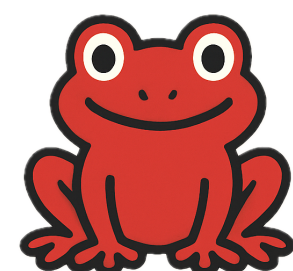


Hop A Modern Transport and Remote Access Protocol



Paul Flammariion

George Hosono

Wilson Nguyen

Laura Bauman

Daniel Rebelsky

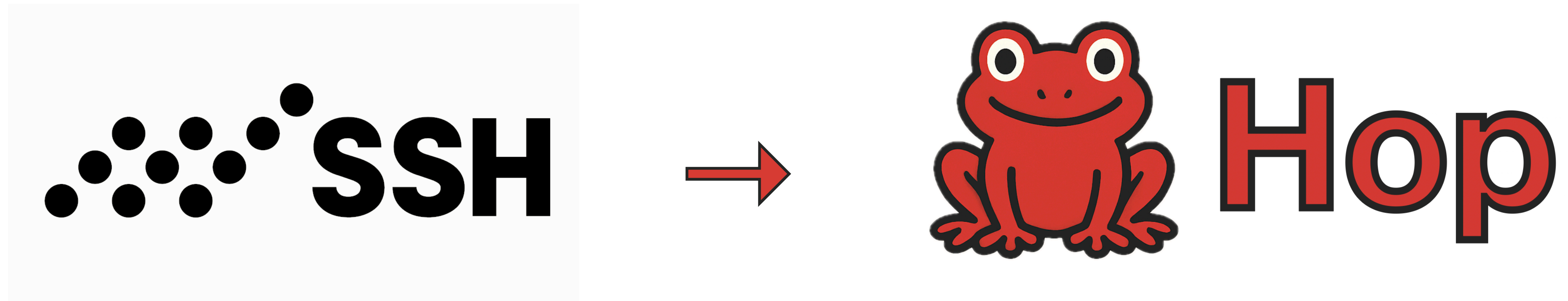
Gerry Wan

David Adrian

Zakir Durumeric



What is Hop?



Hop is a simpler and more secure alternative to SSH

Why SSH Struggles in Today's Environment

1. **Changing Wi-Fi?** → Staring at frozen terminals & losing work
2. **Server Privacy?** → Public IP instantly becomes a scanner magnet
3. **Bastion Access?** → Blindly running `ssh -A` socket hijacking
4. **Security Warnings?** → Blindly accept the host key fingerprint hash

What Happens If...?

- Existing tools **patch isolated symptoms** without fixing SSH's underlying architecture
- 30 years of incremental extensions (35 RFCs) have created **unsustainable protocol complexity** and expanded the attack surface

What happens if we have a clean-slate approach instead of just patching SSH?

