Key Agility Requirements for IPsec

Steven M. Bellovin

smb@research.att.com

http://www.research.att.com/~ smb

+1 973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

How Important is Key Agility?

- We're now selecting AES — how important is key agility?
- Some ciphers have very fast key setup time; others are slow.

⇒ You can (somewhat) compensate for slow key setup by caching key schedules.

Our Setup

- FreeS/WAN gateway at central site.
- FreeS/WAN “appliances in people’s houses.
- /28 or /29 protected LAN on far side of appliance.

Methodology

- Capture packet headers on plaintext side of our IPsec gateway.
- Intuit SPI (and hence key) from remote address and knowledge of our addressing plan.
- Simulate an infinite-depth LRU cache.
- Calculate how many hits at each depth.
- Calculate cumulative hit rate for each depth.

Measurements

- 145 gateways; 300 different machines protected.
- More packets to the home than from it.
- Many more bytes to the home than from it.
- 406 bytes/packet downstream; 106 bytes/packet upstream.

Downstream Cache

Depth	Packets	Cum. %
0	1791239	42.76
1	712719	59.77
2	470323	70.99
3	298255	78.11
4	203250	82.96
5	149886	86.54
6	116415	89.32
7	92641	91.53
8	73355	93.28
9	58140	94.67
10	44887	95.74

Upstream Cache

Depth	Packets	Cum. %
0	942192	33.53
1	367564	46.61
2	269794	56.21
3	217387	63.95
4	175852	70.21
5	145346	75.38
6	120891	79.68
7	100418	83.26
8	81884	86.17
9	64991	88.48
10	50992	90.30
11	40071	91.72
12	30991	92.83
13	23835	93.67
14	18649	94.34
15	14680	94.86

Conclusions

- For 80% hit rate, a cache size of 5 is needed for encryption.
  8-element cache needed for decryption.
- For 95% hit rate, caches of 11 and 17 elements are needed.
- Smaller packet sizes upstream mean more free time for key setup.
- Difference probably due to delayed acks, smaller packets (and hence more interleaving), and maybe “packet trains” downstream.