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

Ethylene Whitelist Transaction

- Command and Control
  - Publish Update as Ethereum Transaction
  - Whitelist data stored as hash inside transaction data

- Router running Agent
  - Monitor Blockchain for Tx’s to and from specific addresses
  - Parse, unpack and apply JSON data from Transaction as a new whitelist config

SOLUTION OVERVIEW

Lightweight Architecture

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

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

Firmware & Device Updates

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

Device Provisioning

- Ropsten Ethereum Test Network transaction Hashes
  - 0xa70cb53034ff4f15d567a97b90d685648d22a7633815b3e5681c87c42d3b63d7
  - 0x39471ed242cc69da9556d71966d76b83f05b4f0a3b0f7947795ae893ce0929

- Contact: maloneye@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.