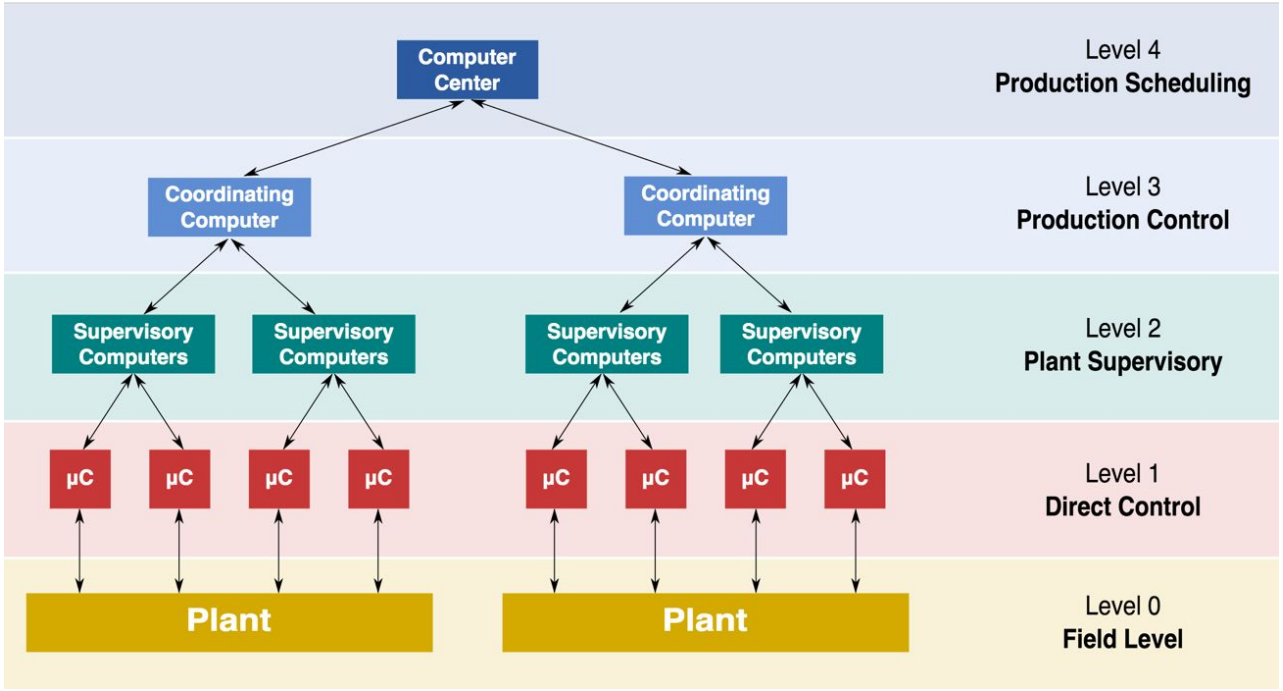
# An Internet-Wide View of ICS Devices

A. Mirian, **Zane Ma,** D. Adrian, M. Tischer, T. Chuenchujit,
T. Yardley, R. Berthier, J. Mason, Z. Durumeric, J. Halderman, M. Bailey

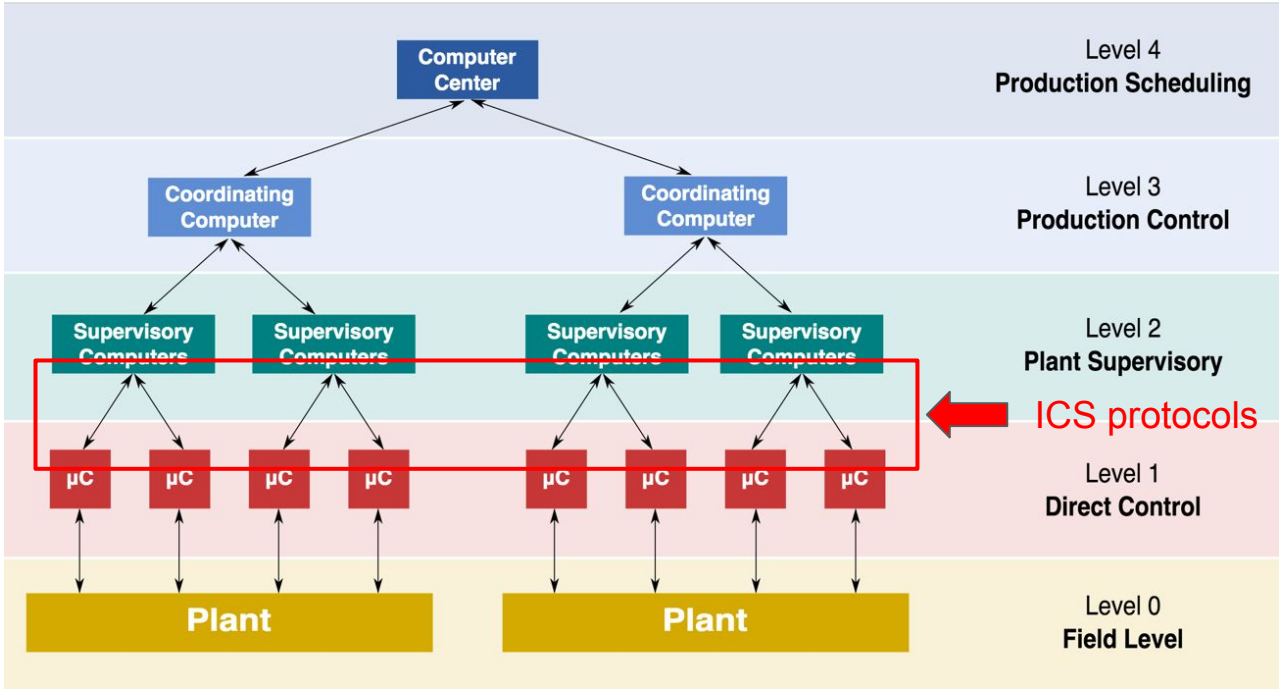
# Industrial Control Systems (ICS)

