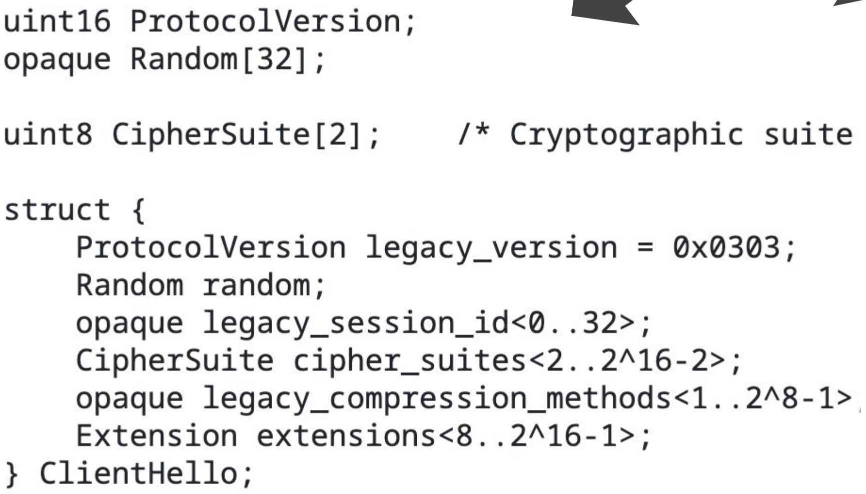
Measuring and Understanding ECH Deployment

Evidence from OONI on how ECH strengthens end-to-end resilience

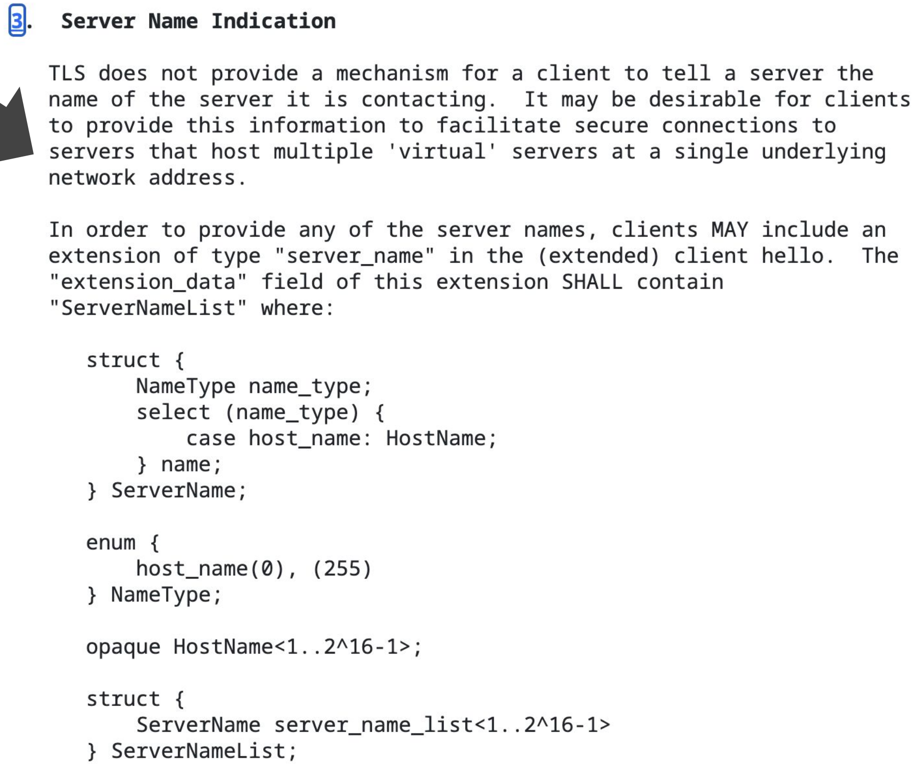
IETF 124, Montreal, 3rd November 2025

Why?