How **Hop** Fixes SSH: 4 Key Focuses

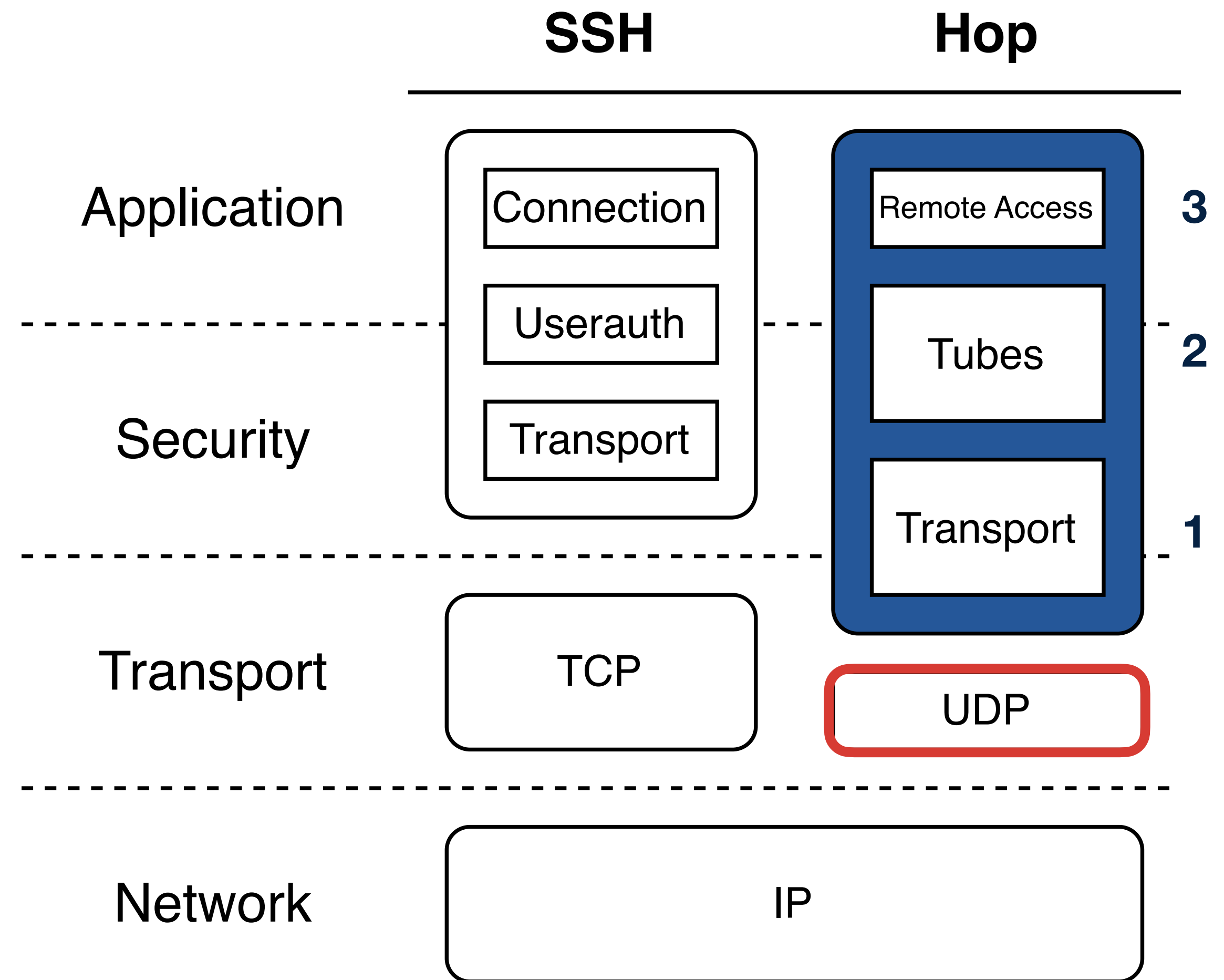
- 1. Changing Wi-Fi? → **UDP Based Protocol**
- 2. Server Privacy? → **Hop Protocol Handshake**
- 3. Bastion Access? → **Secure Delegation Scheme**
- 4. Security Warnings? → **Hop Identity Management**

Hop Inner Sub-Protocols over UDP

1.

Client roaming and intermittent connectivity

- *SSH operates* over TCP
- *Mosh switches* from TCP to UDP after Auth
- *Hop natively* runs over UDP



Hop Layered Architecture

SSH Handshake Shortcomings

2.