Operational control and monitoring for industrial processes




# Industrial Control Systems (ICS)

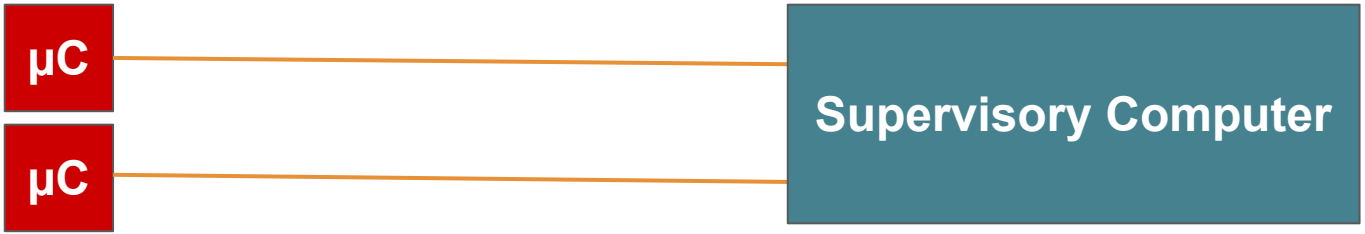
Operational control and monitoring for industrial processes




# Insecurity of ICS

ICS protocols assume system isolation

Evolution: **analog wire** → digital fieldbus → Ethernet



# Insecurity of ICS

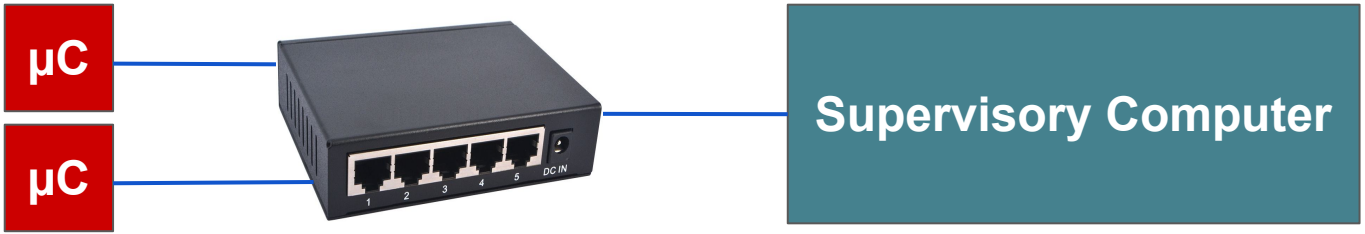
ICS protocols assume system isolation

Evolution: analog wire → **digital fieldbus** → Ethernet

# Insecurity of ICS

ICS protocols assume system isolation

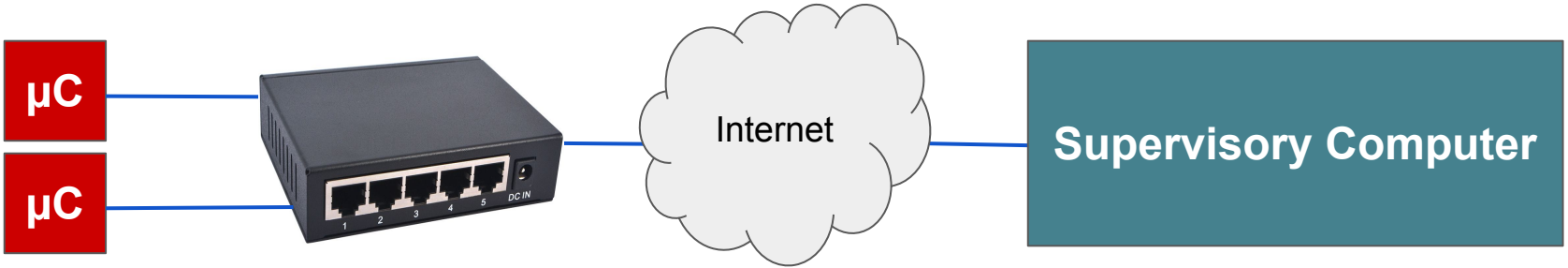
Evolution: analog wire → digital fieldbus → **Ethernet**



