

DYPOSIT: Dynamic Policies for Shared Cyber-Physical Infrastructures under Attack

Professor Awais Rashid

Director, Security Lancaster

<https://dyposit.eu/>



The Context

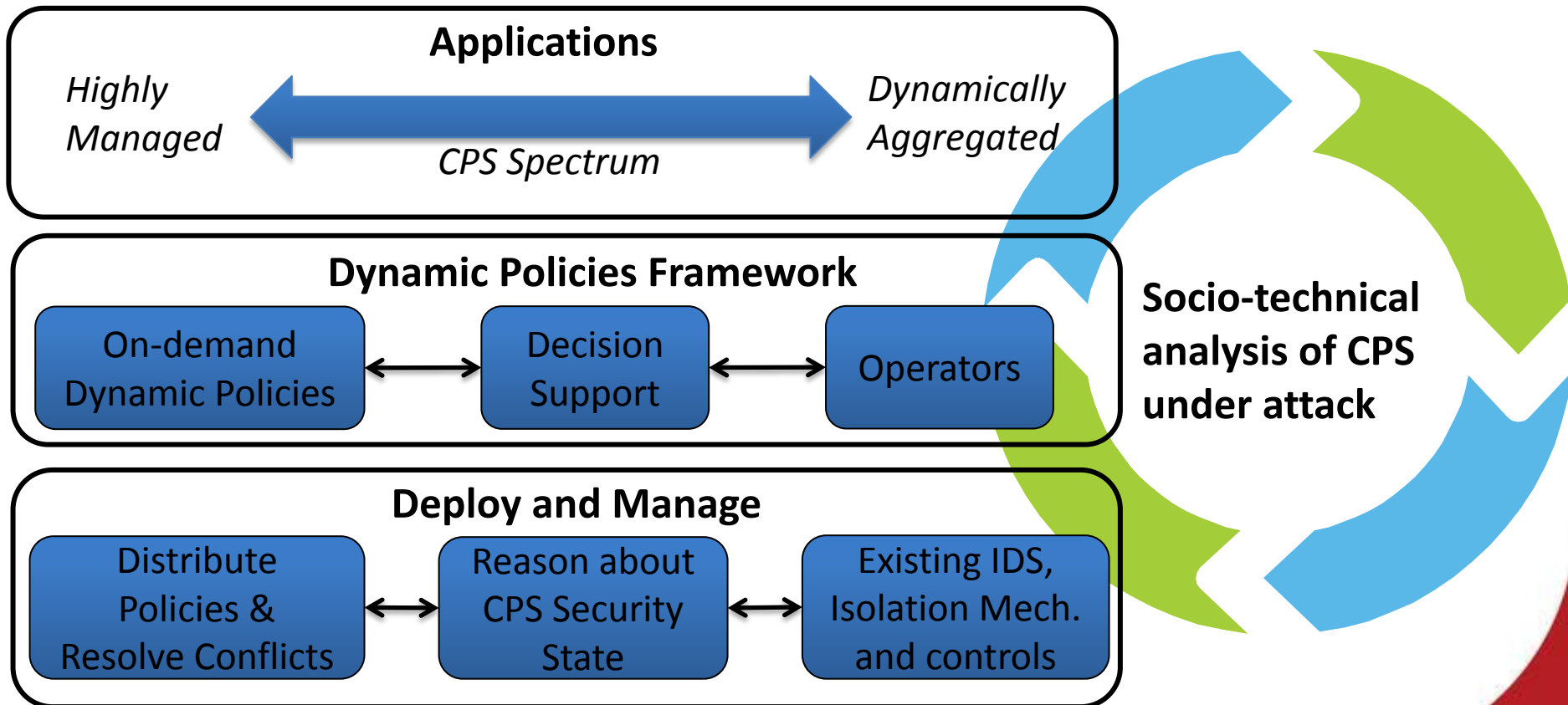


Key Challenges

- Security policy formulation and enforcement in a volatile, multi-stakeholder environment
- CPS security and human factors
- Real-world constraints of shared CPS infrastructures under attack

DYPOSIT

Testbeds



Key Results to date

Attack analysis

- How and why security vulnerabilities are introduced into cyber-physical systems such as industrial control systems
- Analysis of attack scenarios and their implementation for studying system and operator behaviours under attack

Attack detection

- Specialised vulnerability scanners and intrusion detection systems for cyber-physical infrastructures

Dynamic policy models

- Model for dynamic change in an ICS configuration

Key Results to date

Platforms to support dynamic policies

- A CPS Operating System that supports secure loading of third-party application micro-services, strong application isolation, confidentiality of application data and contractually limited access to device resources.

