Design and deployment of secure, robust, and resilient SDN Controllers

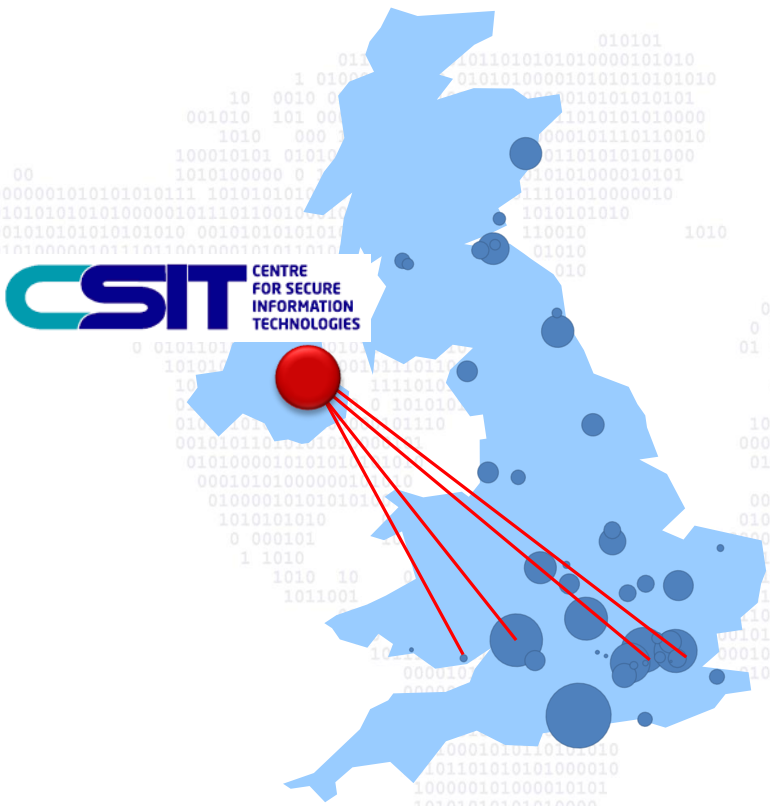
SDNRG @ IETF 93

Wednesday, 22 July 2015

Sandra Scott-Hayward

s.scott-hayward@qub.ac.uk

Centre for Secure Information Technologies (CSIT)



Est.2009, Based in The ECIT Institute

Initial funding over £30M (CSIT 2 - £38M)

80 People
- Researchers
- Engineers
- Business Development

Largest UK University lab for cyber security technology research

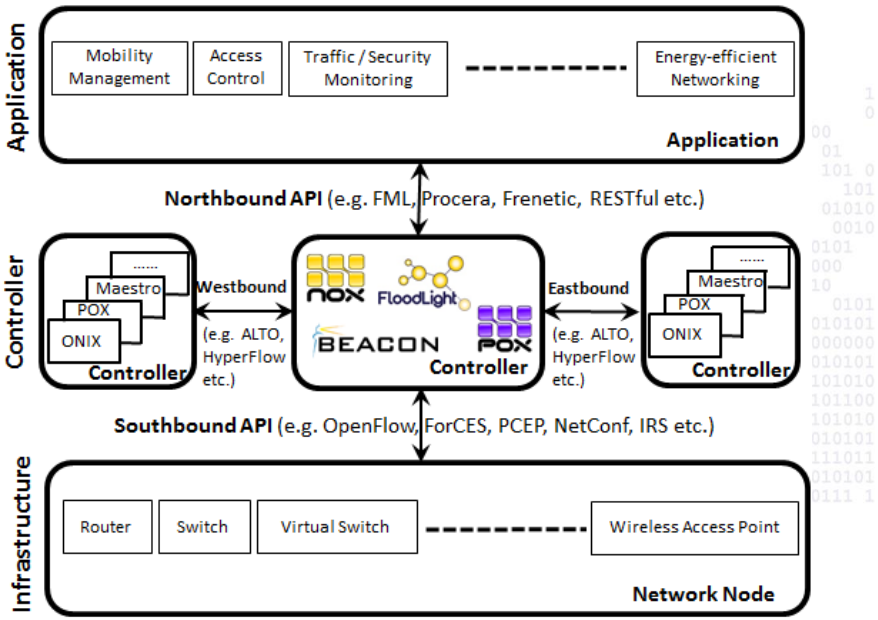
GCHQ Academic Centre of Excellence

Industry Informed
- Open Innovation Model

Strong international links
- ETRI, CyLab, GTRI, SRI International
- Cyber Security Technology Summit