# Insecurity of ICS

ICS protocols assume system isolation

Evolution: analog wire → digital fieldbus → Ethernet

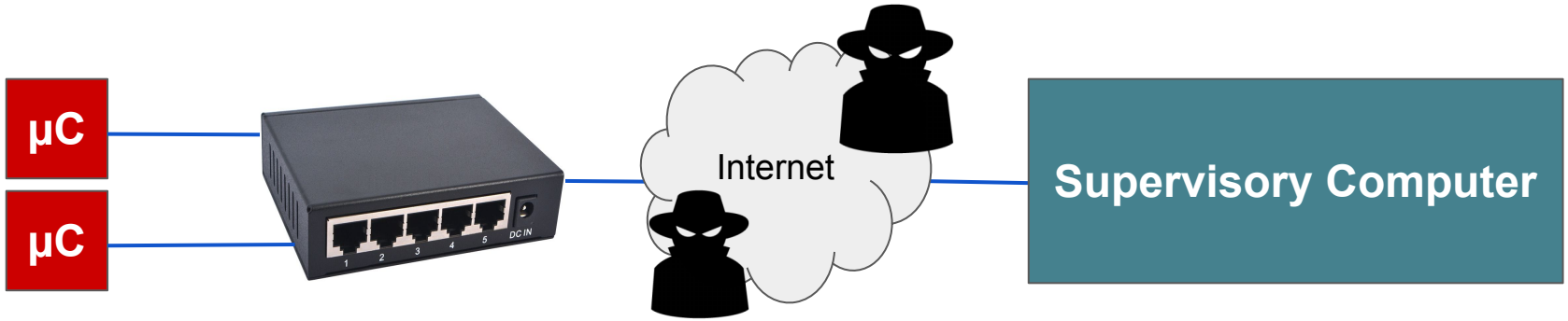



Internet connectivity allows remote control of multiple ICSes

# Insecurity of ICS

ICS protocols assume system isolation

Evolution: analog wire → digital fieldbus → Ethernet




Internet connectivity allows remote control of multiple ICSes

Public Internet = exposure to malicious attackers

# Remote ICS attack

U.S. investigators find proof of cyberattack on Ukraine power grid

CNN

December 2015

30 substations remotely disabled

225,000 people without power

# Research Questions

Understanding the ICS security ecosystem:

1) **Vulnerability assessment** - What ICS protocols and devices are exposed on the public Internet?

2) **Threat landscape** - Who is actively scanning for these vulnerable devices? Why are they scanning?

# ZMap: Fast IPv4 Scanning


Port scanning tool by Durumeric et. al in 2013 *USENIX Security Symposium*

**Fast**: ZMap is *1300 times* faster than NMap

Single port IPv4 scan on one machine in under 45 mins

**Extensible**: architecture for application-level protocol scanners (i.e. HTTP, SSH)

**Well-tooled**: *Censys* scan database and querying infrastructure

Used in hundreds of academic studies

# Detecting ICS Devices

1) Port scans - 10 most common ICS protocol ports

   *Upper-bound*: port overlap with non-ICS services

2) Protocol scans - Implemented 5 protocol parsers

   Modbus, BACnet, Tridium Fox, Siemens S7, DNP3

   *Lower-bound*: only query common configs / protocol device addresses

# Ethical Scanning

## Reducing scan impact

Scan in random order to avoid overwhelming networks

Signal benign nature over HTTP and w/ DNS hostnames

Honor all scan exclusion requests

# Ethical Scanning

## Reducing scan impact

- Scan in random order to avoid overwhelming networks
- Signal benign nature over HTTP and w/ DNS hostnames
- Honor all scan exclusion requests

## Special ICS considerations

- Extensive local testing prior to scanning
- Benign queries that do not alter device state

# Found: ICS Devices

Full IPv4 scans between March 14-19, 2016

Upper bound: **~4 million** devices  Lower bound: **69,000 devices** for 5 protocols

**31.5%** more devices found than previously reported by Matherly, J.C.

Top protocols:

| | | |
|---|---|---|
| 1) | Tridium Fox | 26,299 devices |
| 2) | Modbus | 21,596 devices |
| 3) | BACnet | 16,752 devices |
| 4) | Siemens S7 | 2,357 devices |
| 5) | DNP3 | 419 devices |

# Tridium Fox

Proprietary protocol for building automation

Coordinates supervisory systems

| Country | Hosts | Percent |
|---|---|---|
| United States | 19,219 | 71.6% |
| Canada | 1,590 | 5.9% |
| United Kingdom | 928 | 3.5% |
| Netherlands | 892 | 3.3% |
| Australia | 718 | 2.7% |
| Other (79 countries) | 1,601 | 6.0% |

# Modbus

Designed in 1979!

