



The AFIT of Today is the Air Force of Tomorrow.

Towards Characterization of Cyber Attacks on Industrial Control Systems: Emulating Field Devices Using Gumstix Technology

**Maj Jonathan Butts, PhD
Air Force Institute of Technology**

Disclaimer:

The views expressed in this document are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the US Government



Motivation



The AFIT of Today is the Air Force of Tomorrow.

- Current defense focus
 - Protect network perimeter
 - Network segmentation and enclaves
 - Trusted communication paths
 - Maintain system security updates
 - IT focused
- Limitations
 - Lack of security at field device level
 - No logging capabilities
 - Not designed to incorporate additional applications
 - Extensive costs to retrofit



Exposures



The AFIT of Today is the Air Force of Tomorrow.

- History of targeted and untargeted failures
 - Sobig infects Amtrak headquarters
 - Slammer disables OH nuclear plant safety monitoring
 - Traffic spike disrupts Browns Ferry recirculation pump
 - Stuxnet
- Growing concerns and uncertainty
 - Project Basecamp
 - Metasploit modules released for ICS-specific devices
 - Leverett identifies 10,000 ICS devices exposed to the Internet



Anatomy of a Hack



The AFIT of Today is the Air Force of Tomorrow.

- Reconnaissance
 - Obtain information about targeted system
- Scanning
 - Intrusion detection systems
 - Antivirus
 - Honeypots
- Gaining access
- Maintaining access
- Covering tracks



Field Device Emulation



The AFIT of Today is the Air Force of Tomorrow.

- Requirements
 - Functionality consistent with actual devices
 - Conform to protocol standards
 - Maintain state
 - Identify reconnaissance and scanning activities
 - Provide logging and alert capabilities
 - No impact to operations
 - Inexpensive



Gumstix Technology



The AFIT of Today is the Air Force of Tomorrow.

- Inexpensive (\$200)
- Open embedded framework
- Readily configurable
- Expansion capabilities



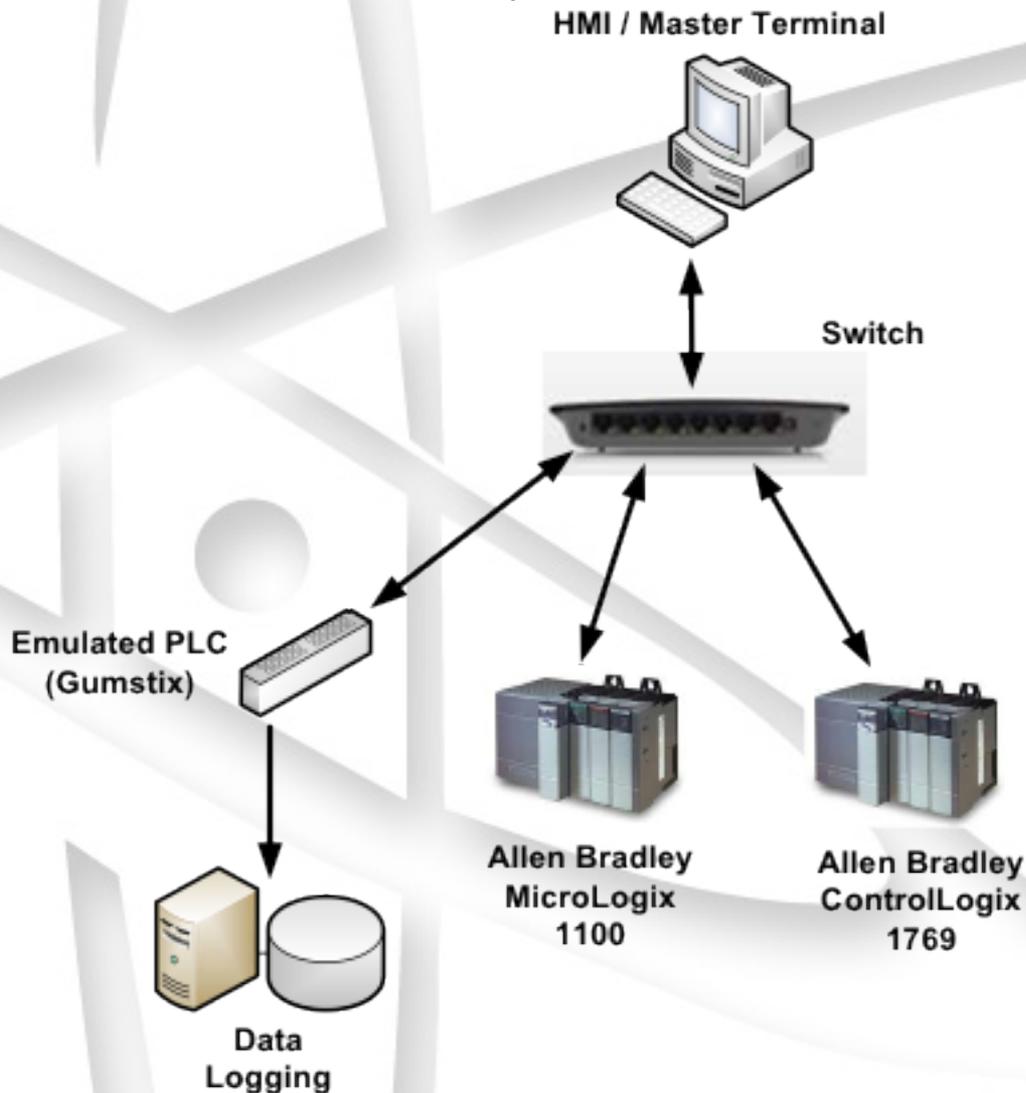
*Air University: The Intellectual and Leadership Center of the Air Force
Fly, Fight, and Win, in Air, Space, and Cyberspace*



Functional Architecture



The AFIT of Today is the Air Force of Tomorrow.



