Ghana DNSSEC Validation Success Story & DNS Operational Best Practices

Presentation By:

Isaac Sakyi

Godsway Kubi

In this presentation:

- Describe Ghana ecosystem
- Problem statement
- Collaboration and resolution
- Adopting ICANN's KINDNS Framework
- Common myths busted
- Learnings and key takeaways

Ghana Internet Ecosystem

35million+

26million+ internet users, online penetration 75%

3 MNO, 70+ ISP, 5 submarine Cable Providers, 2 IXP

Problem statement

- .gh Domain not signed
- Very low DNSSEC Validation < 24%, Now 99% 
  - DNS records could be altered and users redirected to malicious websites
  - Low online resource trust
  - Poor cybersecurity outlook for companies and country

Collaboration and Resolution

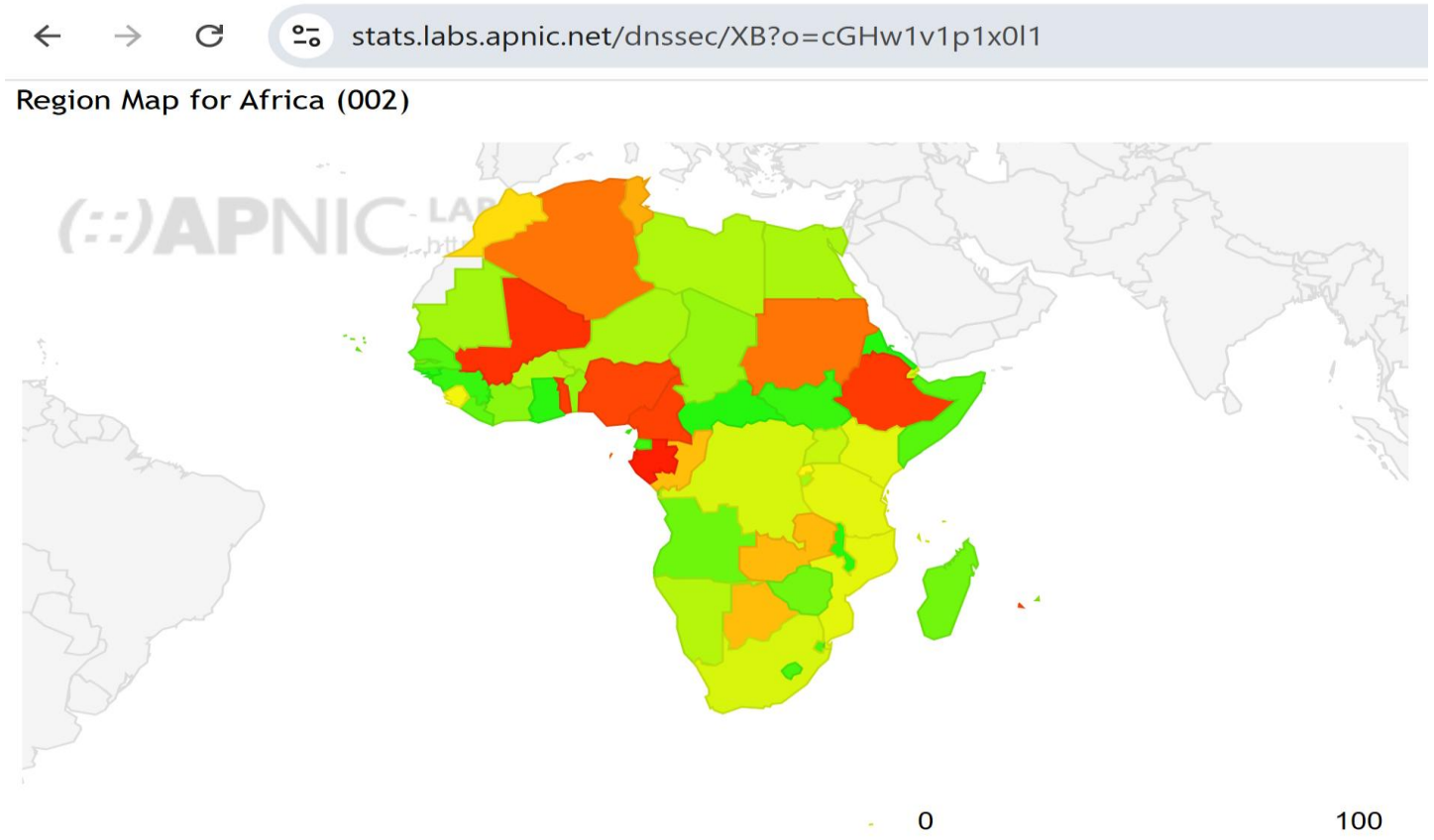
Supportive government policies and framework

Key stakeholder engagement and consultation

Awareness creation, Training and capacity building

Feedback and continuous improvement

DNSSEC Validation: Region Map for Africa



Adopting ICANN's KINDNS Framework
(Recommended practices for DNS operators)

- Voluntary journey of the largest MNO/ISP—MTN Ghana

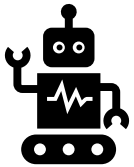
- Recommendations include:
  - ✓Enabling DNSSEC validation
  - ✓employing ACL to limit queries to specific IPS
  - ✓Separation of function; host Authoritative and recursive resolvers separately
  - ✓Redundancy in design setup
  - ✓Enhanced privacy
  - ✓Monitoring of services

Debunking the myths

DNSSEC Validation is difficult to configure

Difficult to understand, only reserved to tech savvy

Heavy resource utilization: memory, CPU, link



Domains/URLs will fail to open

Learnings and Key Takeaways

- Ensure hardware is not EOL and software is up to date
- DNSSEC validation configuration is fairly straight forward an simple
- Expertise is readily available in the community. Just ASK!
- Continuous awareness creation, community and stakeholder engagement is key
- Capacity training: Leverage local technical expertise

Thank you