Master-slave architecture

Limited to 247 devices on network

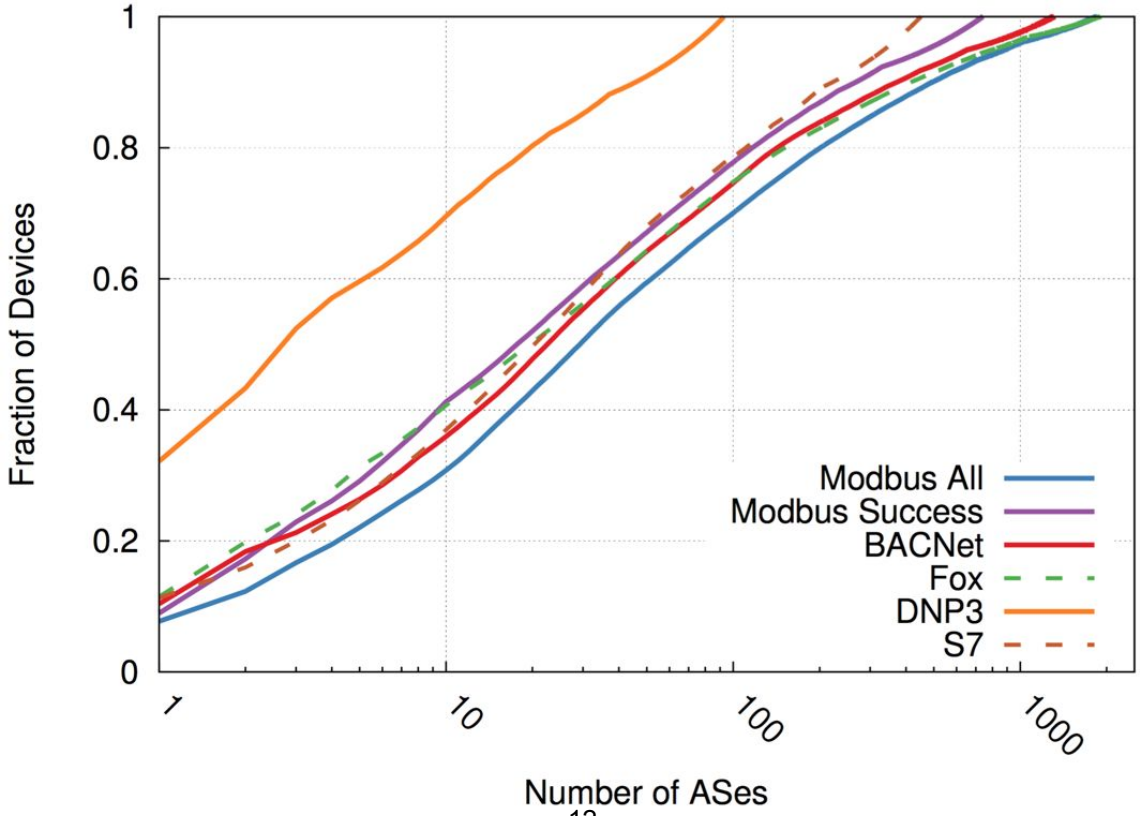

WHOIS lookups for Orange AS

| **Industry** - Orange A.S. ASes | **Hosts** | **Percent** |
|---|---|---|
| Energy | 71 | 7.1% |
| Water and Sanitation | 13 | 1.3% |
| Food and Beverage | 8 | 0.8% |
| Government | 6 | 0.6% |
| Education | 2 | 0.2% |
| HVAC | 1 | 0.1% |
| Industrial Supply | 1 | 0.1% |
| Uncategorized | 897 | 89.8% |

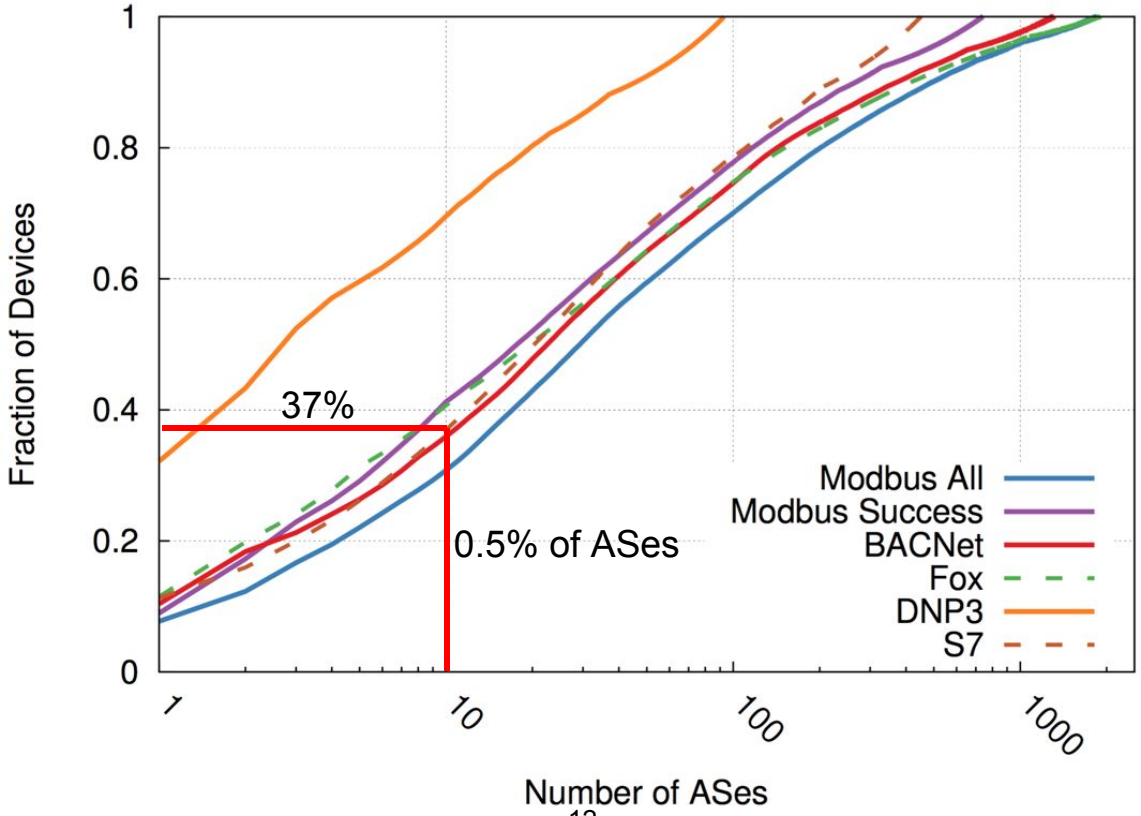
# Increasing ICS Exposure

| Protocol | December 2015 | March 2016 | Percent Increase |
|---|---|---|---|
| BACnet | 16,752 | 16,813 | 0.4% |
| DNP3 | 419 | 429 | 2.3% |
| Modbus | 21,596 | 23,120 | 7.1% |
| Fox | 26,299 | 26,535 | 0.9% |
| S7 | 2,357 | 2,798 | 18.7% |

