DoH and DoT

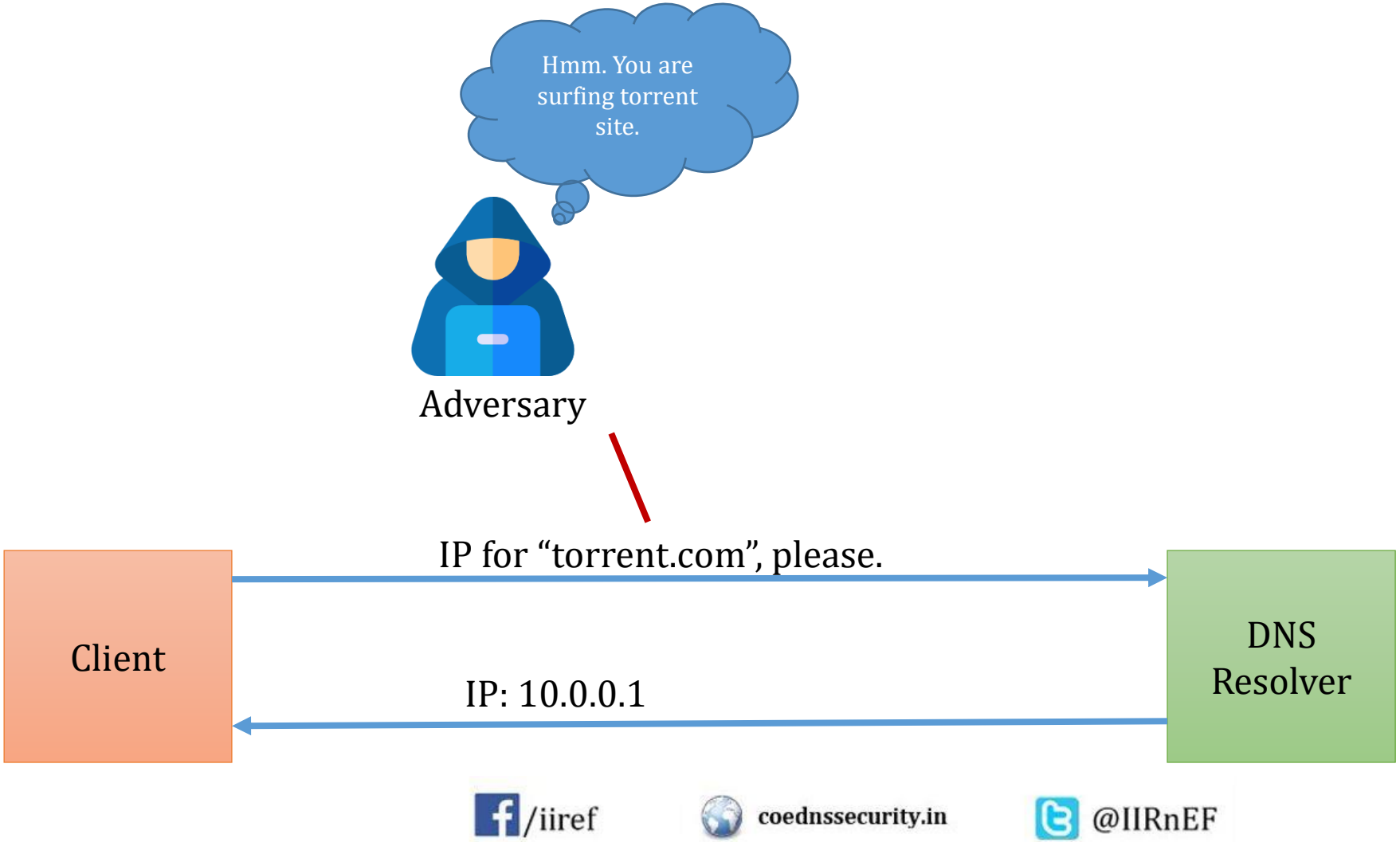
Anoop Kumar Pandey
Principal Technical Officer
Centre for Development of Advanced Computing (C-DAC)
Electronics City, Bangalore 560 100

