Secure shell over HTTP/3 connections

draft-michel-ssh3

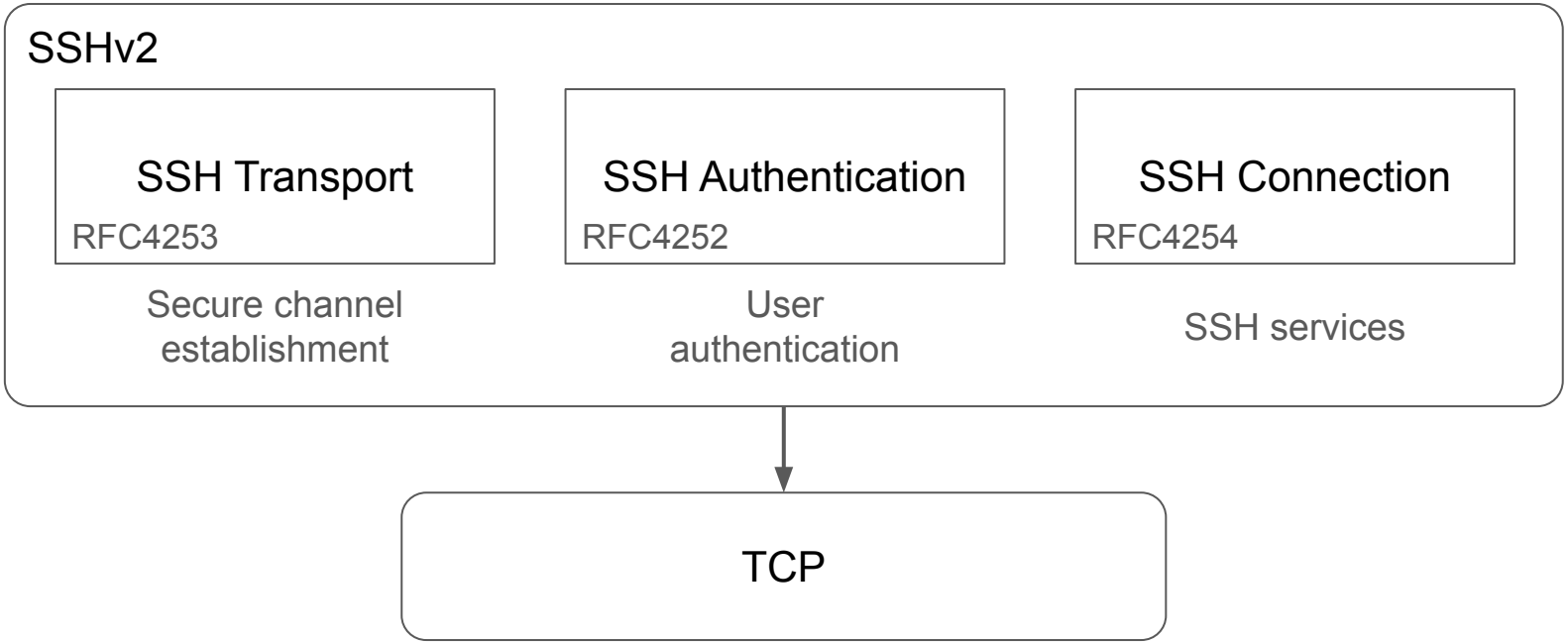
François Michel

Secure Shell (SSH) services

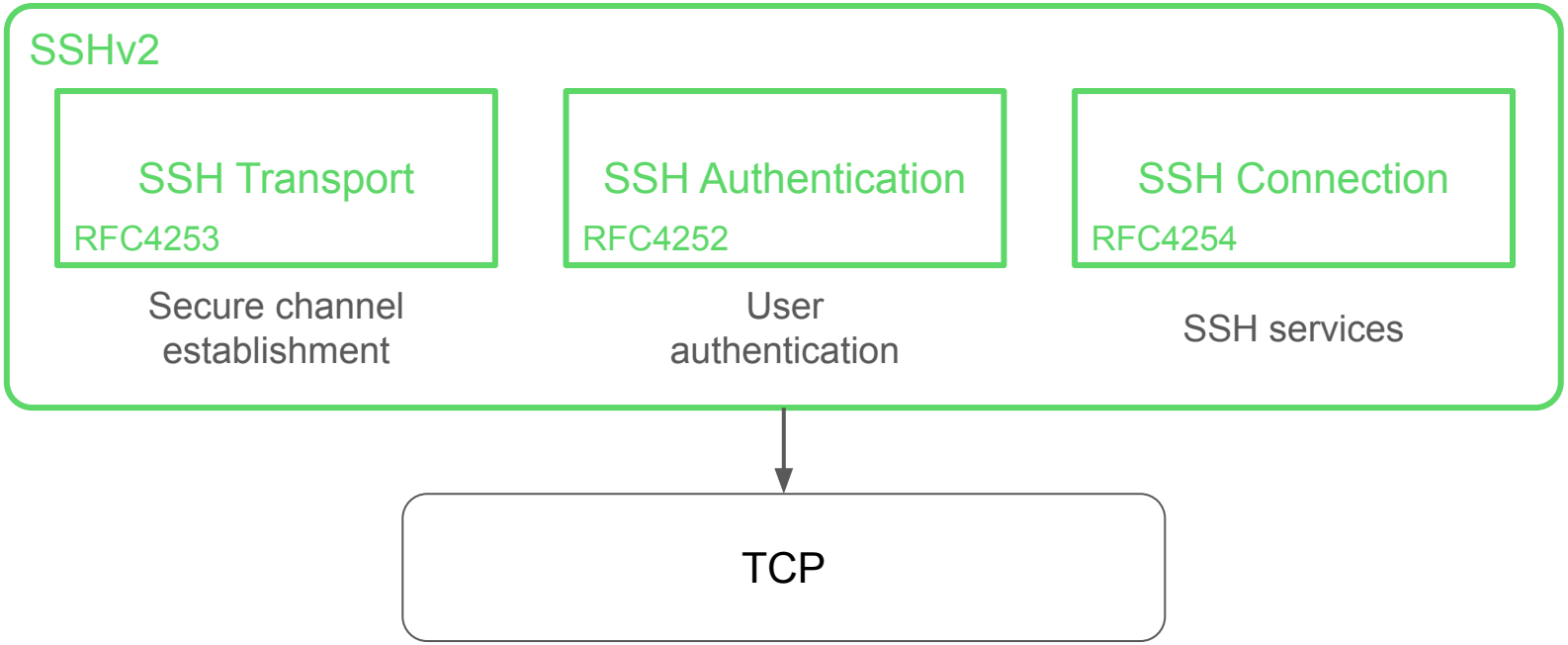
SSH(v2) provides secure services on a remote host over an insecure network.