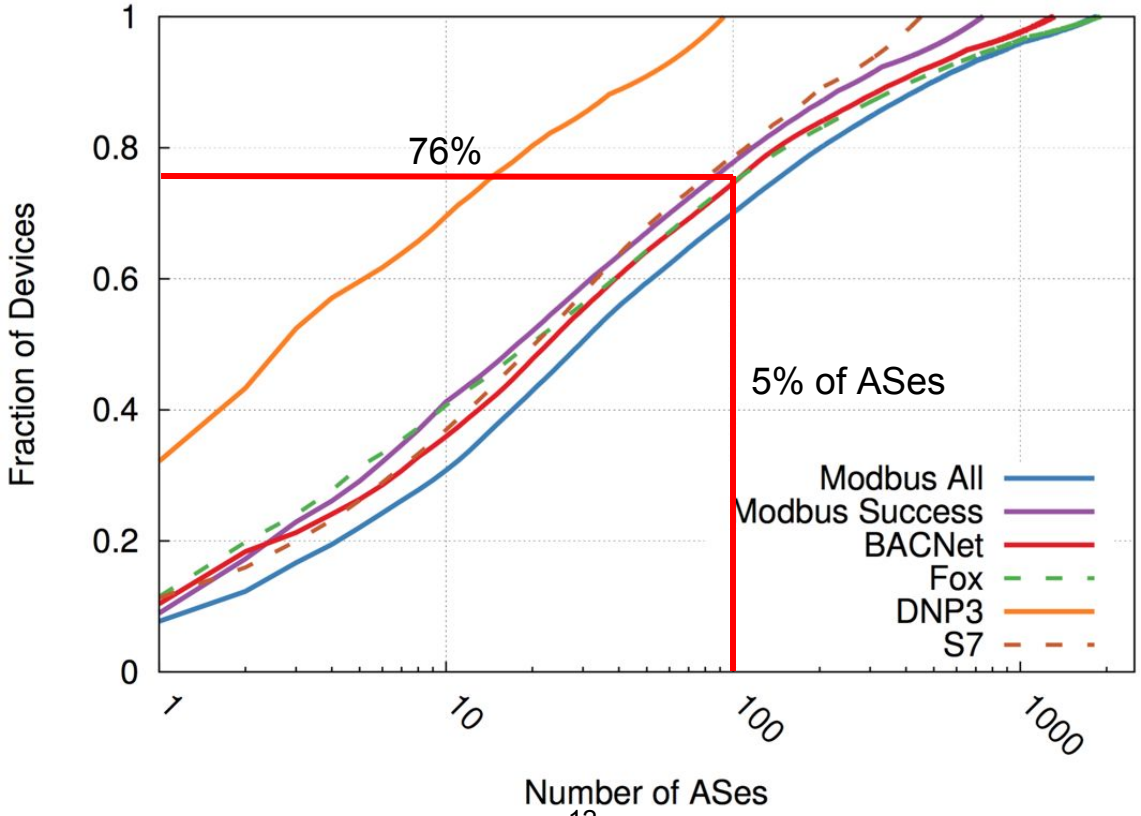
# ICS Network Exposure



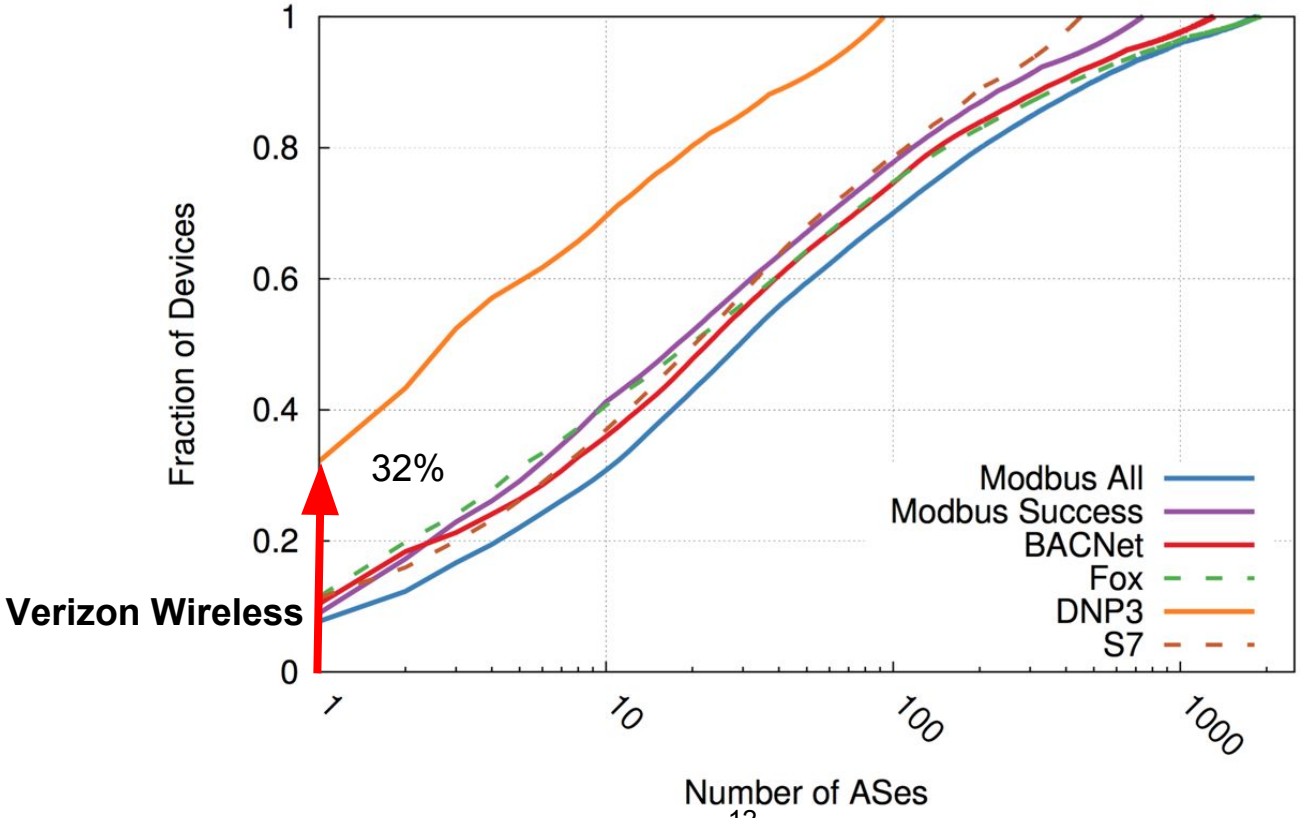
# ICS Network Exposure



# ICS Network Exposure



# ICS Network Exposure



# Research Questions

Understanding the ICS security ecosystem:

1) **Vulnerability assessment** - What ICS protocols and devices are exposed on the public Internet?

2) **Threat landscape** - Who is actively scanning for these vulnerable devices? Why are they scanning?

# Network Telescope

Darknet = large blocks of unused IP address space

Any darknet traffic is attributable to:

1) misconfiguration
2) spoofed IP backscatter
3) active scanning

*Passively* collect UDP/TCP traffic for all ports on a /8 subnet

# Network Telescope

| | Modbus | BACnet | TCP/102 | DNP3 | Ethernet | Fox | Hart | All Protocols |
|---|---|---|---|---|---|---|---|---|
| All ICS Traffic | 41.7% | 30.6% | 8.7% | 5.1% | 8.4% | 3.1% | 2.4% | |
| Shodan Search Engine | 5.1% | 7.2% | 24.5% | 65.5% | 51.8% | 71.2% | 90% | 18.5% |
| Kudelski Security | 61.1% | 86.2% | | | | | | 51.8% |
| Chinanet | 4.2% | | 20.3% | 29.3% | 19.3% | 21.2% | | 9.1% |
| University of Michigan | 16.2% | | | | | | | 6.7% |
| SoftLayer Technologies* | 3.5% | | | | 23% | | | 3.5% |
| ECATEL/Quasi Networks* | 3.8% | | 9.3% | 2.7% | 2.8% | | 4.0% | 2.4% |
| FDC Servers* | | | | 1.8% | 2.2% | 3.0% | 3.8% | 2.5% |
| Amazon EC2* | | | 13% | | | | | 1.1% |
| PlusServer AG* | 1.8% | | 8.7% | | | | | 1.6% |
| Reseau National de telecommunications pour la Technologie | | | 5.7% | | | | | 0.5% |
| Ukrainian Data Center* | | | 5.3% | | | | | 0.5% |
| *Other* | 4.3% | 6.6% | 13.2% | 0.7% | 0.9% | 4.6% | 2.2% | 1.8% |

Scans during August 2015

# Network Telescope

| | Modbus | BACnet | TCP/102 | DNP3 | Ethernet | Fox | Hart | All Protocols |
|---|---|---|---|---|---|---|---|---|
