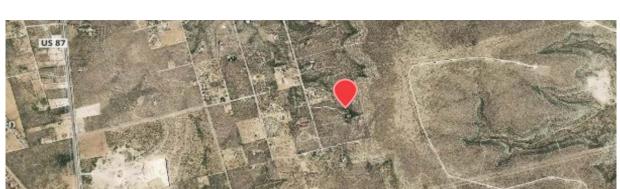


Evaluating Effectiveness of an Embedded System Endpoint Security Technology on EDS: Defeating the hackers of IIoT Devices

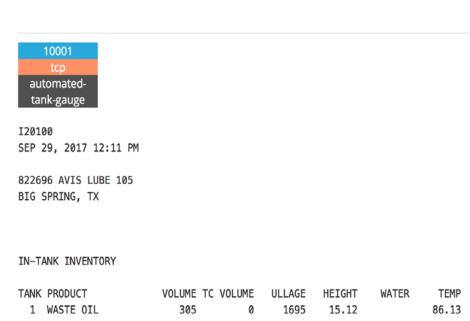
Michael Siegel, Greg Falco, Matt Maloney, Elizabeth Reilly

VULNERABLE DEVICES EASILY DISCOVERED





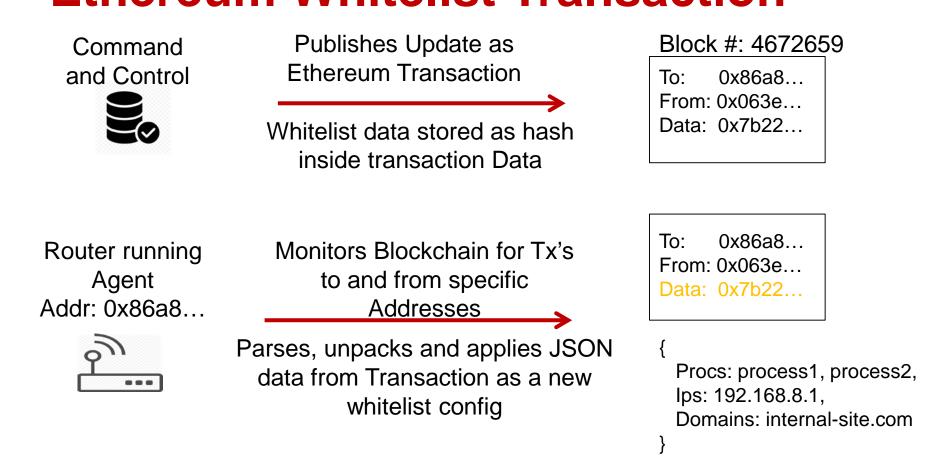
- Protocol & port # available
- Exact address
- DB info & timestamps
- Vulnerable to attack