- Remote interactive shell access
- Remote commands execution
- TCP port forwarding
- X11 forwarding

SSHv2 architecture

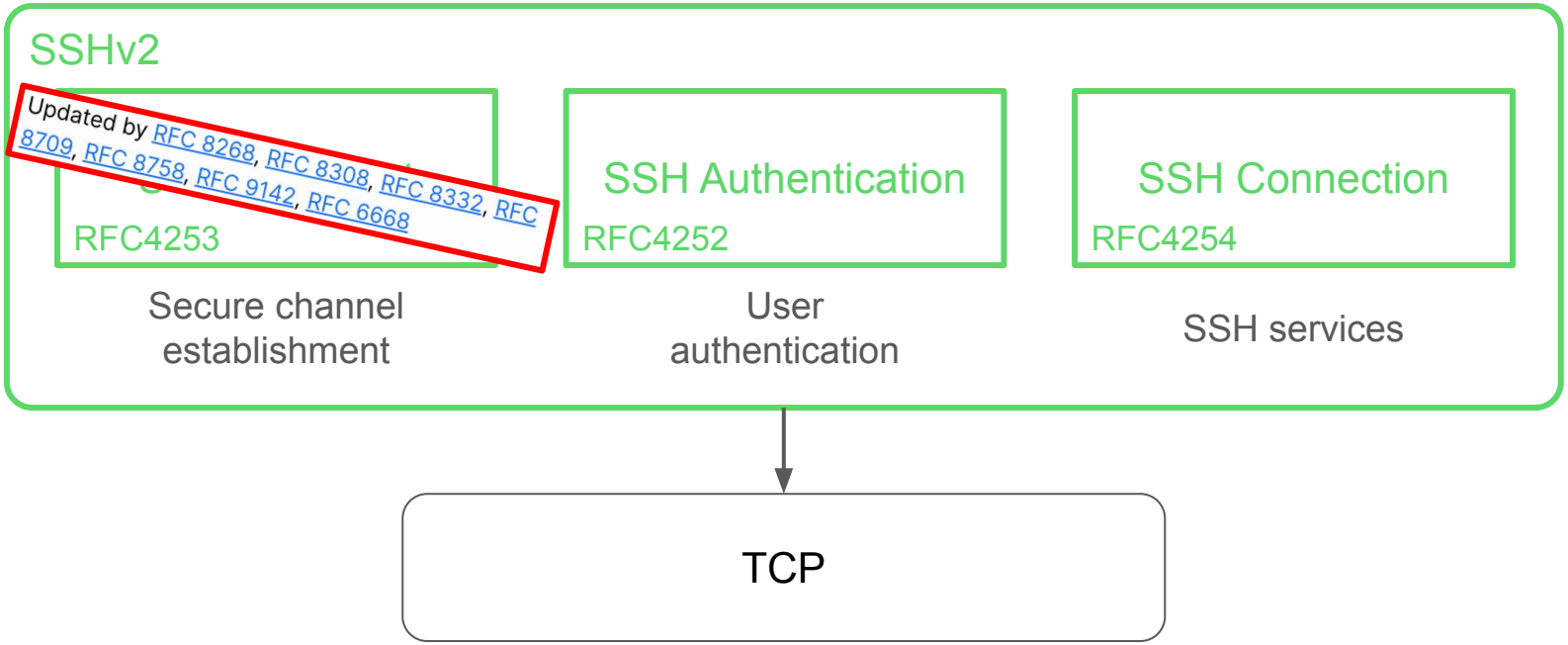


SSHv2 architecture



Implementing SSH means implementing RFC4253, RFC5252 and RFC4254.

SSHv2 architecture

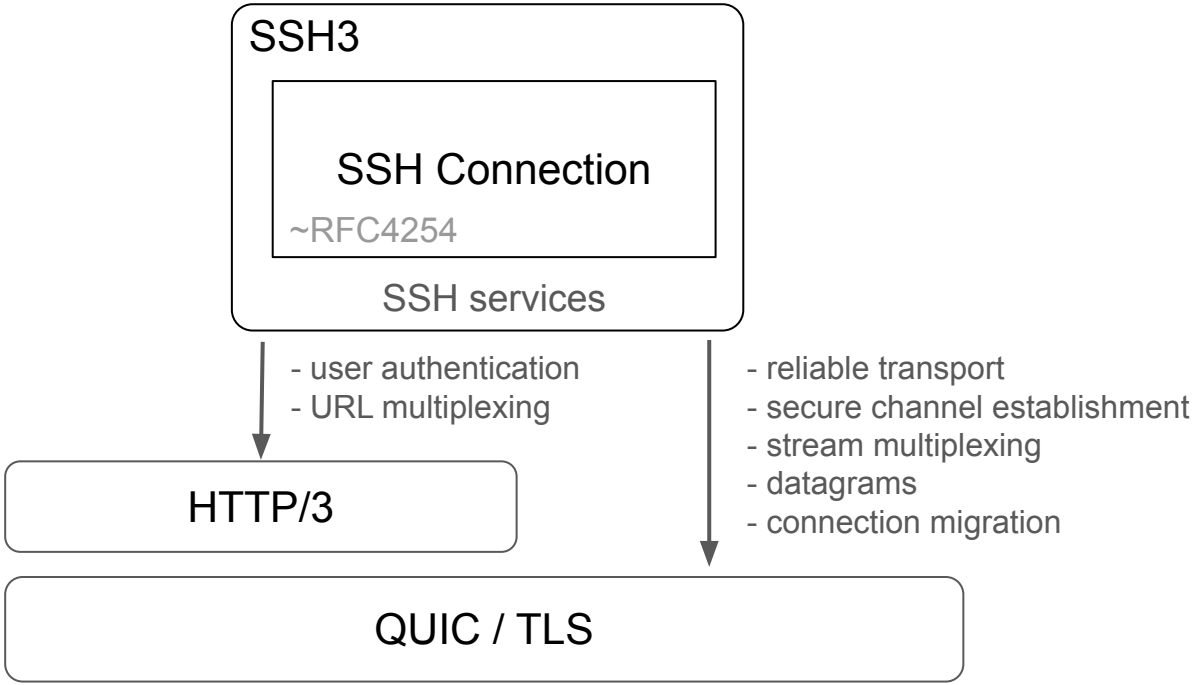


Implementing SSH means implementing RFC4253, RFC5252 and RFC4254.
Adding new crypto algorithms (e.g. PQC) means updating RFC4253 and every implementation.

