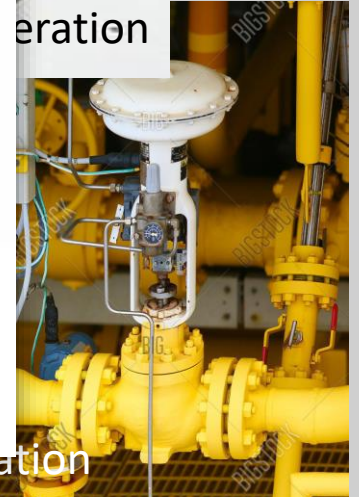


What do all



eration

Gas pressure regulation



Prison gate

Leveraging the SRTP protocol for over-the-network memory acquisition of a GE Fanuc Series 90-30

George Denton, Filip Karpíšek, Frank Breitingner, Ibrahim Baggili

Filip Karpíšek: Brno University of Technology, Czech Republic



| University of New Haven
Cyber Forensics Research & Education Group



Terminology / overview



- A **Supervisory Control And Data Acquisition (SCADA)** system is a remote monitoring and control unit that operates with coded signals over a communication channel used in a variety of applications
 - E.g., in prisons to operate cell doors, in dams to open or close gates, or in gas transmission for pressure regulation.
- A **Programmable Logic Controller (PLC)** are digital devices usually used for automation of industrial / mechanical / electrical processes. Typical applications include control of machines in factories and amusement park rides.
- *In other words, they are found in critical infrastructures and opportunity of attack.*

Prominent example – Stuxnet



- Malicious worm, first identified in 2010 that targeted industrial computer systems and was responsible for causing substantial damage to **Iran's nuclear program**.
 - Designed to erase itself in 2012 thus limiting the scope of its effects.
 - The worm is believed by many experts to be a jointly built American-Israeli **cyber weapon**, although no organization or state has officially admitted responsibility.
 - **Note:** Stuxnet manipulated the controlling software as well as the PLC!
- Stuxnet reportedly ruined almost one fifth of Iran's nuclear centrifuges.

Besides Stuxnet



- In 2011 researchers published 34 exploits in a computer security mailing list [...] and targeted seven vulnerabilities in SCADA systems produced by Siemens, Iconics, 7-Technologies and DATAC.
 - Can be employed by worms and were demonstrated at Black Hat Asia.
- The worm scans the network for new targets (PLCs), attacks these targets and replicates itself onto the found targets.
 - Original main program running on the target is not modified.

Main problem



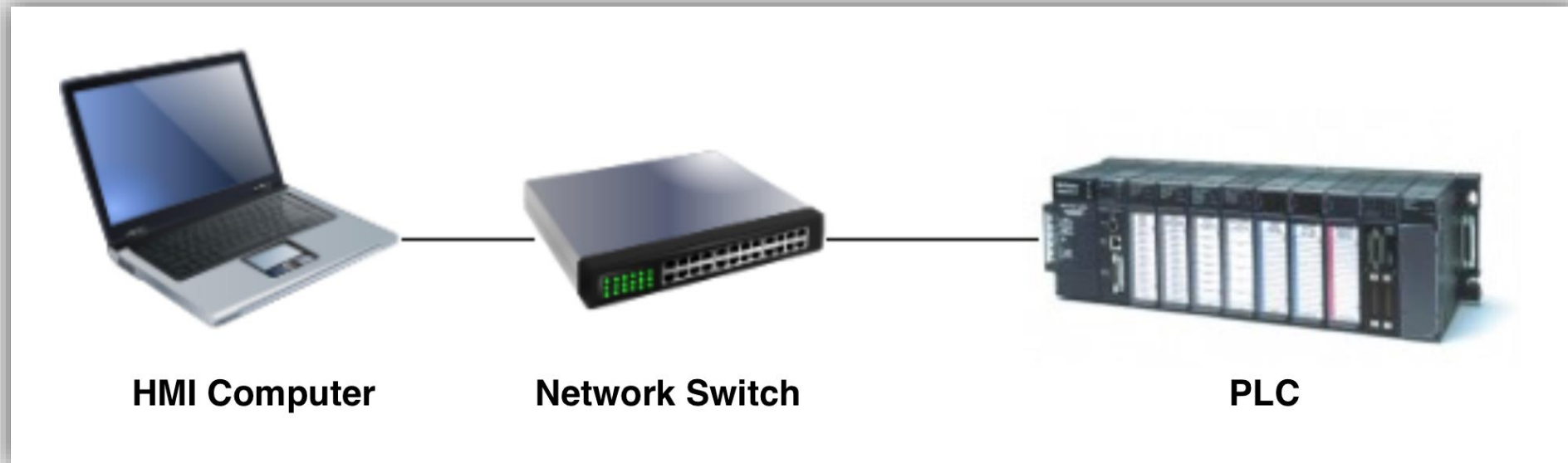
- PLCs are often installed decades ago and are still running their original configuration
 - True to the motto: “Never kill a running system”.
- That means:
 - Insecure protocols
 - No/weak passwords
- The “good”:
 - Usually not directly accessible from the Internet
 - Most protocols / tools / software is proprietary