plaintext :(



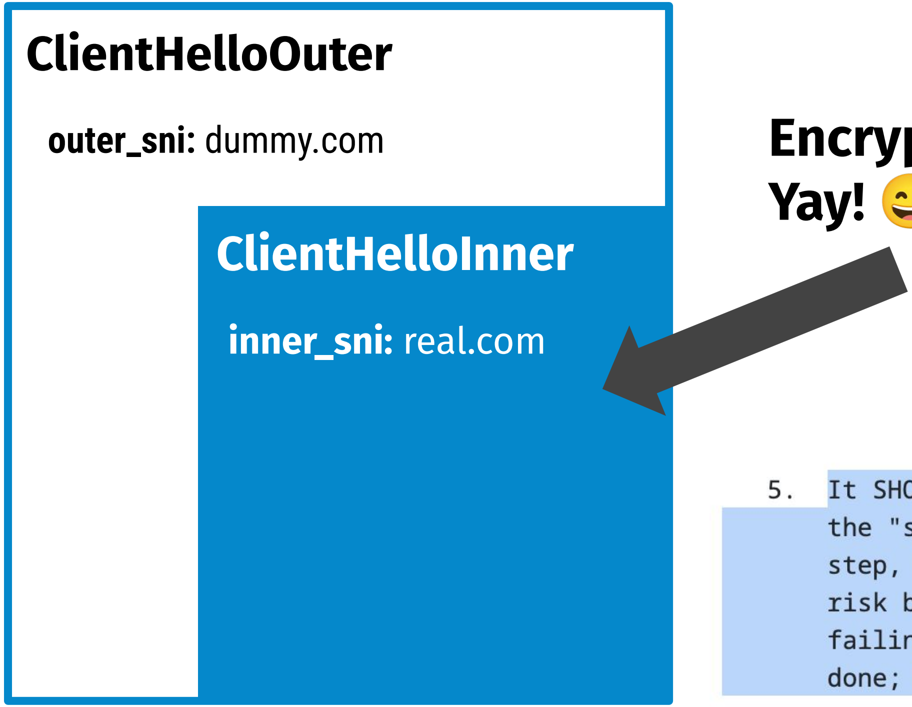
```
uint16 ProtocolVersion;
opaque Random[32];

uint8 CipherSuite[2];    /* Cryptographic suite

struct {
    ProtocolVersion legacy_version = 0x0303;
    Random random;
    opaque legacy_session_id<0..32>;
    CipherSuite cipher_suites<2..2^16-2>;
    opaque legacy_compression_methods<1..2^8-1>
    Extension extensions<8..2^16-1>;
} ClientHello;
```



```
3.  Server Name Indication

   TLS does not provide a mechanism for a client to tell a server the
   name of the server it is contacting.  It may be desirable for clients
   to provide this information to facilitate secure connections to
   servers that host multiple 'virtual' servers at a single underlying
   network address.

   In order to provide any of the server names, clients MAY include an
   extension of type "server_name" in the (extended) client hello.  The
   "extension_data" field of this extension SHALL contain
   "ServerNameList" where:

      struct {
          NameType name_type;
          select (name_type) {
              case host_name: HostName;
          } name;
      } ServerName;

      enum {
          host_name(0), (255)
      } NameType;

      opaque HostName<1..2^16-1>;

      struct {
          ServerName server_name_list<1..2^16-1>
      } ServerNameList;
```

ClientHello

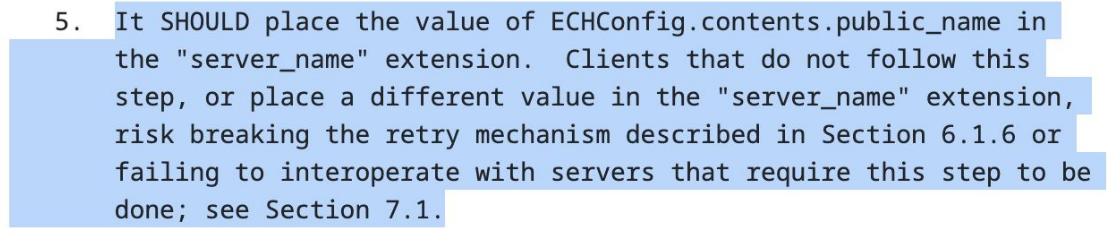
How?



Encryption!
Yay! 😄

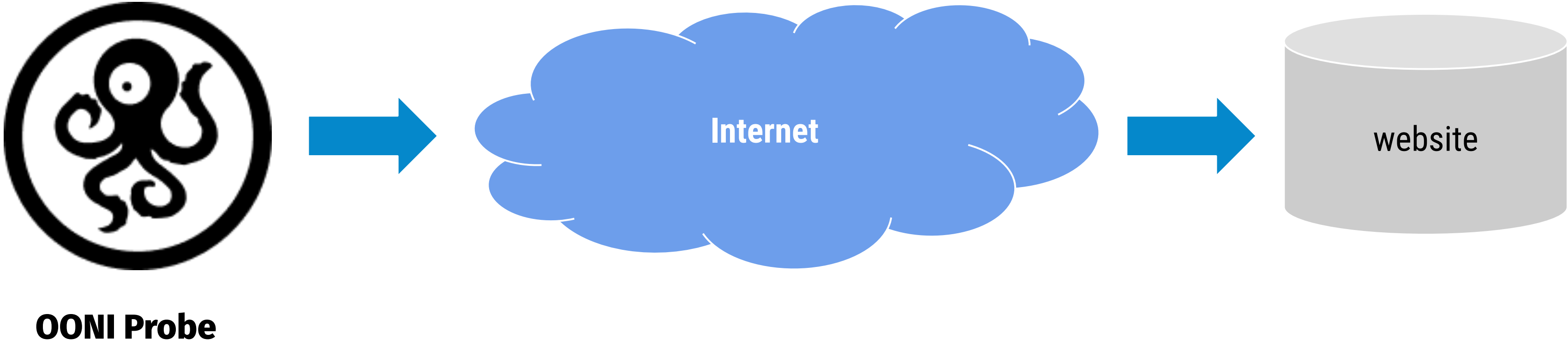
ECHConfig

- HPKE crypto
- public_name
- Distributed out of band (in practice DoT/DoH)