SDN Research

Software Defined Networking …. and Security



Security Issue/Attack	SDN Layer Affected or Targeted				
	Application Layer	App-Ctl Interface	Control Layer	Ctl-Data Interface	Data Layer
Unauthorized Access e.g.					
Unauthorized Controller Access			✓	✓	✓
Unauthenticated Application	✓	✓	✓		
Data Leakage e.g.					
Flow Rule Discovery (Side Channel Attack on Input Buffer)					✓
Forwarding Policy Discovery (Packet Processing Timing Analysis)					✓
Data Modification e.g.					
Flow Rule Modification to Modify Packets			✓	✓	✓
Malicious Applications e.g.					
Fraudulent Rule Insertion	✓	✓	✓		
Controller Hijacking			✓	✓	✓
Denial of Service e.g.					
Controller-Switch Communication Flood			✓	✓	✓
Switch Flow Table Flooding					✓
Configuration Issues e.g.					
Lack of TLS (or other Authentication Technique) Adoption			✓	✓	✓
Policy Enforcement	✓	✓	✓		

Sezer, S., et al. “Are We Ready for SDN? Implementation Challenges for Software-Defined Networks” *IEEE Communications Magazine*, July 2013

Scott-Hayward, S.; Natarajan, S.; Sezer, S., "A Survey of Security in Software Defined Networks," *Communications Surveys & Tutorials, IEEE* , 10.1109/COMST.2015.2453114

Problem Description

Increase in components and interfaces for the evolved SDN implementation increases the security challenges of the SDN controller design.

Objective:

- Identify requirements of a secure, robust, and resilient SDN controller;
- Analyse state-of-the-art open-source SDN controllers with respect to the security of their design;
- Provide recommendations for security improvements

Definition of ‘Security’

Secure, Robust and Resilient (referred to as ‘security’):

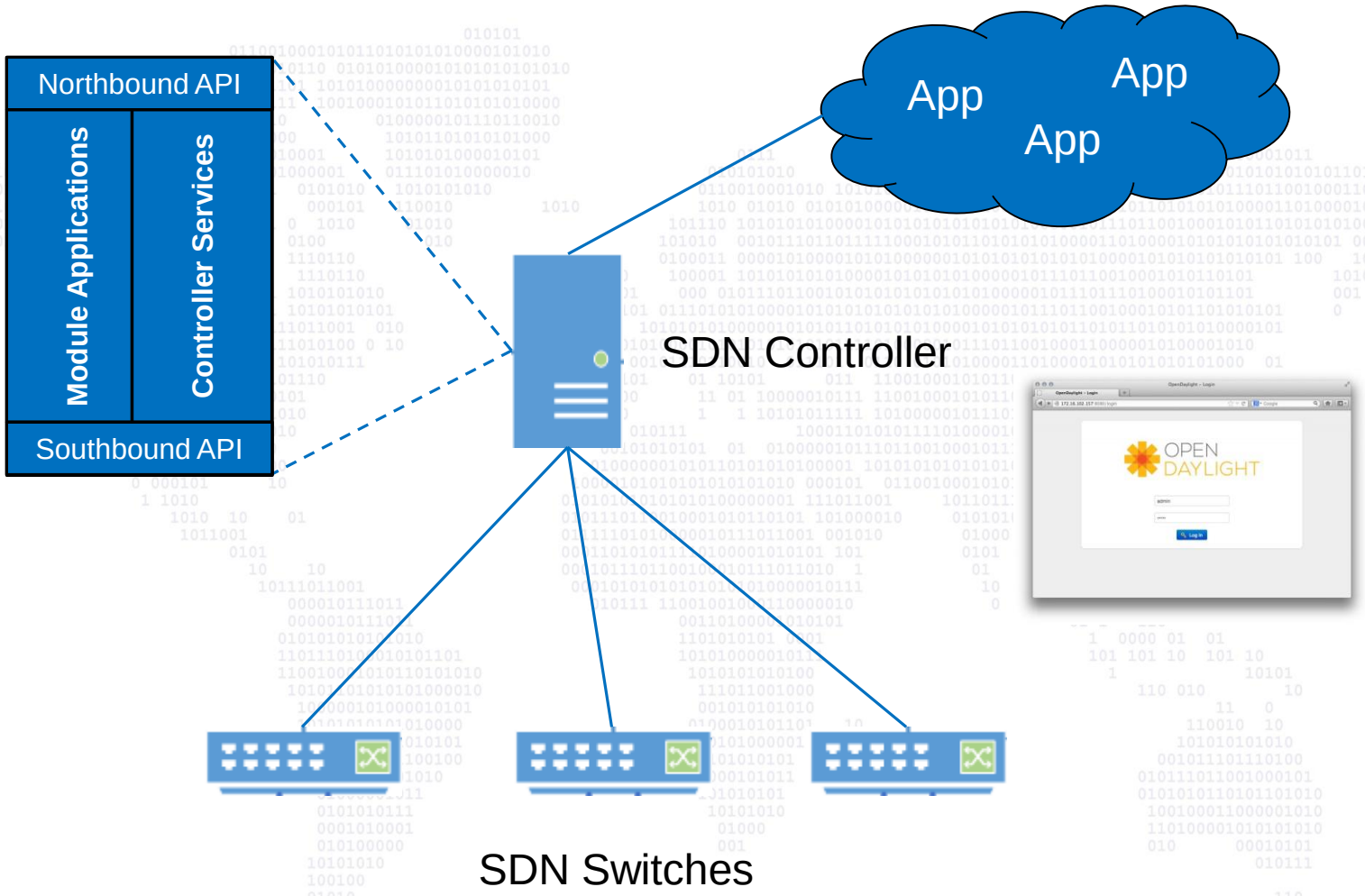
- The controller is designed to reduce the risk of intrusion/attack at the network control layer;
- The controller is able to withstand errors in control layer logic;
- The controller is able to recover quickly from disruption and maintain an acceptable level of service in the face of faults.

