A Profile Of Industrial Control System Measaured by Internet-wide Scanning

Xiaohan Wang, Yunze Li

Internet-wide scanning is a newly emerging technique for security research which can evaluate the vulnerability of the network. Industrial Control Systems (ICS) are physical equipment oriented technologies and systems for actual running of plants and devices. These specialized systems are required to meet numerous, and often conflicting safety, performance and reliability requirements, so any compromise by malicious adversaries will cause servere detriment to the public. In this project, we started with a study of web-camera, which is widely-used in industrial field. Then we further explored the Internet, analysed five major Industrial Control System protocols and concluded a security issue profile by using Shodan, a search engine of internet-connected devices. Our outcomes show that although many actions have been taken to prevent attacks, vulnerbilities still exist due to both protocol inherent security flaw and operational fault.

ICS Protocols

We studied five widely-used protocols in ICS:

Open Control Systems Protocol

Modbus is a serial communication protocol published in 1979 for programmable logic controllers. It provides easy, raw access to the control system without requiring any authentication.

BACnet is a communication protocol for building automation and control networks for heating, air-conditioning, lighting, and fire detection systems.

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation. It combines standard Ethernet technologies with the media-independent Common Industrial Protocol (CIP).

Proprietary Control Systems Protocol

TRIDIUM: The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

SIEMENS S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

Web Camera

Web Cameras are highly used in industry field such as production line monitoring, warehouse surveillance and abnormality detection. In this case, we focused on serveral AVTECH Company's camera models (AVM503, AVM561)which are mainly installed in factories and plants. Our study shows that: poor authentication, bad cache control policy and weak password configuration are three major reason which make web camera insecure.