| All ICS Traffic | 41.7% | 30.6% | 8.7% | 5.1% | 8.4% | 3.1% | 2.4% | |
| Shodan Search Engine | 5.1% | 7.2% | 24.5% | 65.5% | 51.8% | 71.2% | 90% | 18.5% |
| Kudelski Security | 61.1% | 86.2% | | | | | | 51.8% |
| Chinanet | 4.2% | | 20.3% | 29.3% | 19.3% | 21.2% | | 9.1% |
| University of Michigan | 16.2% | | | | | | | 6.7% |
| SoftLayer Technologies* | 3.5% | | | | 23% | | | 3.5% |
| ECATEL/Quasi Networks* | 3.8% | | 9.3% | 2.7% | 2.8% | | 4.0% | 2.4% |
| FDC Servers* | | | | 1.8% | 2.2% | 3.0% | 3.8% | 2.5% |
| Amazon EC2* | | | 13% | | | | | 1.1% |
| PlusServer AG* | 1.8% | | 8.7% | | | | | 1.6% |
| Reseau National de telecommunications pour la Technologie | | | 5.7% | | | | | 0.5% |
| Ukrainian Data Center* | | | 5.3% | | | | | 0.5% |
| *Other* | 4.3% | 6.6% | 13.2% | 0.7% | 0.9% | 4.6% | 2.2% | 1.8% |

Scans during August 2015

# Network Telescope

| | Modbus | BACnet | TCP/102 | DNP3 | Ethernet | Fox | Hart | All Protocols |
|---|---|---|---|---|---|---|---|---|
| All ICS Traffic | 41.7% | 30.6% | 8.7% | 5.1% | 8.4% | 3.1% | 2.4% | |
| Shodan Search Engine | 5.1% | 7.2% | 24.5% | 65.5% | 51.8% | 71.2% | 90% | 18.5% |
| Kudelski Security | 61.1% | 86.2% | | | | | | 51.8% |
| Chinanet | 4.2% | | 20.3% | 29.3% | 19.3% | 21.2% | | 9.1% |
| University of Michigan | 16.2% | | | | | | | 6.7% |
| SoftLayer Technologies* | 3.5% | | | | 23% | | | 3.5% |
| ECATEL/Quasi Networks* | 3.8% | | 9.3% | 2.7% | 2.8% | | 4.0% | 2.4% |
| FDC Servers* | | | | 1.8% | 2.2% | 3.0% | 3.8% | 2.5% |
| Amazon EC2* | | | 13% | | | | | 1.1% |
| PlusServer AG* | 1.8% | | 8.7% | | | | | 1.6% |
| Reseau National de telecommunications pour la Technologie | | | 5.7% | | | | | 0.5% |
| Ukrainian Data Center* | | | 5.3% | | | | | 0.5% |
| *Other* | 4.3% | 6.6% | 13.2% | 0.7% | 0.9% | 4.6% | 2.2% | 1.8% |