*Air University: The Intellectual and Leadership Center of the Air Force
Fly, Fight, and Win, in Air, Space, and Cyberspace*



Implementation Details



The AFIT of Today is the Air Force of Tomorrow.

- Programmed to emulate Modbus PLC device
 - Implements common set of function codes
 - Triangle Microworks Protocol Test Harness
- Functional examination
 - Comparison with Omron and AB PLC devices
- Syslog remote logging capability
 - Out-of-band reporting



Examination



The AFIT of Today is the Air Force of Tomorrow.

```
14:35:47.321: <=== mMB      Application Header, Read Coils
14:35:47.321:                Starting Register=1, Quantity=1
14:35:47.321:                01 00 01 00 01

14:35:47.726: ===> mMB      Application Header, Read Coils
14:35:47.726:                Byte Count=1
14:35:47.726:                01 01 00
14:35:47.742:                Coil 1 = 0

14:36:38.427: <=== mMB      Application Header, Write Single Coil
14:36:38.427:                05 00 01 ff 00

14:36:38.786: ===> mMB      Application Header, Write Single Coil
14:36:38.786:                05 00 01 ff 00

14:36:45.696: <=== mMB      Application Header, Read Coils
14:36:45.696:                Starting Register=1, Quantity=1
14:36:45.696:                01 00 01 00 01

14:36:46.102: ===> mMB      Application Header, Read Coils
14:36:46.102:                Byte Count=1
14:36:46.102:                01 01 01
14:36:46.102:                Coil 1 = 1
```



Examination



The AFIT of Today is the Air Force of Tomorrow.

```
10:14:43.980: ==> nMB Application Header, Read Encapsulated (DeviceId or Encapsulated Interface)
10:14:43.980: Jb 0e 01 01 00 00 00 00 0d 41 6a 6a 65 6e 20 42
10:14:43.980: 72 61 64 6a 65 79 01 0f 4d 69 63 72 6f 6a 6f 67
10:14:43.980: 69 78 20 31 35 30 30 02 07 54 31 2e 31 32 2e 31
10:14:43.980: Device Identification Object Id = 0
10:14:43.980: Allen Bradley
10:14:43.980: Device Identification Object Id = 1
10:14:43.980: Micrologix 1500
10:14:43.980: Device Identification Object Id = 2
10:14:43.980: V1.12.1
10:14:43.980: Device Identification Conformity Level = 0x1 Next Object Id = 0
```



Examination



The AFIT of Today is the Air Force of Tomorrow.

```
⊗ Ethernet II, Src: Siemens_b6:1f:56 (00:0e:8c:b6:1f:56), Dst: Dell_ad:d8:3c (00:26:b9:ad:d8:3c)
⊗ Internet Protocol Version 4, Src: 192.168.1.66 (192.168.1.66), Dst: 192.168.1.120 (192.168.1.120)
⊗ Transmission Control Protocol, Src Port: asa-app1-prot0 (502), Dst Port: 14591 (14591), Seq: 1, Ack: 13, Len: 10
⊗ Modbus/TCP
  transaction identifier: 0
  protocol identifier: 0
  length: 4
  unit identifier: 1
⊗ Modbus
  function 1: Read coils
  byte count: 1
  data
```



Examination



The AFIT of Today is the Air Force of Tomorrow.

```
11:11:21 172.16.1.10 overo python: 192.168.1.120 is connecting to the Honeypot Device
11:11:36 172.16.1.10 overo python: 192.168.1.120 sent a valid Read Coil request
11:12:00 172.16.1.10 overo python: 192.168.1.120 sent a valid Write Single Coil request
11:12:17 172.16.1.10 overo python: 192.168.1.120 sent a valid Read Discrete Input request
11:12:32 172.16.1.10 overo python: 192.168.1.120 sent a valid Read Holding Registers request
11:12:47 172.16.1.10 overo python: 192.168.1.120 sent a valid Write Single Register request
11:13:23 172.16.1.10 overo python: 192.168.1.120 sent a valid Read Input Registers request
11:13:51 172.16.1.10 overo python: 192.168.1.120 is closing the connection to the Honeypot Device
```



Utility and Conclusions



The AFIT of Today is the Air Force of Tomorrow.

- Deployment to operational environment
 - Identify reconnaissance and scanning attempts
 - Early detection against propagating malware
- Offers situational awareness
 - Augments IT security protection
 - Indicators other than inherent operational functionality
 - What is the current state of adversary activity?
- Attributes
 - Inexpensive
 - Configurable
 - Event logging