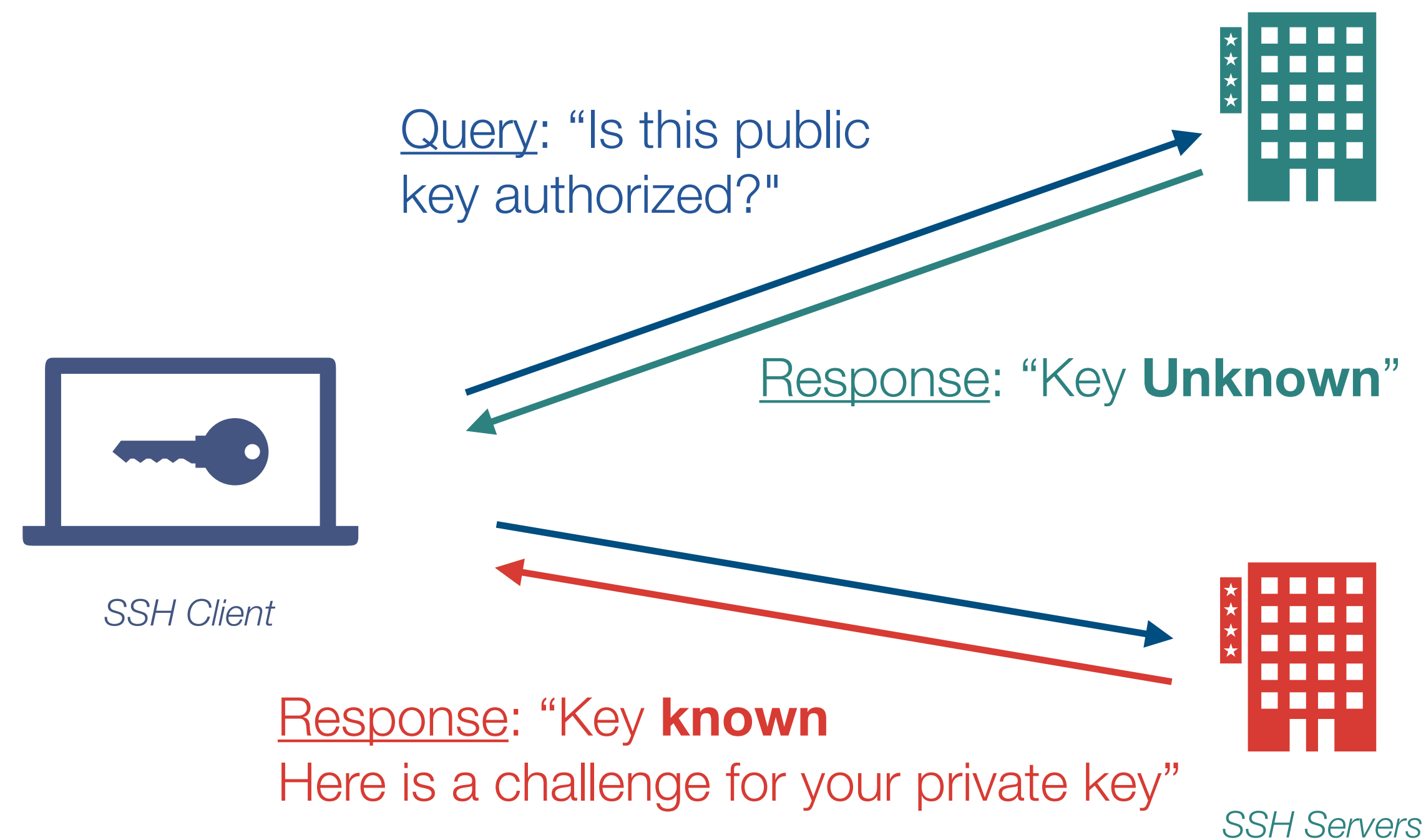
A. Transcript Tampering



Terrapin Attack

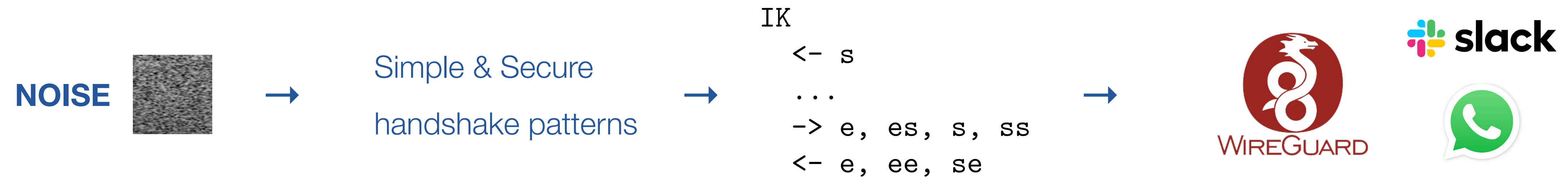
- No full transcript protection
- Protocol sequence manipulation
- **Silently downgrade security** guarantees

