CTIT

SMART NETWORK ACCESS CONTROL FOR SMART SCADA

Dina Hadžiosmanović, Damiano Bolzoni, Pieter Hartel

PROBLEM

How to protect SCADA systems from security **threats**

1. unauthorised devices that connect and start operating
   and
2. authorised devices that start misbehaving

when systems are (fully) **automated,** port numbers **(pseudo) random** and protocol specifications **unknown**?

PREVIOUS WORK

- Rule-based network access control (NAC) (e.g., firewalls, VLAN)
  CAN ADDRESS THREAT: **1.**
- Behaviour-based NAC using **known** port numbers on regular networks [1]
  CAN ADDRESS THREAT: **2.**

OUR SOLUTION

Behaviour-based network access control for SCADA which:

- does **not use port numbers**,
- does **not use protocol specifications**,
- can detect misbehaviour of authorised devices (e.g., as in the Stuxnet case [2]).

CAN ADDRESS THREATS: 1. AND 2.

APPROACH

- Profile usual network communication between devices as:

  device A $\xrightarrow{\{X,Y,Z,\ldots\}}$ **device B**

- A link profile (e.g., {X,Y,Z}) is based on four pattern aspects:
  (1) device fingerprint, (2) connectivity pattern, (3) pseudo-protocol pattern, (4) packet content.

- Validate approach on a real-life SCADA (*Figure 1.*)

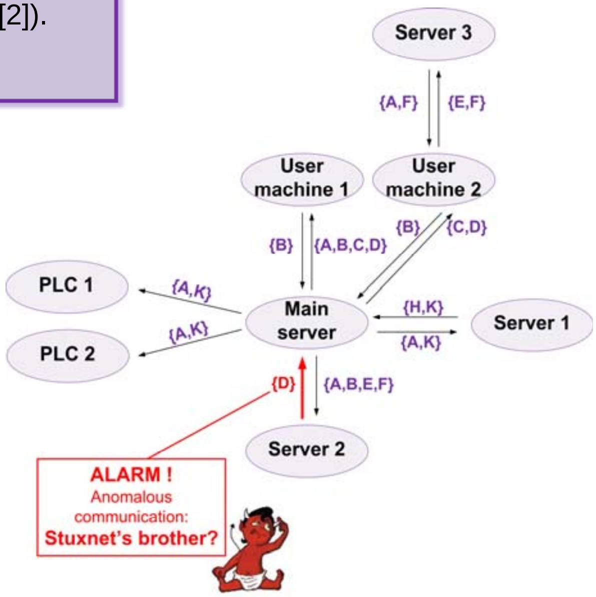

Figure 1. Anonymised communication model of a real-life plant.

References:

[1] Vanessa Frias-Martinez, Joseph Sherrick, Salvatore J. Stolfo, and Angelos D. Keromytis. A network access control mechanism based on behavior profiles. In *Proceedings of the 2009 Annual Computer Security Applications Conference, ACSAC* '09, pages 3–12, Washington, DC, USA, 2009. IEEE Computer Society.

[2] Nicholas Falliere, Liam O Murchu, and Eric Chien. Symantec security response: W32.stuxnet Dossier, 2011.

UNIVERSITEIT TWENTE.