44% 200 OK no authentication at all

40% 401 Unauthorized digest authentication

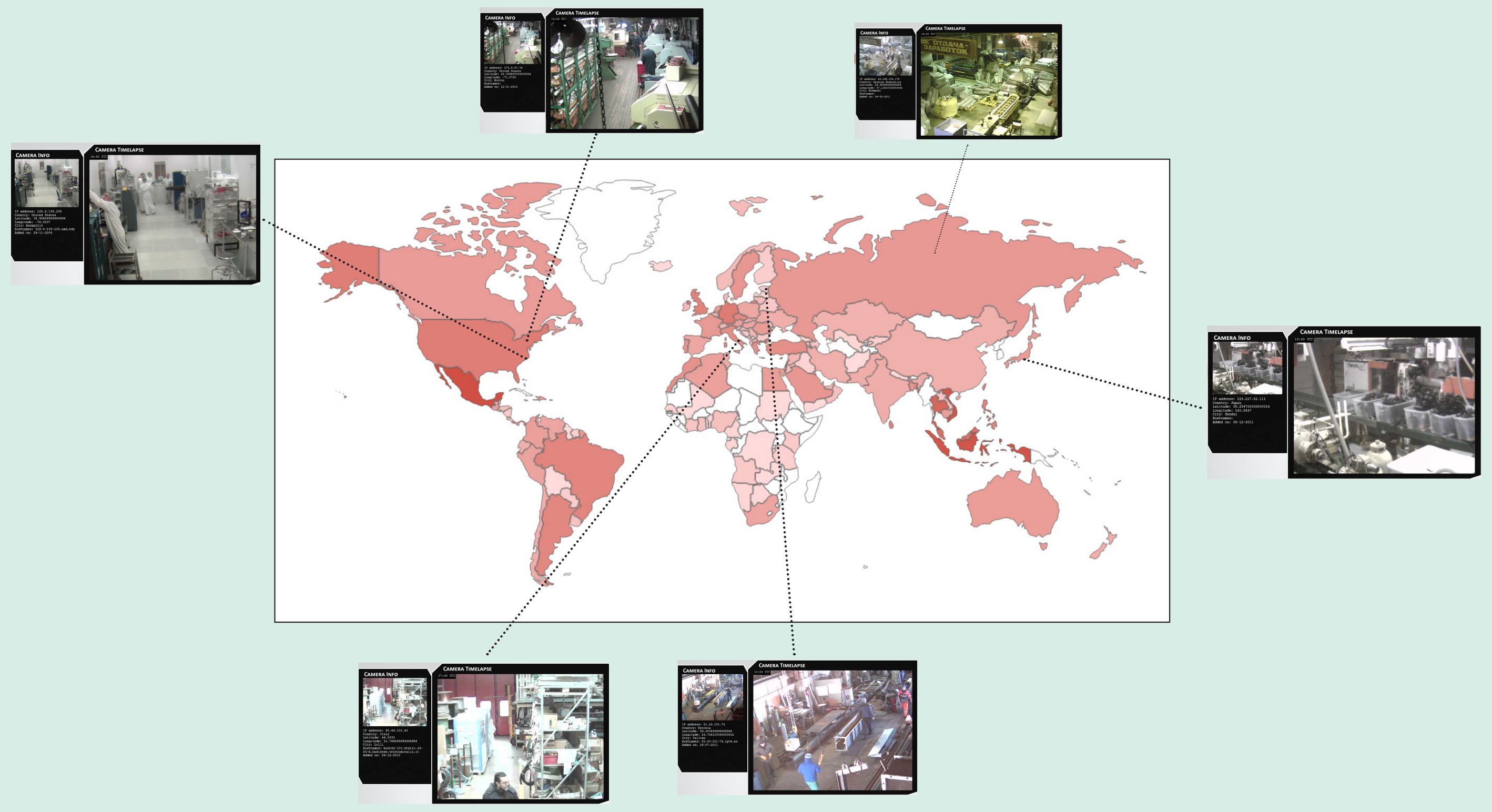
22% no-store & no-cache

26% only no-cache

AVTECH

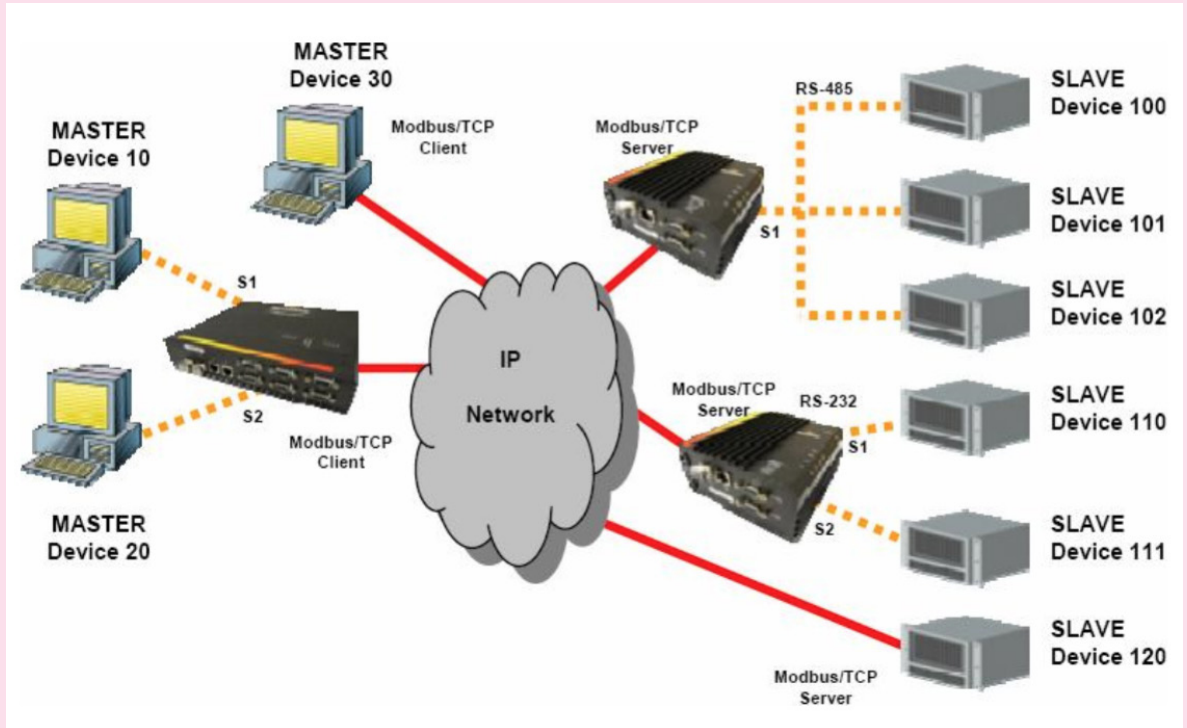
AVM503

AVM561



Modbus

MODBUS is a network protocol with primary purpose of building network from programmable logic controllers. Through the years it became one of the most common communication protocol. MODBUS is a Master-Slave protocol with several Slaves connected by only one Master. Master initiates the communication, the Slave acknowledges the request and send back the required data. MODBUS is always a target of many types of attacks and becomes much more vulnerable because of the fast spread of the internet.



Vulnerability

Reconnaissance Vulnerability

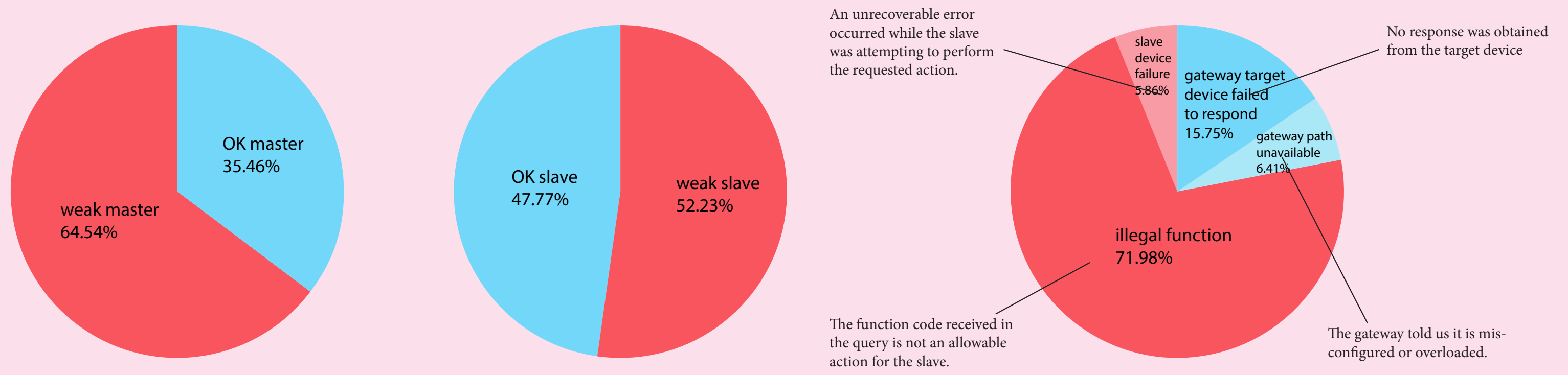
A MODBUS slave device may return Illegal Function or Illegal Address Exception responses for queries that contain an unsupported function or an illegal slave address. So an unauthenticated, remote attacker could send queries with crafted function codes or invalid addresses to carry out reconnaissance and gather information on the targeted network.

