Elektrotehnički fakultet
Univerziteta u Sarajevu

cost
EUROPEAN COOPERATION
IN SCIENCE & TECHNOLOGY

IoT HoneyBot

Haris Šemić and Saša Mrdović

Cryptacus: Workshop and MC meeting
Nijmegen, Netherlands, 2017

Honeypots

- Emulation of a network resource
- Built to be discovered, attacked and compromised
- Data collection with goal to:
  - Prevent/detect future attacks
  - Implement new or adapt existing security controls

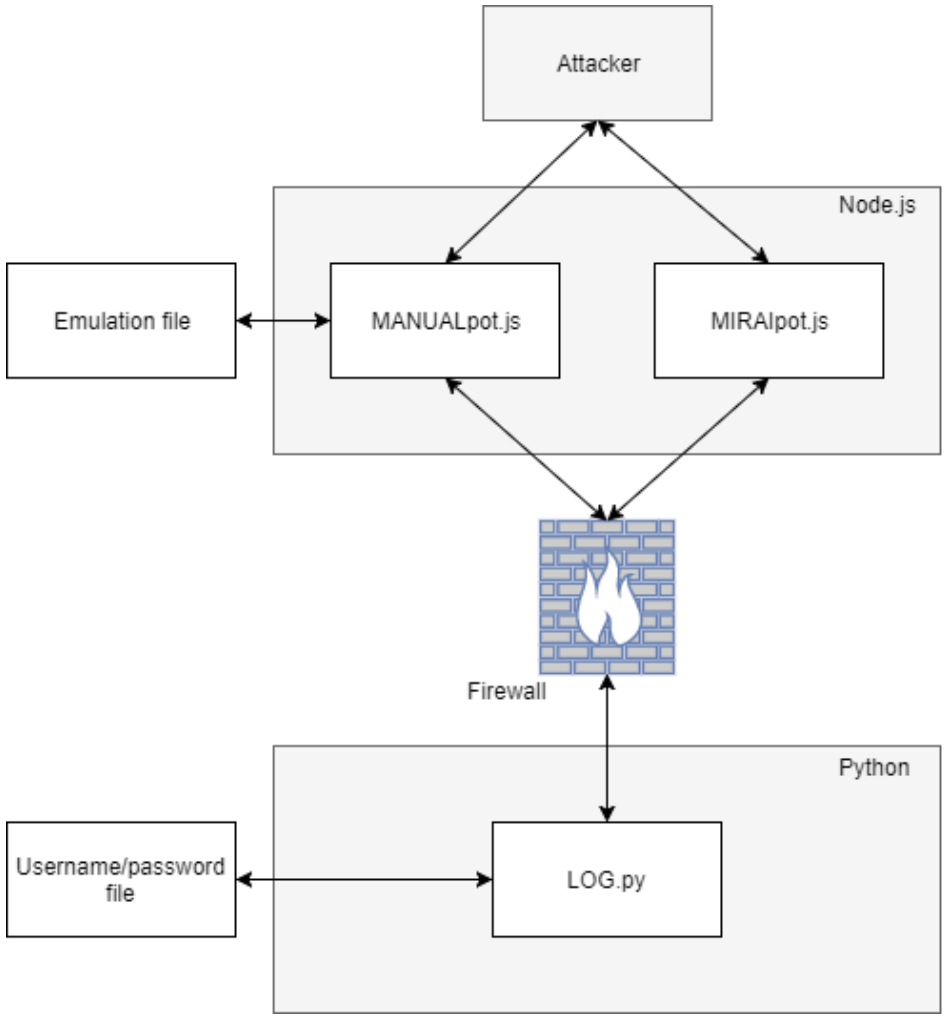
Internet of Things

- Billions of special-purpose devices connected to the Internet
- Automatization of all aspects of modern life
- Remote control of IoT devices using distant network nodes
- 30+ billion IoT devices expected by year 2020