Centre of Excellence in DNS Security
27th November 2020

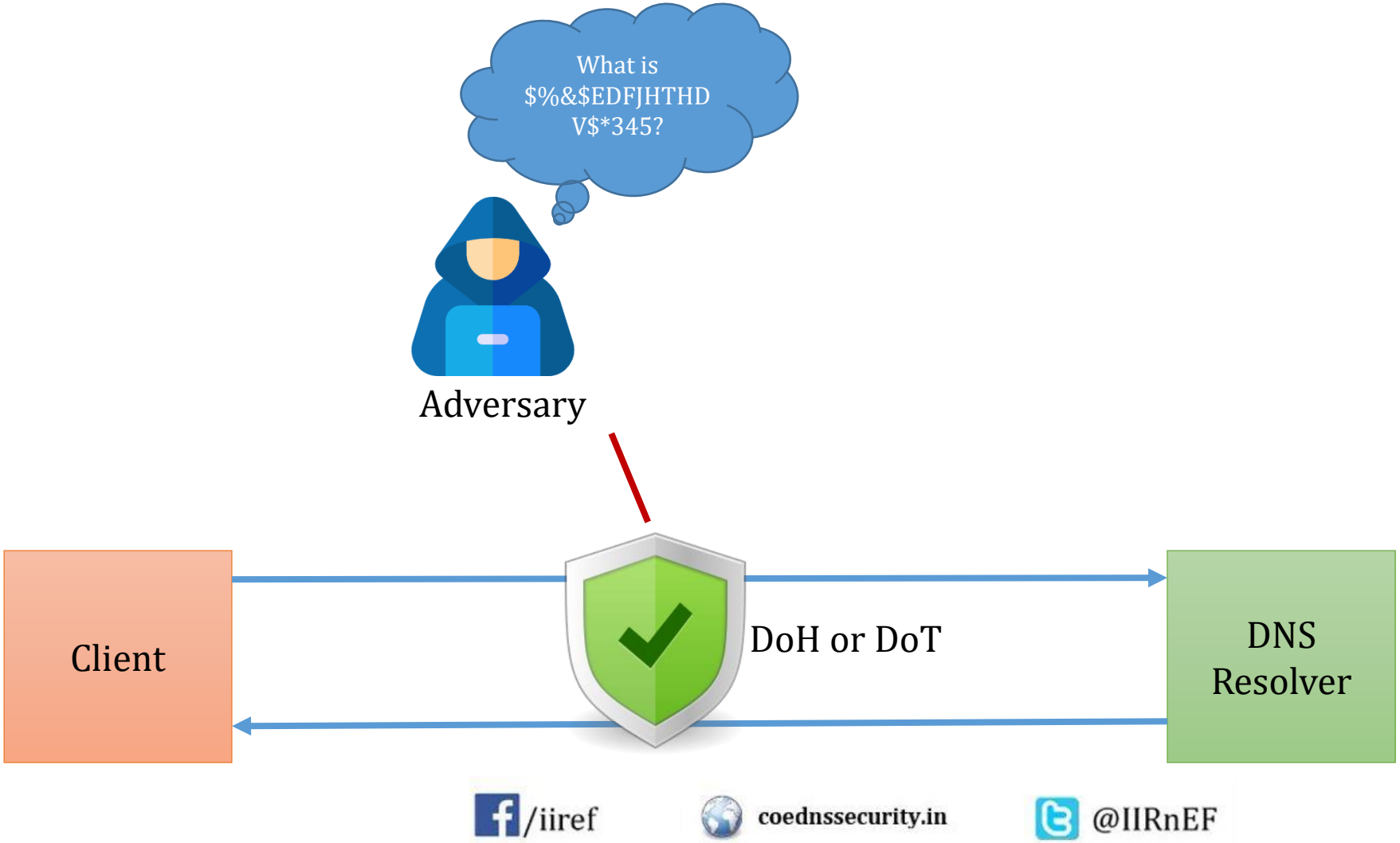
Agenda

- Motivation
- DNS over TLS (DoT)
- DNS over HTTP (DoH)
- DoH vs DoT
- DoH/DoT implementations using DNSDist