Authorization Problem

Due to lack of sufficient security checks in the MODBUS, protocol does not include an authentication mechanism for validating communication between MODBUS Master and Slave devices. This flaw could allow an unauthenticated, remote attacker to issue arbitrary commands to any Slave device via a MODBUS Master.

Remote Code Execution

This vulnerability lies in the Modbus Serial Driver bundled with 11 currently supported products by Schneider Electric. Any attacker capable of connecting to the Modbus Serial Driver listening port can cause a stack-based buffer overflow. If an attacker successfully compromises the system, the attacker can in turn target any PLC connected to the system.



An unrecoverable error occurred while the slave was attempting to perform the requested action.

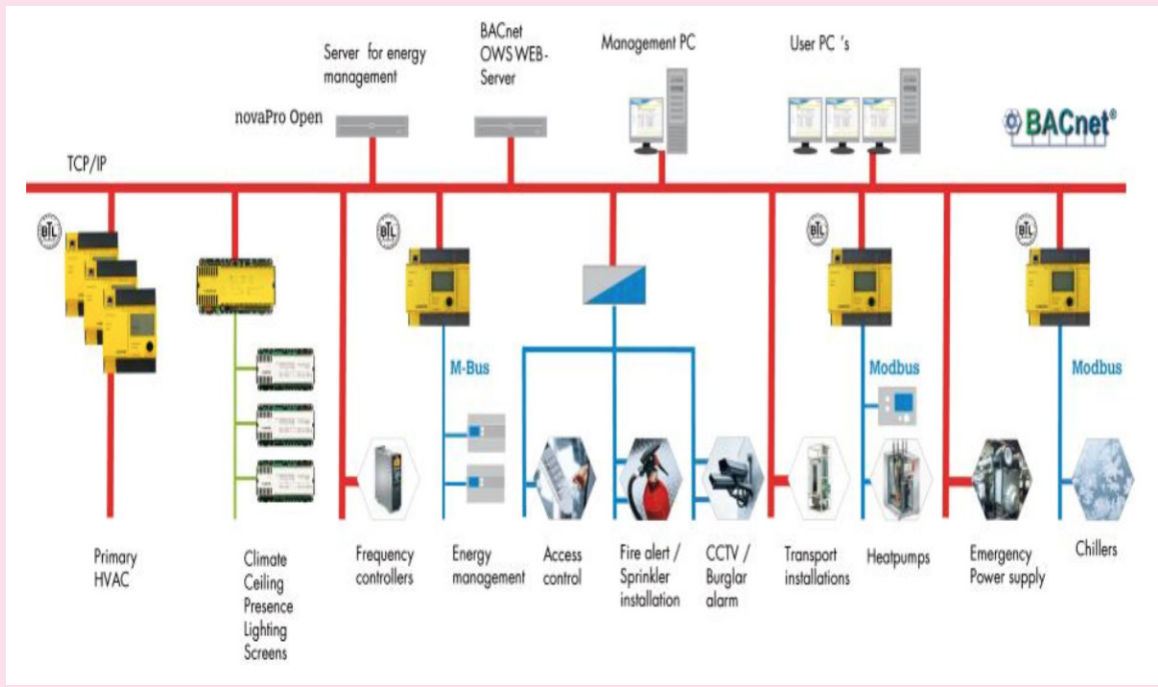
No response was obtained from the target device

The function code received in the query is not an allowable action for the slave.

The gateway told us it is misconfigured or overloaded.

BACnet

BACnet is designed to allow communication for control of heating, ventilating, air-conditioning, lighting and fire detection. Generally building control systems should not be directly connected to the internet: they are secure by isolation. However, it is more and more common to connect the separate BACnet networks together. This connection may be entirely confined behind a firewall, but more likely includes the public Internet. To be secured, most commonly it is done by virtual private networking. A router implementing VPN takes BCS traffic at one end, encrypts it with IPsec and sends to router at far end that decrypts traffic and delivers it to the destination BACnet.



Vulnerability

Authentication

The BACnet security architecture allows multiple methods for user authentication, but currently only a single method of user authentication is implemented. One solution for this lies in BACnet Network Security Clause 24. But in this clause the authentication is still vulnerable to certain attacks including man-in-the-middle, parallel interleaving attacks, replay attacks and implementation dependent flaws.

Snooping

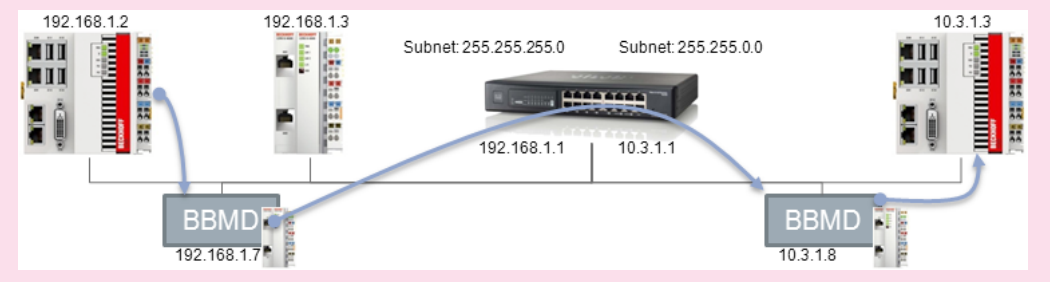
Using Read Property service to gather knowledge of device(status, location, vendor, software), device objects(sensor information), supported services and property information to understand network and plan active attacks. The Who-Has and Who-Is services also can be used to scope out devices and objects on the network.