B. Public Key Probing Oracle

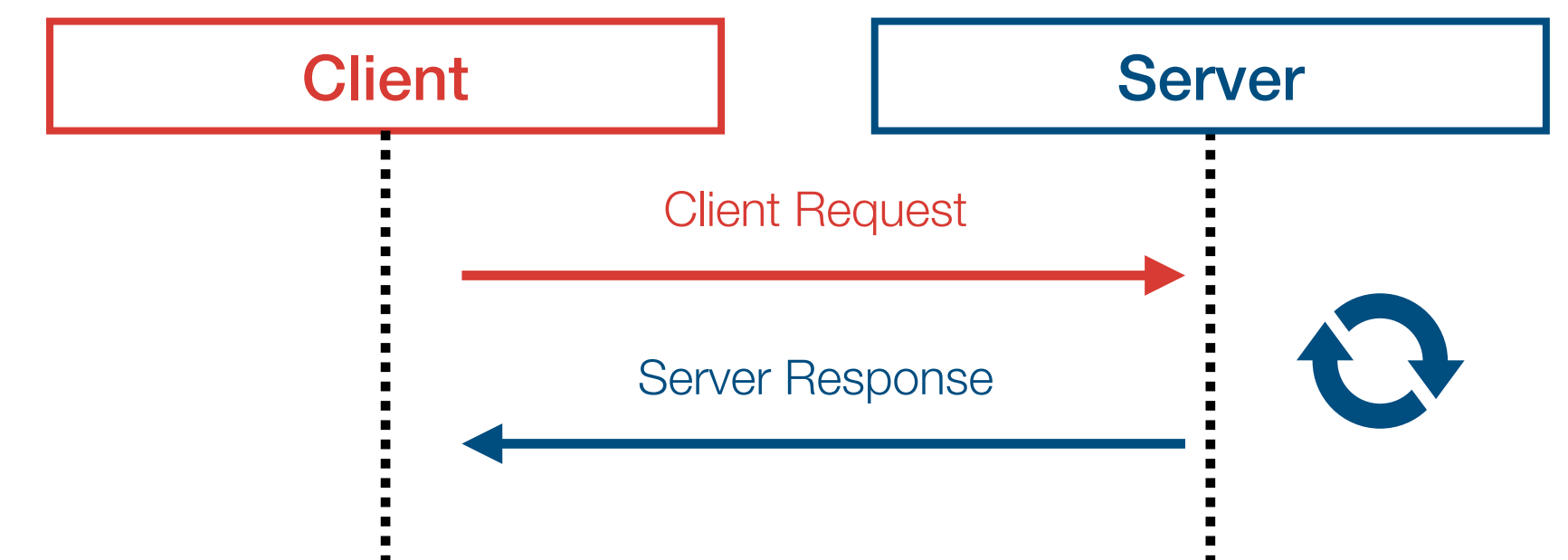


Hop Handshake for Simplicity and Security

2.



