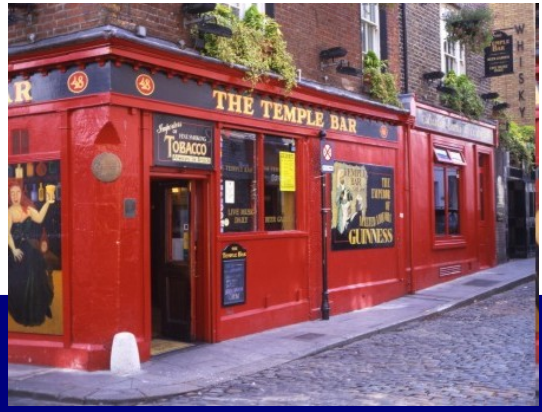

IKE Session Resumption

Yaron Sheffer, Check Point

IETF-72

Chartered Work Item

- Session resumption in a client-gateway situation
  - Upon temporary gateway or network failure
- Client, and a **single** gateway
  - Or a closely synchronized gateway cluster
- Motivation
  - Eliminate CPU bottleneck when 100K clients reconnect to a gateway
  - Eliminate need for user interaction, AAA server interaction
- Analogous to TLS stateless session resumption (RFC 5077)

Out of Scope

- “Resumption” into a different gateway
  - That is, failover
- Detection of network/gateway failure
- Specification of a state “ticket”

Starting Point and Delta

- Starting point: draft-sheffer-ipsec-failover-04
  - With Lakshminath Dondeti, Vidya Narayanan, Hannes Tschofenig
  - Note also the new draft-xu-ike-sa-sync-00
- Rename draft: failover → resumption
  - Modify the problem statement sections accordingly
  - And minor tweaks to the solution
- An ongoing discussion on number of round trips vs. security guarantees
  - -04 has 1 mandatory RT, and an optional 2nd RT
- Eliminate ticket format, or weaken the language

Backup

Ticket Presentation (Resume)

```
HDR, Ni, N(TICKET_OPAQUE), [N+,] SK {IDi,
  [IDr,] SAi2, TSi, TSr [, CP(CFG_REQUEST)] →
← HDR, SK {IDr, Nr, SAr2, [TSi, TSr],
  [CP(CFG_REPLY)]}
```

- Note:
  - Use of temporary IKE SA
  - Processing to create a new IKE SA (not directly the key from the ticket) and Child SA
  - An optional protected cookie, stronger than the regular IKEv2 cookie (not shown here)

draft-xu-ike-sa-sync-00

- Extensive discussion of usage scenarios
  - Including a new *load balancing* scenario
- Ticket mechanism
  - IKE_SA_SYN payload
- 3 architectural entities: endpoint, gateways, and a stub (ticket) database
  - Database may be central, or distributed to several gateways
  - A few operations define on the ticket, like set, get, update