CENTRE FOR SECURE INFORMATION TECHNOLOGIES

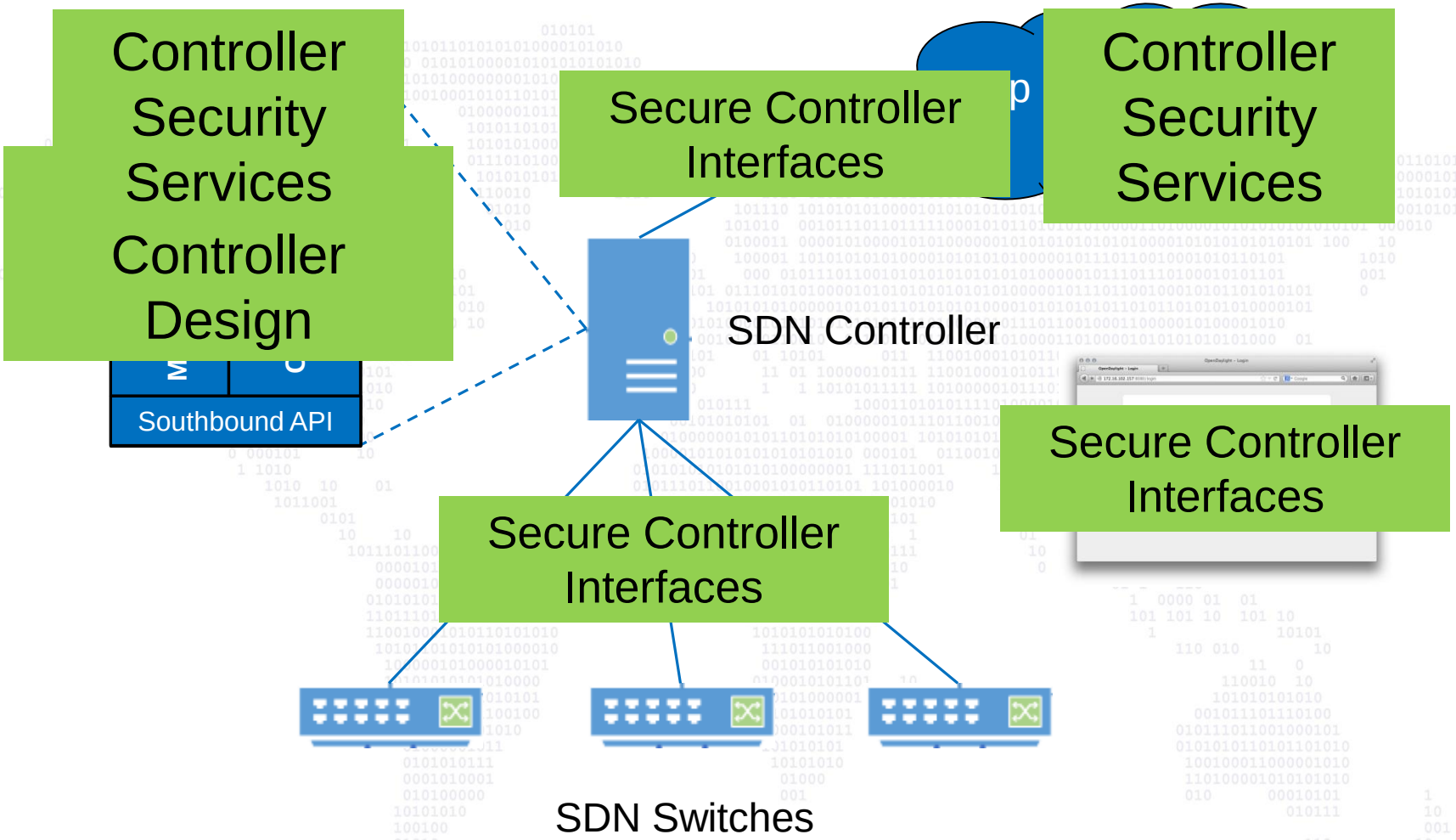
Selected SDN Controllers

Controller	Source	Version	Release	Architecture	Objective	Security Features
ONOS	ON.Lab	Avocet 1.0.0	2014	Distributed	High-availability, Scale-out, Performance	Security-mode ONOS proposed for v2
OpenDaylight	OpenDaylight Project	Helium (Karaf 0.2.0)	2014	Distributed	Enterprise-Grade Performance, High Availability	AAA Service, Foundation of Security Group
ROSEMARY	KAIST, SRI International	-	2014	Centralized	Robust, secure, and high-performance NOS	Process Containment, Resource Usage Monitoring, App PermissionStructure
Ryu	NTT	3.13	2012	Centralized, Multi-Threaded	High quality controller for production environments	Secure control layer communication
SE-Floodlight	SRI International	Beta 2	2013	Centralized	Security-enhanced version of Floodlight controller	Security enforcement kernel (AAA)