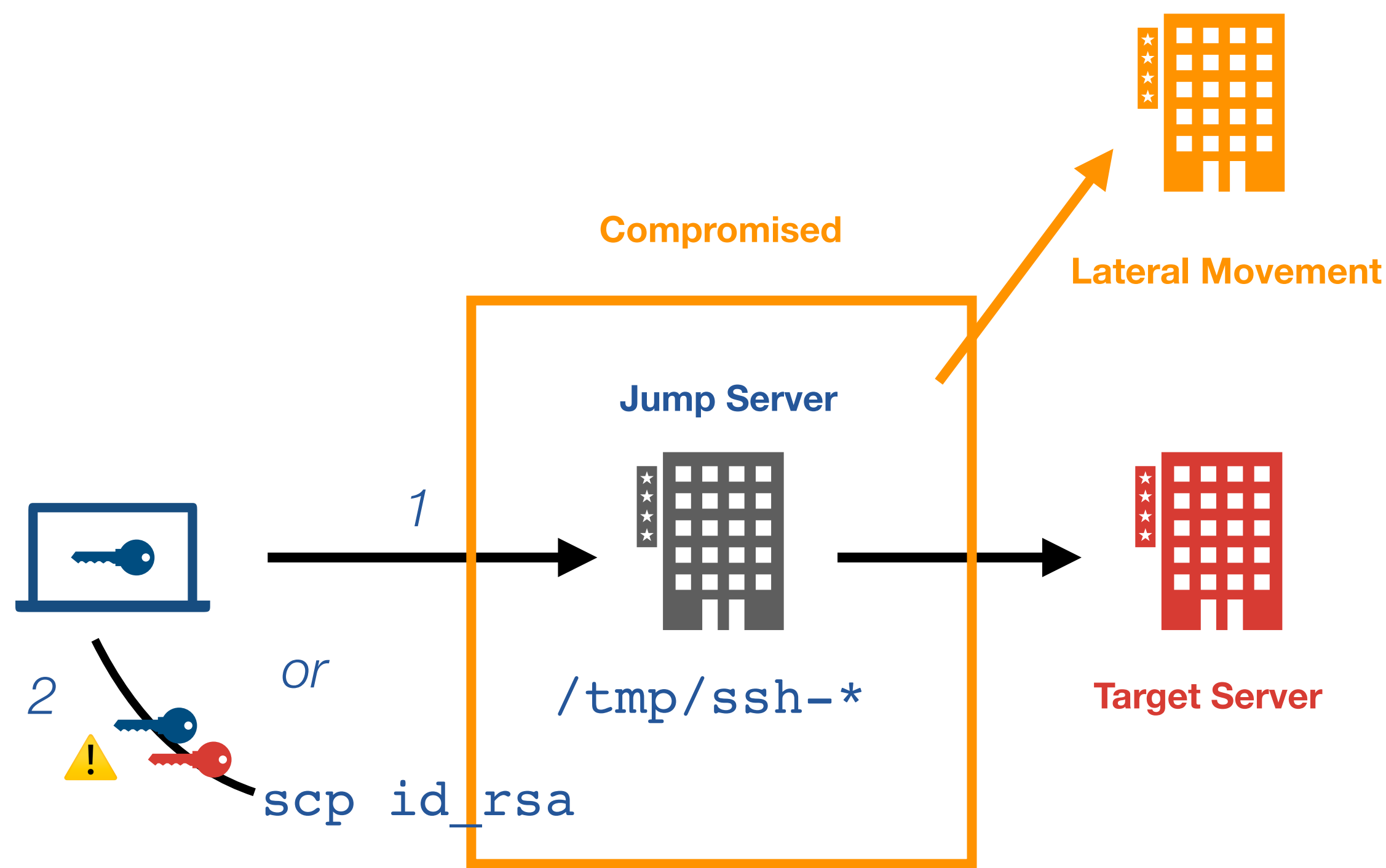
- Fixed cipher suites (**no downgrade**)
- Unauthenticated probes receive no response (**no scanner**)