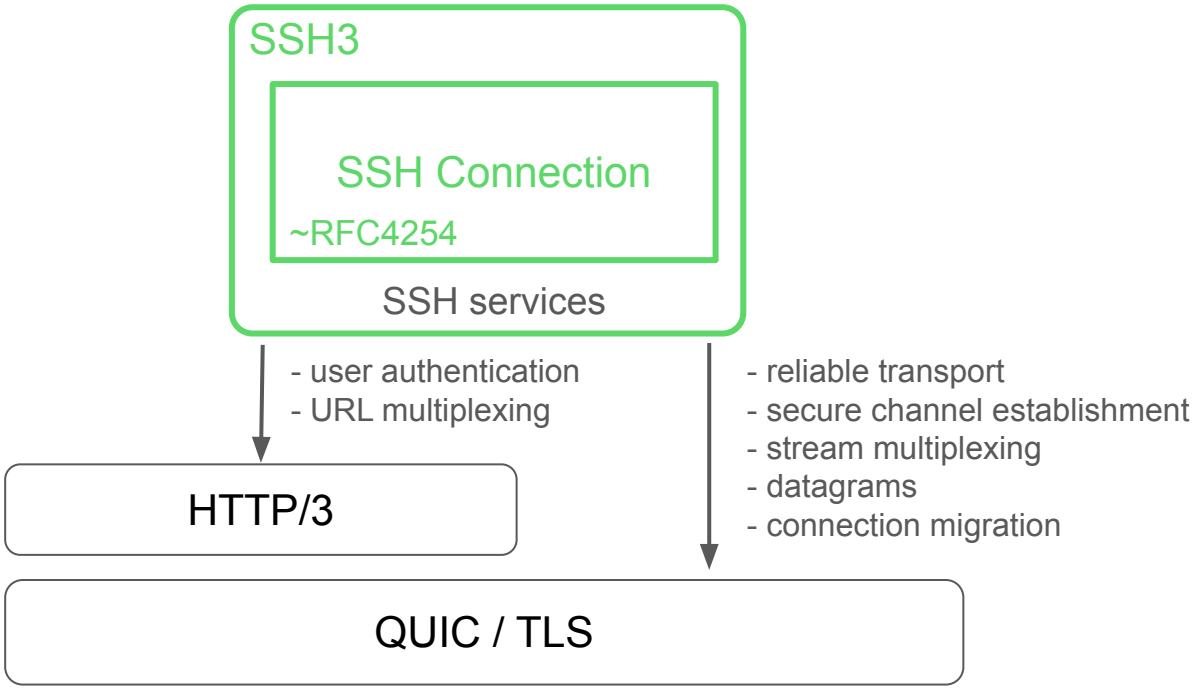
SSHv2 limitations

- Cannot forward UDP
  - QUIC cannot be forwarded through SSH
  - Can’t provide access to real-time resources
- Can easily be blocked or detected
  - blocking port 22
  - Blocking TCP connections exchanging SSHv2 version strings
- TCP is subject to RST/seqnum manipulation attacks
  - The TERRAPIN attack was about tampering with the TCP sequence number
  - TCP-AO addresses it for BGP, but not for SSH.
- Not well integrated with modern web infrastructures
  - These infrastructure propose their own HTTP-based authentication methods (SAML/OIDC/WebAuthn/…)
  - Often requires middlewares and tunnelling to integrate remote shells
- Evolves *in parallel* to TLS and HTTP, which also propose security and authentication
  - SSH certs are not well-defined and still not widely used. Certs used everywhere in HTTP/TLS.
  - Many individuals own HTTPS servers but still ssh to it using host keys and Trust-On-First-Use.

SSH over HTTP/3 architecture

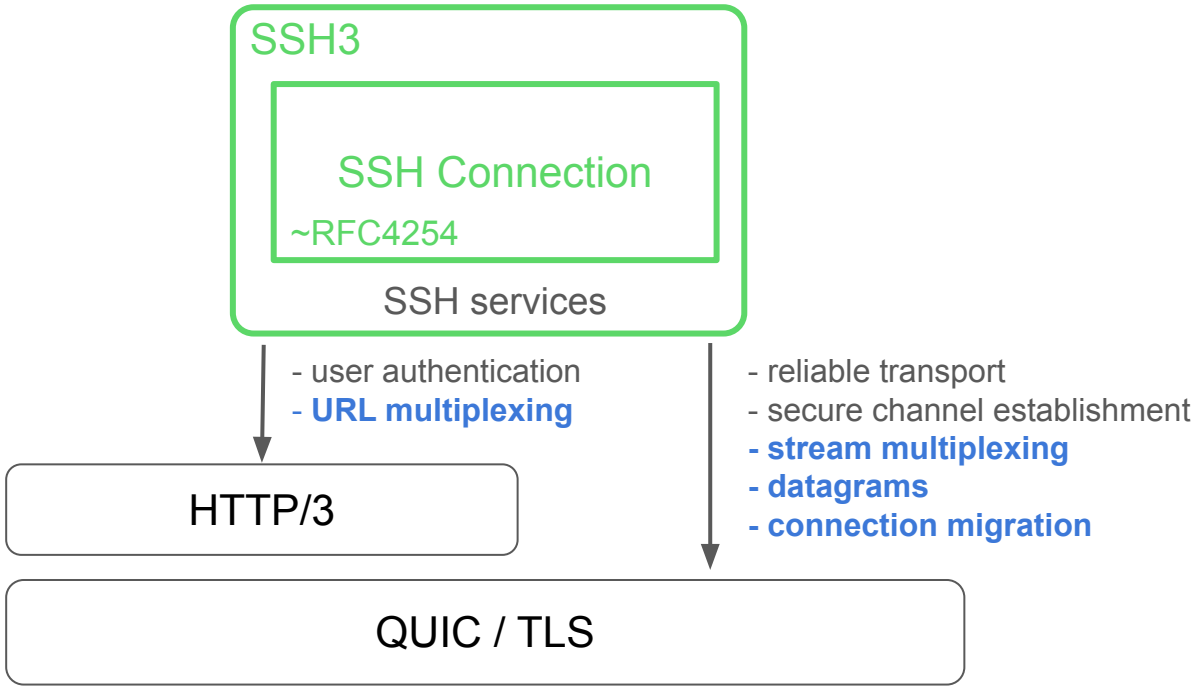


SSH over HTTP/3 architecture



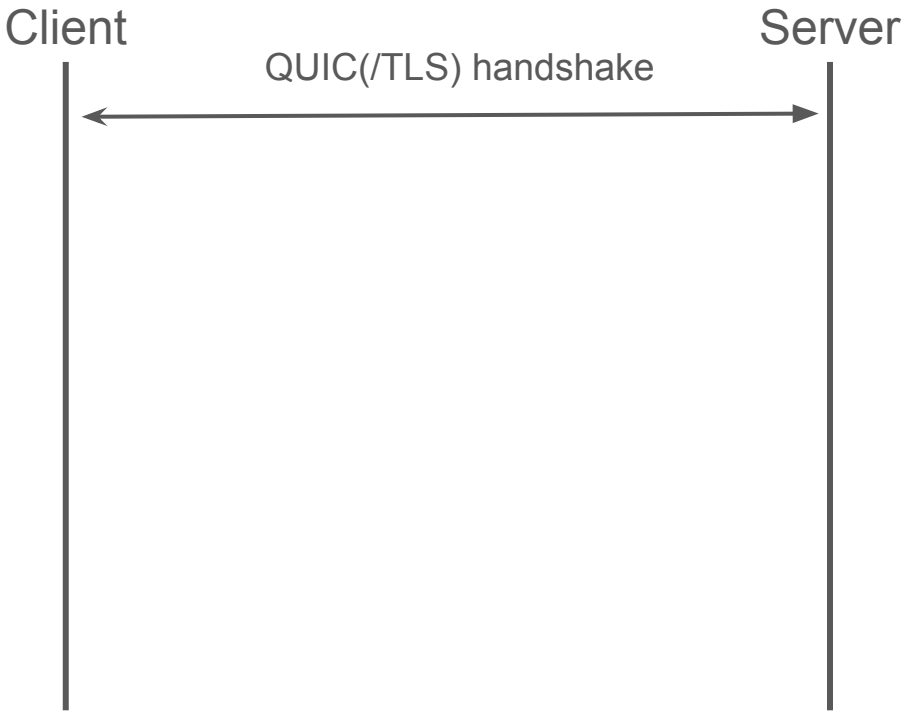
Security and transport can evolve independently from SSH, **implementation** focuses on SSH services

