

## **Your DNS, My DNS - National risk and DNS infrastructure**

*Tuesday, 5 December 2017 14:00 (30 minutes)*

The Domain Name System (DNS) is critical to the operation of the majority of services on the Internet at large. Many organisations however pay relatively little attention to this foundational protocol. Whether this be in terms of the operational aspects of the DNS infrastructure, or even the choice of registrars and domain name servers. This talk explores the analysis of several snapshots of one of the internet TLD zones, and the subsequent identification of 'hotspots' within the system which serve as potential areas of weakness. Attacks against these identified infrastructural points, whether by malicious actions such as seen in 2016 with the Marai botnet or by national interests in which those systems reside, could have far reaching impacts on network infrastructure. A number of recommendations are put forward as to how to improve the state of DNS security. In particular a checklist for organisations to consider when considering operational risk in operating DNS.

### **HPC content**

The Domain Name System (DNS) is critical to the operation of the majority of services on the Internet at large. This talk explores the analysis of one of the internet TLD zones, and the subsequent identification of 'hotspots' within the system which serve as potential areas of weakness. A number of recommendations are put forward as to how to improve the state of DNS security. In particular a checklist for organisations to consider when considering operational risk in operating DNS.

**Primary author:** Prof. IRWIN, Barry (Rhodes University)

**Presenter:** Prof. IRWIN, Barry (Rhodes University)

**Session Classification:** SA NREN

**Track Classification:** SA NREN