Our contribution



- At the time of writing, no openly accessible account for the GE-SRTP protocol, invented by General Electric (GE) and is used by many of their Ethernet connected controllers.
- We implemented a software application that allows direct network-based communication with the PLC (no intermediate server is needed).
- Even though our apparatus was the GE-FANUC 90-30 PLC, our results are applicable to all appliances that utilize the protocol.

Typical and lab setup



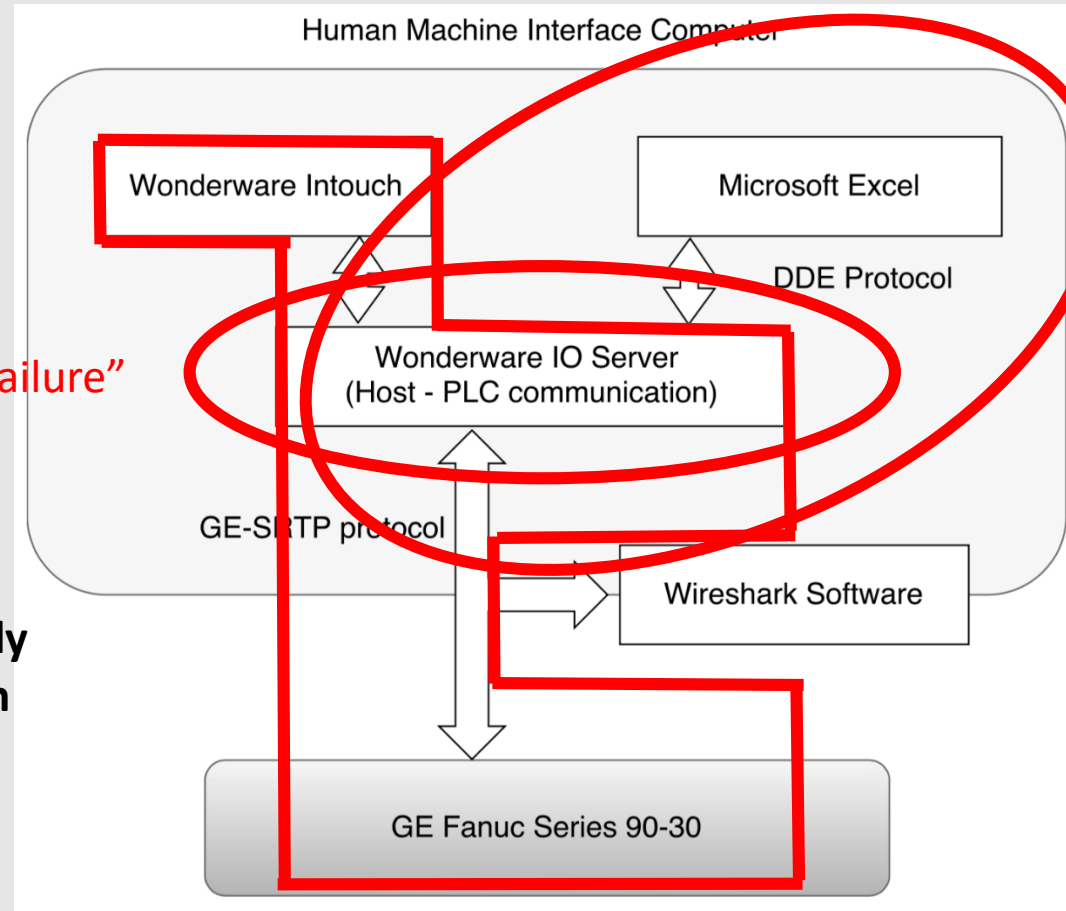
Typical dataflow



Typical flow

Problem: single point of "failure"

Conclusion: You cannot necessarily trust what you see on your screen

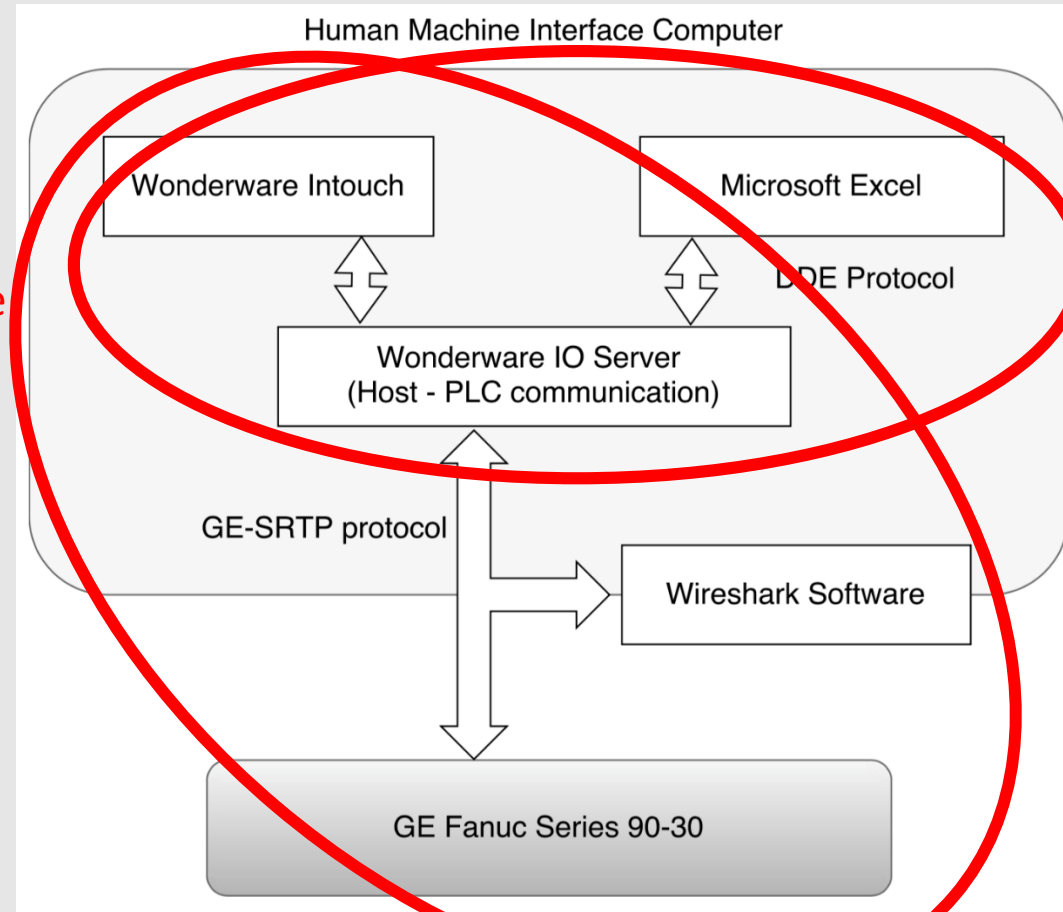


Microsoft Excel can be used as an alternative

Our work



Avoid all existing tools and communicate with the device directly.