SSH over HTTP/3 architecture

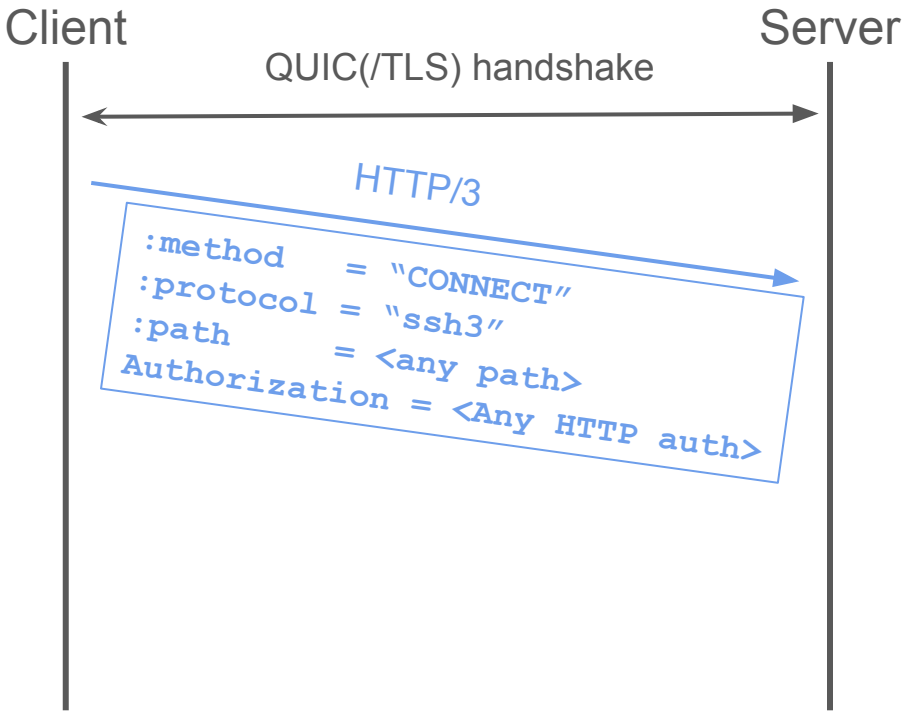


Security and transport can evolve independently from SSH, **implementation** focuses on SSH services
New features come along these modern protocols.

