UNIVERSITY OF TWENTE.

ON THE FEASIBILITY OF DEVICE FINGERPRINTING IN INDUSTRIAL CONTROL SYSTEM

Marco Caselli, Dina Hadziosmanovic, Emmanuele Zambon, Frank Kargl

CRISALIS SECURING CRITICAL INFRASTRUCTURES

CRitical Infrastructure Security AnaLysIS

INTRODUCTION
WHAT ARE WE GOING TO SEE IN THIS PRESENTATION?

I. *What is "fingerprinting"?*
II. *Why fingerprinting?*
III. *Fingerprinting and ICS*
IV. *What is there already in place?*
V. *What is still missing?*

Is it feasible to do fingerprinting in ICS environments?

WHAT IS THIS ALL ABOUT?
FINGERPRINTING DEFINITION

In the ICT field, the **fingerprinting** is the process of determining hardware and software components by remotely looking at some properties (network packets characteristics, time patterns, etc.)

It can be of two types: **active** and **passive**.

MOTIVATIONS
WHY FINGERPRINTING? WHY FINGERPRINTING ON ICS?

- Penetration Testing
- Support to Network Administrators
- Support to Security Systems

FINGERPRINTING TECHNIQUES
EXAMPLES ON THE ISO/OSI MODEL

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data link
1. Physical

Application Fingerprinting

TCP/IP Stack Fingerprinting

Analog Fingerprinting

TESTING
DOES STANDARD FINGERPRINTING WORK IN ICS?

TCP/IP stack fingerprinting

- Two examples:
  - Nmap: the "*lack of integration*" problem
  - Xprobe2++: the "*extra information*" problem

Analog fingerprinting

- Unfeasible. No guarantee to directly perceive signals from components

Application fingerprinting

- It depends on the protocols

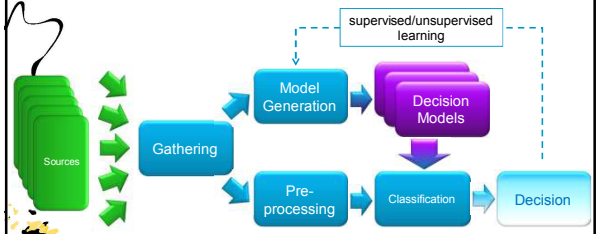
OUR APPROACH
THREE STEPS TOWARDS APPLYING FINGERPRINTING ON ICS

Step 1: Define guidelines for fingerprinting tools developments

Step 2: Define properties and limitations of ICS environments

Step 3: Merge the outputs of the two previous steps to lay the foundations for developing effective ICS fingerprinters

STEP 1 - FINGERPRINTING TOOLS
A REFERENCE MODEL

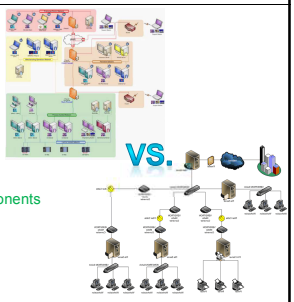


STEP 2 - ICS SCENARIO
SIMILARITIES AND DIFFERENCES WITH A STANDARD LAN SCENARIO

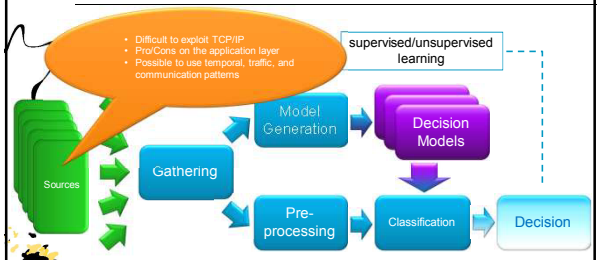
Fingerprinting "pros/cons"

- Device Heterogeneity
- Proprietary protocols
- Device computational power
- Long-running TCP sessions