Testbeds for real-world experimentation

- Experimental set up and implementation of attacks in ICS testbed at Lancaster
- Design of an additional IoT infrastructure testbed at KUL

How and why security vulnerabilities are introduced in ICS?



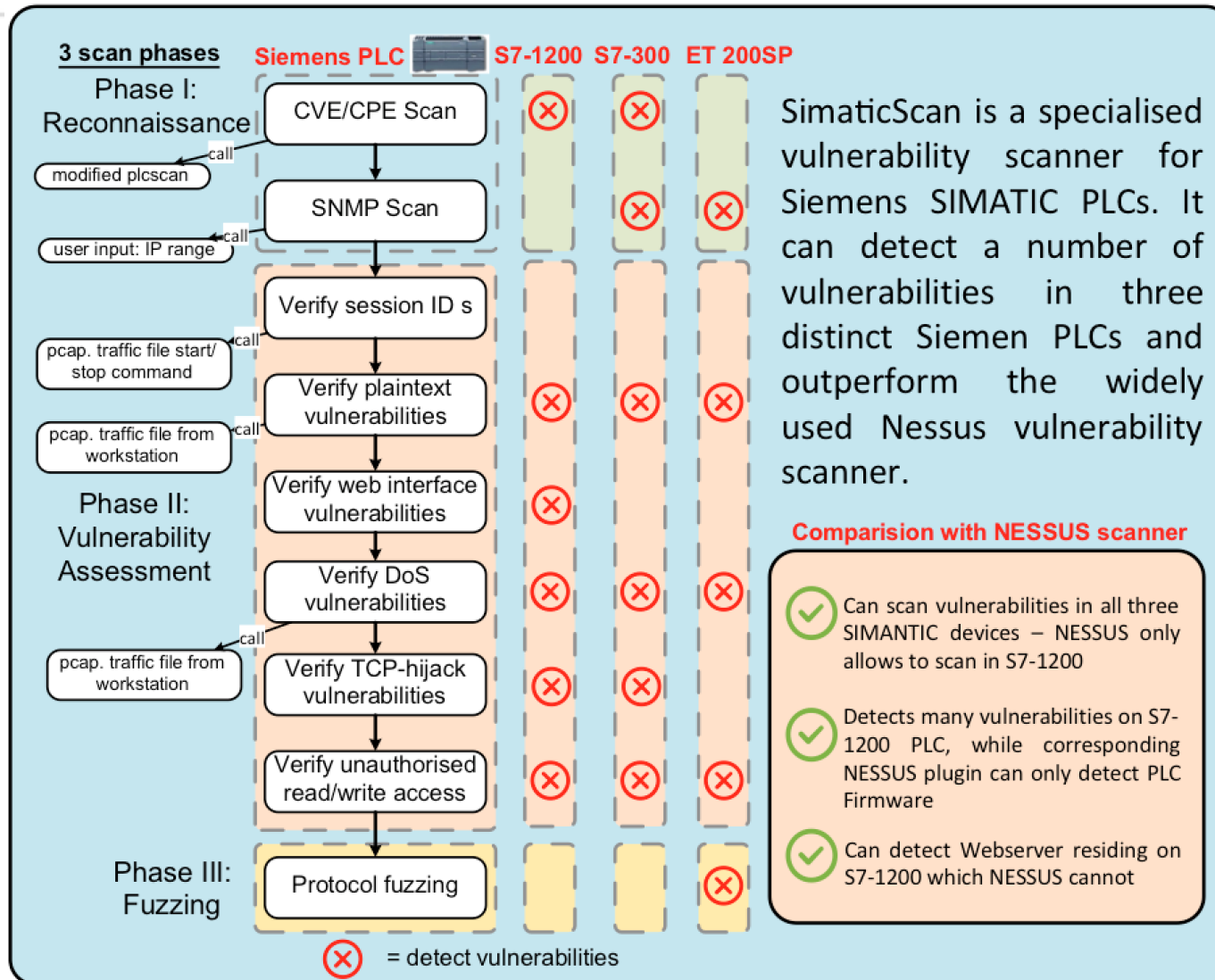
Shodan used as an ICS search engine



- ✓ Many security objectives to consider
- ✓ Vulnerabilities are repeatedly introduced in revisions.
- ✓ Security objectives are considered in terms of security policy refinement.
- ✓ Defenses ensure any policy change is an acceptable replacement (refinement) of previous policy.