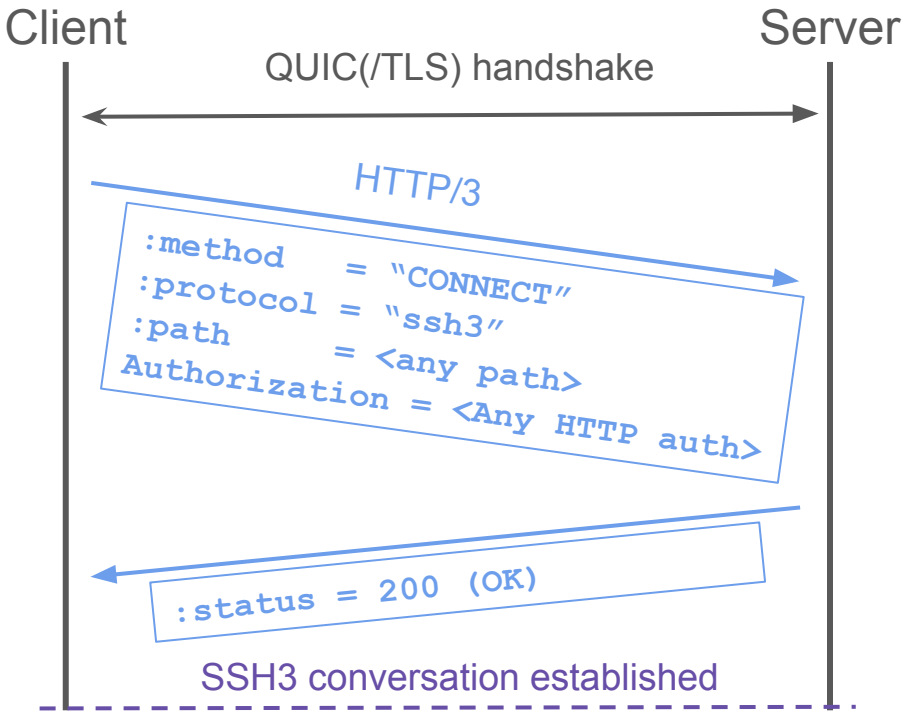
SSH3 conversation establishment



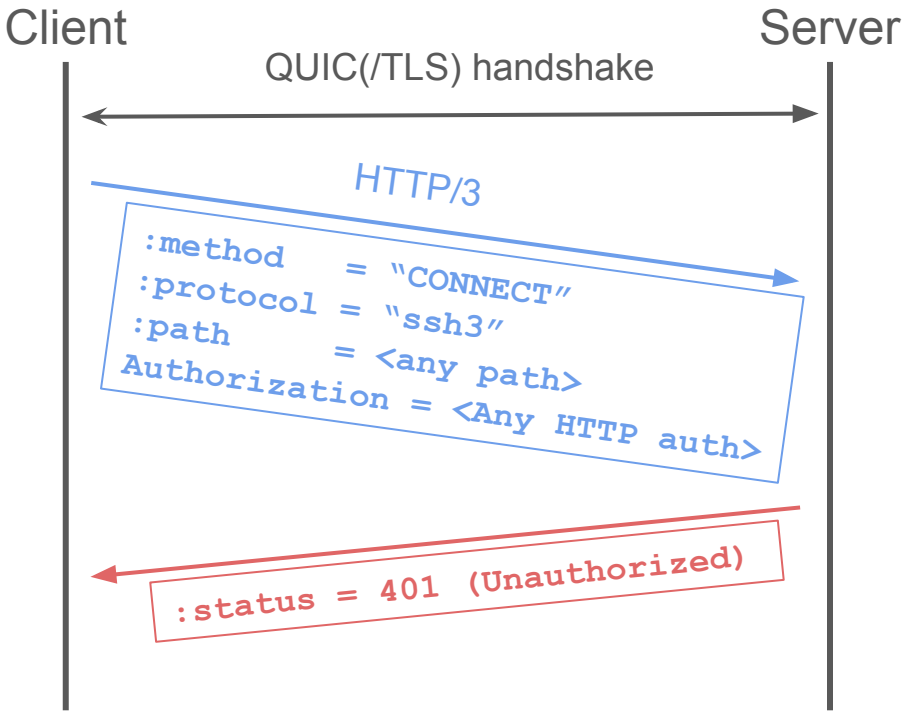
SSH3 conversation establishment



SSH3 conversation establishment

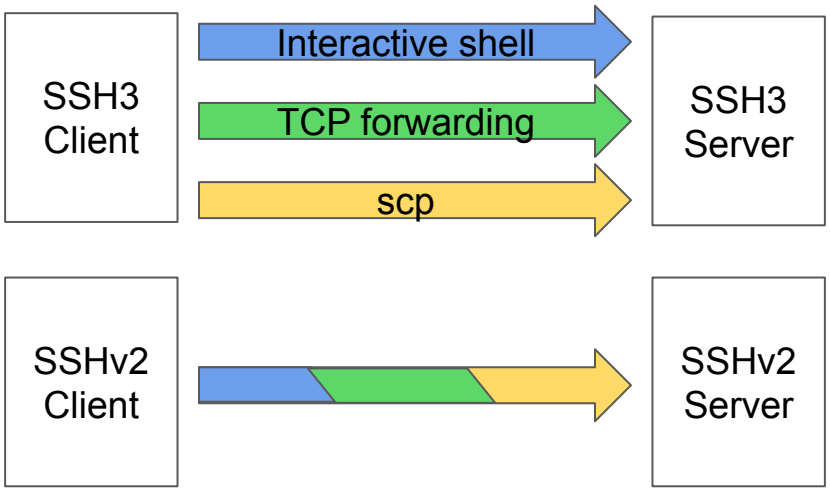


SSH3 conversation establishment



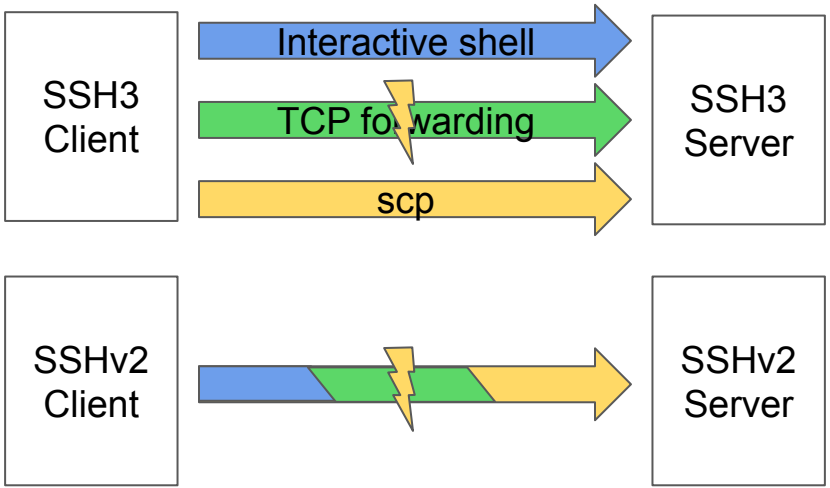
Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
  - Stream multiplexing



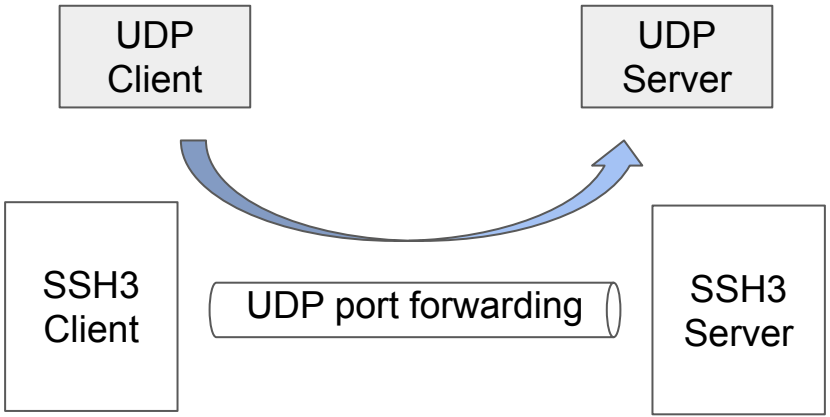
Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
  - Stream multiplexing



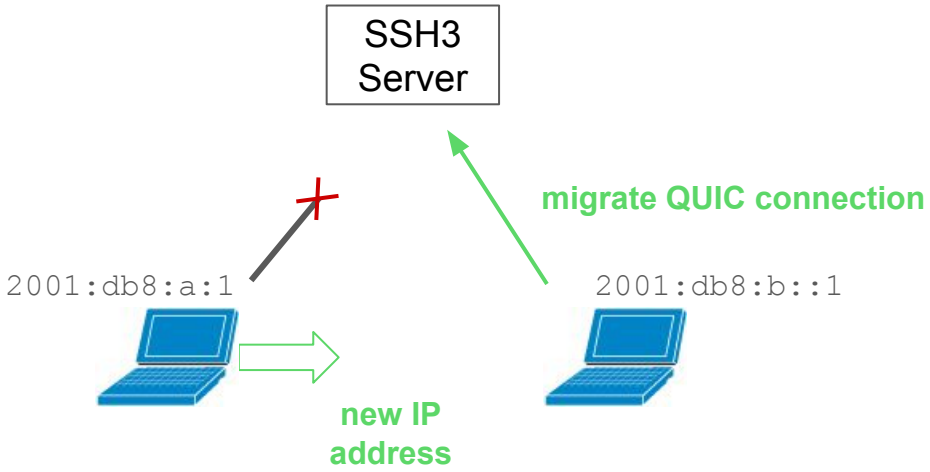
Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
  - Stream multiplexing
  - Datagrams



Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
  - Stream multiplexing
  - Datagrams
  - Connection migration

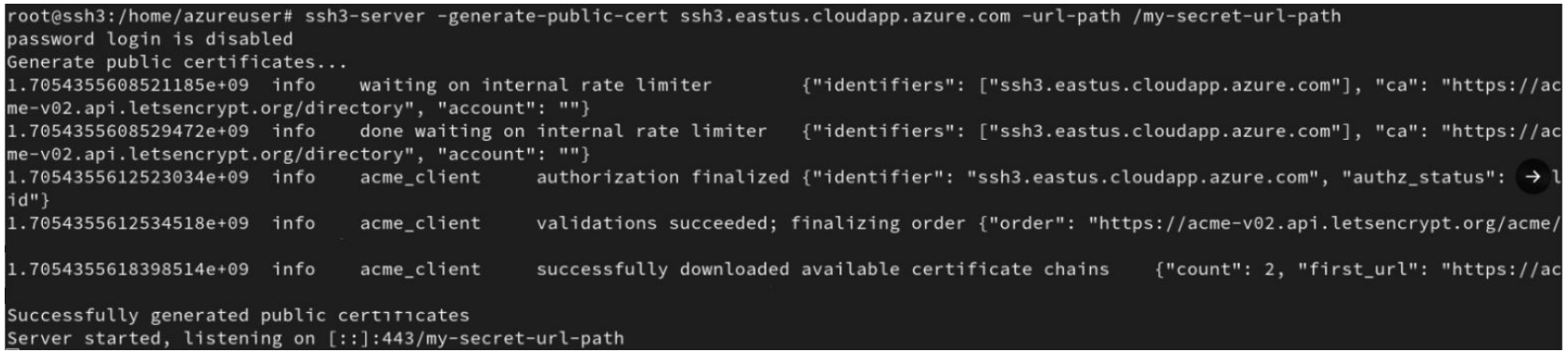


Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
- Encrypted/authenticated QUIC transport fields

Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
- Encrypted/authenticated QUIC transport fields
- Access to the X.509 ecosystem with low effort



Starting an SSH3 server for the 1st time and generating a public certificate for the domain name automatically

Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
- Encrypted/authenticated QUIC transport fields
- Access to the X.509 ecosystem with low effort
- URL multiplexing

