IETF 105 TLSWG

Encrypted SNI

E. Rescorla, K. Oku, N. Sullivan, C. Wood

draft-ietf-tls-esni-04

Major Changes in -04

Clarify server HRR behavior and use separate KDF labels #168

Trial decryption text #166

GREASE ESNI #125

Move DNS extensions out of ESNIKeys #153

Minor Changes in -04

Replace ServerNameList with plain name #165

Remove checksum #163 and not_before and not_after #161

Update recommended padding text #162, A/AAAA anonymity set text #157, and discuss related traffic leaks #167

Open Issues

Can the ESNI values change upon HRR? #121

Adopt HPKE #145

Consider dropping split mode altogether #130

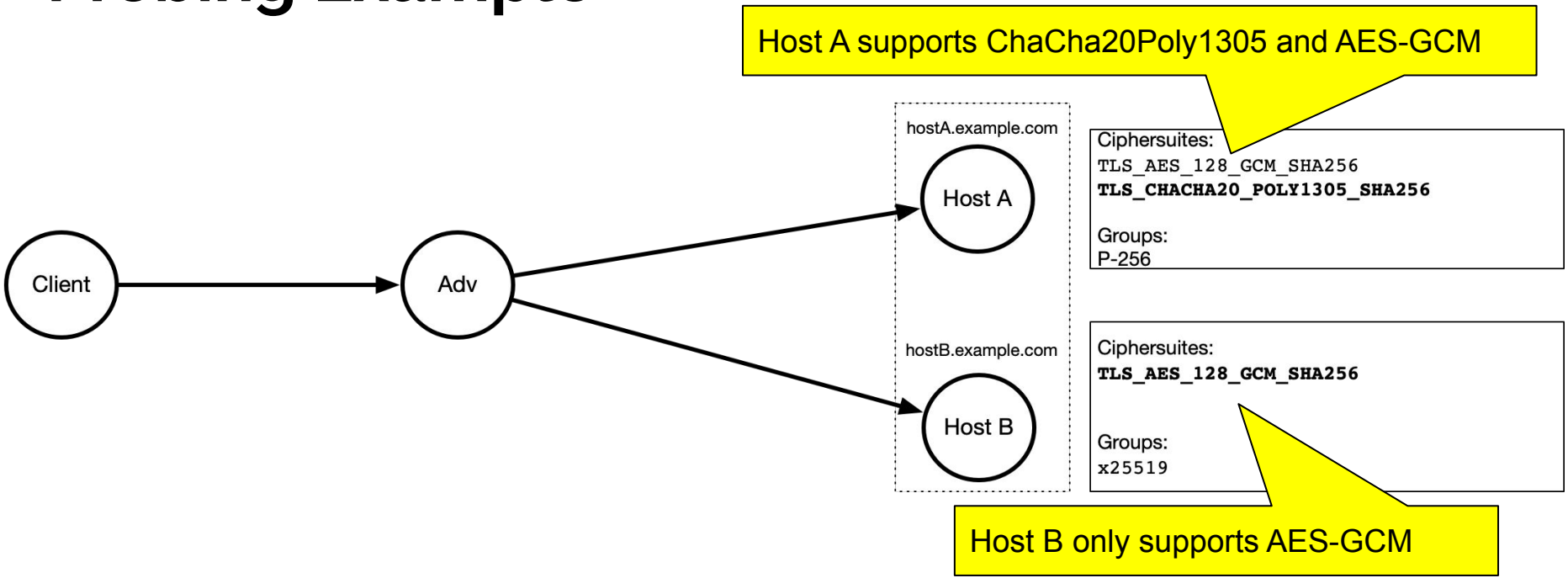