Hop Hidden Mode - Noise IK pattern

SSH Delegation: Agent Hijack & Copy-Paste Keys

3.



The Case For Secure Delegation

Dmitry Kogan, Henri Stern, Ashley Tolbert, David Mazières, and Keith Winstein
Stanford University

Who, —
what, —
to whom, —
and when? —

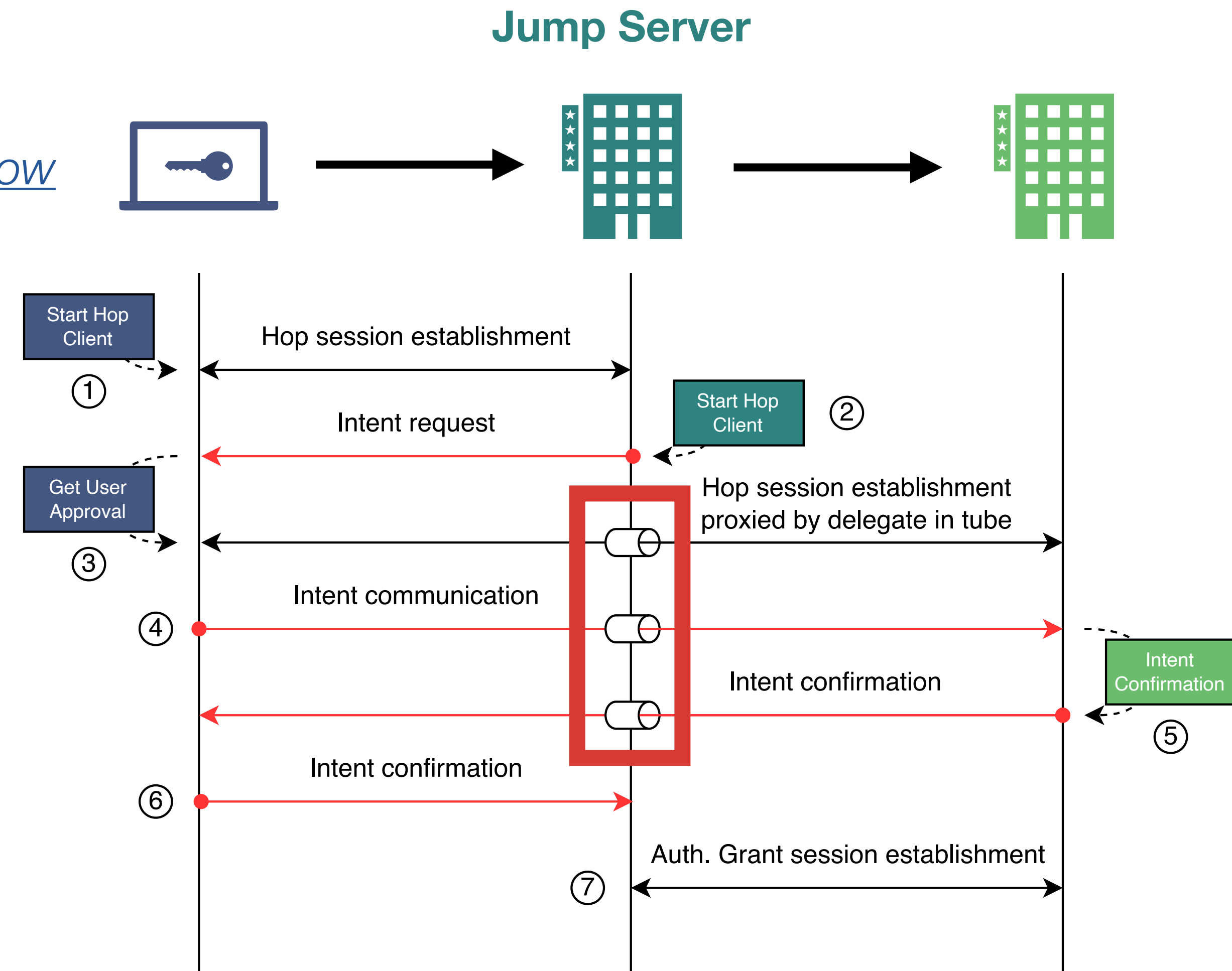
```
Would you like to
| allow bob.cloud.com
| to run the command 'sudo reboot'
| as alice
| on private.server.com
| from Wed Apr 9 16:03:28 EDT 2025
| until Wed Apr 9 16:04:28 EDT 2025?
```

Hop Enables Secure Delegation With AuthGrant

3.

- Binds authorization to User, Action, Target, and Time window
- Authentication materials **never leave** principal's device
- Jump servers operate as “**dumb pipes**”

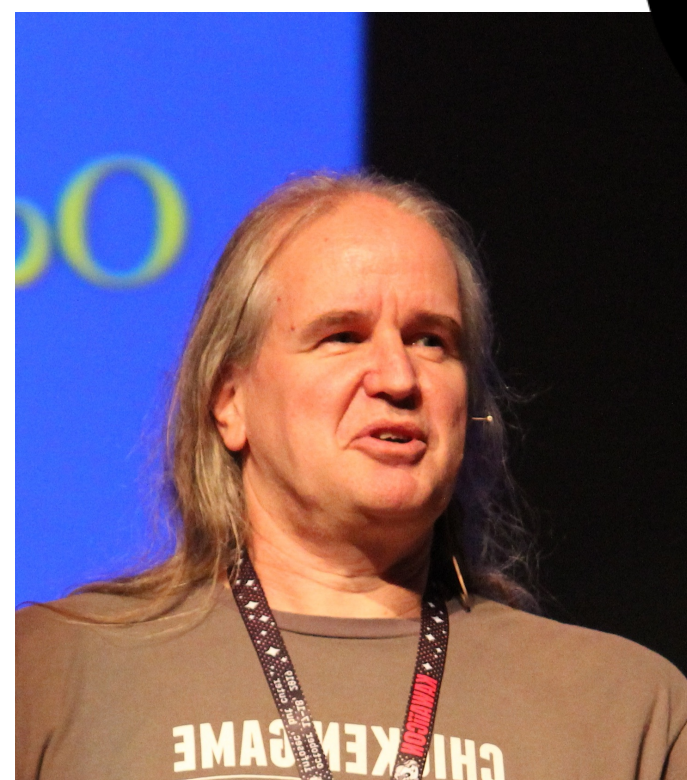
```
Would you like to
allow bob.cloud.com
to run the command 'sudo reboot'
as alice
on private.server.com
from Wed Apr 9 16:03:28 EDT 2025
until Wed Apr 9 16:04:28 EDT 2025?
Yes
> No
```



SSH (*not*) Trustworthy Host Identification

4.