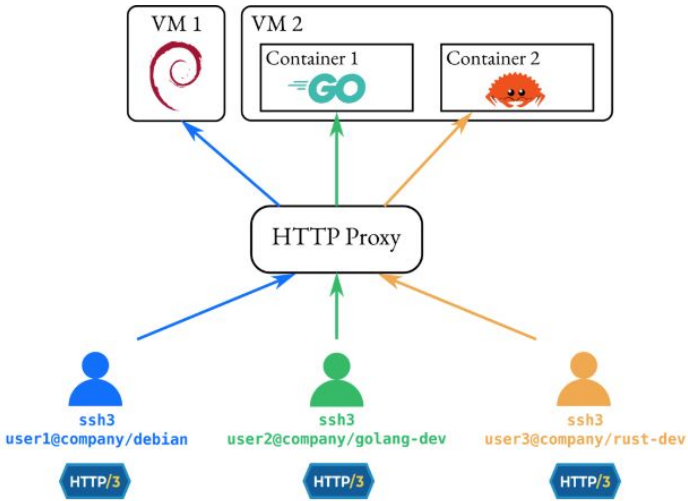
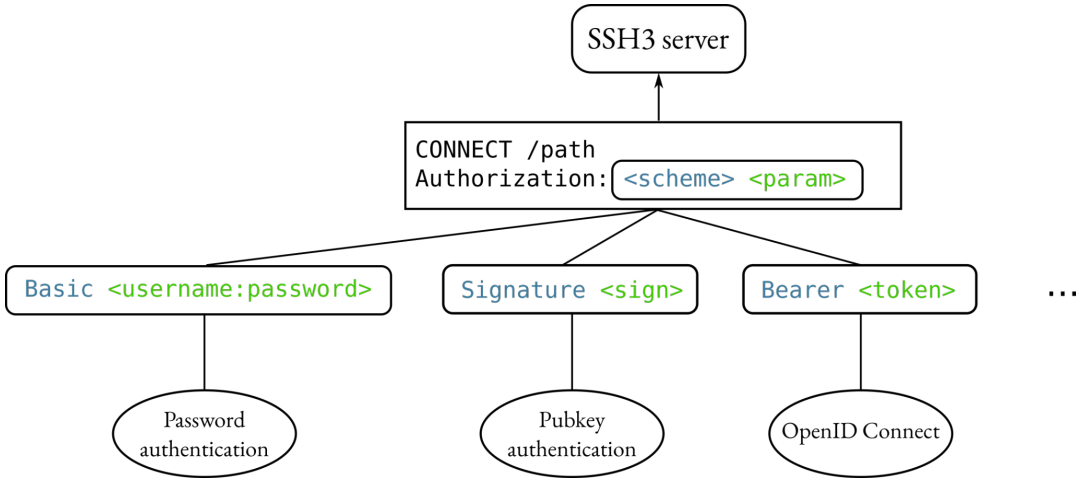


Figure 7 — Multiplexing SSH3 connections on a URL-basis using a classical HTTP/3 reverse proxy. Multiplexing can also be done based on the hostname and/or username.

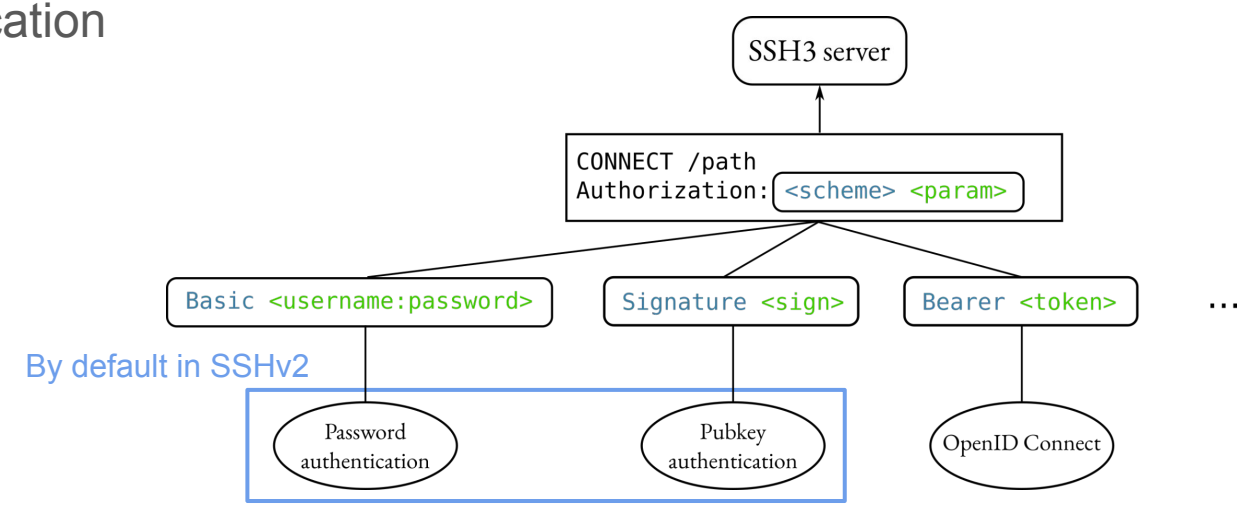
Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
- Encrypted/authenticated QUIC transport fields
- Access to the X.509 ecosystem with low effort
- URL multiplexing
- HTTP Authentication



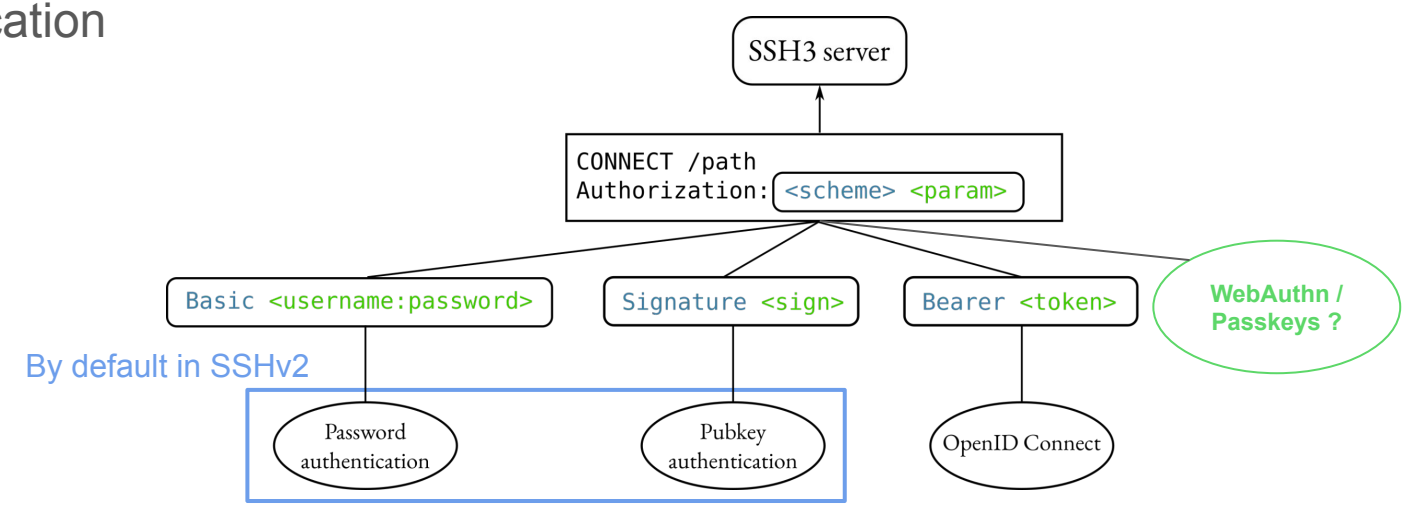
Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
- Encrypted/authenticated QUIC transport fields
- Access to the X.509 ecosystem with low effort
- URL multiplexing
- HTTP Authentication



Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
- Encrypted/authenticated QUIC transport fields
- Access to the X.509 ecosystem with low effort
- URL multiplexing
- HTTP Authentication



Opportunities: Interesting features of HTTP/3

- Accessing the QUIC API
- Encrypted/authenticated QUIC transport fields
- Access to the X.509 ecosystem with low effort
- URL multiplexing
- HTTP Authentication
- It fits well how the Internet is evolving

Threat: TCP-only networks

SSHv2 runs over TCP port 22 that is well supported on the Internet

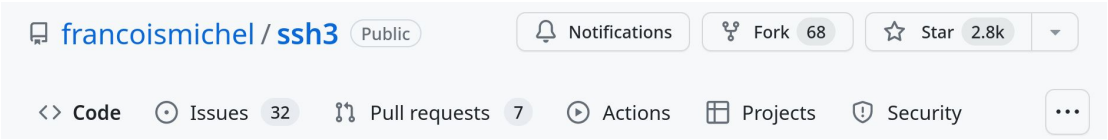
HTTP/3 currently runs over UDP port 443.