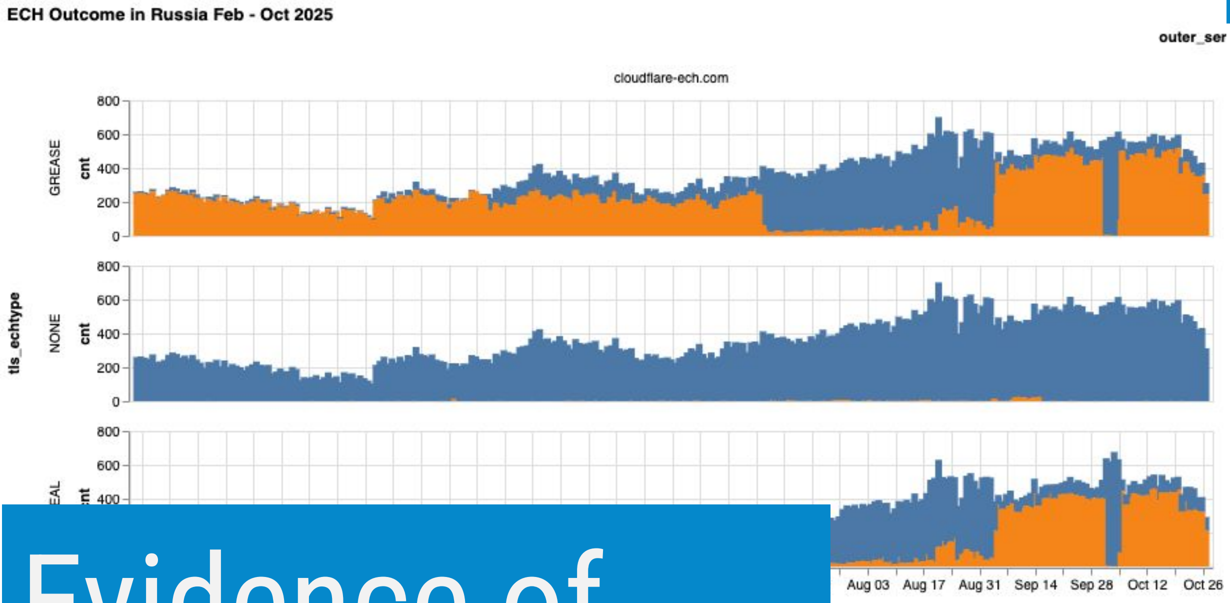
```
5.  It SHOULD place the value of ECHConfig.contents.public_name in
    the "server_name" extension.  Clients that do not follow this
    step, or place a different value in the "server_name" extension,
    risk breaking the retry mechanism described in Section 6.1.6 or
    failing to interoperate with servers that require this step to be
    done; see Section 7.1.
```