Scans during August 2015

# Network Telescope

| | Modbus | BACnet | TCP/102 | DNP3 | Ethernet | Fox | Hart | All Protocols |
|---|---|---|---|---|---|---|---|---|
| All ICS Traffic | 41.7% | 30.6% | 8.7% | 5.1% | 8.4% | 3.1% | 2.4% | |
| Shodan Search Engine | 5.1% | 7.2% | 24.5% | 65.5% | 51.8% | 71.2% | 90% | 18.5% |
| Kudelski Security | 61.1% | 86.2% | | | | | | 51.8% |
| Chinanet | 4.2% | | 20.3% | 29.3% | 19.3% | 21.2% | | 9.1% |
| University of Michigan | 16.2% | | | | | | | 6.7% |
| SoftLayer Technologies* | 3.5% | | | | 23% | | | 3.5% |
| ECATEL/Quasi Networks* | 3.8% | | 9.3% | 2.7% | 2.8% | | 4.0% | 2.4% |
| FDC Servers* | | | | 1.8% | 2.2% | 3.0% | 3.8% | 2.5% |
| Amazon EC2* | | | 13% | | | | | 1.1% |
| PlusServer AG* | 1.8% | | 8.7% | | | | | 1.6% |
| Reseau National de telecommunications pour la Technologie | | | 5.7% | | | | | 0.5% |
| Ukrainian Data Center* | | | 5.3% | | | | | 0.5% |
| *Other* | 4.3% | 6.6% | 13.2% | 0.7% | 0.9% | 4.6% | 2.2% | 1.8% |

Scans during August 2015

# Network Telescope

| | Modbus | BACnet | TCP/102 | DNP3 | Ethernet | Fox | Hart | All Protocols |
|---|---|---|---|---|---|---|---|---|
| All ICS Traffic | 41.7% | 30.6% | 8.7% | 5.1% | 8.4% | 3.1% | 2.4% | |
| Shodan Search Engine | 5.1% | 7.2% | 24.5% | 65.5% | 51.8% | 71.2% | 90% | 18.5% |
| Kudelski Security | 61.1% | 86.2% | | | | | | 51.8% |
| Chinanet | 4.2% | | 20.3% | 29.3% | 19.3% | 21.2% | | 9.1% |
| University of Michigan | 16.2% | | | | | | | 6.7% |
| SoftLayer Technologies* | 3.5% | | | | 23% | | | 3.5% |
| ECATEL/Quasi Networks* | 3.8% | | 9.3% | 2.7% | 2.8% | | 4.0% | 2.4% |
| FDC Servers* | | | | 1.8% | 2.2% | 3.0% | 3.8% | 2.5% |
| Amazon EC2* | | | 13% | | | | | 1.1% |
| PlusServer AG* | 1.8% | | 8.7% | | | | | 1.6% |
| Reseau National de telecommunications pour la Technologie | | | 5.7% | | | | | 0.5% |
| Ukrainian Data Center* | | | 5.3% | | | | | 0.5% |
| *Other* | 4.3% | 6.6% | 13.2% | 0.7% | 0.9% | 4.6% | 2.2% | 1.8% |

Scans during August 2015

# Conpot: ICS Honeypot

Open source low-interaction honeypot

Simulates protocol behavior of a real device

Interactive traffic indicates live scanner

Supports S7, Modbus, BACnet

*Actively* collect interactive scanner behavior

# Conpot: ICS Honeypot

20 Conpot instances on Amazon EC2

Dec 4, 2015 - Feb 14, 2016

Protocol / scanner distribution consistent with network telescope

Scanning is not correlated to the number of exposed devices

| | Modbus | BACnet | Siemens S7 | All |
|---|---|---|---|---|
| All ICS Traffic (total) | 1954 | 520 | 2778 | 5252 |
| All ICS Traffic (%) | 37.2% | 9.9% | 52.9% | 100% |
| University of Michigan | 18.1% | 58.5% | 29.2% | 27.9% |
| Shodan Search Engine | 23.5% | 9.4% | 24.1% | 22.4% |
| PlusServer AG* | 13.4% | 0.2% | 6.5% | 8.4% |
| ChinaNet | 3.8% | 0.0% | 12.0% | 7.8% |
| Kudelski Security | 13.5% | 16.7% | 0.0% | 6.7% |
| ECATEL: PLCScan* | 10.3% | 0.0% | 5.0% | 6.5% |
| China169 | 2.1% | 0.0% | 8.4% | 5.2% |
| ZNet* | 3.1% | 2.9% | 3.6% | 3.3% |
| ECATEL: Other* | 4.0% | 3.3% | 2.6% | 3.2% |
| Amazon EC2* | 1.5% | 1.9% | 0.0% | 1.0% |
| Rapid7 | 0.0% | 6.5% | 0.0% | 0.6% |
| *Other* | 6.7% | 0.4% | 8.6% | 7.0% |

