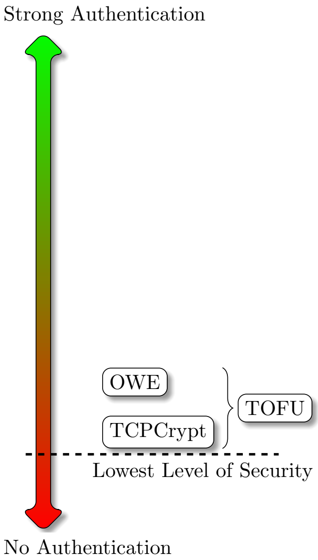
PILA: Pervasive Internet-Wide Low-Latency Authentication

Cyrill Krähenbühl Markus Legner Silvan Bitterli
Adrian Perrig
Department of Computer Science
ETH Zurich, Switzerland

1. July 2021

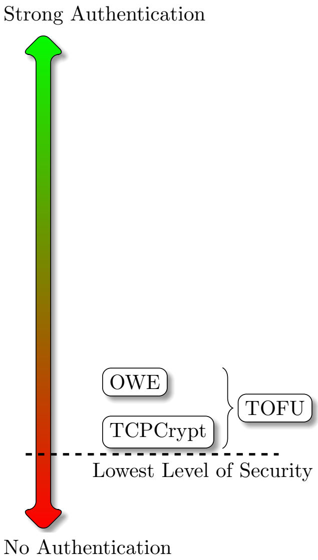
Motivation

- Trust on first use (TOFU):
  - every on-path entity can attack



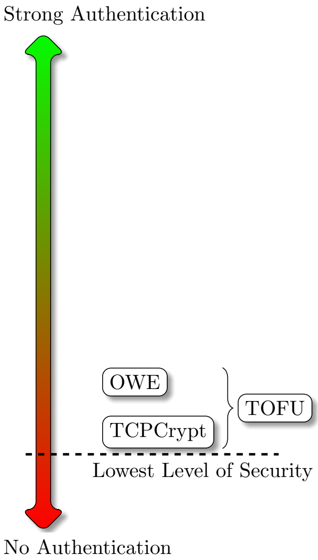
Motivation

- Trust on first use (TOFU):
  - every on-path entity can attack
  - cannot reliably detect attacks



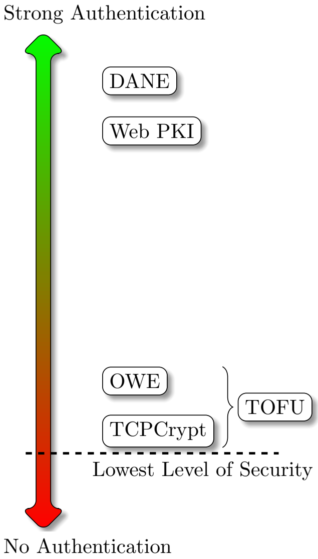
Motivation

- Trust on first use (TOFU):
  - every on-path entity can attack
  - cannot reliably detect attacks
  - cannot pinpoint attacker



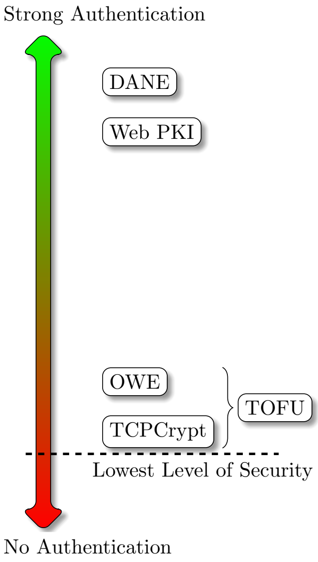
Motivation

- Trust on first use (TOFU):
  - every on-path entity can attack
  - cannot reliably detect attacks
  - cannot pinpoint attacker
- Strong Authentication:
  - based on PKI (Web PKI or DNSSEC)



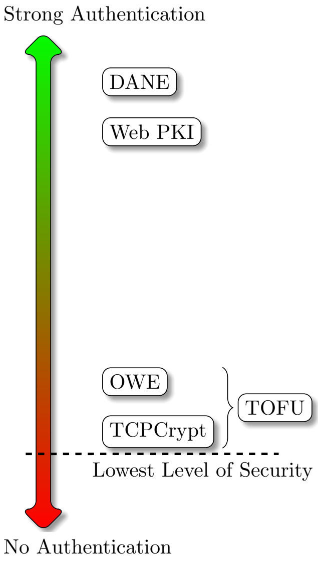
Motivation

- Trust on first use (TOFU):
  - every on-path entity can attack
  - cannot reliably detect attacks
  - cannot pinpoint attacker
- Strong Authentication:
  - based on PKI (Web PKI or DNSSEC)
  - name-based authentication