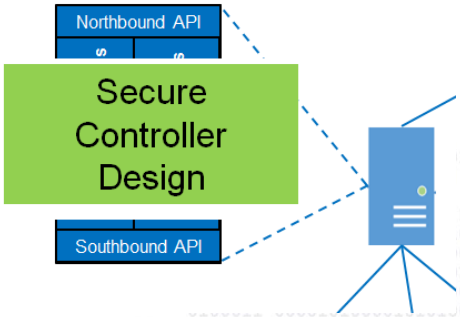
Security Attributes



Security Attributes

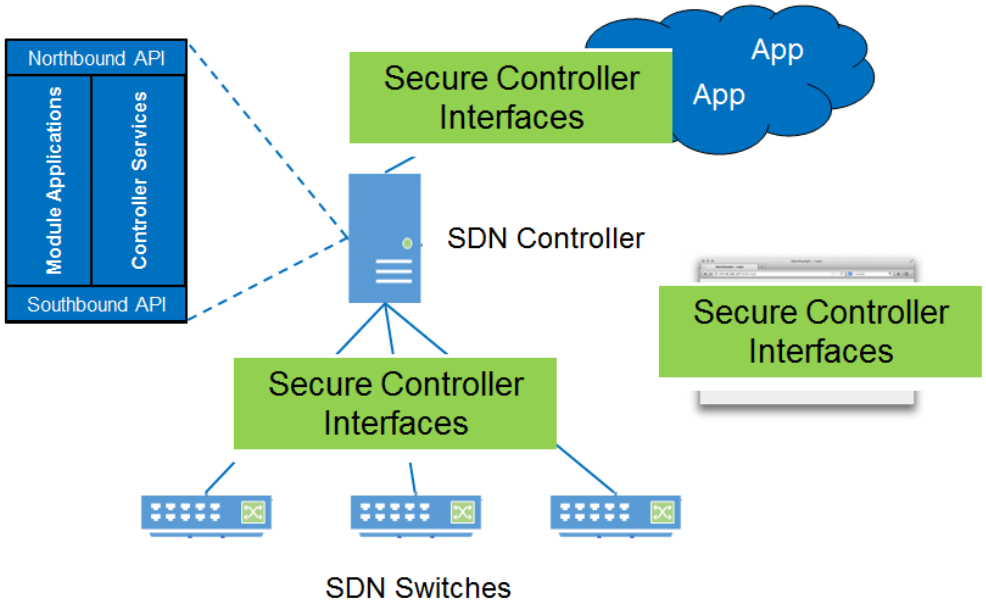


Secure Controller Design



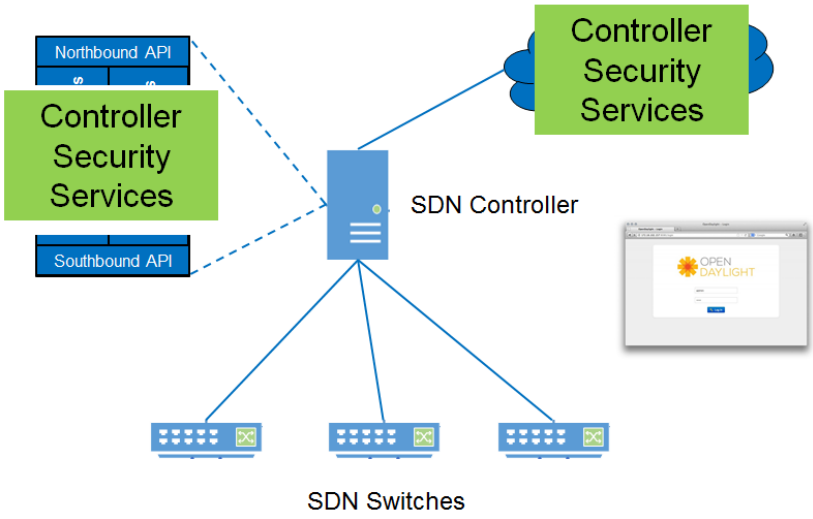
Controller	ONOS	ODL	ROSEMARY	Ryu	SE-Floodlight
Control Process (Application) Isolation	✗	✗	✓ (micro-NOS)	✗	✓ (Privilege-Based)
Implementation of Policy Conflict Resolution	✓ (Data-Store)	✗	✗	✗	✓ (Algorithm)
Multiple Controller Instances – Resilience	✓ (Clustering)	✓ (Clustering)	✗	✗	✗
Multiple Application Instances – Resilience	✗	✗	✗	✗	✗
Secure Storage	✓	✓	✓	✓	✓

Secure Controller Interfaces



Controller	ONOS	ODL	ROSEMARY	Ryu	SE-Floodlight
Secure Control Layer Communication	✗	✓ (D-CPI)	✗	✓ (D-CPI)	✓ (D-CPI, A-CPI)
GUI/REST API Security	✗	✓ (weak)	n/a	✗	✗

Controller Security Services



Controller	ONOS	ODL	ROSEMARY	Ryu	SE-Floodlight
IDS/IPS Integration	✗	✓ (Defense4All)	✗	✓ (Snort)	✓ (BotHunter, Sec. Actuator)
Authentication and Authorization	✗	✓	✓	✗	✓
Resource Monitoring	✗	✗	✓	✗	✗
Logging/Security Audit Service	✓	✓	✓	✓	✓

Recommendations

Recommendations for Future Security Improvements:

1. Design with Software Security Principles
2. Secure Default Controller Settings
3. Application Future-Proofing

Conclusion

ONOS, OpenDaylight

Focus on the provision of a distributed architecture

=>

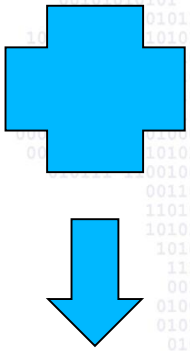
High availability, Performance

ROSEMARY, SE-Floodlight

Introduce control layer resilience and a security-enforcement kernel

=>

Security, Resilience



Next Evolution in SDN Controller Design …
Security, Robustness, and Resilience

Thank you!

Questions?

s.scott-hayward@qub.ac.uk

Controller References

ONOS — ON.LAB, “ONOS: Open Network Operating System.” [Online]. Available: http://onosproject.org/