Need for Encrypted DNS Query



Encrypted DNS Traffic



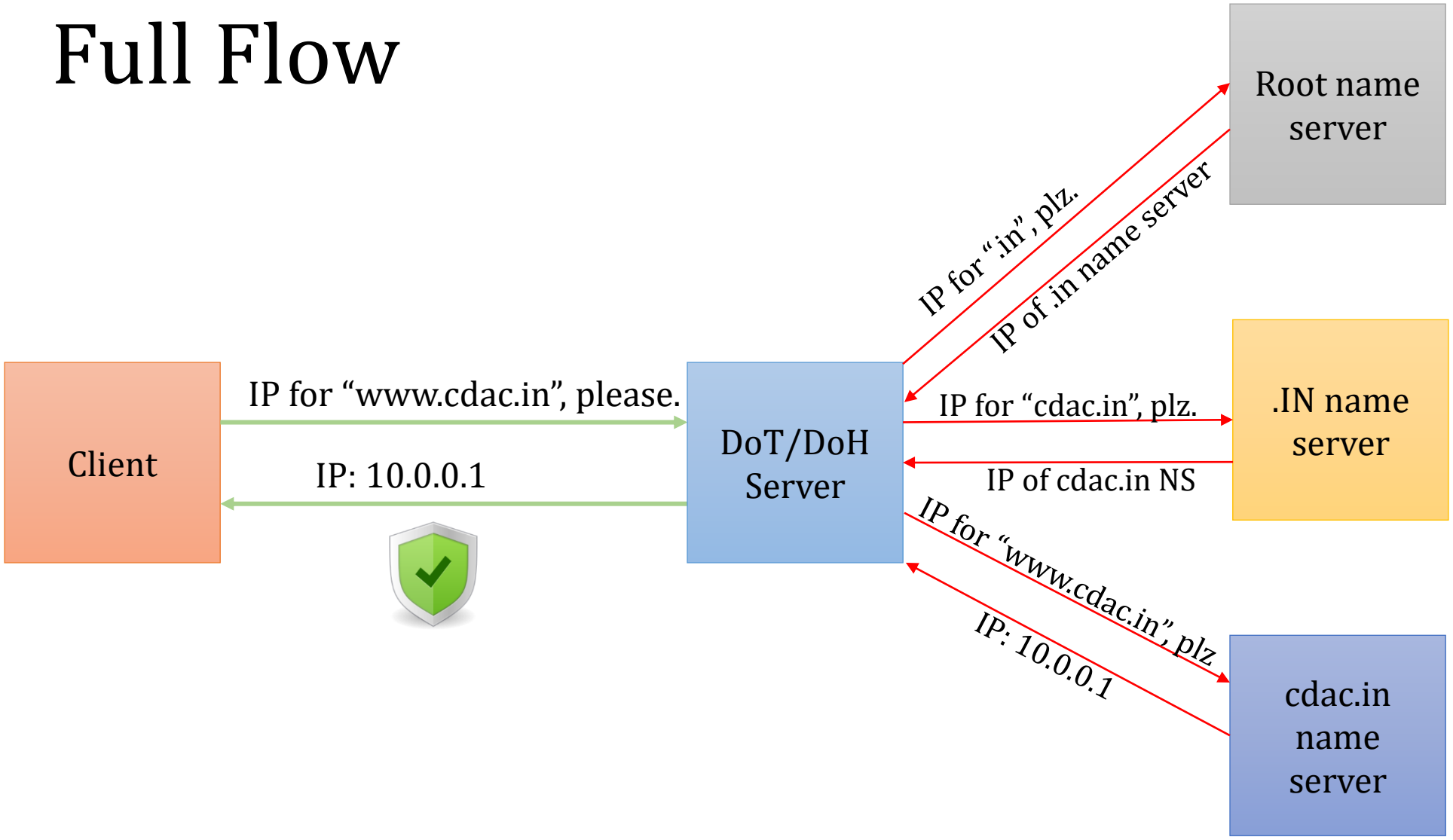
DNS over TLS (DoT)