Appplication Service Attacks

Any device can claim to be any other device using the I-Am service to spoof other devices and malicious device can send out globally broadcast Who-Is requests with no specified device instance number range so that all devices on the inter-network respond with I-Am and flood the network..

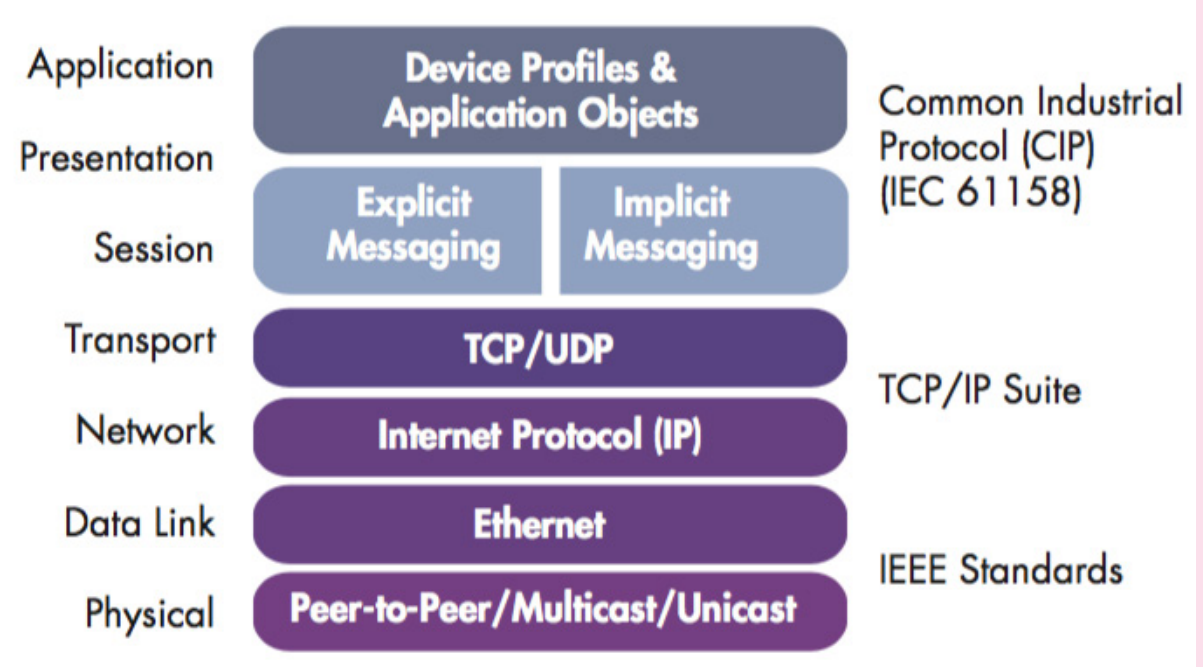
23% exposed Boradcast Managent devices

The BACnet relies on the use of broadcasts. However, since IP does not support broadcasts, a special device is required: the BACnet Broadcast Management Device (BBMD). BBMD stores global broadcast addresses, once global broadcast addresses are exposed, adversary can generate a malicious broadcast message with unknown message type and a spoofed source address. Each router receiving the broadcast will pass it on, at the same time check the message type and, not understanding the message, reply a Reject-Message-To-Network message. This will effectively deny service to the network. In our study, many captured BBMDs also exposed their broadcast address.



EtherNet/IP

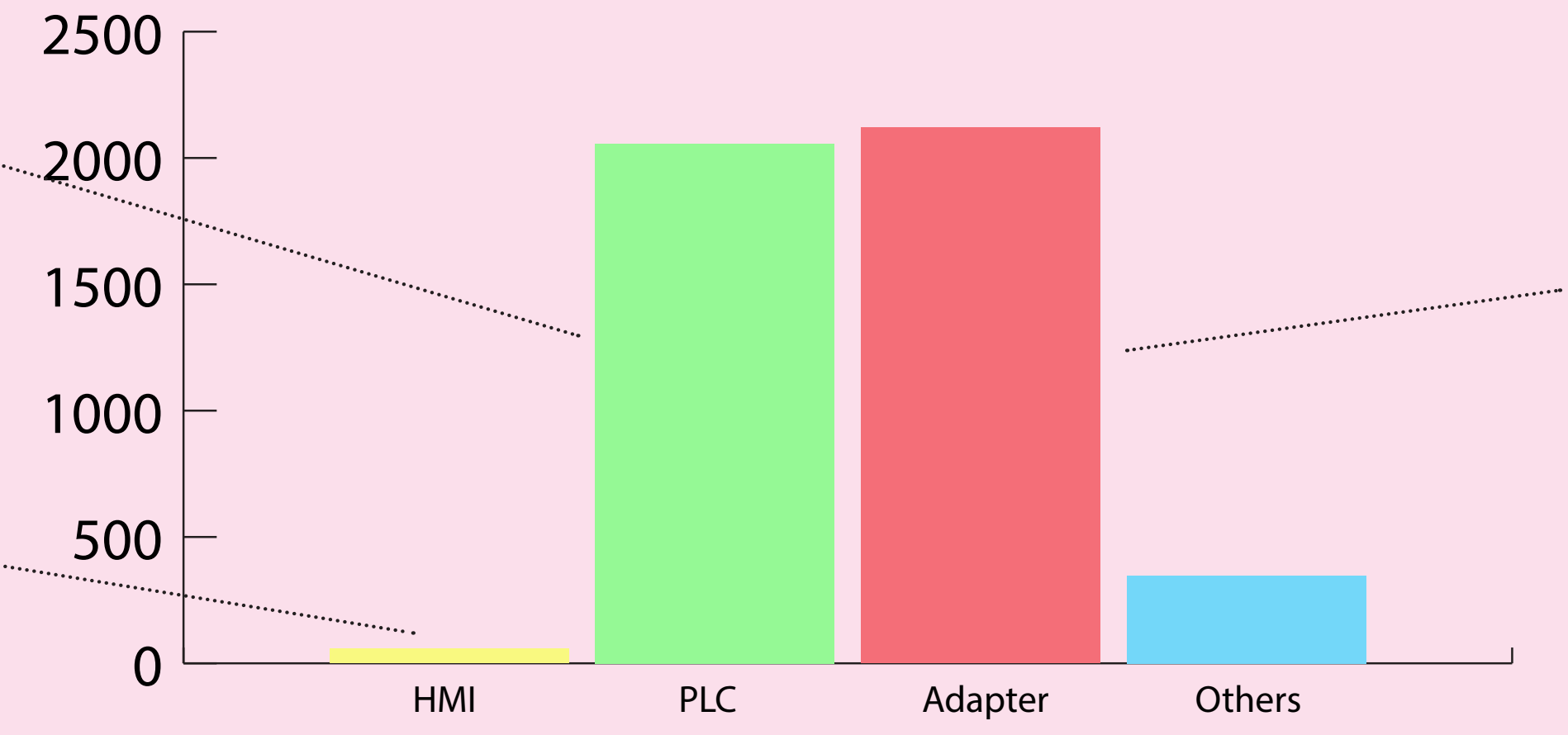
An important part of EtherNet/IP is Common Industrial Protocol (CIP) messaging. CIP encompasses a comprehensive suite of messages and services for manufacturing automation applications. Driven by industrial demands, control system becomes more accessible to wider range of users, this increases the exposure of systems to external malicious adversaries. To make matters worse, network protocols like EtherNet/IP were never designed with security. Mechanisms to ensure the authentication, confidentiality, integrity, or availability of messages were not included in the protocol.