ED25519 key fingerprint is: *SHA256:Jwal7UC2dCpcM64yGXeE4NgSNxCbXUAOctMPu4n4i1k*
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?



Peter Gutmann

"Do Users Verify
SSH Keys?"

"No..."



Tatu Ylönen

Hop Solves SSH Identities With Hop Certificates

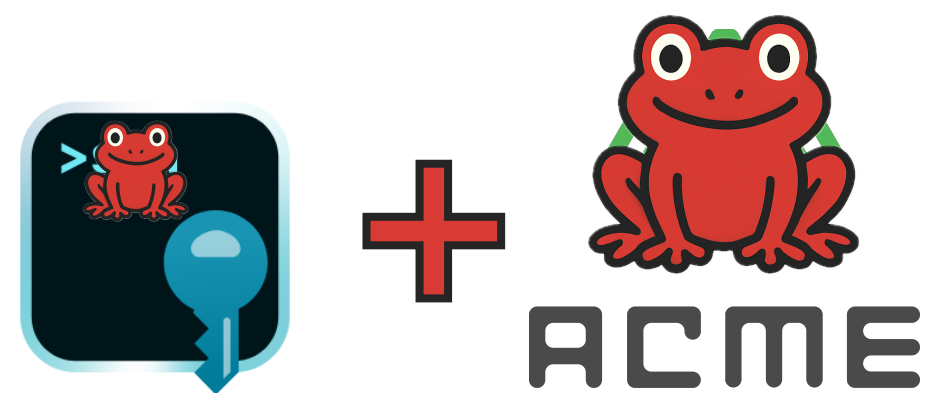
4.



- Unknown, underused, cumbersome to deploy
- Lack of automated issuance & no chain of trust



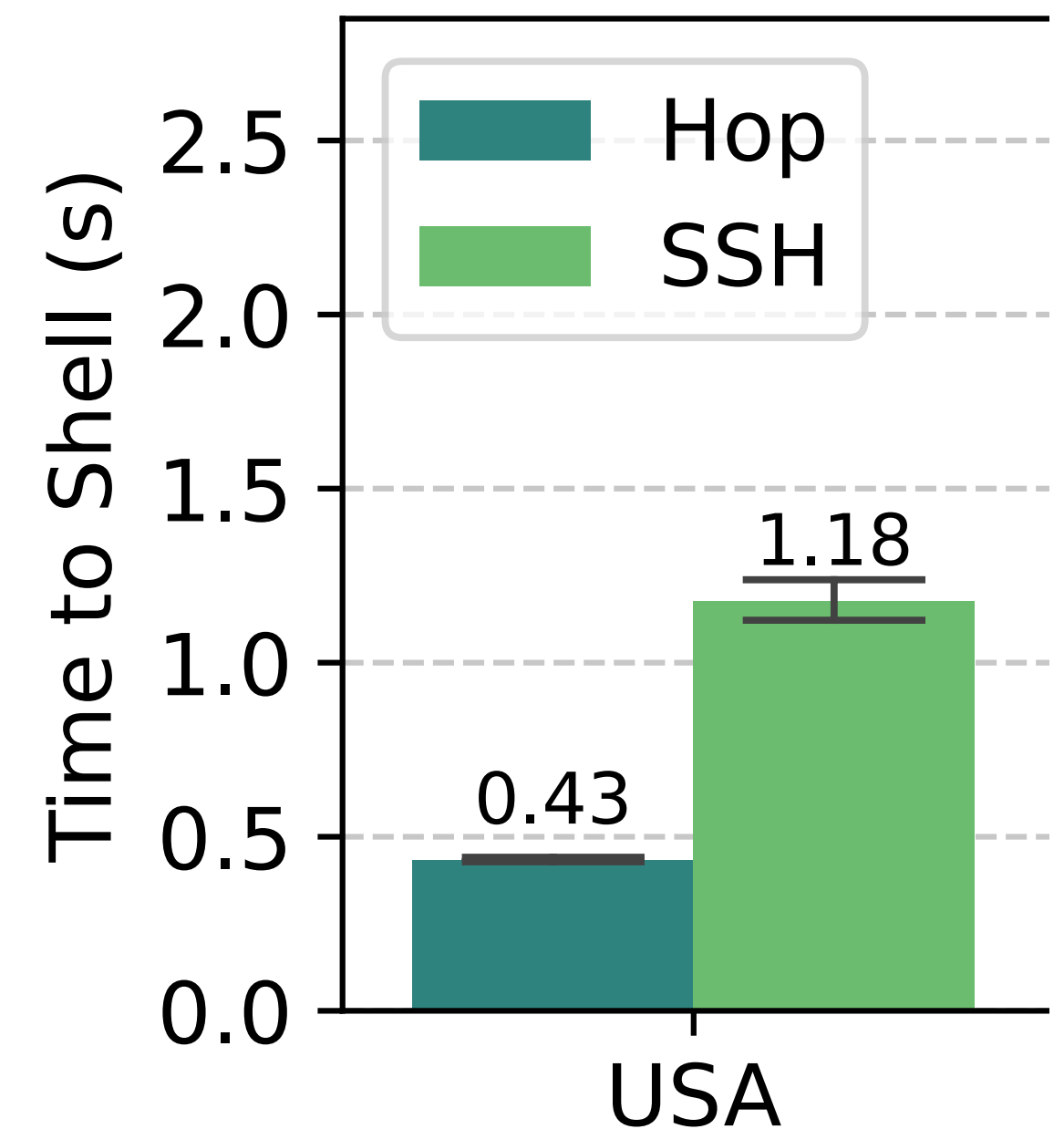
- Revolutionized Web PKI by **fully automating** server identity issuance
- Challenge: X.509/ASN.1 structures introduce **massive parsing complexity**