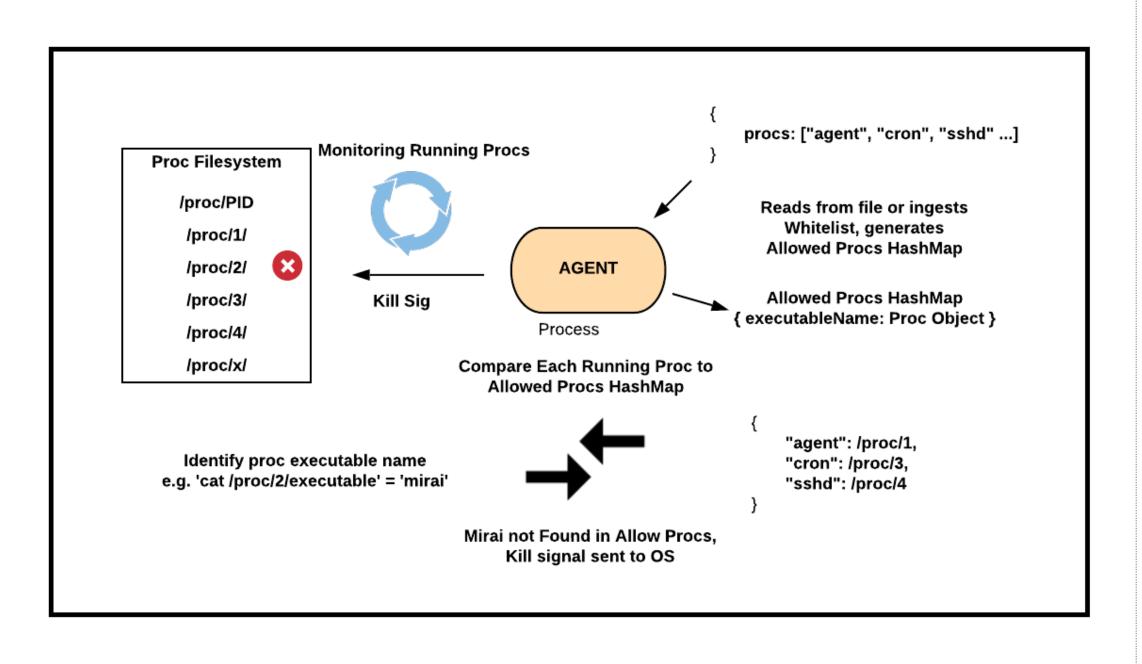
BLOCKCHAIN AS A SOLUTION

- 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



LIGHTWEIGHT AGENT PROCESS MONITORING

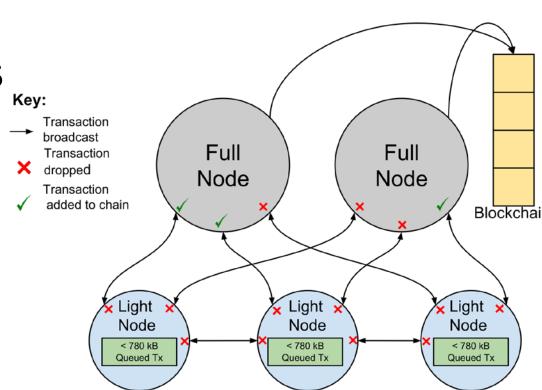


RESEARCH VISION

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

ETHEREUM LIGHT CLIENT ARCHITECTURE

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



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

0x{"sha256":"97f66761bb2f799c95fb4ac5b3d6fb6fde24317f4c9641b2
58ffbe4b87eede4e","url":"https://transfer.sh/2EE4h/qsdkupdate-3.027.img","version":"3.027"}

Device Provisioning

\nMIIEGDCCAwCgAwIBAgIJAJwjzdzrbVSmMA0GCSqGSIb3DQEBCwUAMG4xCzAJBgNV\nBAYTAlVTMQswCQYDVQQIDAJNQTEPMA0GA1UEBwwGQm9zdG9uMREwDwYDVQQKDAhD\nQU1TIExhYjENMASGA1UEAwwEQ0FNUzEfMB0GCSqGSIb3DQEJARYQbWFsb25leW1A\nbWl0LmVkdTAeFw0yMDAxMTMwMDA2MzNaFw0yMTAxMTIwMDA2MzNaMG4xCzAJBgNV\nBAYTAlVTMQswCQYDVQQIDAJNQTEPMA0GA1UEBwwGQm9zdG9uMREwDwYDVQQKDAhD\nQU1TIExhYjENMAsGA1UEAwwEQ0FNUzEfMB0GCSqGSIb3DQEJARYQbWFsb25leW1A\nbWl0LmVkdTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANGkWtV8Icur\nhPi9s+N8PXvecTW+bjPd3RSG/oRtFw7HMBLW5I3gVBtcMbeWEWypSRI39e0z3Mt/\nc5r18ilZffjVLs8xs1P01N/tcdp3NJG+a+lPnWck0GYWtroouTAM8gW3yiTBQHrT\nbqQxTH8/cP3xursE9ffAvYD6X9RvCMlWj5WI3hTIr+/l1joyLai8jhleyNvhlYgk\nroCc+m8RuUygYZ2eDNsnyjoGkviB2ahB94bx80G7FAzZxCvYeW/93WzZzT89Gjly\nPHAhE5Zc//CrenuoS+mKr7ayAYT1a05q7fhp4tc/cnarTr/pjRDy7goFJgNS2w9b\n+VSdGN28ym0CAwEAAa0BuDCBtTCBiQYDVR0jBIGBMH+hcqRwMG4xCzAJBgNVBAYT\nalvTMQswCQYDVQQIDAJNQTEPMA0GA1UEBwwGQm9zdG9uMREwDwYDVQQKDAhDQU1T\nIExhYjENMASGA1UEAwwEQ0FNUzEfMB0GCSqGSIb3DQEJARYQbWFsb25leW1AbWl0\nLmVkdYIJAJwjzdzrbVSmMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgTwMA8GA1UdEQQI\nMAaCBENBTVMwDQYJKoZIhvcNAQELBQADggEBADLgj+2CuYmc1rjgYmPHWUgC/xwR\nPDnCzl5KmDZ1R7ZrnPzS/YzswjZdFuxeuzK9iFcnnwGYnUuHa8RioGARjApwccja\noRsygnZ3eB36f99GmBlG8zTDiMKiNnYoItHgKdupPIszFwoaZ+87+E8rN3K2MISr\ncJBl+60pItrLCQAsEuNAeMMkLY9YIBQfH2gTHDHJQNwmdjB0KDzJXqoNtagDONm6\nJsKr/yZjLJgh2QWue3bGlsdYHhaFiif1NGgSCopD+v3/UziJRSn5qfhxqm7Tgy2\nr2wB0SGA7g/WfysxHr4DuAFQcm+i0UFfFi1upGFK

yNdslLrqR+AvcarG1Gs=\n----END CERTIFICATE----"}

Ropsten Ethereum Test Network transaction Hashes:

0xa70cb53034ff4f15d567a97b90d685648d22a7633 815b3e5681c87c42d3b63d7

0x39471ed242cc69da9556d71966d76b83f05b4f0a3 baff5947795a45d6f0fca09

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: <u>maloneym@mit.edu</u> <u>msiegel@mit.edu</u>