Contribution ID: **124** Type: **Keynote Talk**

Cyber Intelligence at Scale: Risk Evaluation of DNS as Critical infrastructure

Tuesday, 3 December 2024 09:45 (45 minutes)

The domain name system, or DNS, is a critical component of the Internet ecosystem we use. Almost every single transaction and connection from email to online commerce makes use of DNS as an initial a fundamental step. While the primary purpose in the eyes of the public is to mask the complexities of host addressing, and location, it's use has evolved to be critical for a whole lot more, One of the oldest and arguably the second most important use being its foundation for email delivery though the use of MX records. In recent years we have seen the introduction and gradual adoption of several security measures rooted within and implemented by extending the DNS protocol. These include DNSSEC, SPF, and more recently CAA for improving e the security of SSL certificate issuance. In essence the global domain Domain Name Systems should be regarded as critical infrastructure. However, for many organisations, especially those reliant on hosting providers, ISPs or MSPs, despite the requirement for functional DNS, the deployment and operation of the servers (as outlined in RFC 2182) and associated domain zones, are often neglected. This may be due to the 'care and feeding' been seen as 'too complex', mundane or unexciting in comparison to more exciting areas with 'Cyber operations' such as Threat Intelligence, Malware Analysis and ML/AI based security solutions. The irony is these all have a strong dependence on DNS!

This talk has a dual focus initially presents an overview of the state of DNS operations for several ccTLD's and top domains globally. A concern worth raising particularly considering the increased global geopolitical tensions is where is ones DNS hosted physically and logically, and who has control? An evaluation of risk, particularly the dependency on key providers (for example about a third of the .no domains surveyed are hosted by a single provider), as well as adherence to good practice is presented. The secondary part of the talk presents several short case studies of the adoption rate of security functionality (primarily the adoption of DNSSEC and CAA records) within and offered by DNS for ccTLDs investigated.

The final element is a discussion about undertaking research such as this at 'internet scale', including data collection, processing storage and validation.

Student or Postdoc?

Email address

Co-Authors

CHPC User

CHPC Research Programme

Workshop Duration

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

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

Session Classification: Keynote

Track Classification: SA NREN