- Fixed-size, deterministic certificates
- *Host* - ACME protocol **directly over Hop** transport
- *Client* - Short-lived, time-bounded **client certificates**

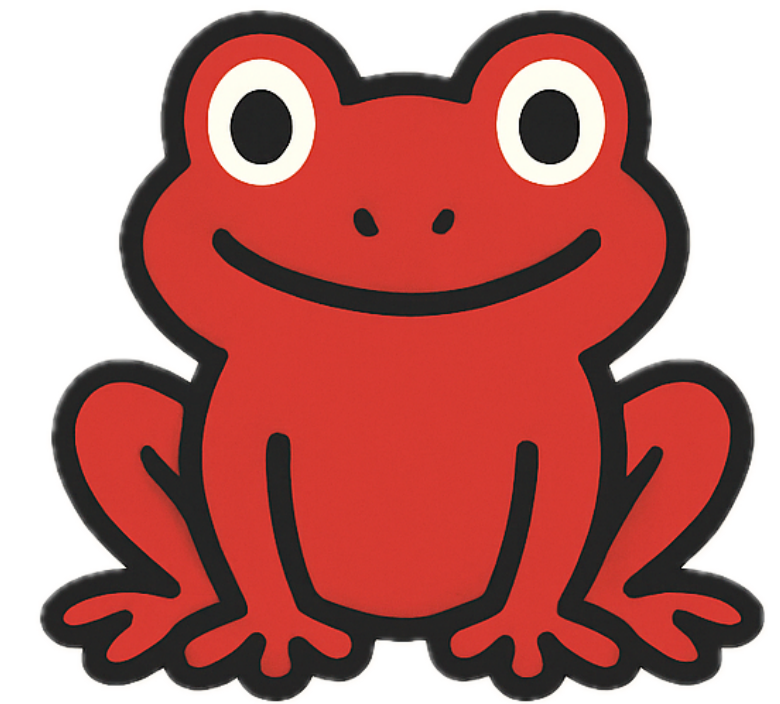
Hop in Practice

- We developed an **open-source reference implementation** of Hop in Go
- **Compact and easy-to-audit** codebase (~18k LoC)
- Feature **parity with SSH capabilities**:
 - Interactive remote login shell
 - Remote command execution
 - Local and remote port forwarding
- Performance on par with standard SSH, with **faster session establishment**



Hop A Modern Transport and Remote Access Protocol

- We **learned from real-world** modern Internet security standards
- We designed Hop, a three-layer protocol as a **secure SSH alternative**
- We **developed Hop**'s reference implementation available open-source



→ We hope that our work prompts conversation on the future of server remote access



github.com/hop-proto/hop-go

Paul Flammariion

paul.f@uci.edu