SIPS, IPPS, or Oops!
An Analysis of the Security and Privacy of DNS Service Discovery

Joseph Call jbcall@wm.edu
Mostafa Noshy Ahmed mnahmed@wm.edu
Stephen Herwig smherwig@wm.edu

William & Mary, Chartered 1693

/etc/lab Extending Trust in Computing Lab

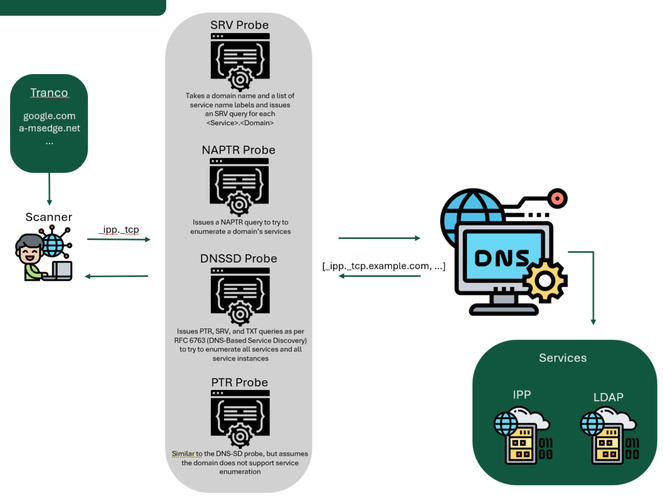
MOTIVATION

- Assess the security practices employed by domains when publishing services
- Identify potential vulnerabilities or misconfigurations in the DNS service discovery ecosystem that could impact user privacy or system security

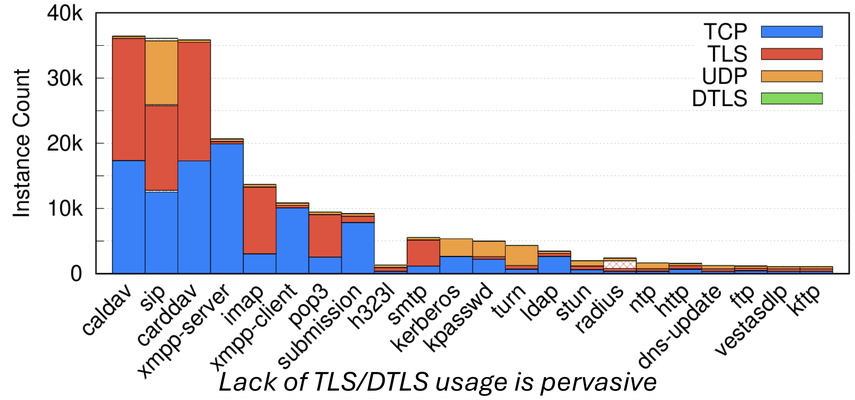
GOALS

- What services do domains publish?
- Do domains publish these services securely?
- Do these services provide strong authentication and privacy for their clients?