# Conpot: ICS Honeypot

20 Conpot instances on Amazon EC2

Dec 4, 2015 - Feb 14, 2016

**Protocol / scanner distribution consistent with network telescope**

Scanning is not correlated to the number of exposed devices

| | Modbus | BACnet | Siemens S7 | All |
|---|---|---|---|---|
| All ICS Traffic (total) | 1954 | 520 | 2778 | 5252 |
| All ICS Traffic (%) | 37.2% | 9.9% | 52.9% | 100% |
| University of Michigan | 18.1% | 58.5% | 29.2% | 27.9% |
| Shodan Search Engine | 23.5% | 9.4% | 24.1% | 22.4% |
| PlusServer AG* | 13.4% | 0.2% | 6.5% | 8.4% |
| ChinaNet | 3.8% | 0.0% | 12.0% | 7.8% |
| Kudelski Security | 13.5% | 16.7% | 0.0% | 6.7% |
| ECATEL: PLCScan* | 10.3% | 0.0% | 5.0% | 6.5% |
| China169 | 2.1% | 0.0% | 8.4% | 5.2% |
| ZNet* | 3.1% | 2.9% | 3.6% | 3.3% |
| ECATEL: Other* | 4.0% | 3.3% | 2.6% | 3.2% |
| Amazon EC2* | 1.5% | 1.9% | 0.0% | 1.0% |
| Rapid7 | 0.0% | 6.5% | 0.0% | 0.6% |
| *Other* | 6.7% | 0.4% | 8.6% | 7.0% |

# Conpot: ICS Honeypot

20 Conpot instances on Amazon EC2

Dec 4, 2015 - Feb 14, 2016

Protocol / scanner distribution consistent with network telescope

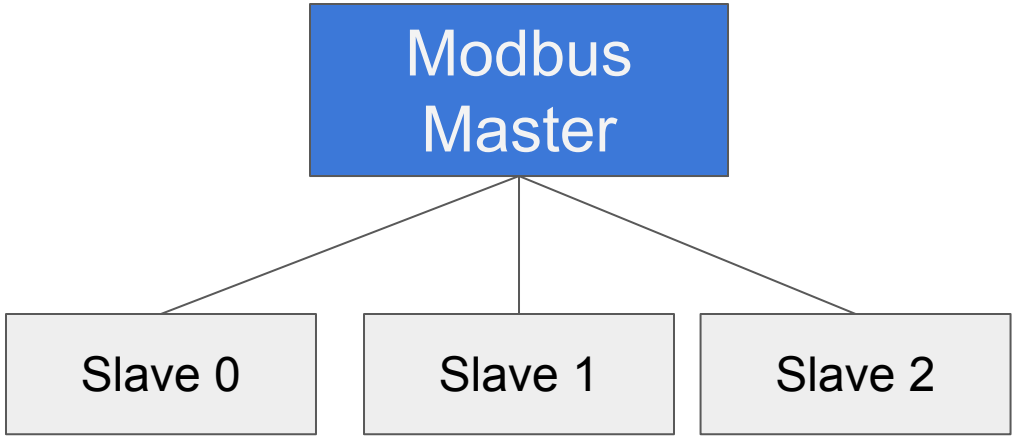
**Scanning is not correlated to number of exposed devices**

| # ICS Devices Found | | |
|---|---|---|
| Modbus | 21,596 devices | (53%) |
| BACnet | 16,752 devices | (41%) |
| Siemens S7 | 2,357 devices | (6%) |

| | Modbus | BACnet | Siemens S7 | All |
|---|---|---|---|---|
| All ICS Traffic (total) | 1954 | 520 | 2778 | 5252 |
| All ICS Traffic (%) | 37.2% | 9.9% | 52.9% | 100% |
| University of Michigan | 18.1% | 58.5% | 29.2% | 27.9% |
| Shodan Search Engine | 23.5% | 9.4% | 24.1% | 22.4% |
| PlusServer AG* | 13.4% | 0.2% | 6.5% | 8.4% |
| ChinaNet | 3.8% | 0.0% | 12.0% | 7.8% |
| Kudelski Security | 13.5% | 16.7% | 0.0% | 6.7% |
| ECATEL: PLCScan* | 10.3% | 0.0% | 5.0% | 6.5% |
| China169 | 2.1% | 0.0% | 8.4% | 5.2% |
| ZNet* | 3.1% | 2.9% | 3.6% | 3.3% |
| ECATEL: Other* | 4.0% | 3.3% | 2.6% | 3.2% |
| Amazon EC2* | 1.5% | 1.9% | 0.0% | 1.0% |
| Rapid7 | 0.0% | 6.5% | 0.0% | 0.6% |
| *Other* | 6.7% | 0.4% | 8.6% | 7.0% |

# Scan Behaviors

Relatively benign scanning




Modbus example:

70% - *Read device identification*

30% - *Report slave ID* for slave address 0 or 255 (default if empty)

No actuating commands or configuration enumeration

# Responsible Disclosure

Part of a study by Li et. al in 2013 *USENIX Security Symposium*

Vulnerability notifications for 79% of hosts with abuse WHOIS contacts

~7% of notified WHOIS contacts removed their ICS devices from Internet

Still a large remainder of exposed devices - repeat notifications ineffective

# Recap

**ICS insecurity:** ICS protocols were designed for *isolated* systems

- No built-in Internet security

**Vulnerability assessment:** Found 69,000 Internet-exposed ICS devices

- Increasing over time

**Threat landscape:** Majority of scanning is by researchers

- Some from suspicious bulletproof hosts

# An Internet-Wide View of ICS Devices

A. Mirian, **Zane Ma,** D. Adrian, M. Tischer, T. Chuenchujit,
T. Yardley, R. Berthier, J. Mason, Z. Durumeric, J. Halderman, M. Bailey