Procedure

1. Setup lab environment
2. Produce network traffic
3. Sniff traffic with Wireshark
4. Created Lua protocol dissector
5. Create a specification of the protocol
6. Create a tool for forensic acquisition

Results



TABLE I
REQUEST MESSAGE STRUCTURE.

byte offset	field type	common value
0	type	0x02
1	unknown/reserved	0x00
2	sequence number	
3	unknown/reserved	0x00
4	text length	0x00
5-8	unknown/reserved	0x00
9	unknown/reserved	0x01
10-16	unknown/reserved	0x00
17	unknown/reserved	0x01
18-25	unknown/reserved	0x00
26	time (seconds)	0x00
27	time (minutes)	0x00
28	time (hours)	0x00
29	unknown/reserved	0x00
30	sequence number	
31	message type	0xc0
32-35	mailbox source	0x00 00 00 00
36-39	mailbox destination	0x10 0e 00 00
40	packet number	0x01
41	total packet number	0x01
42	service request code	
43-47	request type dependent	
48-55	unknown/reserved	0x00

TABLE II
TYPES OF SERVICE REQUEST CODES.

Hex value	Service request Code
0x00	PLC short status request
0x03	return control program names
0x04	read system memory
0x05	read task memory
0x06	read program memory
0x07	write system memory
0x08	write task memory
0x09	write program block memory
0x20	programmer logon
0x21	change PLC CPU Privilege Level
0x22	set control ID(CPU ID)
0x23	set PLC (run vs stop)
0x24	set PLC time/date
0x25	return PLC time/date
0x38	return fault table
0x39	clear fault table
0x3f	program store (upload from PLC)
0x40	program load (download to PLC)
0x43	return controller type and id information
0x44	toggle force system memory

TABLE IV
ACK REPLY MESSAGE STRUCTURE.

byte offset	field type	common value
0	type	0x03
1	unknown/reserved	0x00
2	sequence number	
3	unknown/reserved	0x00
4	text length	0x00
5-16	unknown/reserved	0x00
17	unknown/reserved	0x01
18-25	unknown/reserved	0x00
26	time (seconds)	
27	time (minutes)	
28	time (hours)	
29	unknown/reserved	0x00
30	unknown/reserved	value varies
31	message type	0xd4
32-35	mailbox source	0x10 0e 00 00
36-39	mailbox destination	0x20 5a 00 00
40	packet number	0x01
41	total packet number	0x01
42	status code	
43	minor status code	
44-49	return data	
50-55		

Tool summary



- Condensed our knowledge of GE-SRTP protocol into a tool → communicates with the PLC directly (TCP/IP layer)
 - No need for the Wonderware IO server
- Main focus was the forensic aspect → **read memory and identify attacks**
 - Also capable of writing to the different memory types!
- **Capabilities:** read / write to device, turn it on / off, change password, ...

GE Fanuc Controller

View

Log and PLC

Programmer log on [19]
Programmer log on [19] done
Setting PLC state [20]
Setting PLC state [20] done
Reading PLC type and ID [21]
Reading PLC Type and ID [21] done
Setting PLC state [22]
Setting PLC state [22] done
Reading PLC type and ID [23]
Reading PLC Type and ID [23] done
Setting PLC state [24]
Setting PLC state [24] done
Reading PLC type and ID [25]
Reading PLC Type and ID [25] done
Setting PLC state [26]
Setting PLC state [26] done
Reading PLC type and ID [27]
Reading PLC Type and ID [27] done
Setting PLC state [28]
Setting PLC state [28] done
Reading PLC type and ID [29]
Reading PLC Type and ID [29] done
Programmer log off [30]
Programmer log off [30] done
Programmer log on [31]
Programmer log on [31] done
Programmer log off [32]
Programmer log off [32] done