Layer	EtherNet/IP	
Application	Device Profiles & Application Objects	Common Industrial Protocol (CIP) (IEC 61158)
Presentation		
Session	Explicit Messaging / Implicit Messaging	
Transport	TCP/UDP	TCP/IP Suite
Network	Internet Protocol (IP)	
Data Link	Ethernet	IEEE Standards
Physical	Peer-to-Peer/Multicast/Unicast	

Because authentication is only required in the establishment of a new EtherNet/IP session. After session is established between PLC and computer, the attacker can easily modify critical values in the device such as the IP, network mask and DNS servers. Further worst, expanding on this attack scheme, an attacker could listen to an active session and add a CIP packet within the sequence to modify a running PLC's IP address, thus severing the legitimate session.

A poorly designed HMI can provide an off-by-one error within the EtherNet/IP length field. This may cause problem in the size field and make the PLC into thinking a massive data message is on its way when there is none(or vice versa). Without properly ensuring a request packet is of the correct form, vulnerabilities could exists.

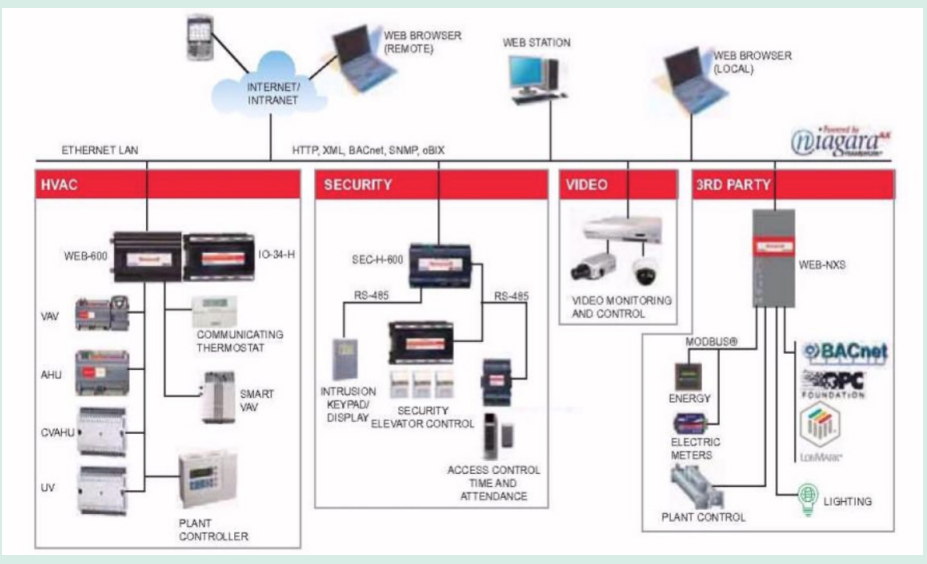


The vulnerability hiding in PLC also affects other devices such as communication adapter. For example, a PLC vulnerability was revealed in 2014, it was exploitable by transmitting arbitrary commands to the programmable logic controller or network interface card. This vulnerability could allow loss of confidentiality, integrity, and availability of the device. Although related company released patches to fix the problem, there is no following update. In this vulnerability discovery, product 1788-ENBT FLEXLogix adapter is affected, and we find 20 devices (1%) in our result.

TRIDIUM

Connecting minds and machines

Tridium Niagara Framework is widely deployed throughout enterprises, military and government. Tridium has applications for building control, industrial automation, medical equipment, physical security, energy information systems, telecommunications, smart homes, machine-to-machine (M2M) and smart services. Tridium Niagara Framework is built on IP and meant to provide web-based management, it is a boon for efficiency, but also a chance for security nightmares.