IoT botnets

- Client-server botnets
  - Eg. Mirai, IoT Reaper
  - Notable attacks: Krebs on Security 620 Gbs DDoS attack in 2016, Dyn DDoS attack
- Peer to peer botnets
  - Eg. Hajime
  - At the moment not malicious

Current system



Front-end

- Manual component
  - Handles manual attacks
  - Requires complementary configuration file
  - Emulates the look and feel of a real IoT device
- Mirai component
  - Handles mirai attacks
  - Emulates specific responses which are expected by Mirai

Back-end

```
Sat Aug 26 2017 19:53:36 GMT+0200 (CEST): NEW CONNECTION: 8.8.8.4
Sat Aug 26 2017 19:53:41 GMT+0200 (CEST): NEW (FAILED!) LOGIN ATTEMPT - Username: neko ime,
Password: neka lozinka, IP address: 8.8.8.4
Sat Aug 26 2017 19:53:44 GMT+0200 (CEST): NEW (FAILED!) LOGIN ATTEMPT - Username: pokusaj, P
assword: pokusaj, IP address: 8.8.8.4
Sat Aug 26 2017 19:53:47 GMT+0200 (CEST): NEW (SUCCESSFUL!) LOGIN ATTEMPT - Username: root,
Password: admin, IP address: 8.8.8.4
Sat Aug 26 2017 19:54:03 GMT+0200 (CEST): NEW COMMAND - Username: root, Password: admin, com
mand: cd home, IP address: 8.8.8.4
Sat Aug 26 2017 19:54:03 GMT+0200 (CEST): NEW COMMAND - Username: root, Password: admin, com
mand: ls, IP address: 8.8.8.4
Sat Aug 26 2017 19:54:07 GMT+0200 (CEST): NEW COMMAND - Username: root, Password: admin, com
mand: neka komanda, IP address: 8.8.8.4
Sat Aug 26 2017 19:54:20 GMT+0200 (CEST): NEW CONNECTION: 8.8.8.5
Sat Aug 26 2017 19:54:46 GMT+0200 (CEST): NEW (FAILED!) LOGIN ATTEMPT - Username: root, Pass
word: pokusaj, IP address: 8.8.8.5
Sat Aug 26 2017 19:54:58 GMT+0200 (CEST): NEW COMMAND - Username: root, Password: admin, com
mand: free, IP address: 8.8.8.4
Sat Aug 26 2017 19:55:09 GMT+0200 (CEST): NEW (SUCCESSFUL!) LOGIN ATTEMPT - Username: admin,
 Password: admin, IP address: 8.8.8.5
Sat Aug 26 2017 19:55:10 GMT+0200 (CEST): NEW COMMAND - Username: admin, Password: admin, co
mmand: ls, IP address: 8.8.8.5
```