Replay attack and timestamp #149

Compress server name in ClientHello #116

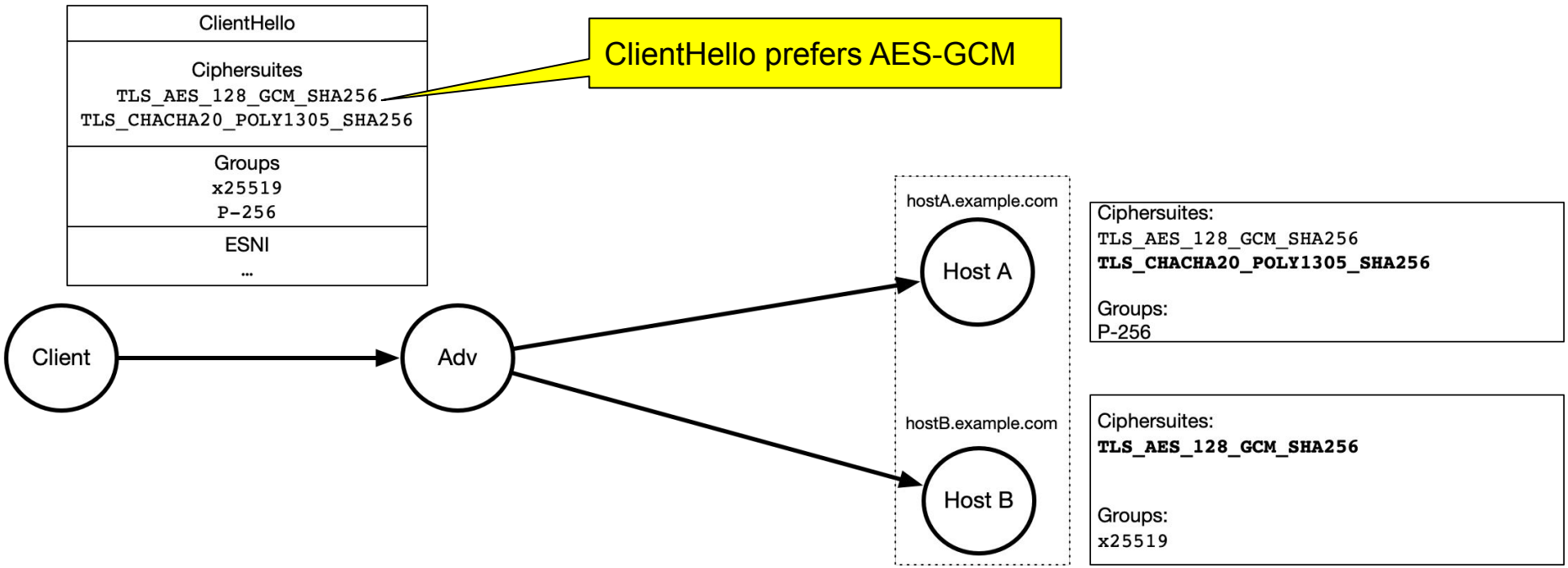
GREASE ESNI extensions stand out #177

ESNIInclude (zone apex) #110

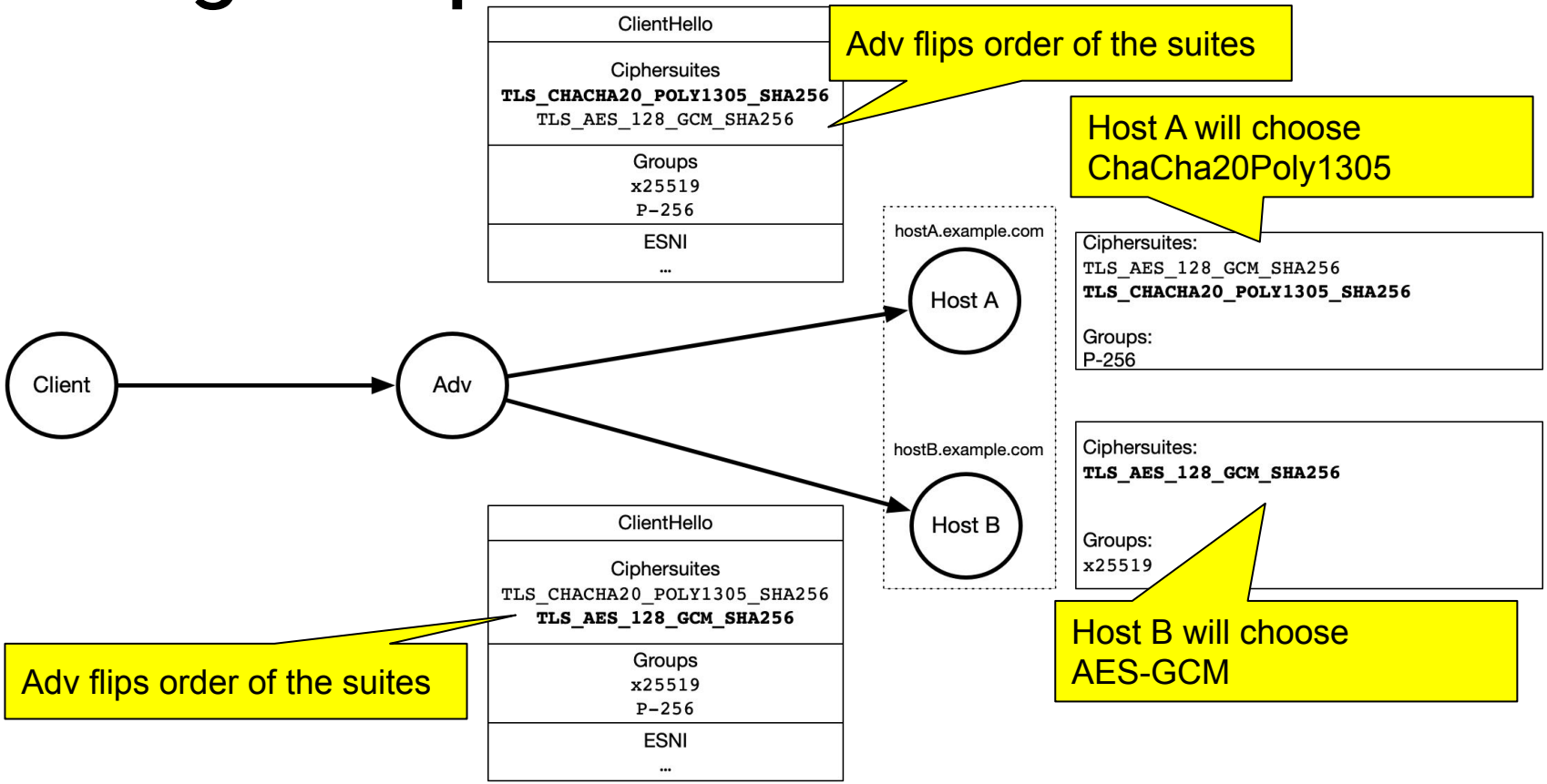
Probing Example



Probing Example (cont'd)



Probing Example (cont'd)



