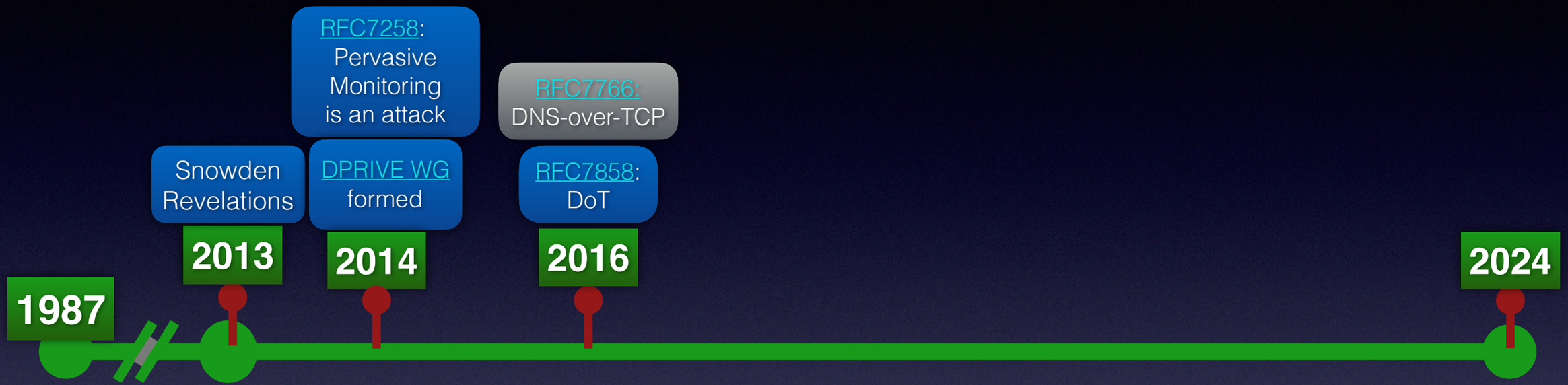
10 Years of Encrypted Stub to Recursive DNS

(Why have 1 protocol when you can have 3…?)

Sara Dickinson sara@sinodun.com

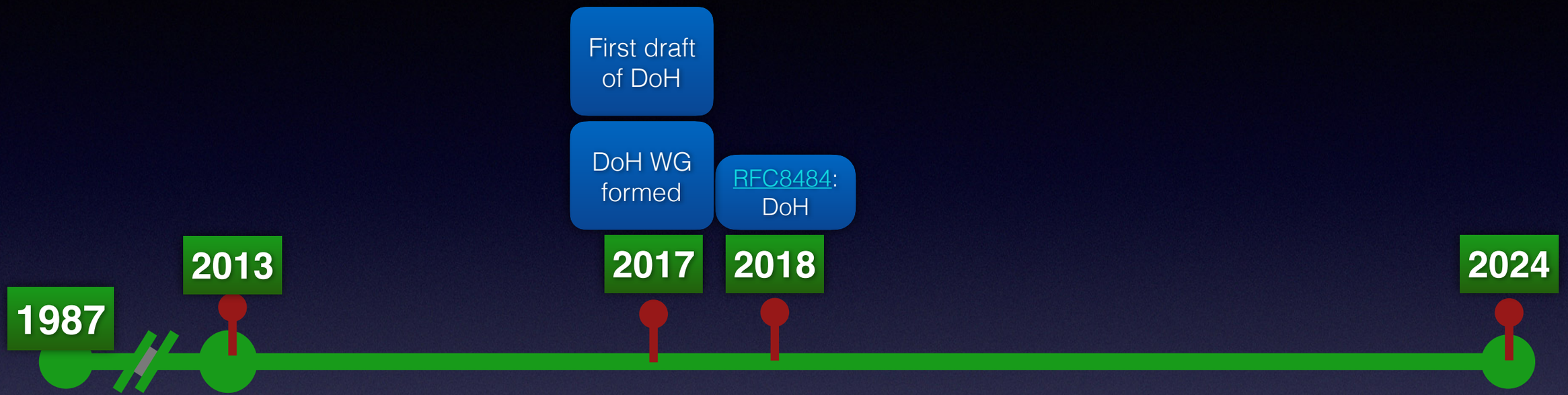
DINR 2024

DNS-over-TLS (DoT)



1	Driven by IETF	Push back from operators/ implementors on scalability	Bad historic TCP in DNS made transition to TLS much harder….
2	Lack of forum for stub implementors (including OS)	*getdns* and Phones led the way	DNSSEC had/has same problem
3	Discovery problem! (static configs)	Big players eased path	Hampered deployment

DNS-over-HTTP (DoH)



1	Driven by Web browsers (perf/priv)	Push back from operators/ implementors as ‘heavyweight’	New use case for DNS stub (in applications)
2	New control point (don’t need OS)	Frequent browser updates, rapid deployment	Debate focussed on default settings (2018) and user GUIs….
3	Bypass network blocking	Bypass network blocking	Debate focussed on impact for network operators

DNS-over-QUIC (DoQ)

1	Driven by Google, browsers	Encryption is default but must be fast!	Spin bit debate….
2	As DoT/DoH happening, QUIC emerging	Could not wait…	Interesting timing for DNS efforts
3	QUIC still immature in some ways	Can require more fine tuning	DoH3/DoQ is the future

ADD WG - Discovery

1	**DNR** (First discussion in 2016)	***RFC 9463:*** DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers
2	**DDR & SVCB**	***RFC 9462*****:** Discovery of Designated Resolvers ***RFC 9461:*** Service binding Mapping for DNS Servers
3		Active work continues…..

Today and the Future?

- A few % of DNS stub-rec traffic encrypted today

- **STUB side**
    1. **Devices/apps** MUST/SHOULD encrypt DNS by default where possible
    2. Still BIG challenges with **CPE equipment** and cert management

- **Recursives**
    - Continued roll out at ISPs/enterprise to **decentralise**

- **Policy**
    - **Organisation policy changes** governments and bank/companies continuing to requiring encrypted DNS