- It may be blocked by default in many networks.

Possible solutions:

- Run SSH over HTTP/2 as well
- QUIC on Streams ?
- Run SSH over WebTransport that supports both QUIC and TCP

What's next ?



Is it interesting ?

What would be the best outcome for this proposal ?

- An actual SSHv3 candidate ?
- Integrating SSH3 to MASQUE ? (e.g. `CONNECT-SHELL`, `CONNECT-PROCESS`)
- Other design ? (e.g. SSH over TLS, over QUIC, …)

Anyone interested to collaborate on the draft ?

Is it interesting enough to integrate an existing wg or start discussions on a list ?

Anyone wants to implement and interoperate ?

Current design:draft-michel-ssh3-00.
Implem on Github: https://github.com/francoismichel/ssh3

Additional slides

Compatibility with SSHv2

Shipping SSH3 in newly deployed VMs should be easy.

However, SSHv2 is ubiquitous and will probably be around for years to come

- Like HTTP/1.1 and HTTP/2 coexist with HTTP/3

“upgrade” mechanisms (SSHv2->SSH3) could be defined & cached, using e.g. SSHv2’s version string:

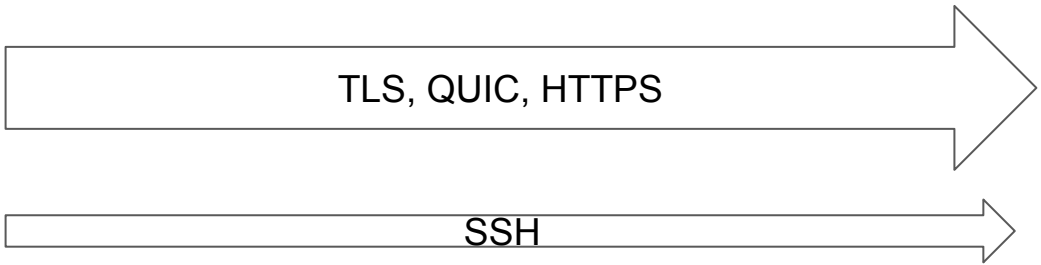
```
SSH-protoversion-softwareversion SP comments CR LF
```

Modern transports

Modern protocols developed after SSHv2 bring several benefits.

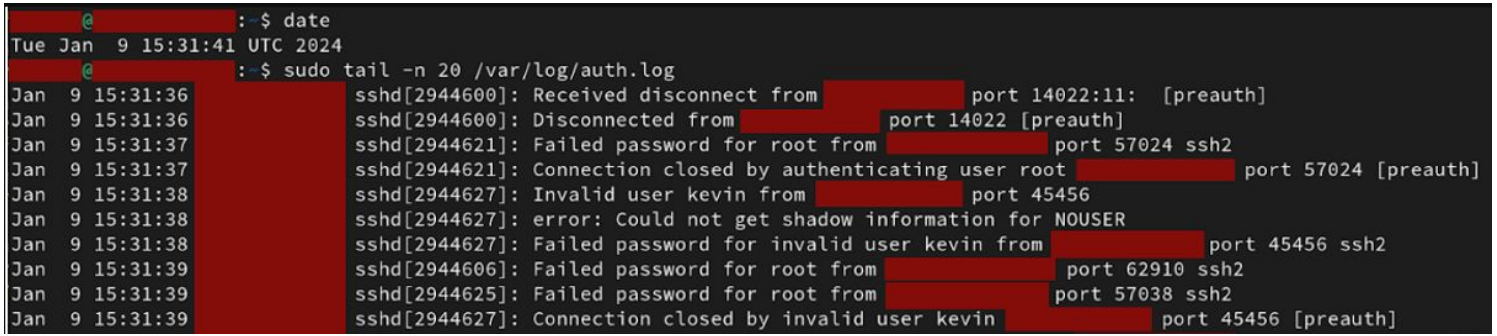
- TLS 1.3: reduced handshake, early data, SNI multiplexing, X.509
- QUIC: encrypted control information, streams multiplexing, datagrams, connection migration
- HTTP/3: URL multiplexing, authentication methods, Extended CONNECT

The IETF work of SSH is still done in parallel of TLS/QUIC/HTTPS.



Opportunities: Interesting features of HTTP/3

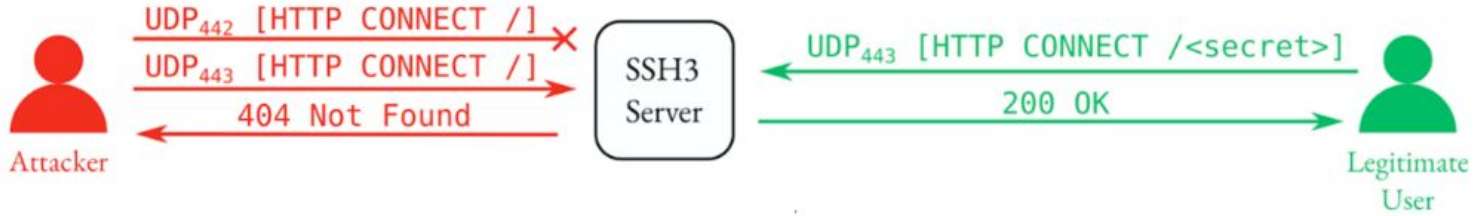
- Accessing the QUIC API
- Encrypted/authenticated QUIC transport fields
- Access to the X.509 ecosystem with low effort
- URL multiplexing
- Undiscoverability if demanded



Classical SSHv2 log output

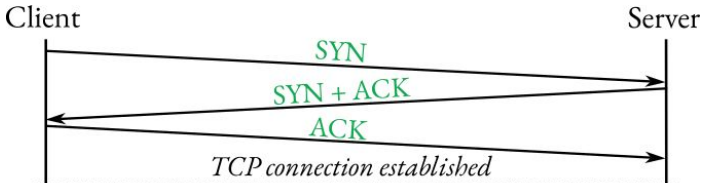
Opportunities: Interesting features of HTTP/3

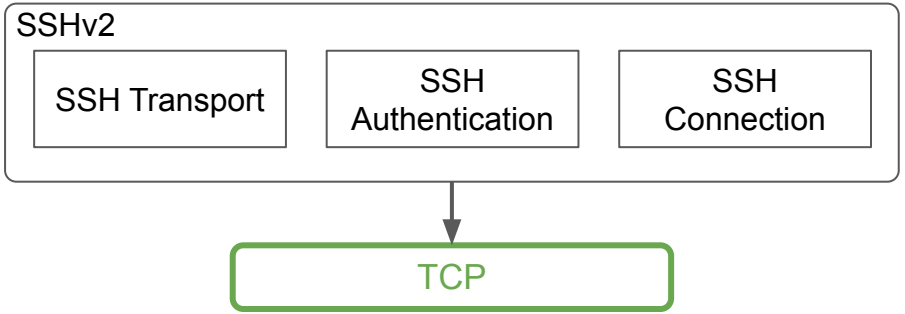
- Accessing the QUIC API
- Encrypted/authenticated QUIC transport fields
- Access to the X.509 ecosystem with low effort
- URL multiplexing
- Undiscoverability if demanded