OONI ECHCheck test



We can now measure where ECH **works, fails, or is deliberately blocked**

Evidence of Adversarial Interference



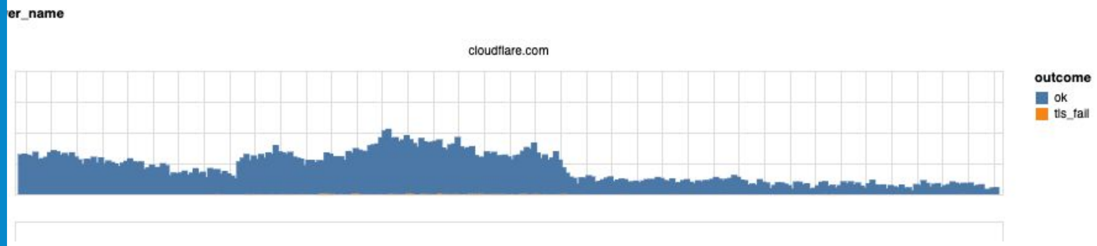
ECH Outcome in Russia Feb - Oct 2025

GREASE

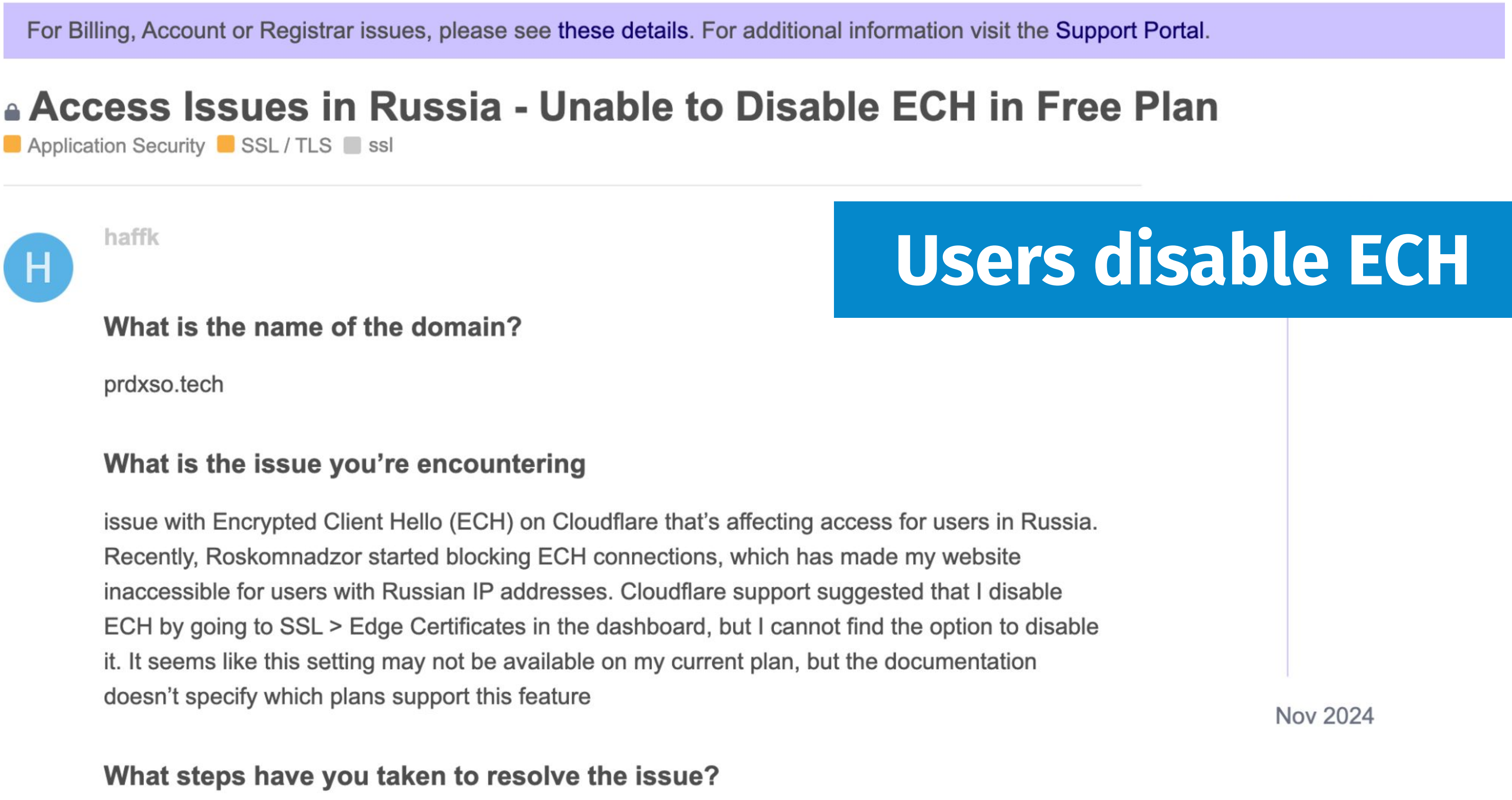
NONE

REAL

GREASE + cloudflare.com



Users disable ECH



For Billing, Account or Registrar issues, please see these details. For additional information visit the Support Portal.

Access Issues in Russia - Unable to Disable ECH in Free Plan

🟧 Application Security 🟧 SSL / TLS ▢ ssl

haffk

What is the name of the domain?

prdxso.tech

What is the issue you're encountering

issue with Encrypted Client Hello (ECH) on Cloudflare that's affecting access for users in Russia. Recently, Roskomnadzor started blocking ECH connections, which has made my website inaccessible for users with Russian IP addresses. Cloudflare support suggested that I disable ECH by going to SSL > Edge Certificates in the dashboard, but I cannot find the option to disable it. It seems like this setting may not be available on my current plan, but the documentation doesn't specify which plans support this feature

Nov 2024

What steps have you taken to resolve the issue?

ECH as ARMOR in Action

ECH deployment, testing, and defense are exactly what **ARMOR** stands for: **measurable, empirical resilience of the open Internet.**

Let’s make sure ECH doesn’t just exist,
Let’s make sure it

survives

https://ooni.org

OONI