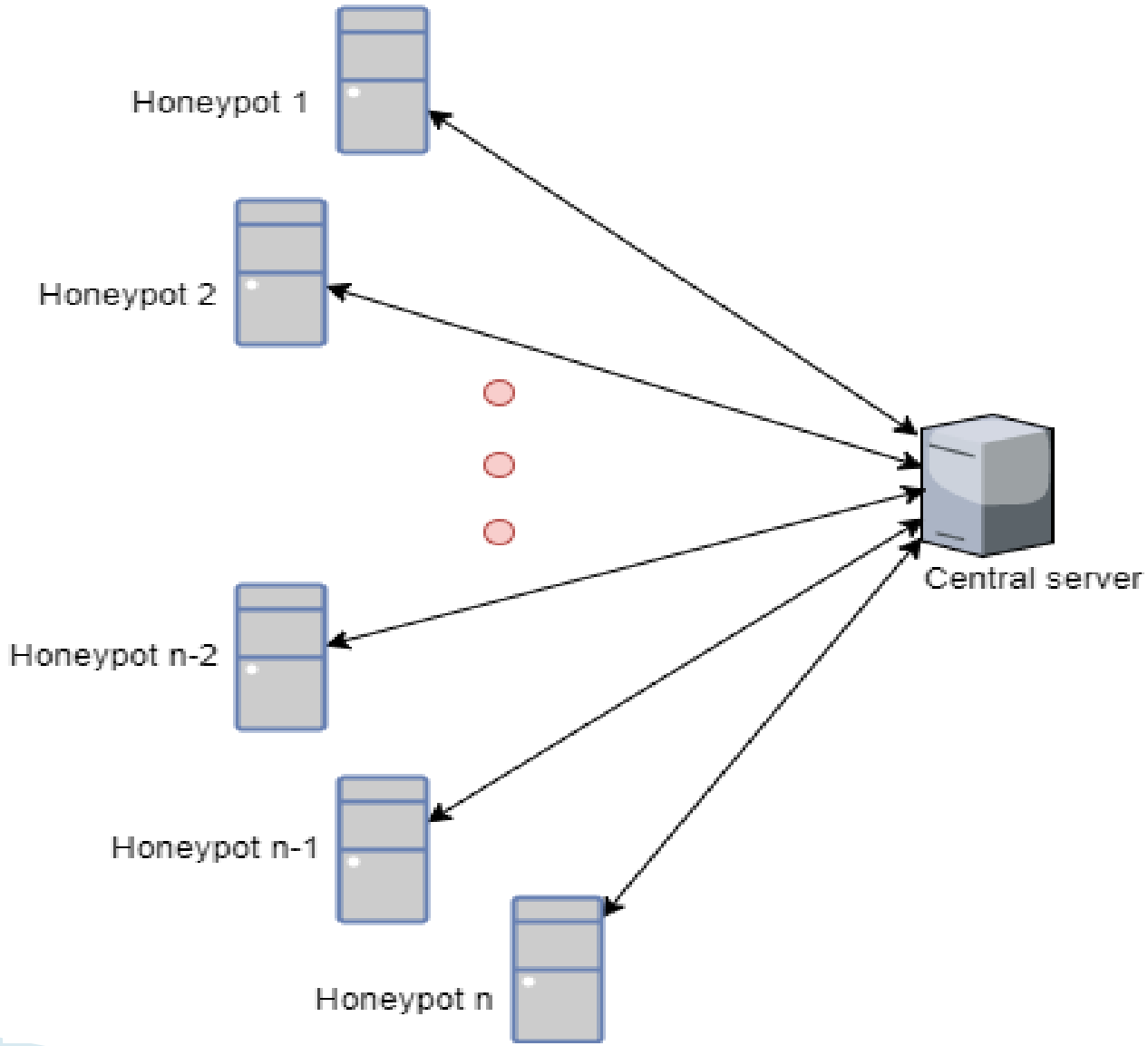
Elektrotehnički fakultet
Univerziteta u Sarajevu

cost
EUROPEAN COOPERATION
IN SCIENCE & TECHNOLOGY

Can multi-component design be applied for large-scale malware observation and research?

The Idea

- Mass-deployment of IoT honeypots
- Malware research
- Anti-botnet
- Propagation observation
- Employment of machine learning to handle new types of attacks
- Encrypted communication