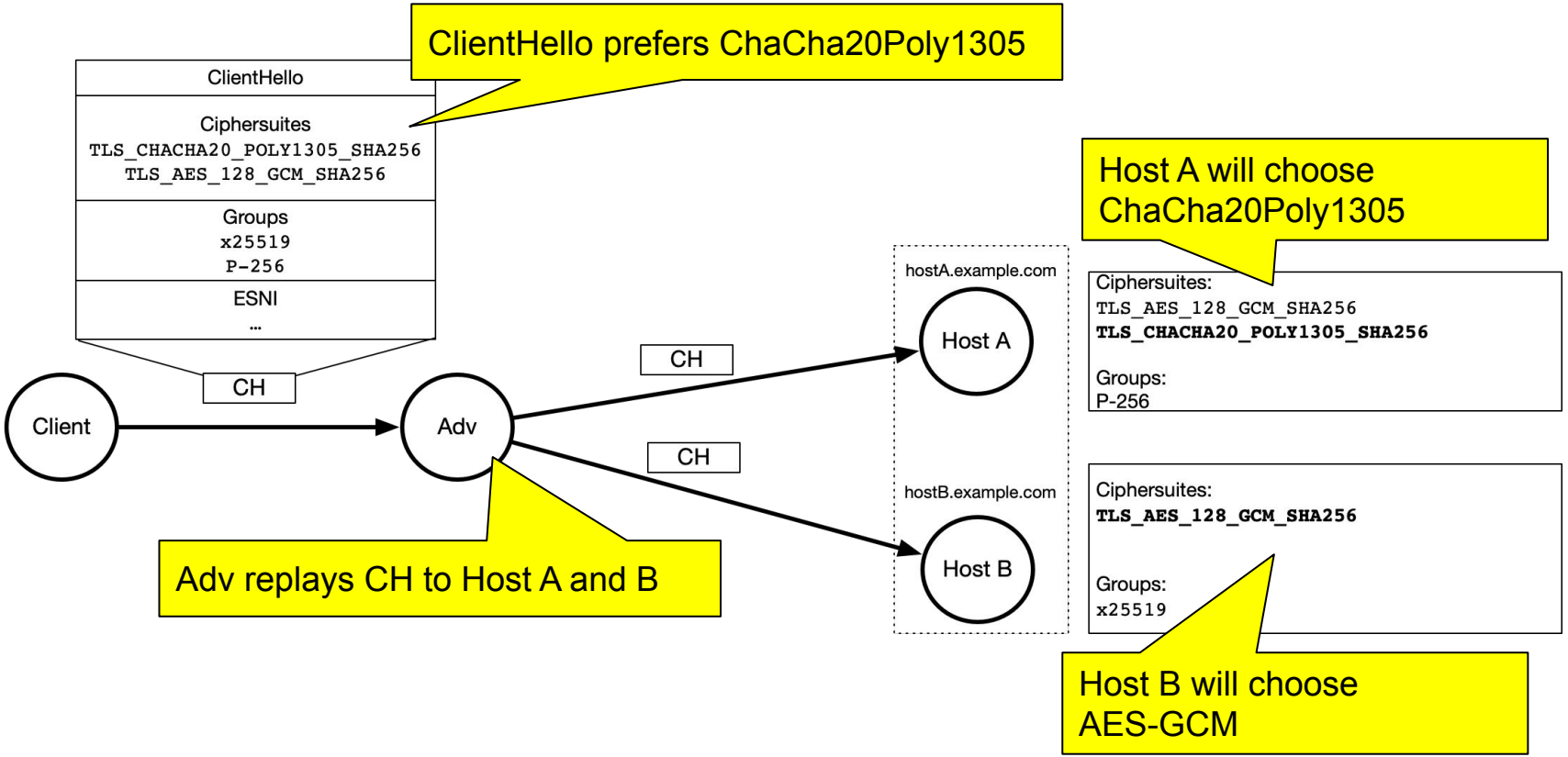
Incomplete Binding

All non-ESNI extensions must be bound to the ESNI extension

- Prevents select probing based on unbounded parameters (ciphersuites, etc)
- Prevents cut-and-paste of ESNI value(s) from one CH to another

