draft-am-dprive-eval-01

IETF 93, Prague

July 24, 2015

Changes since -00

- Incorporated a number of suggestions and comments from Stephane Bortzmeyer, and others.
- An entity breaching privacy is now called actor or monitor, rather than attacker or adversary.
- Replaced attack model with risk model
- Definitions from the Privacy Considerations RFC (6973) are no longer quoted at length.

Changes since -00

- Attack models simplified:
  - Type 1 – Passive Pervasive Monitor (RFC 7258)
  - Type 2 – Active Monitor – selection of target, potential use of MITM
- Templates examples added
  - Encrypted channel cases (upgrade-based TLS, IPSEC)
  - Qname minimisation
- Section added to mention evaluation criteria other than privacy measures, such as protocol change requirements.

TLS evaluation example

- Does not achieve undetectability given use of a DNS-specific port.
- STARTTLS in the clear further impacts privacy measures, perhaps (will have language about this in next rev).
- Omitting more details for brevity here.

```
Eval(Qname_minimisation ([...],
     System_Settings([S, P, R, A], [R-A]),
     Risk_Model(Type=2),
     Privacy_Mechanism{
            Mechanism_name =
Qname_minimisation
            Parameters{
                Qtype_used = NS
           }
        },
     System_settings{
        Entities = S, P, R and A;  Links = R-A
     },
     Risk_model{
        Type = 2,  Links = R-A
     }
     Privacy_guarantee =  unlinkability
     Privacy_measure = analytical
    [snip]
```

S = STUB
P = PROXY
R = RECURSIVE
A = AUTHORITATIVE

TYPE2 = ACTIVE
MONITOR

Linkabiity definition modified: ability of a monitor to link two labels of minimized queries to each other and relate them to the original source of the query

Changes to come

- More clean-up, such as replacing 1A/1B in templates with Type-1 and Type-2
- Reference DTLS draft
- Incorporate comments from Haya Shulman
- Incorporate results from template assessment effort (authors and Minsuk Kang)

Working group adoption?