METHODOLOGY

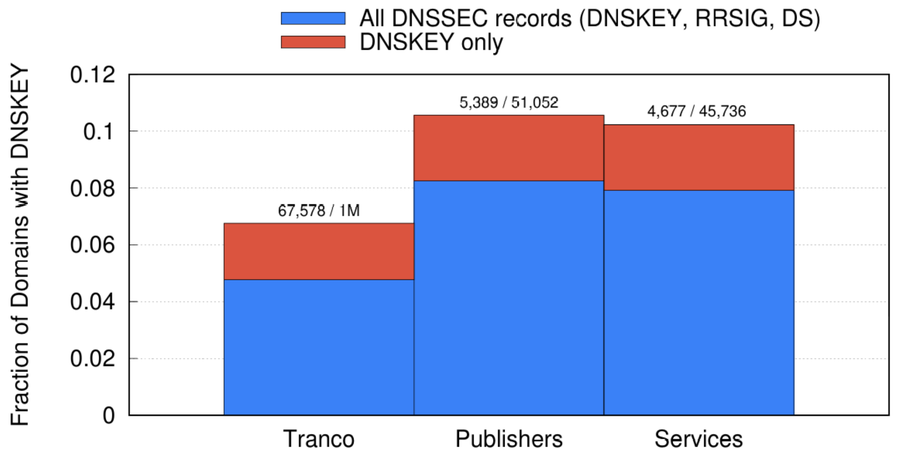


CHARACTERISTICS



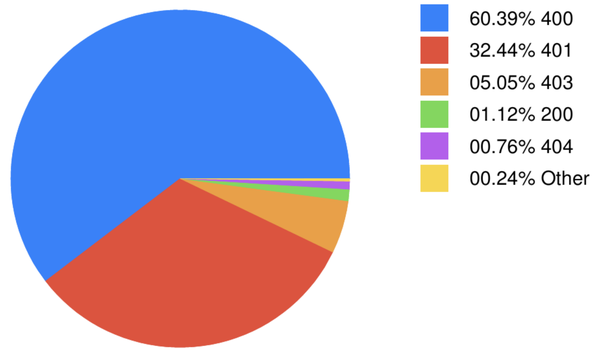
Lack of TLS/DTLS usage is pervasive

DNSSEC



Only 8% of domains that advertise services use proper DNSSEC

HTTP CODES



A 401 code indicates HTTP authentication; 403 suggests a firewall

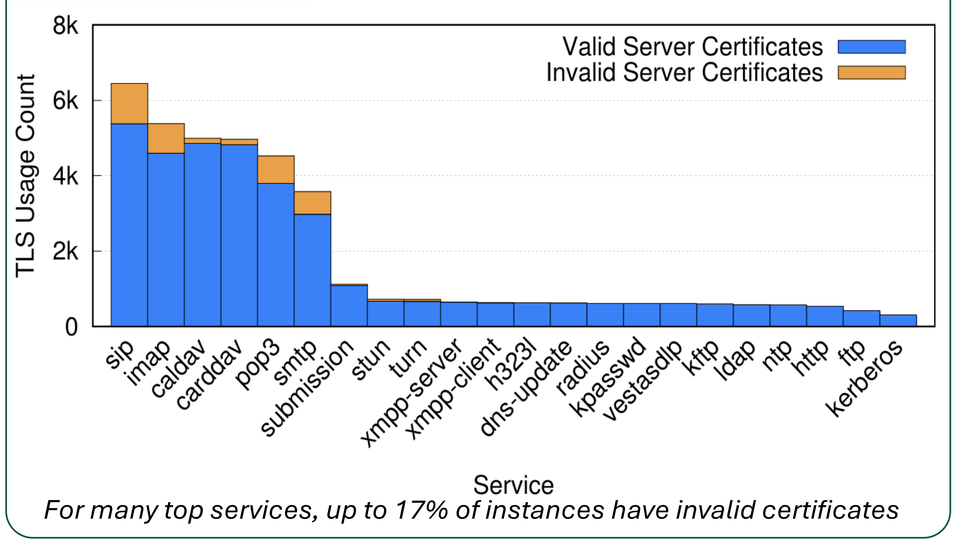
RADIUS

Authentication/authorization protocol common in enterprise Wi-Fi networks

Country	% of advertised *instances as _radius._udp.*
United States	50.14 %
China	46.11 %
Taiwan	2.31 %
Others	1.44 %

Domains	% of advertised *instances as _radsec._tcp.*
Eduroam	7.73 %
Academic Domains	19.08 %
Other Domains	73.19 %

TLS



For many top services, up to 17% of instances have invalid certificates

FUTURE WORK

- Investigate DTLS usage
- Investigate forms of HTTP-based and digest-based authentication
- Assess the potential for amplification attacks on UDP services
- Incorporate additional DNS service discovery methods into our scanner, including the recently proposed SVCB record