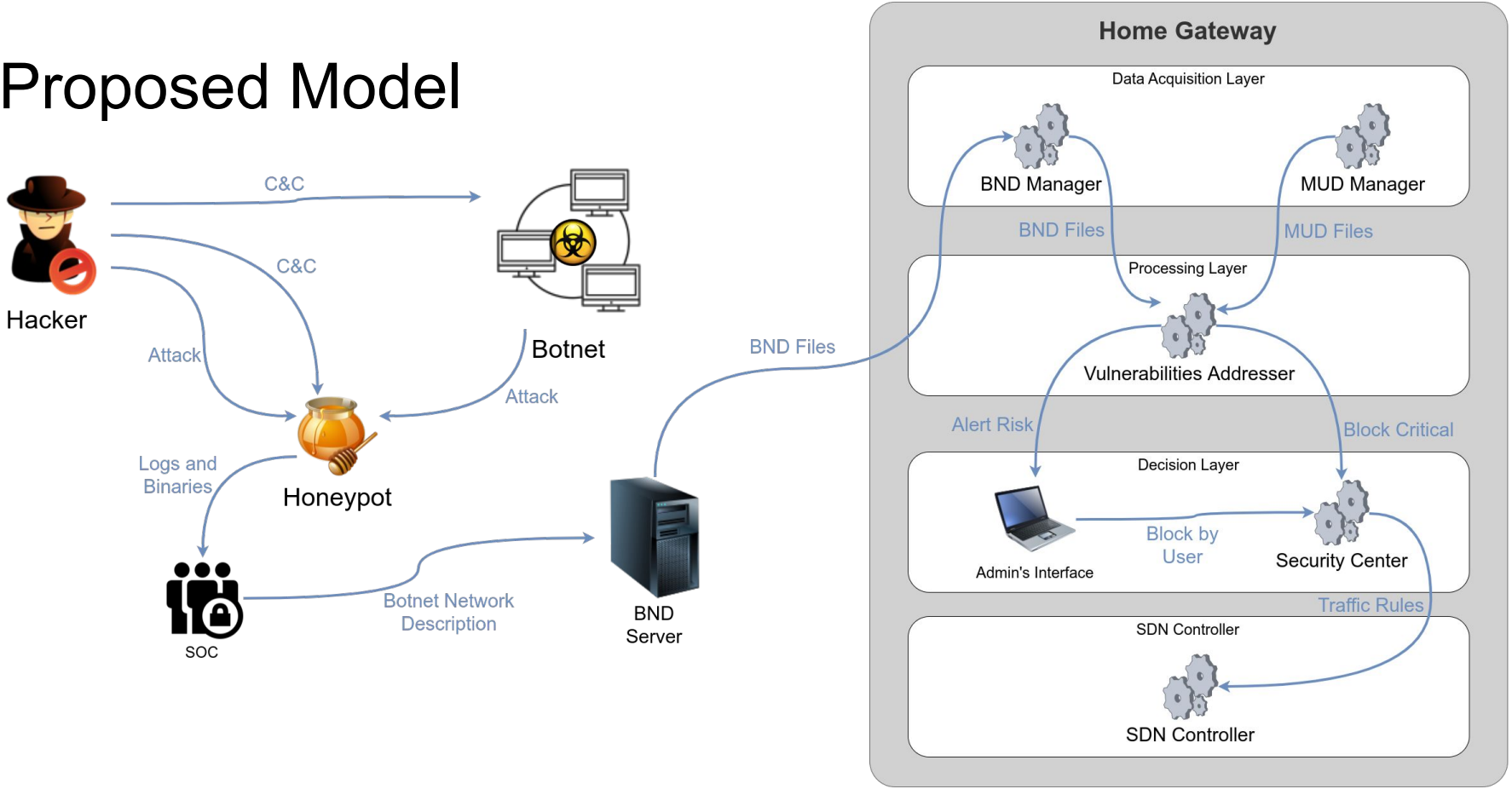
Motivation

- Botnets leave fingerprints -> Security Operation Centers (SOCs) discover their signatures
  - Describe how is the network communication
  - Disclose the information for protect others
- DDoS traffic consumes a lot of bandwidth -> ISPs do not like it
  - They may get interested in support security actions
- Users value their security and privacy

Proposed Extension

- A SOC maintain a security authority with an entity similar to a MUD Server - a Botnet Network Description (BND) server:
  - Describe the new vulnerabilities or botnets network communication
  - Make available descriptions via a HTTPS server
- The end user configures the client to the SOC’s server
- Home gateway compares BNDs with MUDs and finds devices exposed to the botnet.

Proposed Model



C&C = Command and Control

MUD Extension

Fast Response to New Vulnerabilities

Thank You!

Questions?

E-mail me:

savyovm@gmail.com

savyo.morais@labnet.nce.ufrj.br