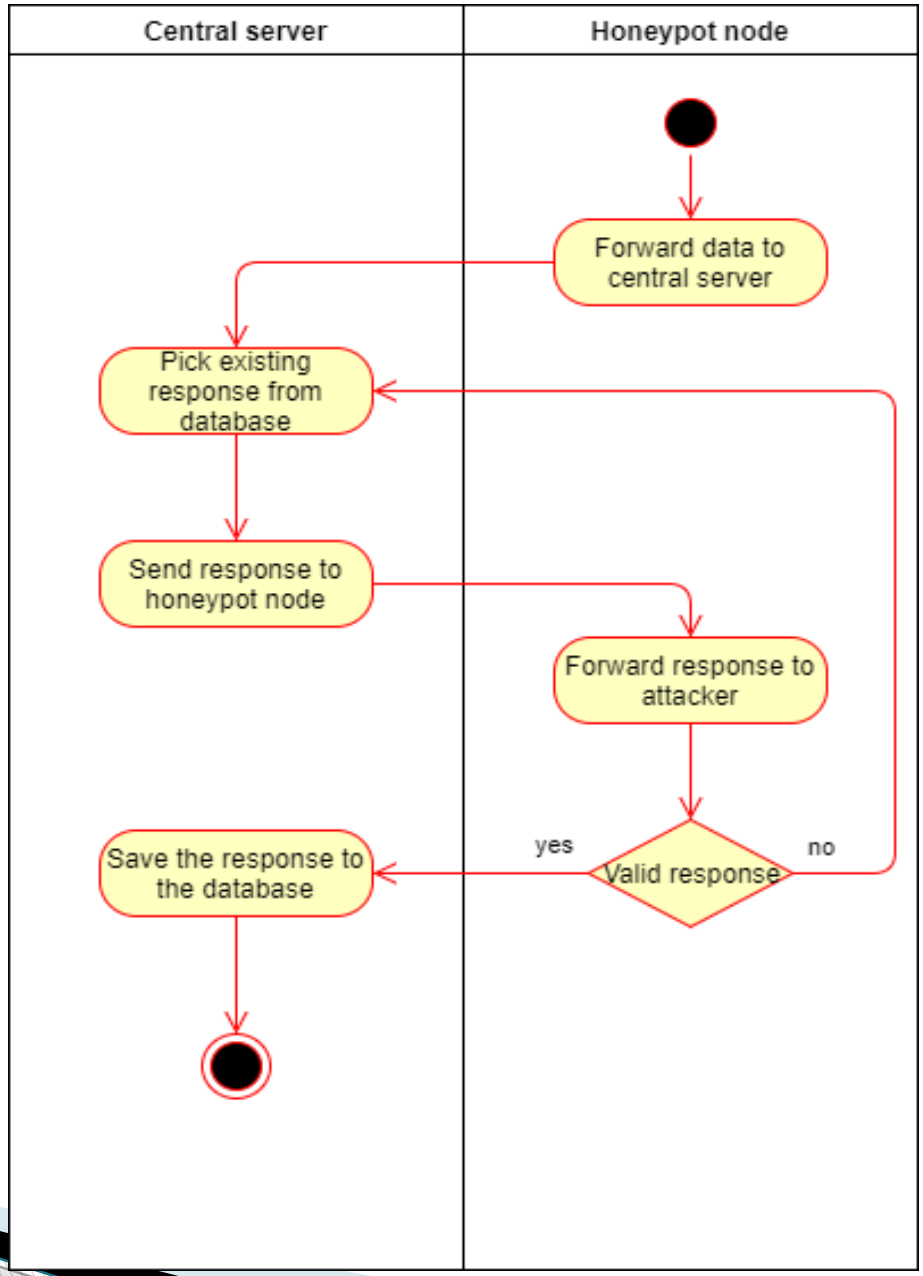

Honeypot 1
Honeypot 2
Honeypot n-2
Honeypot n-1
Honeypot n
Central server

Single honeybot node

- Implemented using Node.js
- Interacts with malicious traffic and supports:
  - Telnet protocol
  - SSH protocol
  - HTTP, HTTPS
- Interaction with central server includes:
  - Receiving configuration
  - Login attempt validation
  - Delivering and receiving encrypted data

Central server

- Stores and reports captured data:
  - One file for each unique IP address
  - Each file contains a history of attacks from any specific source
- Contains:
  - Username-password combinations
  - Database of known attacks
  - Emulation configurations
- Implements machine learning to handle new types of attacks
- Threaded implementation

