Evaluating Effectiveness of an Embedded System Endpoint Security Technology on EDS: Defeating the hackers of IIoT Devices

Michael Siegel, Greg Falco, Matt Maloney, Elizabeth Reilly

VULNERABLE DEVICES EASILY DISCOVERED

- Protocol & port # available
- Exact address
- DB info & timestamps
- Vulnerable to attack

BLOCKCHAIN AS A SOLUTION

- Blockchain is a distributed ledger of transactions
- The blockchain is decentralized, no one central power exists which prevents corruption/failure
- The blockchain is immutable
- Used to distribute application whitelists
- Whitelist controls what is run on the IoT device

Ethereum Whitelist Transaction

<table>
<thead>
<tr>
<th>Command and Control</th>
<th>Publishes Update as Ethereum Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router running Agent Addr: 0x86a8...</td>
<td>Whitelisted data stored as hash inside transaction data</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Block #: 4672859</th>
<th>From: 0x86a8...</th>
</tr>
</thead>
<tbody>
<tr>
<td>To: 0x86a8...</td>
<td>Data: 0x7b22...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Whitelist data stored as hash inside transaction data</th>
</tr>
</thead>
<tbody>
<tr>
<td>{Procs: process1, process2, Ips: 192.168.8.1, Domains: internal-site.com}</td>
</tr>
</tbody>
</table>

Blockchain Technology

- Foundation for command and control
- Send/receive security updates

Machine Learning

- Intelligently whitelist/blacklist processes
- Learn from connections to whitelist IP ranges

GOING BEYOND WHITELISTS

The team has built several other proof of concepts on top of the underlying technology

SOLUTION OVERVIEW

Lightweight Architecture

- Software enforces security policies on IoT device
- Prevent unauthorized applications from running

Blockchain Technology

- Standard Ethereum stores entire blockchain of data
- Light Client does not store any chain data

DEVICE PROVISIONING

Public Ethereum transaction used to update and provision a device with a public key

COLLABORATION OPPORTUNITIES

Cooperation, support and involvement from industry partners would benefit this research:

- Visibility into plant hardware configurations
- Network topologies of hardware
- Contact: maloneym@mit.edu msiegel@mit.edu

RESEARCH VISION

Develop software that helps secure industrial control systems by leveraging our Ethereum light client to address industrial IoT security challenges.

ETHERNE LIGHT CLIENT ARCHITECTURE

Software enforces security policies on IoT device