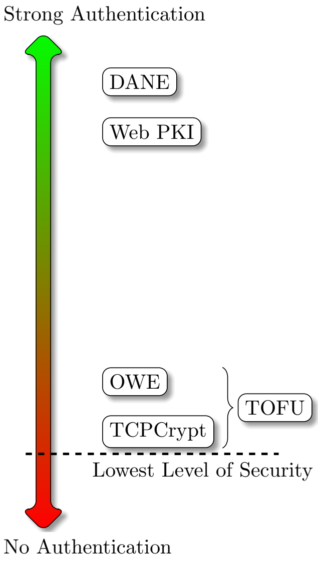
Motivation

- Trust on first use (TOFU):
  - every on-path entity can attack
  - cannot reliably detect attacks
  - cannot pinpoint attacker
- Strong Authentication:
  - based on PKI (Web PKI or DNSSEC)
  - name-based authentication
  - requires configuration



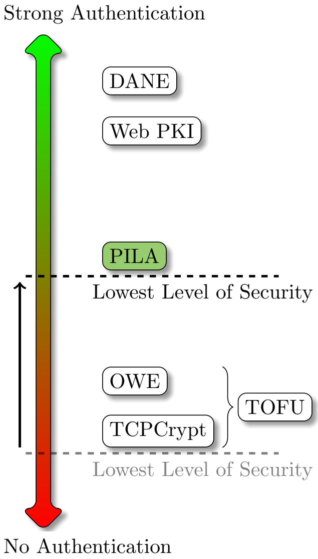
Motivation

- Trust on first use (TOFU):
  - every on-path entity can attack
  - cannot reliably detect attacks
  - cannot pinpoint attacker
- Strong Authentication:
  - based on PKI (Web PKI or DNSSEC)
  - name-based authentication
  - requires configuration
- Can we fill the gap between TOFU and strong authentication?



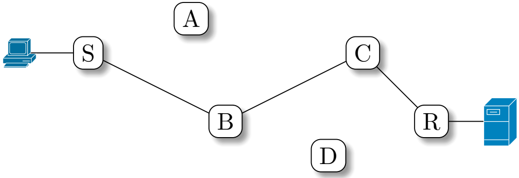
Motivation

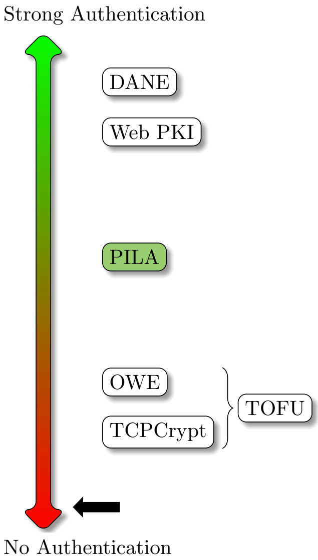
- Trust on first use (TOFU):
  - every on-path entity can attack
  - cannot reliably detect attacks
  - cannot pinpoint attacker
- Strong Authentication:
  - based on PKI (Web PKI or DNSSEC)
  - name-based authentication
  - requires configuration
- Can we fill the gap between TOFU and strong authentication?
  - PILA **improves** the base layer for encryption on the Internet



Trust Amplification

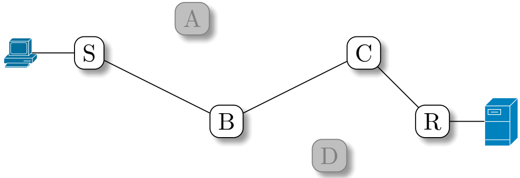
- No Authentication

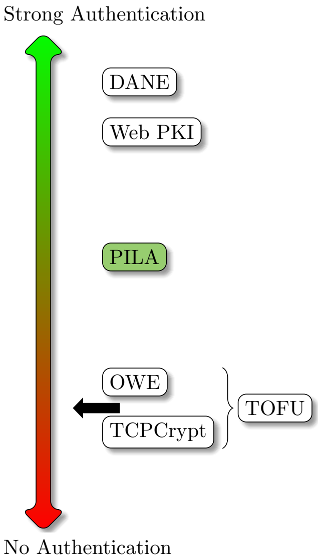




Trust Amplification

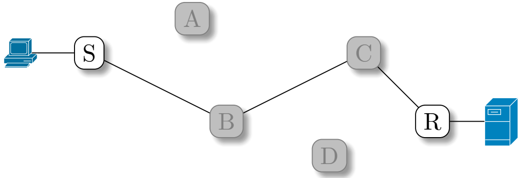
- No Authentication
- Trust on first use

