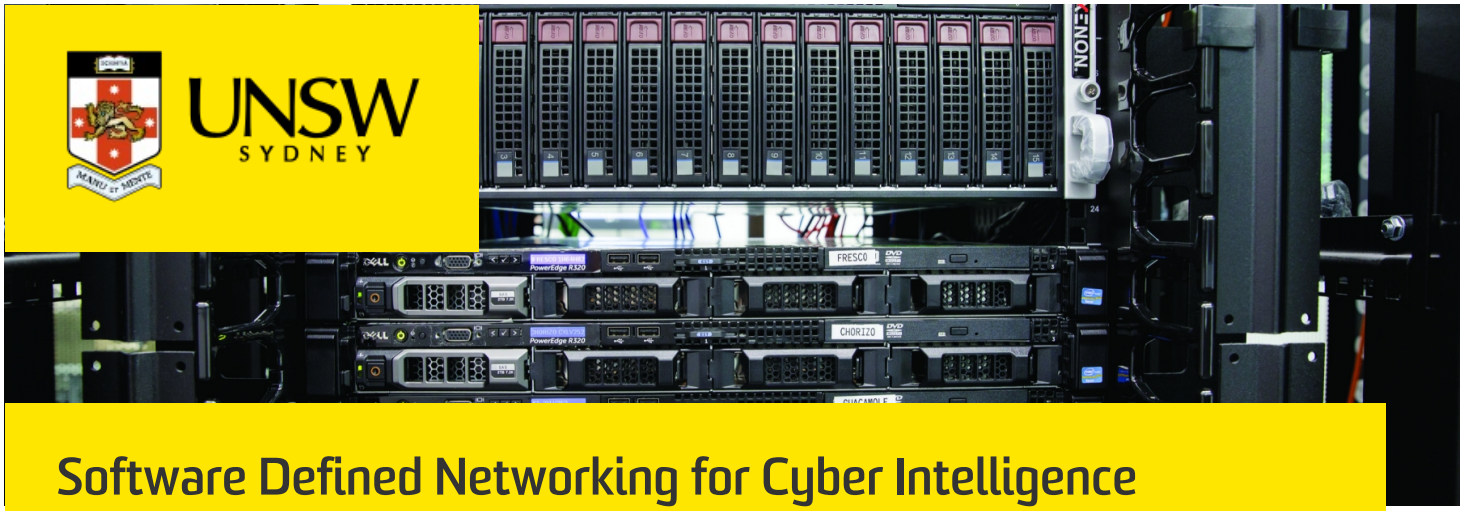

Software Defined Networking for Cyber Intelligence

Software Defined Networking (SDN) enables improved visibility, management and control of networks using software decoupled from switching hardware. Use-cases include analytics of video traffic in carrier networks and flexible cyber-security for enterprise networks.

Competitive advantage

- Research, development and commercialisation expertise in:
- Improved network telemetry and analysis for fine-grained asset and threat visibility
- Automation and orchestration of network operations for enhanced security
- Experience in operational deployments and commercial trials of on local area networks through to carrier scale networks
- End-to-end solutions with full ecosystem integration
- Patent protected technology

Impact

- More reliable and secure communications
- Detection of intrusions into and exfiltration from Defence Networks
- Network activity monitoring of embedded devices in contained environments like submarines
- Detection and quarantining of compromised devices in battlefield environments

Successful applications

- SDN solutions in trials with Optus, Asre Telecom, AmLight and Cenic
- Intellectual property being incorporated into Cisco switches
- Real-time visibility into individual video streams in a Tier-1 carrier network
- Flexible inter-domain inter-connects for research networks in USA
- Real-time health monitoring of complex Internet-of-Things (IoT) environments

Capabilities and facilities

- Large-scale SDN test-bed spanning 10 Australian organisations
- Fully-equipped SDN lab with state-of-the-art hardware and software

More Information

Professor Vijay Sivaraman

School of Electrical Engineering and Telecommunications

T: +61 (0) 2 9385 6577
E: vijay@unsw.edu.au

UNSW Knowledge Exchange

knowledge.exchange@unsw.edu.au

www.capabilities.unsw.edu.au

+61 (2) 9385 5008