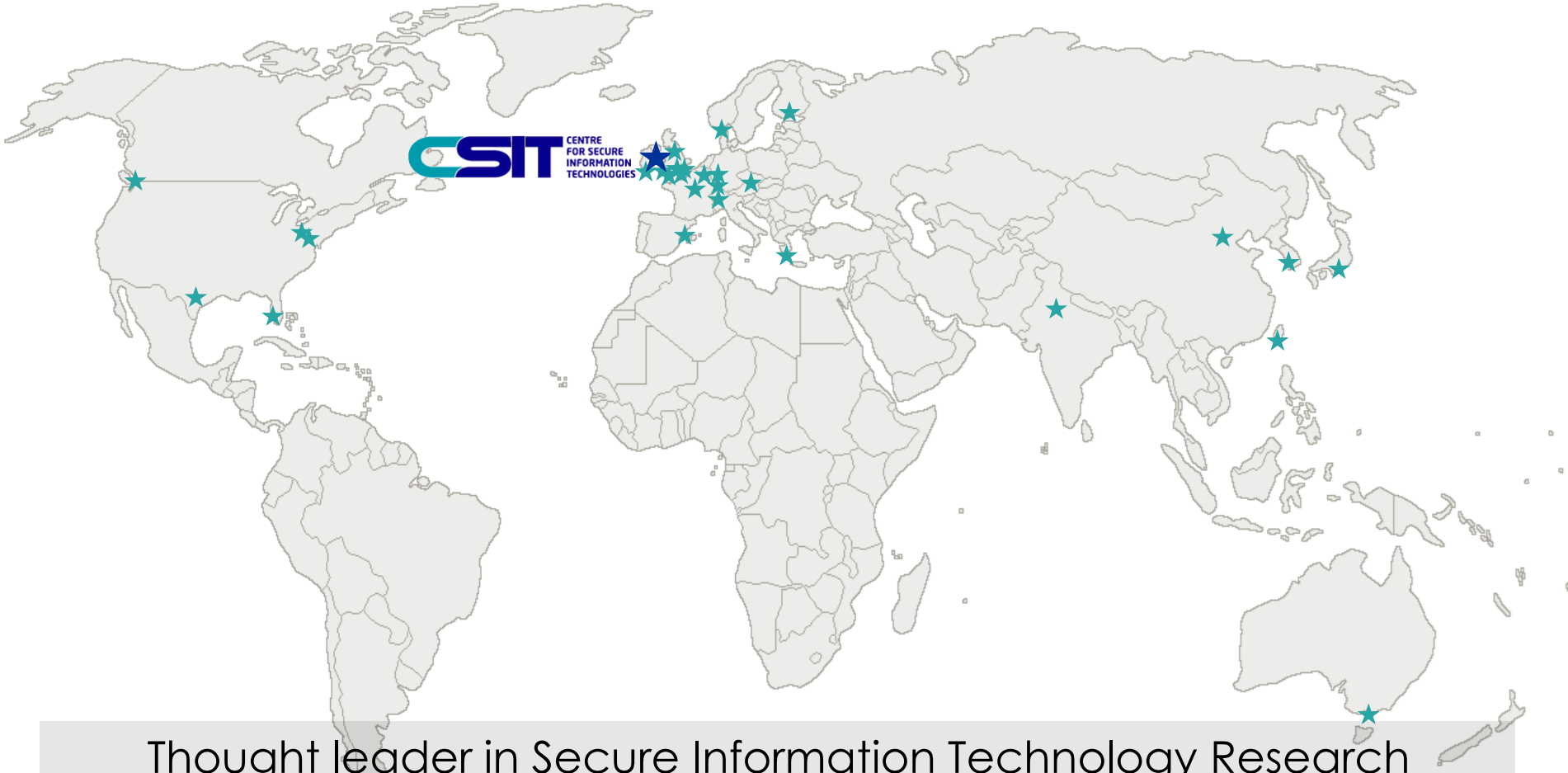
OpenDaylight — OPENDAYLIGHT, “OpenDaylight: A Linux Foundation Collaborative Project.” [Online]. Available: http://www.opendaylight.org

ROSEMARY — S. Shin, Y. Song, T. Lee, S. Lee, J. Chung, P. Porras, V. Yegneswaran, J. Noh, and B. B. Kang, “Rosemary: A Robust, Secure, and High-Performance Network Operating System,” in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.* ACM, 2014, pp.78-89.

Ryu — Nippon Telegraph and Telephone Corporation, “Ryu Network Operating System.” [Online]. Available: http://osrg.github.io/ryu/

SE-Floodlight — P. Porras, S. Cheung, M. Fong, K. Skinner, and V. Yegneswaran, “Securing the Software-Defined Network Control Layer,” in *Proceedings of the 2015 Network and Distributed System Security Symposium (NDSS)*, February 2015.

CSIT: A Global Cyber Innovation Hub



Thought leader in Secure Information Technology Research
Network of Commercial & Research partnerships
Portfolio of successful Technology Transfer