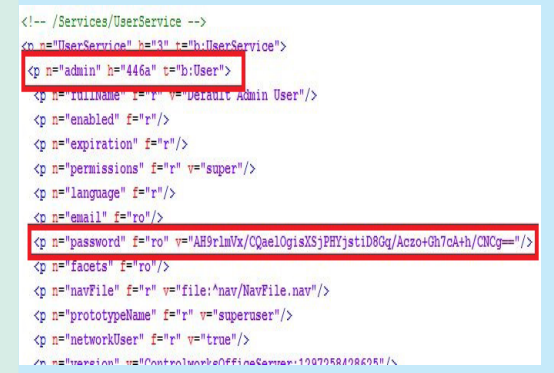
DIRECTORY TRAVERSAL

By default, the Tridium Niagara AX software is not configured to deny access to restricted parent directories. This vulnerability allows a successful attacker to access the file that stores all system usernames and passwords.

PLAINTEXT STORAGE IN A COOKIE

Usernames and passwords are stored using Base64 encoding in a cookie within the default authentication configuration. This significantly lowers the difficulty of exploitation by an attacker.

WEAK CREDENTIAL STORAGE

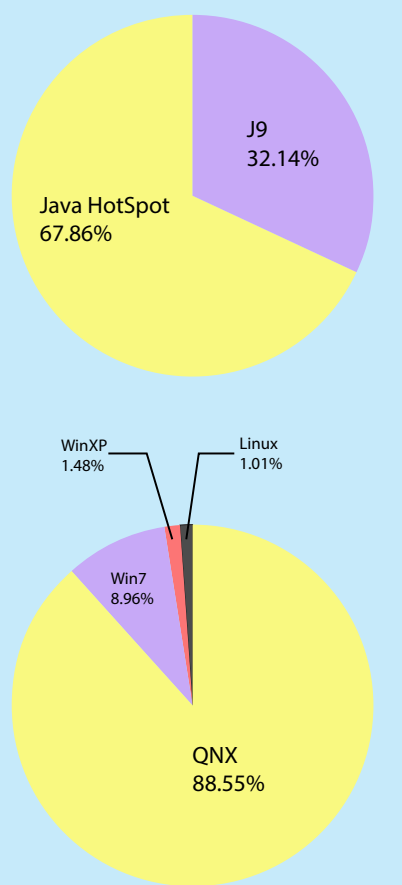


```
<!-- /Services/UserService -->
<p n="UserService" h="3" t="b:UserService">
<p n="admin" h="446a" t="b:User">
  <p n="fullName" f="r" v="Default Admin User"/>
  <p n="enabled" f="r"/>
  <p n="expiration" f="r"/>
  <p n="permissions" f="r" v="super"/>
  <p n="language" f="r"/>
  <p n="email" f="ro"/>
  <p n="password" f="ro" v="AH9rlmVx/CQael0gisXSjPHYjstiD8Gq/Aczo+Gh7cA+h/CNCg=="/>
  <p n="facets" f="ro"/>
  <p n="navFile" f="r" v="file:^nav/NavFile.nav"/>
  <p n="prototypeName" f="r" v="superuser"/>
  <p n="networkUser" f="r" v="true"/>
```

The system insecurely stores user authentication credentials, which are susceptible to interception and retrieval. User authentication credentials are stored in the Niagara station configuration file: config.bog, which is located in the root of the station folder.

Software Company Cylance launched a project which investigated the vulnerable part of Fox protocol, they easily retrieved enough information from Tridium device such as the specific platform version (a slightly outdated version) and OS specifics (QNX running on an embedded device). By using this information, they further hacked into the device and extracted the most sensitive config.bog file on a Tridium device which contains the usernames and passwords for all the users on the device.

Exploring the device information always is the first step of an attack, and collecting device information is surprisingly easy. In our project, we also simulated data collection step and found running environment information of 20127 Tridium devices in total.



PREDICTABLE SESSION IDs

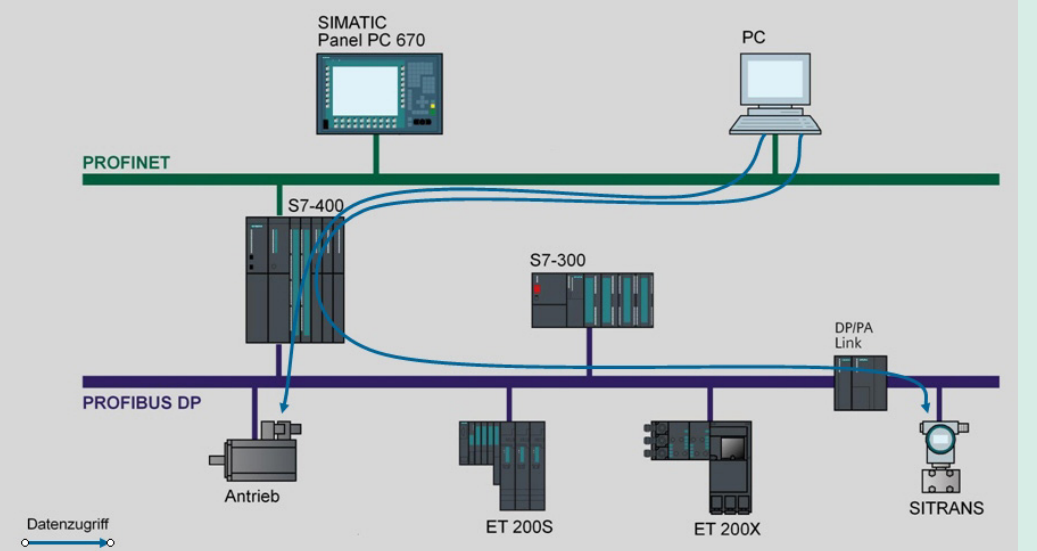
The software generates a predictable session ID or key value, allowing an attacker to guess the session ID or key.