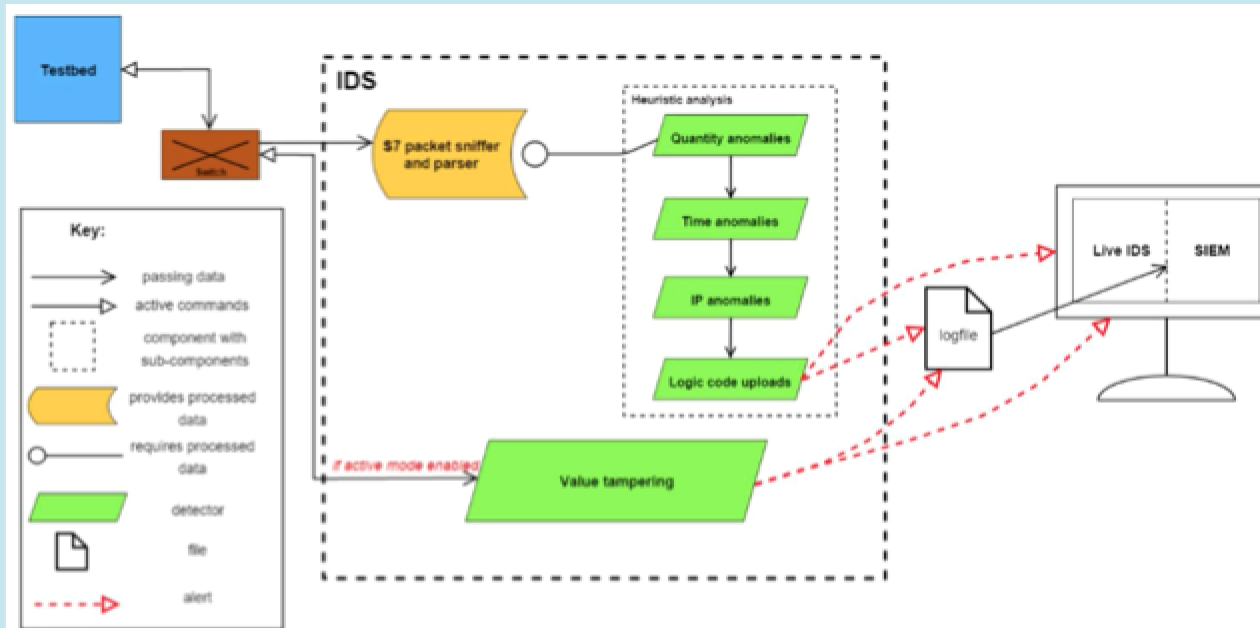
An ethnographic style study of an Internet-connected SCADA system yields insights into the the nature of security flaws in an ICS. This informs our thinking on how to model and dynamically defend against attacks that attempt to exploit these flaws.

SimaticScan: A Specialised Vulnerability Scanner for ICS





SENAMI: Selective, Non-invasive, Active Monitoring for Intrusion Detection



- ✓ Detect 99% purely passive attacks
- ✓ Detect 81-93% active value tampering attacks
- ✓ Recall values 0.96 (small false negative)

SENAMI combines passive network monitoring and selective active monitoring based on attack vectors specific to an ICS context. Implemented and evaluated in Lancaster testbed.