PLC IP Address: 10.111.40.4

PLC TCP Port: 12345

Connect

Disconnect

Log In

Log Out

Read Mode: Fast Slow

CPU Controller ID:
Major Type: 90-20 or 90-30
Minor Type: 90-30 CPU 331
Main Program: LITANK1

Program Number: Master is not logged in (-1)

Privilege Level: 2

Last Sweep Time[us]: 3500
Oversweep Flag: 0
Constant Sweep Mode: not active
New PLC Fault: yes
New I/O Fault: yes

PLC Fault Table Empty: no
I/O Fault Table Empty: no
Programmer Found: no
Front Panel Outputs: enabled
Front Panel RUN/STOP: STOP
OEM Protection: disabled
PLC State: Run I/O enabled

Export

Read System Memory

Discrete Inputs (%I)	Discrete Outputs (%Q)	Discrete Temporaries (%T)	Discrete Internals (%M)	System Discrete A (%SA)	System Discrete B (%SB)	System Discrete C (%SC)	System Discrete (%S)	Genius Global Data (%G)	Analog Inputs (%AI)	Analog Outputs (%AQ)	Registers (%R)
			m1: 1 m2: 1 m3: 0 m4: 1 m5: 1 m6: 0 m7: 0 m8: 0 m9: 0 m10: 0 m11: 0 m12: 0 m13: 0 m14: 0 m15: 0 m16: 0 m17: 0 m18: 0 m19: 0 m20: 0 m21: 0 m22: 0 m23: 0 m24: 0 m25: 0 m26: 0 m27: 0 m28: 0 m29: 0 m30: 0 m31: 0 m32: 0								r1: 0 r2: 32 r3: 0
Count: 512	Count: 512	Count: 256	Count: 32	Count: 32	Count: 32	Count: 32	Count: 32	Count: 1280	Count: 128	Count: 64	Count: 3
Refresh	Refresh	Refresh	Refresh	Refresh	Refresh	Refresh	Refresh	Refresh	Refresh	Refresh	Refresh
Refresh All Bit Memory Values								Refresh All Word Memory Values			
Refresh All Memory Values											

processing took 0.181s

Testing and Validation



Future work



- Add new features to the tool
- To acquire system memory, we had to send two initialization packets prior to sending a request messages
 - Need to test this on other PLCs that support GE-SRTP
- Put a different angle on the research
 - Tool was used as a Master device, to request data from a Slave PLC
 - Interesting to explore if we can make our tool behave like a Slave to steal a connection from a Slave PLC on the network
 - Read / writes from HMI IO server will be sent to impersonator and response messages sent back to the master


Take home messages




- Attackers are not only focusing on computers anymore but on all connected devices like smart phones, Internet of Things and PLCs.
- While when creating newer devices and protocols, developers may have cyber security in mind, this may not have been of priority one or two decades ago when PLCs and their protocols were developed.
- Once an attacker gains access to the network, it is possible to turn a PLC with default configuration on/off, downloading/uploading software codes or send arbitrary commands.

How easy are these PLCs to find online?



 SHODAN



[Explore](#)

[Enterprise Access](#)

[Contact Us](#)

[New to Shodan?](#)

[Login or Register](#)



Industrial Control Systems

Spotlight



XZERES Wind Turbine

XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

[Explore](#)

 **GE** Industrial Solutions

Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

[Explore GE-SRTP](#)



The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

[Explore HART-IP](#)



PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

[Explore PCWorx](#)

Tool



- You can download the tool for both
 - Win-x86
 - Win-x64
- <https://www.unhcfreg.com/datasetsandtools>

Contact & Questions?



- ibaggili@newhaven.edu
- <http://www.unhcfreg.com>
- <http://www.baggili.com>

@UNHcFREG



ResearchGate