- TLS Encryption on top of UDP
- Detailed in RFC 7858 (https://tools.ietf.org/html/rfc7858)
- Safeguard from MiTM
- Client doesn't query Authoritative Sever, rather DoT server makes traditional recursive queries.
- Default Port: 853
- Support
  - Android 9+
  - iOS 14+
  - Windows/Linux through packages

DNS over HTTPS (DoH)

- DNS Queries sent over HTTPS
- Request/Response in JSON format, GET/POST
- Port: 443
- Detailed in RFC 8484 (https://tools.ietf.org/html/rfc8484)
- Client doesn't query Authoritative Sever, rather DoH server makes traditional recursive queries.
- Support
  - Android 9+
  - iOS 14+
  - Windows, Linux (coming soon)
  - Firefox (working), others (intermittently)
- Server Examples
  - doh.iiref.in
  - dns.google
  - cloudflare-dns.com

Full Flow


Root name server
IP for ".in", plz.
IP of .in name server
Client
IP for "www.cdac.in", please.
IP: 10.0.0.1
DoT/DoH Server
IP for "cdac.in", plz.
IP of cdac.in NS
.IN name server
IP for "www.cdac.in", plz
IP: 10.0.0.1
cdac.in name server

To do or not to do!!

- Issues
  - Enterprise Security: No DNS Filtering
  - Centralization of internet?
  - Real Privacy? What about tracking through IP?
  - Weak Cyber Security?
  - Bypass legitimate blocklists
    - E.g. child abuse websites, terrorism content, and websites with stolen copyrighted material.
  - Helpful to people in oppressive countries?
- Hiding web traffic: VPNs and Tor may be used with DoH as an extra layer of protection.

DoH or DoT

- DoH
  - Uses TCP 443
  - Difficult to segregate DoH traffic from usual https
  - Privacy from even network administrators
- DoT
  - Uses TCP 853
  - can be blocked/monitored
- Who supports what?