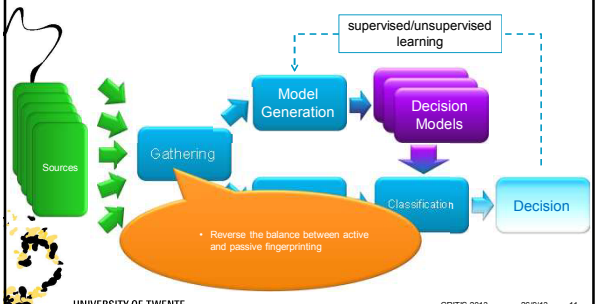
- Long life-cycle of devices
- Predictable behavior of components
- Stable topology
- Protocol specification



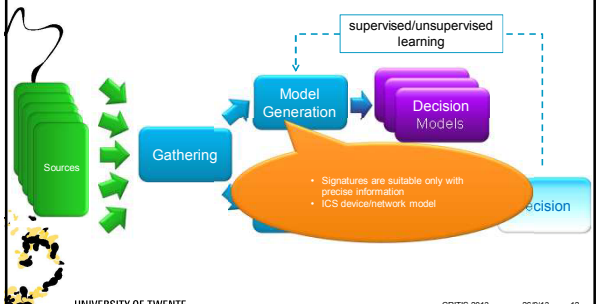
STEP 3 - ICS FINGERPRINTING TOOLS
A REFERENCE MODEL



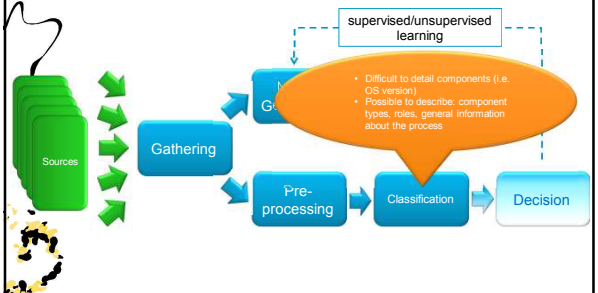
STEP 3 - ICS FINGERPRINTING TOOLS
A REFERENCE MODEL



STEP 3 - ICS FINGERPRINTING TOOLS
A REFERENCE MODEL



STEP 3 - ICS FINGERPRINTING TOOLS
A REFERENCE MODEL



DEVELOPMENT
FROM A "PROOF OF CONCEPT" TO A COMPREHENSIVE FINGERPRINTER

2nd Phase

Fingerprinter Development

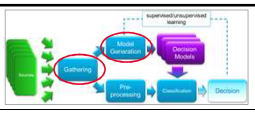
Such implementation has a twofold motivation:

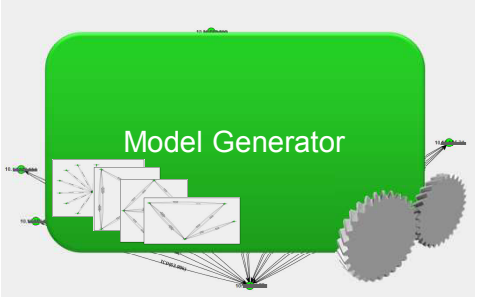
- Verify the proposed framework
- Test the correctness of our considerations

FLOW FINGERPRINTING
AN ALTERNATIVE TO STANDARD FINGERPRINTING METHODS

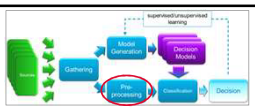
- **Idea:** *recognize devices by traffic and communication patterns. We concentrate on roles devices have in the network.*
- **Key points:**
  - Purely passive fingerprinter
  - No need of much information on protocols or implementations
  - It relies on creating representations of known ICS devices