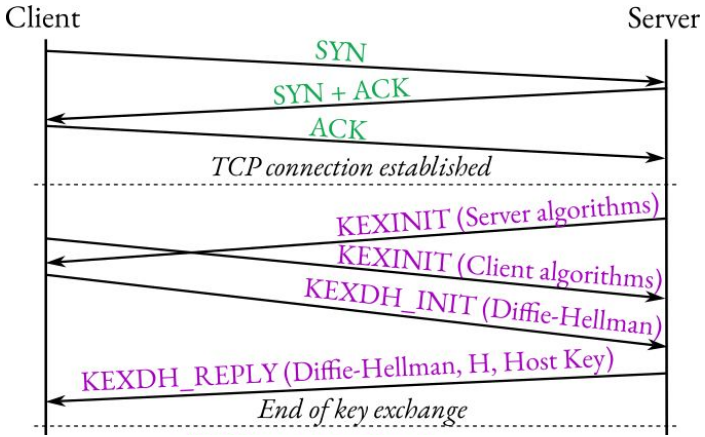
Hidden SSH3 endpoint: drop packet on wrong port, respond 404 on wrong request

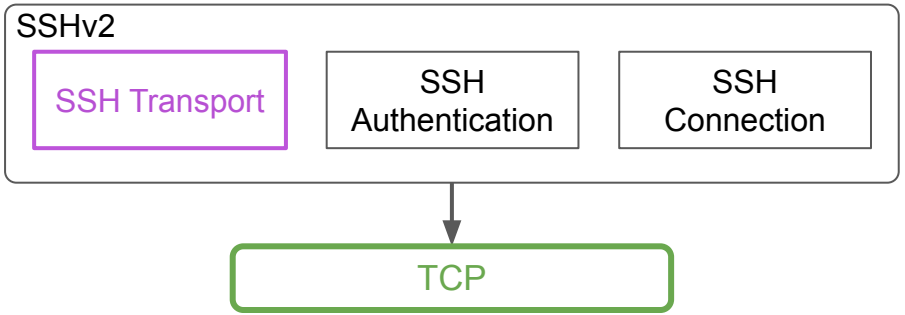
SSHv2 Connection establishment



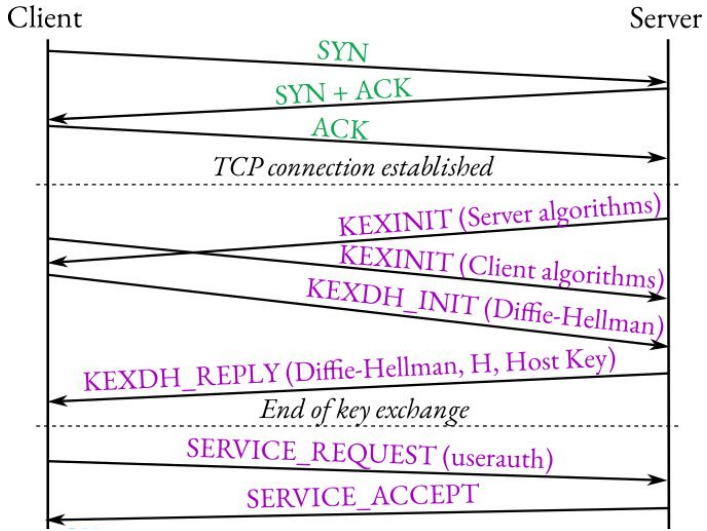


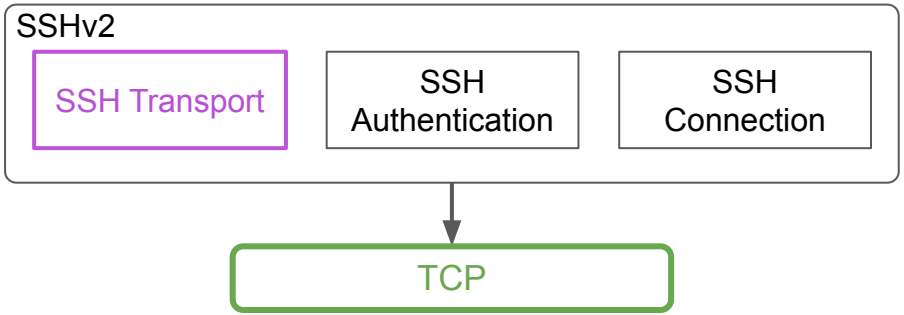
SSHv2 Connection establishment



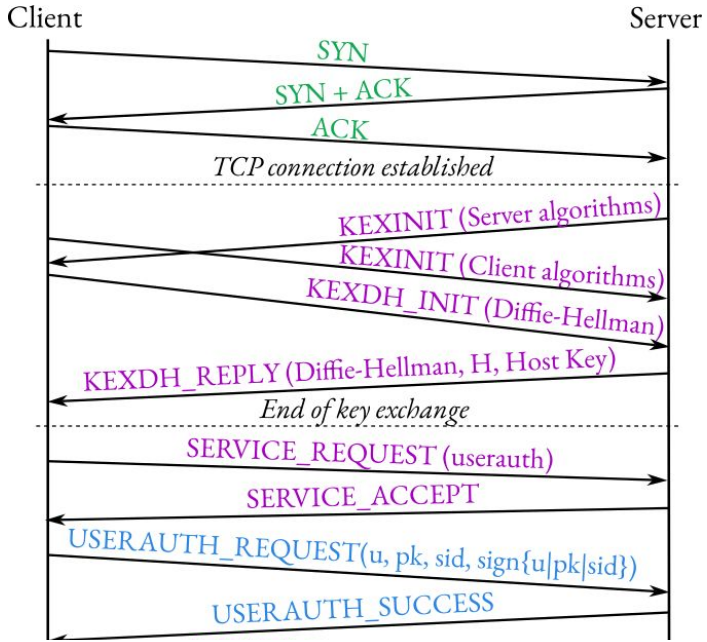


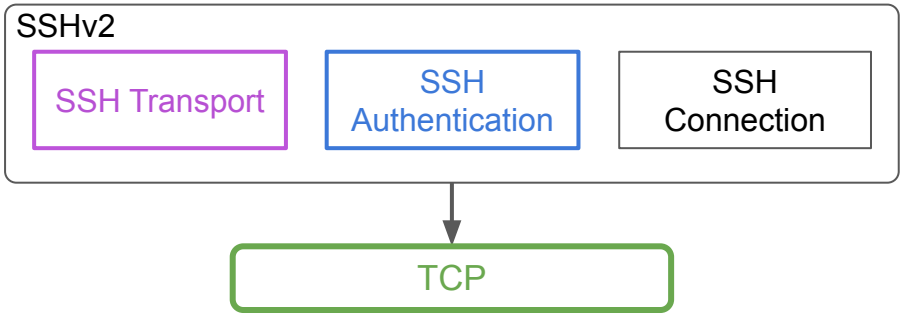
SSHv2 Connection establishment





SSHv2 Connection establishment





SSHv2 Connection establishment