Note: ESNI is currently only bound to CH.KeyShare

Another Probing Example



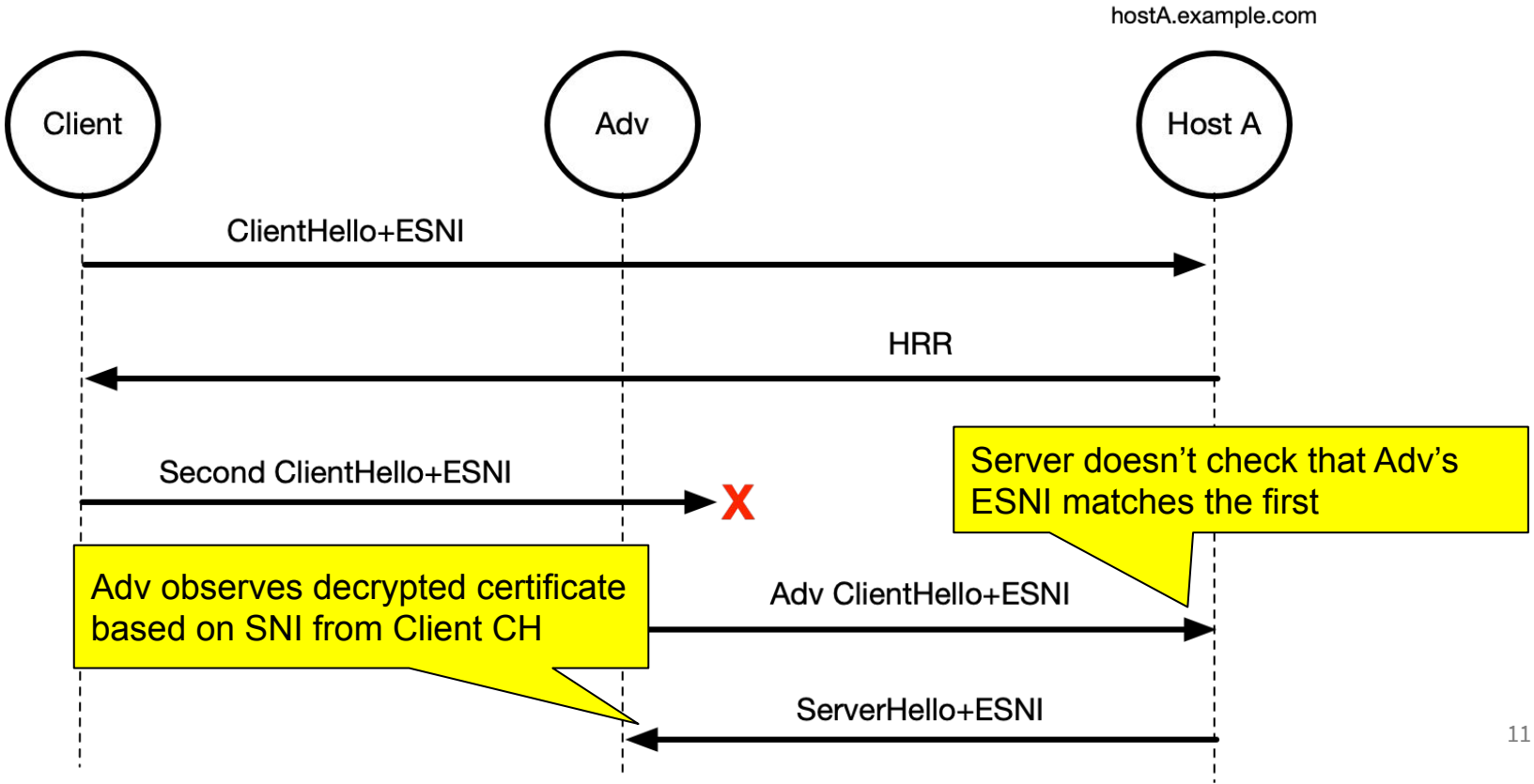
Anonymity Set Partitioning

Servers in the same anonymity set must respond to ClientHello messages identically for every non-ESNI extension

- Prevents probing based on any observable CH

Note: Not much clients can do about this one

On-Path HRR Attack



HRR and Parameter Selection

On first ClientHello, commit to some parameters and then generate HRR

On second ClientHello, check that decrypted nonce and server name match (this is **not** a cryptographic check)

- Prevents attacker from inserting its own KeyShare and ESNI value in second CH and decrypting the result

Note: Currently, clients MUST NOT change ESNI inner contents

ClientHello+ESNI Binding and HRR

Question 1: Do we require that servers in the same anonymity set behave identically?

Question 2: Do we bind the entire CH to the ESNI extension? If so, how?

Question 3: How do we want to bind the first and second CH together?

HPKE vs ESNI Encryption

HPKE: Public key encryption a la ECIES

- *Fresh* key share for each encrypted message
- Separate ciphersuite-based algorithm specification