69%

FoxUsernamePasswordAuthAgent: the fox protocol provides an agent to authenticate user. There are 13824 agents detected. Niagara Framework provides three authentication points including: Workbench-to-station via Fox, Station-to-station via Fox and Web browser-to-station(HTTP).

SIEMENS

S7 Communication is a Siemens proprietary protocol that runs between programmable logic controllers of the Siemens S7 family. It is used for PLC programming, exchanging data between PLCs, accessing PLC data from supervisory control and data acquisition. S7 is developed since 1995, there are many different kinds of vulnerabilities.



Vulnerability

ISO-TSAP

PLCs in S7 communicate over ISO-TSAP on TCP port 102. ISO-TSAP is layered on Top of TCP connections. However, packets transmitted through ISO-TSAP are sent in plaintext.

MIMA

Uses a 'layering principle' which means that even if an encrypted bridge between the client and server on top of the TCP is implemented, it can still be Man-In-The-Middle attacked. The protocol hasn't been revised or even looked at since the late 80s.

Flawed Authentication

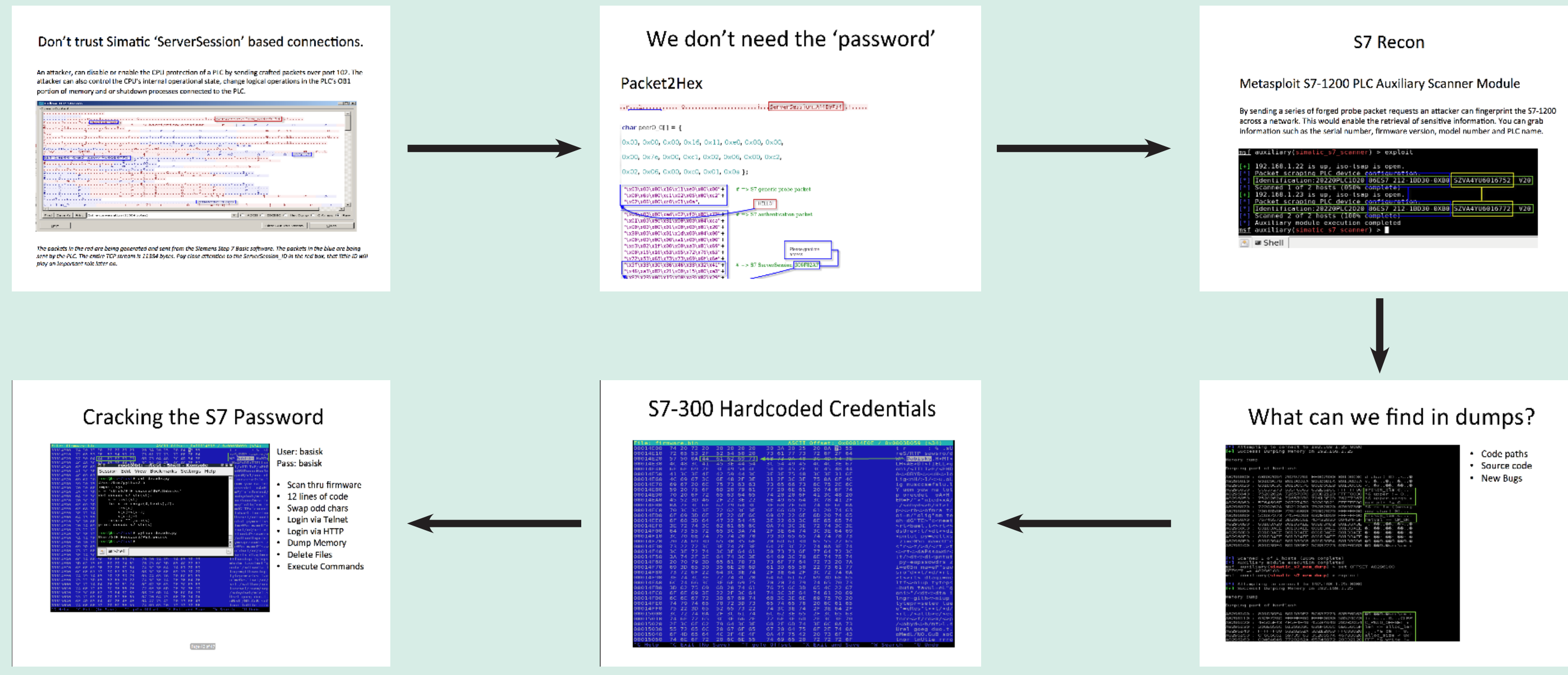
If an attacker has captured packets containing the authenticated server session from the automation network, attacker can re-authenticate using the same packet and bypass this level of protection. It is also possible to generate self-made packets based on pre-existing captured packets and use them to crack the password. Since Siemens doesn't enforce expiring sessions we can simply use any Server Session ID.

CPU Memory Protection

It is possible to read and write data to the PLC's memory even when the password protection is enabled.

It is possible to retrieve sensitive information from the PLC through memory dumping.

Its is also possible to disable the password protection feature on the PLC by flipping the security bit back to an OFF state.



