Rogue7: Rouge Engineering-Station Attacks on Simatic S7 PLCs

Sara Bitan
CyberDay 2020

Joint work:
Eli Biham. Aviad Carmel, Alon Dankner, Uriel Malin, Avishai Wool
Technion Tel-Aviv University
1. Uncovered design vulnerabilities in the S7 protocol
2. An exploit that performs remote stealth programming of an S7-1500 PLC
What are Industrial Control Systems?

• A distributed computerized system
• Operates and monitors physical devices
• Controls critical infrastructure
• The core of the ICS
• A bridge between the virtual and the kinetic worlds
• The target of our attacks
PLC Interfaces - Our Way In!

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs

TIA Portal V15
www.engrsajidrehman.net

The Control Program

S7 Protocol

PLC Operating System
Secure ICS Topology

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs

Source: NCCIC IR-18-214

10-June-20
ICS Security Challenges

• No automatic update or frequent patching
• No inline protection
Stuxnet Malware (9/2010)

• The most famous cyber-attack on ICS
• Targeted Siemens S7-300 PLC
• Infected both HMI and engineering station packages
TIA as a Soft Belly

• Typically attacks are exploiting the engineering station vulnerabilities:
  • CVE-2012-3015: untrusted search path vulnerability in Siemens SIMATIC STEP7 v5.5–July-26-2012
  • CVE-2019-10915: authentication bypass in TIA v15.1 –July-11-19 by Tenable Security
Our Attack

- Exploits vulnerabilities in the PLC Operating System
  - S7 protocol

- Any vulnerable station/device in the network can serve as an attack machine
Siemens S7-1500 PLC

• One of two new members in the SIMATIC PLCs product line
  • S7-1500 is the high-end PLC
  • The other is S7-1200
Why We Targeted S7 PLCs?

- Security enhancements of the S7 protocol
  - Integrity and replay protection of the messages
- PLC access control – password based
  - Blocks our attack, but not always used

<table>
<thead>
<tr>
<th>Protection level</th>
<th>Access</th>
<th>Access permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>HMI</td>
<td>Read</td>
</tr>
<tr>
<td>Full access (no protection)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Read access</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HMI access</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>No access (complete protection)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The S7 Protocol

Session oriented. Session begins with a 4-ways handshake.

ISO transport over TCP.

Session ID:

Client can create, modify and delete objects in the PLC's internal memory.

Example: create a server session object.

Version P3:

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs
The P3 Handshake Protocol

KDK = Key Derivation Key

Enc_{PLC_PUB_KEY}(Keying Material)

Req, Hello, RID, Seq=1

Res, Hello, SID, Model, Firmware version, Challenge, Seq=1

Req, SID, Encrypted Keying Material, Response, Seq=2

Res, OK, Seq=2

Session_key = f(Challenge, KDK)

- Integrity protection: hmac-sha256 over packet with Session_key

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs

10-June-20
1. Generate 20 bytes PreKey
   1. Encrypt it using EC-ElGamal–like encryption with the plc public key and add it to Keying material
2. Calculate KDF on PreKey and get
   1. Checksum Encryption Key (CEK)
   2. Checksum Seed (CS)
   3. Key Encryption Key (KEK)
3. Concatenate the KDK to the challenge, encrypt them using AES-CTR with the KEK, and add to Keying material
4. Initiate a Tabulation Hash with CS and calculate checksum over (3)
5. Encrypt (4) using AES-ECB with CEK and add to Keying material
P3 – Asymmetric Keys

• The public keys are stored in compressed .key files at [TIA INSTALLATION]\Data\Hwcn\Custom

• Each key file contains
  • Metadata (version, key type, key family, etc.)
  • Key data – PLC public key for the EC-ElGamal-like encryption
P3 – An Example .key File

version: 1

orderNumber: s71500-connection

firmwareVersion:

keyType: connection

familyType: S7-1500

key data: 8456...
One Ring to Rule Them All

With Many Working Forged Copies

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs
Attacking the P3 Program
Download Exchange

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs
Control Program Create Message

Create Object Request

HMAC-SHA256 over packet with session key

Object MAC

Create Program Cycle Object Block

Object Code

Source Code

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs
Control Program Representation

Yellow Program

Blue Program

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs
Rogue Engineering Station

- An attack script that impersonates a TIA

Rogue Engineering Station

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs
Rogue Engineering Workstation Program Download Attack

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs

Req, Hello, RID, Seq=1

Res, Hello, SID, n2, Model, Firmware version, Challenge, Seq=1

Req, SID, Encrypted Keying material, Response, Seq=2

Res, OK, Seq=2

Session_key=f(Challenge, Keying material)

Run
Rogue Engineering Workstation
Stealth Program Injection

Req, Hello, RID, Seq=1

Res, Hello, SID, n, Model, Firmware version, Challenge, Seq=1

Req, SID, Encrypted Keying material, Response, Seq=2

Res, OK, Seq=2

Session_key=f(Challenge, Keying material)

Run

Rogue7: Rogue Engineering Station Attacks on Simatic S7 PLCs

≠
Step7 Impersonation

My Lab

The Wall

King’s Landing
Attack Demo
Summary

• Vulnerabilities in the S7 protocol – P3
  • TIA is not authenticated
  • “One Ring to Rule them All”
• A Python attack tool that impersonates TIA
  • Download a recorded program to any S7-1500 PLC
  • Stealth program injection attack
Thank you!

SaraB@cs.technion.ac.il