Practical Observations from Encrypted DNS Deployments by Network Operators

draft-campling-operator-observations-00

IETF 108, Virtual

Andrew Campling **Andrew.Campling@419.Consulting**

Normen B Kowalewski Normen.Kowalewski@Telecom.DE

Gianpaolo A Scalone Gianpaolo-Angelo.Scalone@Vodafone.Com

Chris Box Chris.Box@BT.Com

Alister Winfield Alister.Winfield@Sky.UK

Introduction
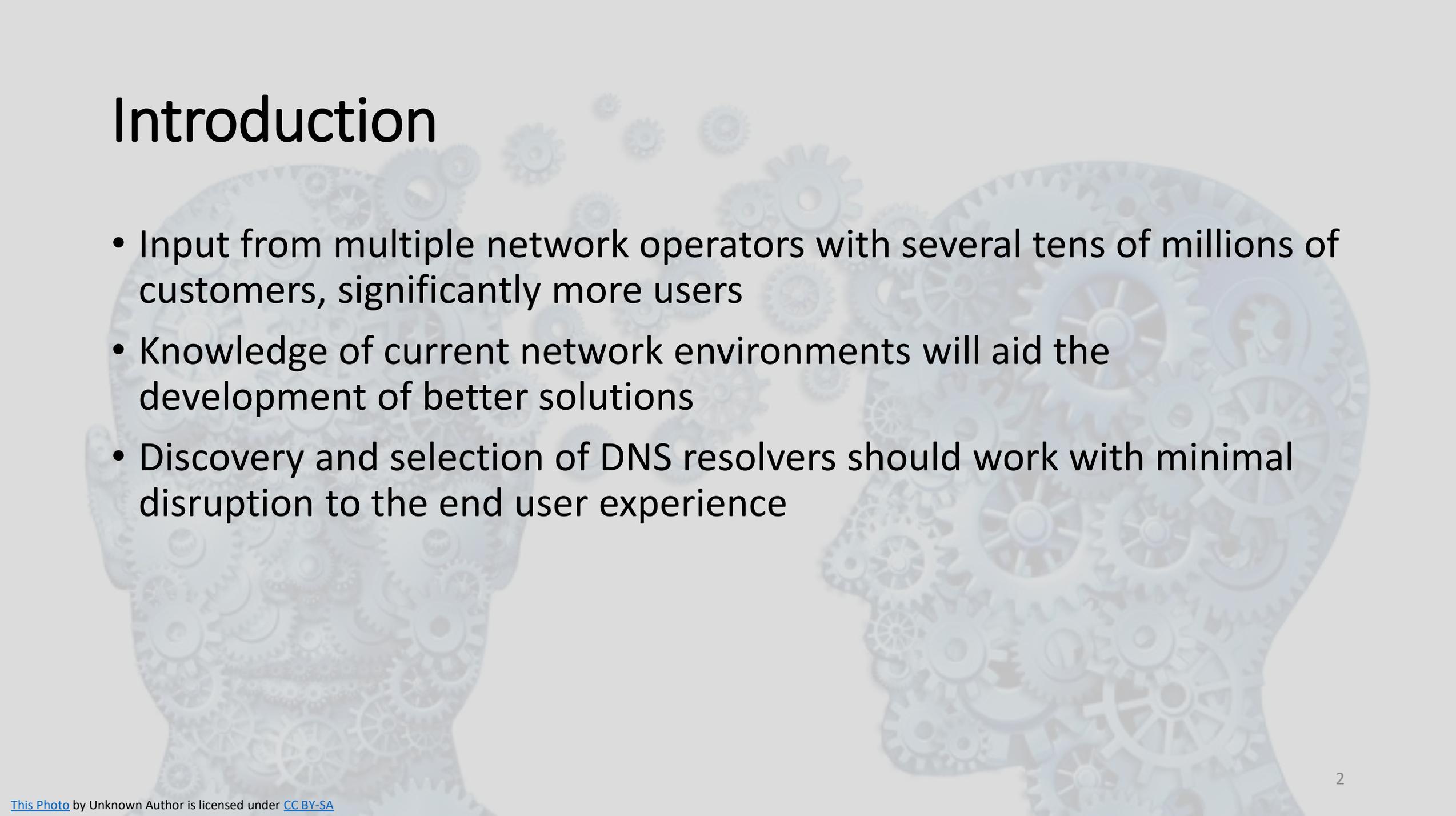
- Input from multiple network operators with several tens of millions of customers, significantly more users

- Knowledge of current network environments will aid the development of better solutions

- Discovery and selection of DNS resolvers should work with minimal disruption to the end user experience

2

Observations: the architecture

- The non-public nature of most network operator DNS services

- CPE using RFC1918 Private Addresses

- CPE acting as a DNS Forwarder

- Manual configuration of DNS is not undertaken by most users

- This architecture
  - Is widely used, at least in Europe
  - There are valid reasons for wanting DNS forwarding on CPE
  - The approach has good privacy, security and performance benefits

Observations: the challenges

- Current Same Provider Auto-Upgrade mechanisms fail because the client DNS resolver is an RFC1918 private address of the CPE device

- Manually configured closed resolvers may cause a client to fail closed

- Consumers have a legal right to use their own CPE

- Obsoleting this model will impact operators that choose architectures for good privacy, security and performance reasons

Conclusions

- The network operator use case is valid

- It describes common and widespread requirements used by tens of millions

- Discovery solutions are needed that work with this DNS-forwarder, private IP to closed resolver approach commonly used by network operators
    - The architecture has good privacy, security and performance benefits
    - Auto-discovery is important
    - Any ADD solution for discovery or selection should measure itself to see whether it meets this use case

- At least one mainstream ADD solution is required that meets this use case
    - Where the client DNS resolver is an RFC1918 private address of the CPE device (i.e. each household has their own private DNS forwarder, which is good for privacy, security and performance)