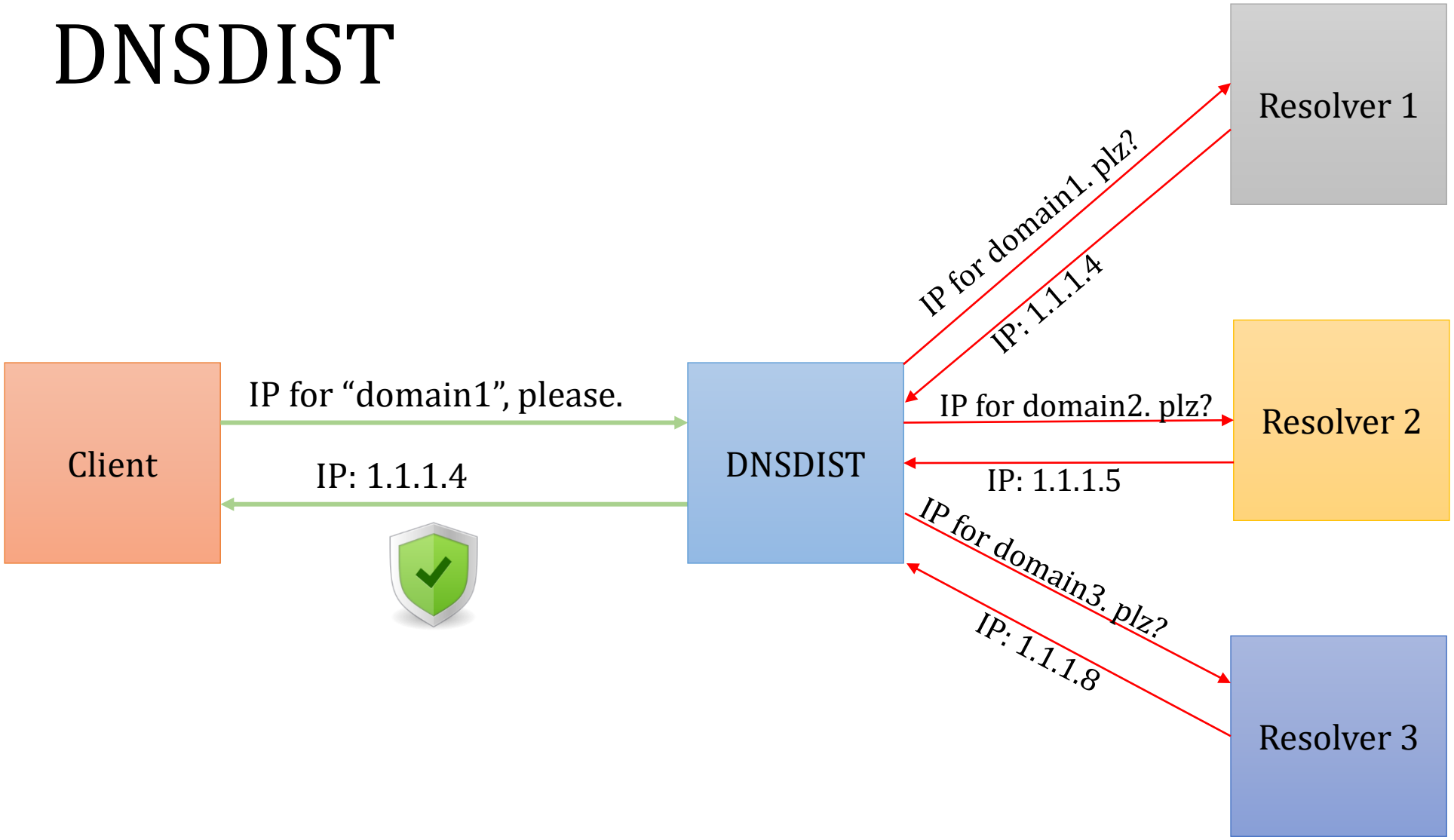
DoH/DoT vs DNSSEC

- DNSSEC
  - Authoritative NS Authentication
  - RR Integrity
- DoH & DoT
  - Confidentiality
  - Communication Channel Security
- Don’t vie, rather enhance security

DNSDIST

- DNS-, DoS- and abuse-aware loadbalancer
- Routes traffic to the best server
- Deliver response to legitimate users
- Shunts/Blocks abusive traffic
- Support for DoH & DoT since 1.4.0+
- Inbuilt Web Server

DNSDIST


Resolver 1
IP for domain1. plz?
IP: 1.1.1.4
Client
IP for “domain1”, please.
IP: 1.1.1.4
DNSDIST
IP for domain2. plz?
IP: 1.1.1.5
Resolver 2
IP for domain3. plz?
IP: 1.1.1.8
Resolver 3

Implementation [Ubuntu]

- Install bind9, dnsdist (1.4.0+)
  - #apt install bind9
  - #apt install dnsdist
- #nano /etc/dnsdist/dnsdist.conf
  - addLocal('0.0.0.0:5300', {doTCP=true, reusePort=true, tcpFastOpenSize=0})
  - addACL('0.0.0.0/0')
  - newServer({address="127.0.0.1", qps=1, name="resolver1"})
  - addTLSLocal('0.0.0.0','/opt/doh.local.crt', '/opt/doh.local.key')
  - addDOHLocal("0.0.0.0:443", "/opt/doh.local.crt", "/opt/doh.local.key", "/", { doTCP=true, reusePort=true, tcpFastOpenSize=0 })
  - webserver("127.0.0.1:8081", "Cdac@123", "Cdac@123")

Implementation [Ubuntu]

- Check DNSDIST configuration
  - #dnsdist --checkconfig
- Install DNSLOOKUP from snap
  - #snap install dnslookup
- Verify DoH/DoT installation
  - #dnslookup www.cdac.in tls://doh.local
    - #VERIFY=0 dnslookup www.cdac.in tls://doh.local [To disable certificate check]
  - #dnslookup www.cdac.in https://doh.local

Thank You

/iiref coednssecurity.in @IIRnEF