ESNI: DH-based encryption a la ECIES

- Re-used key share (for HRR)
- Mixed TLS+ESNI ciphersuite specification

https://datatracker.ietf.org/doc/draft-irtf-cfrg-hpke/

HPKE Adoption

Benefits

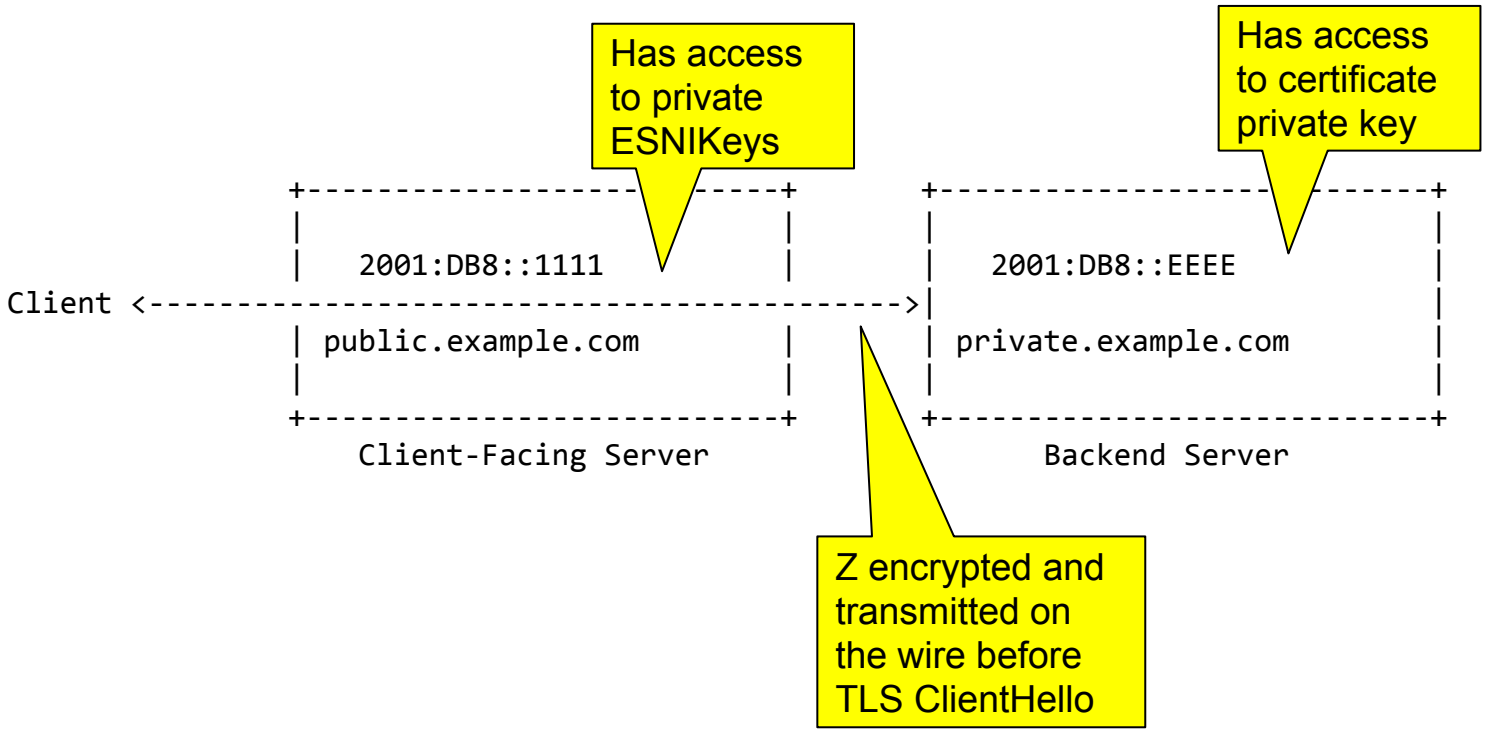
- Vetted and formally analyzed cryptographic construction

Drawbacks

- Requires two public key operations in the event of HRR

Question: Should we move to HPKE?

Split Mode


Has access to private ESNIKeys
Has access to certificate private key
2001:DB8::1111
2001:DB8::EEEE
Client
public.example.com
private.example.com
Client-Facing Server
Backend Server
Z encrypted and transmitted on the wire before TLS ClientHello

Split Mode

Benefits

- Addresses potential use cases

Drawbacks

- Adds complexity
- One part of a more general protocol [1]

Questions: Should we include split mode, and if so, to what extent?

[1] https://datatracker.ietf.org/doc/draft-schwartz-tls-lb/

Replay Attacks and Timestamps

Threat: Replaying ESNI CH to target servers to determine if “still active”

- Valid responses indicate specific services are still online
- Problematic for some use cases, e.g., mDNS discovery

Replay Attacks and Timestamps

Include a fuzzy timestamp

- Problems with clock skew

Rely on robustness mechanism for fallback

- Requires more complicated padding across EE and Certificate messages

Questions: Is this a threat we should aim to address, and if so, what mitigation(s) do we want?

Other Issues

GREASE ESNI extensions stand out #177

Compress server name in ClientHello #116

ESNIInclude (zone apex) #110

Getting to Last Call

Resolve open issues

Security analysis clearly needed

- Any volunteers?

ESNIKeys delivery duplication

- Several vehicles: ESNI RRType, HTTPSVC [1], .well-known [2]

[1] https://tools.ietf.org/html/draft-nygren-httpbis-httpssvc-03
[2] https://datatracker.ietf.org/doc/draft-farrell-tls-wkesni

Questions?

IETF 105 TLSWG

Encrypted SNI

E. Rescorla, K. Oku, N. Sullivan, C. Wood

draft-ietf-tls-esni-04