Model for dynamic change in an ICS security configuration



Reasons about
firewall policies
using refinement
and composition
operators

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
2	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW
3	...	192.168.100.0/24	≥ 1024	PLC	102	ALLOW
4	...	*.*.*.*	*	PLC	102	DROP
5	...	external	≥ 1024	FEP	3389	ALLOW
6	...	ADMIN	≥ 1024	FEP	3389	ALLOW
7	...	*.*.*.*	*	FEP	3389	DROP

UPOL
CPNI
RDP

Siemens FAQ 8970169

CPNI Best practices:
use VPN for SCADA traffic

VPN access control

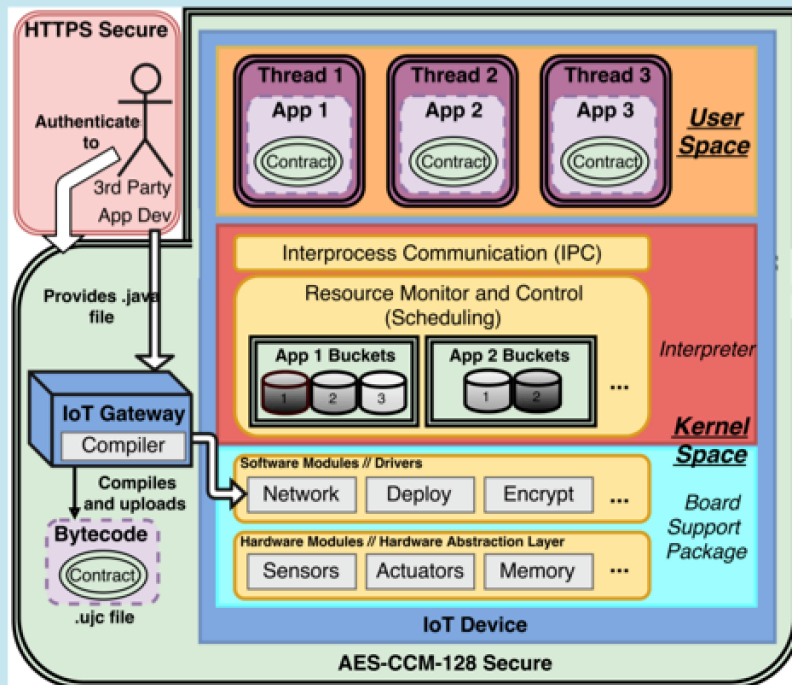
Firewall Algebra: anomaly free composition of policies

- Policy ordering $P \leq Q$: policy P is no less secure than Q
- Set of all policies forms a lattice under $\leq$, with glb $*$ and lub $+$
- Implementation for iptables

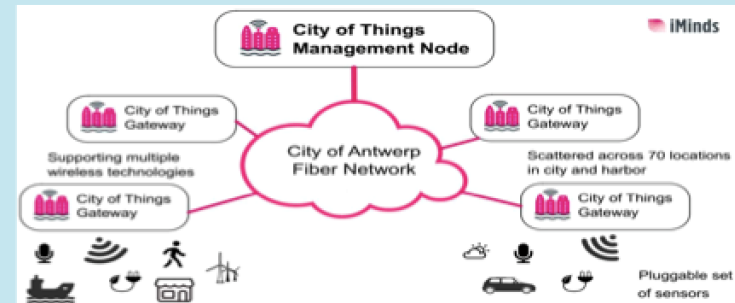
- Anomaly free composition
 $UPOL * (CPNI + RDP)$
- Compliance:
Policy RFC5735
- Dynamic policy update
 $Policy' := Policy * newDefense$

- Reflects firewall policy changes algebraically through operators such as greatest lower-, and lowest upper bound.
- Compares policies based on refinement relation.
- Allows to model dynamic change of firewall policies when configuring ICS security.

CerberOS: A Lightweight Operating System for IoT devices



- ✓ Core OS functionality (pre-emptive multithreading, remote management)
- ✓ Resource access control and accounting
- ✓ General security such as memory isolation
- ✓ Enables shared, multi-stakeholder IoT environments



MicroPnP, an integrated hardware, software and networking solution



- ✓ Integrate any existing IoT device
- ✓ Up to 10 years of battery life
- ✓ Reliable (99.999%) mesh network
- ✓ Accessed from all major programming environments

MicroPnP is a platform aimed at easily deploying an IoT infrastructure and building IoT applications. It offers plug-and-play peripherals with low-power peripheral detection, and automatic driver loading. Used in KU Leuven testbed for experimenting policy exchanges.