Don't trust Simatic 'ServerSession' based connections.

An attacker, can disable or enable the CPU protection of a PLC by sending crafted packets over port 102. The attacker can also control the CPU's internal operational state, change logical operations in the PLC's OB1 portion of memory and or shutdown processes connected to the PLC.

The packets in the red are being generated and sent from the Siemens Step 7 Basic software. The packets in the blue are being sent by the PLC. The entire TCP stream is 11384 bytes. Pay close attention to the ServerSession_ID in the red box, that little ID will play an important role later on.

We don't need the 'password'

Packet2Hex

S7 Recon

Metasploit S7-1200 PLC Auxiliary Scanner Module

By sending a series of forged probe packet requests an attacker can fingerprint the S7-1200 across a network. This would enable the retrieval of sensitive information. You can grab information such as the serial number, firmware version, model number and PLC name.

```
msf auxiliary(simatic_s7_scanner) > exploit

[+] 192.168.1.22 is up, iso-tsap is open.
[*] Packet scraping PLC device configuration.
[*] Identification:20220PLC1020 06ES7 212-1BD30-0XB0 SZVA4YU6016752 V20
[*] Scanned 1 of 2 hosts (050% complete)
[+] 192.168.1.23 is up, iso-tsap is open.
[*] Packet scraping PLC device configuration.
[*] Identification:20220PLC2020 06ES7 212-1BD30-0XB0 SZVA4YU6016772 V20
[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(simatic_s7_scanner) >
```

What can we find in dumps?

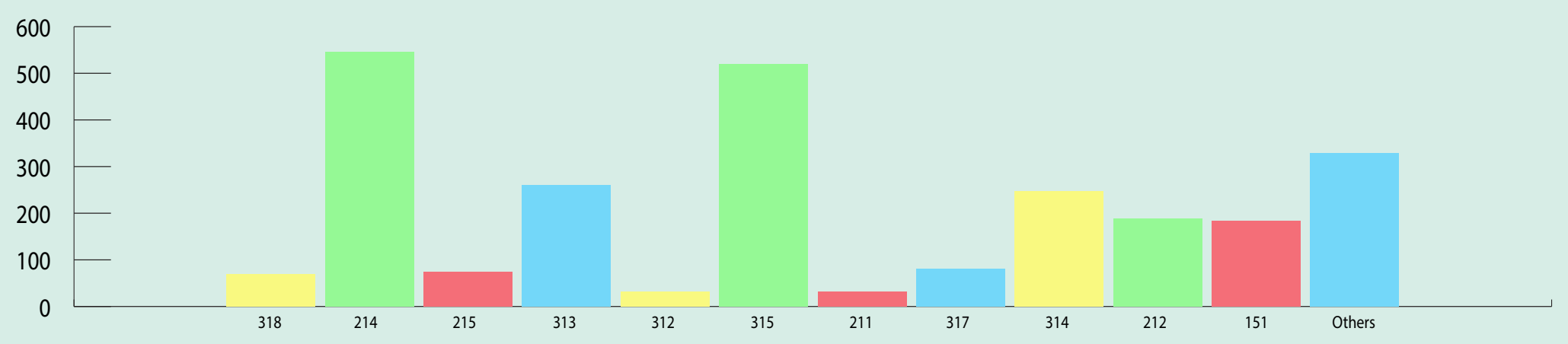
- Code paths
- Source code
- New Bugs

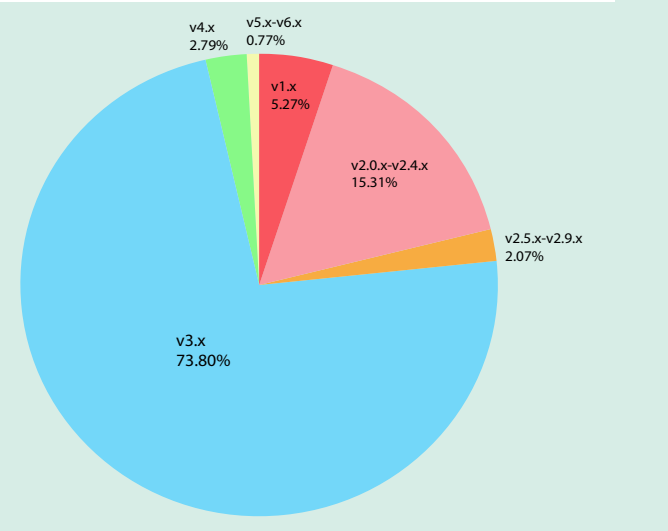
S7-300 Hardcoded Credentials

Cracking the S7 Password

User: basisk
Pass: basisk

- Scan thru firmware
- 12 lines of code
- Swap odd chars
- Login via Telnet
- Login via HTTP
- Dump Memory
- Delete Files
- Execute Commands





In above case study, "6ES7 212" and "6ES7 317" are used as targets. We found 188 devices with the same hardware model of 212 and 80 of 317 (7.7% of the total exposed devices). We also found many devices' firmware version were out dated.

References:

1. Vulnerabilities of MODBUS RTU Protocol - A Case Study, Gabpr Jakaboczki, Eva Adamko.
2. Exploiting controls systems demonstration using Shodan, DB Exploit, Google Hacking, Diggity, Kali Linux, Micheal Chipley.
3. BACnet Wide Area Network Security Threat Assessment, David G.Holmberg.
4. Basecamp Digital Bond, Attacking ControlLogix: ControlLogix Vulnerability Report, 2012.
5. Securing EtherNet/IP Control Systems using Deep Packet Inspection Firewall Technology, Cylance.