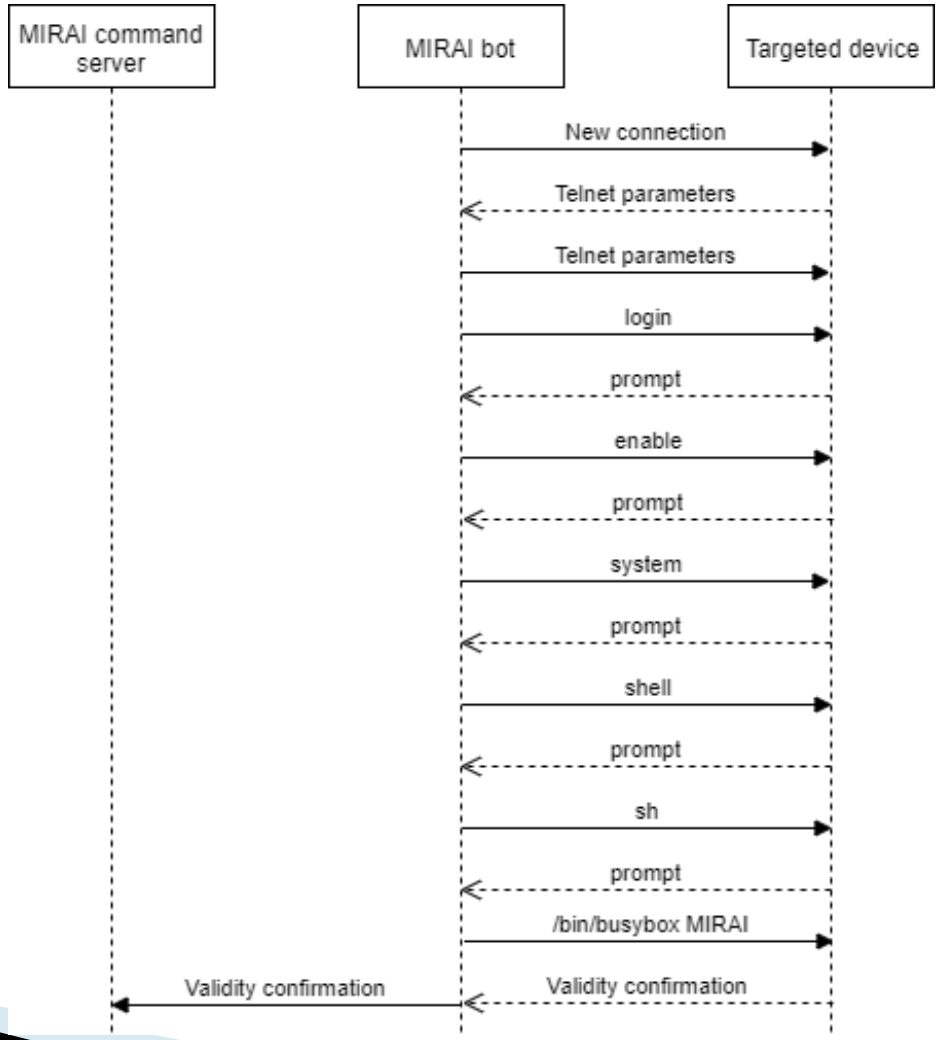

Central server
Honeypot node
Forward data to central server
Pick existing response from database
Send response to honeypot node
Forward response to attacker
Valid response
yes
no
Save the response to the database

Implementation challenges

1. Mass-deployment

- Hundreds (thousands!) of honeypot nodes present two challenges:
  - Deployment
    - Physical location of each machine
    - How many VMs on a single machine
  - Administration
    - Monitoring each node
    - Data reporting

2. Machine learning algorithm



3. Single point of failure

- A single central server with static IP address and domain can easily be blocked and cut off
- Some resilience techniques from existing botnets need to be borrowed:
  - Fast-flux technique (multiple IPs for a single domain name)
  - Domain generation algorithm (continuous generation of random domains)

Elektrotehnički fakultet
Univerziteta u Sarajevu

cost
EUROPEAN COOPERATION
IN SCIENCE & TECHNOLOGY

Thank you