Scientific Dissemination

8 international peer-reviewed papers

2 thesis completed related to DYPOSIT

International workshop organised on security and resilience of cyber-physical infrastructures (with the International Symposium on Engineering Secure Software and Systems, London, UK, 2016)

4 keynotes and invited talks/seminars

Software prototypes

CerberOS: a CPS Operating System for IETF Class-1 devices

SENAMI: Selective Non-Invasive Active Monitoring based Intrusion Detection System for ICS

SimaticScan: A Specialised Vulnerability Scanner for Industrial Control Systems

Publications

- [Akk17] S. Akkermans, W. Daniels, G. Sankar R., B. Crispo, W. Joosen and Danny Hughes, “CerberOS: A Resource-Secure OS for Sharing IoT Devices”, in *Proc. of International Conference on Embedded Wireless Systems and Networks (EWSN)*, 2017, Upsalla, Sweden, Feb. 2017.
- [Antrobus2016] Rob Antrobus, Sylvain Frey, Benjamin Green, and Awais Rashid. “SimaticScan: towards a specialised vulnerability scanner for industrial control systems”. In: *Proceedings 4th International Symposium for ICS and SCADA Cyber Security Research*. BCS, June 2016, pp. 11–18. [DBSec2016] Neville, U., & Foley, S.N., “Reasoning About Firewall Policies Through Refinement and Composition”. In *IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec2016)*.
- [Dec16] Maarten Decat, (supervisor: Wouter Joosen), “Authorization Middleware for Software as a Service”, *Ph.D. Thesis, The Agency for Innovation by Science and Technology in Flanders (IWT)*, 25 January 2016.
- [Green2016] Benjamin Green, Sylvain Frey, Awais Rashid and David Hutchison, “Testbed Diversity as a Fundamental Principle for Effective ICS Security Research”, *Proceedings of the International Workshop on Security and Resilience of Cyber-Physical Infrastructures, SERECIN*, held in conjunction with the International Symposium on Engineering Secure Software and Systems (ESSoS), London, UK.

Publications (contd.)

- [Jardine 2016] William Jardine, Sylvain Frey, Ben Green, and Awais Rashid. “SENAMI: Selective Non- Invasive Active Monitoring for ICS Intrusion Detection”. In: *Proceedings of the Second ACM Workshop on Cyber-Physical Systems-Security*, Vienna, Austria. ACM, 2016, pp. 23–34.
- [Mat16] Nelson Matthys, Fan Yang, Wilfried Daniels, Wouter Joosen, Danny Hughes, “Demonstration of micro-pnp: the zero-configuration wireless sensing and actuation platform”, *Proceedings of the Annual 13th IEEE International Conference on Sensing, Communication, and Networking (SECON)*, London, UK, 27 - 30 June 2016
- [Sio16] Laurens Sion, Dimitri Van Landuyt, Koen Yskout, Wouter Joosen, “Towards systematically addressing security variability in software product lines”, *Proceedings of the 20th International Systems and Software Product Line Conference*, volume 20, pages 342-343, Beijing, China, 16-23 September 2016 .
- [SPW2017] S.N. Foley, “Getting security objectives wrong: a cautionary tale of an Industrial Control System”, *25th International Security Protocols Workshop*, 2017, to appear (post-proceedings).
- [Tho16] Klaas Thoelen, (supervisors: Danny Hughes, Wouter Joosen), “An Application Platform for Multi- purpose Sensor Systems”, *Ph.D. Thesis*, March 2016.

Keynotes and Invited Talks

- A. Rashid (Keynote): *The Internet of (Somewhat Secure) Things: To Boldly Go ...?*, International Conference on Industrial Networks and Intelligent Systems, Leicester, UK, 2016.
- A. Rashid (Invited seminar): *Understanding Cyber Risk as Business Risk in Industrial Control Environments*, Singapore University of Technology and Design, Singapore, 2015.
- A. Rashid (Invited seminar): *Understanding Cyber Risk as Business Risk in Industrial Control Environments*, Cardiff University, UK, 2016.
- S. Foley (Speaker), *CPS Attack Scenarios*, International Workshop on Security and Resilience in Cyber- physical Infrastructures, At ESSoS 2016, London.
S. Foley (Invited seminar), *Secure by Comparison*, Telecom Bretagne, Rennes June 2016.

Questions