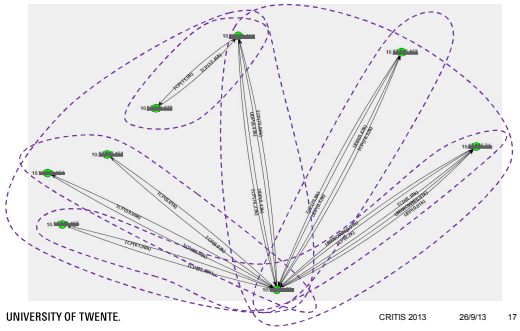
A PRACTICAL EXAMPLE
TESTS ON AN ICS PRODUCTION SYSTEM



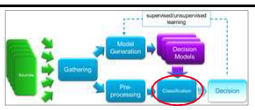


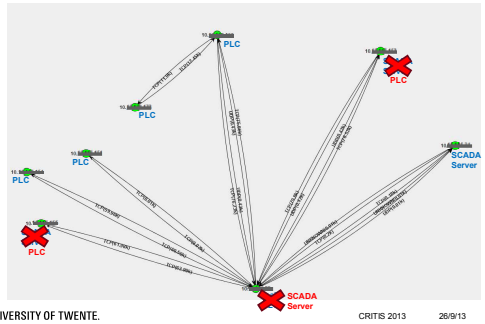
A PRACTICAL EXAMPLE
TESTS ON AN ICS PRODUCTION SYSTEM



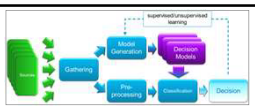


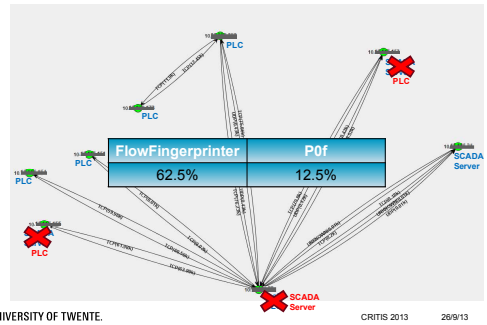
A PRACTICAL EXAMPLE
TESTS ON AN ICS PRODUCTION SYSTEM





A PRACTICAL EXAMPLE
TESTS ON AN ICS PRODUCTION SYSTEM





FINAL REMARKS & FUTURE WORKS

Is it feasible to do fingerprinting in ICS environments? **Yes.**

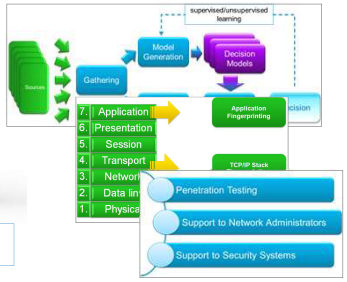
We improve ICS fingerprinting by looking at specific features of industrial control systems

We are still testing the Flow Fingerprinter

Our aim is to integrate flow fingerprinting analysis with standard techniques

THANKS
DANK U WEL

Questions?



Marco Caselli
m.caselli@utwente.nl

REFERENCES

I. C. Pfleeger, S. Pfleeger, and M. Theofanos, "A methodology for penetration testing", Computer & Security, 1989.
II. G. Taleck. Ambiguity resolution via passive os fingerprinting. In Recent Advances in Intrusion Detection, pages 192-206. Springer, 2003.
III. V. Paxson. Automated packet trace analysis of tcp implementations. In ACM SIGCOMM Computer Communication Review, volume 27, pages 167-179. ACM, 1997.
IV. R. Gerdes, T. Daniels, M. Mina, and S. Russell. Device identication via analog signal fingerprinting: A matched filter approach. In Network and Distributed System Security Symposium (NDSS), 2006.
V. T. Kohno, A. Broido, and K. Clay. Remote physical device fingerprinting. Dependable and Secure Computing, IEEE Transactions on, 2(2):93-108, 2005.
VI. A. Moore and K. Papagiannaki. Toward the accurate identication of network applications. Passive and Active Network Measurement, pages 41-54, 2005.
VII. P. Haner, S. Sen, O. Spatscheck, and D. Wang. Acas: automated construction of application signatures. In Proceedings of the 2005 ACM SIGCOMM workshop on Mining network data, pages 197-202. ACM, 2005.
VIII. A. Mahmood, C. Leckie, J. Hu, Z. Tari, and M. Atiquzzaman. Network traffic analysis and SCADA security. Handbook of Information and Communication Security, pages 383-405, 2010.
IX. R. Barbosa, R. Sadre, and A. Pras, "Difficulties in modeling SCADA traffic: A comparative analysis," in Passive and Active Measurement. Springer, 2012.