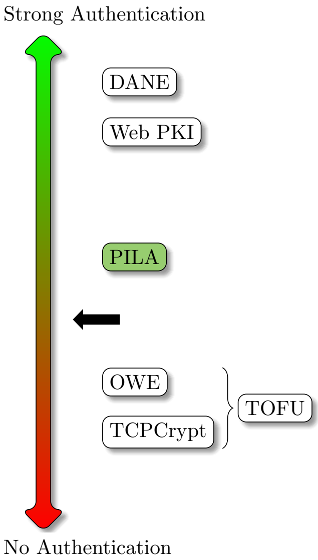




Trust Amplification

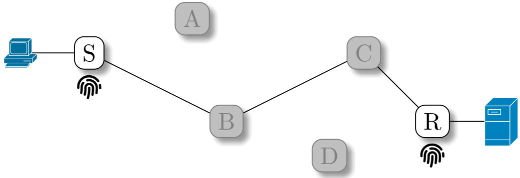
- No Authentication
- Trust on first use
- Trust Amplification
  - Crude Authentication

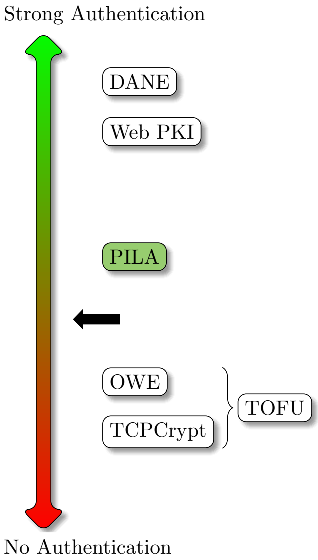




Trust Amplification

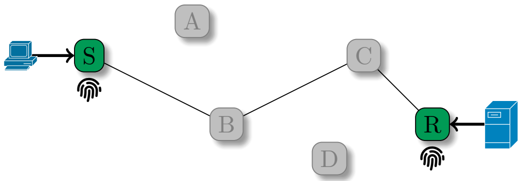
- No Authentication
- Trust on first use
- Trust Amplification
  - Crude Authentication
  - Accountability

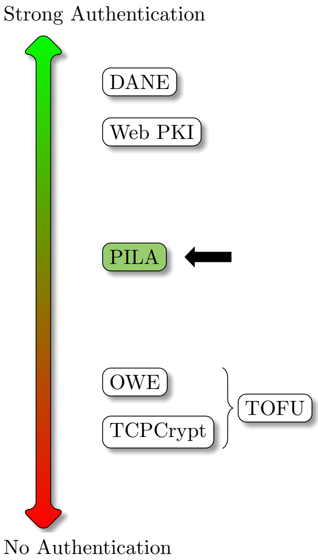




Trust Amplification

- No Authentication
- Trust on first use
- Trust Amplification
    - Crude Authentication
    - Accountability
    - Leverage





Goals

Authentication should ...

- be widely applicable

Goals

Authentication should ...

- be widely applicable
- be low-latency

Goals

Authentication should ...

- be widely applicable
- be low-latency
- require no user interaction

Goals

We propose *PILA*:
Pervasive Internet-Wide Low-Latency Authentication

Authentication should ...

- be widely applicable
- be low-latency
- require no user interaction

Goals

We propose *PILA*:
Pervasive Internet-Wide Low-Latency Authentication

PILA ...

- uses IP-address–based authentication

Authentication should ...

- be widely applicable
- be low-latency
- require no user interaction

Goals

We propose *PILA*:
Pervasive Internet-Wide Low-Latency Authentication

PILA …

- uses IP-address–based authentication
- has a minimal latency overhead

Authentication should …

- be widely applicable
- be low-latency
- require no user interaction

Goals

We propose *PILA*:
Pervasive Internet-Wide Low-Latency Authentication

PILA ...

- uses IP-address–based authentication
- has a minimal latency overhead
- automatically generates and fetches certificates

Authentication should ...

- be widely applicable
- be low-latency
- require no user interaction

Goals

We propose *PILA*:
Pervasive Internet-Wide Low-Latency Authentication

PILA ...

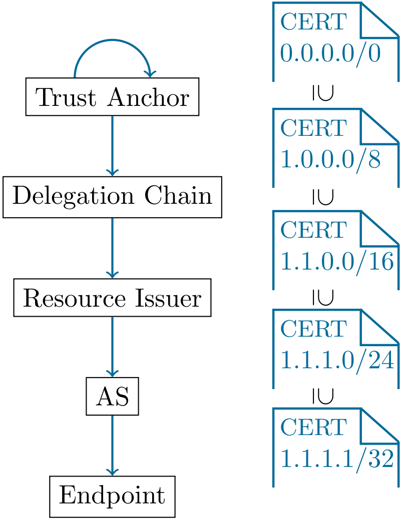
- uses IP-address–based authentication
- has a minimal latency overhead
- automatically generates and fetches certificates
- increases security of TOFU key establishment (only used if strong authentication protocols are not available)

Authentication should ...

- be widely applicable
- be low-latency
- require no user interaction

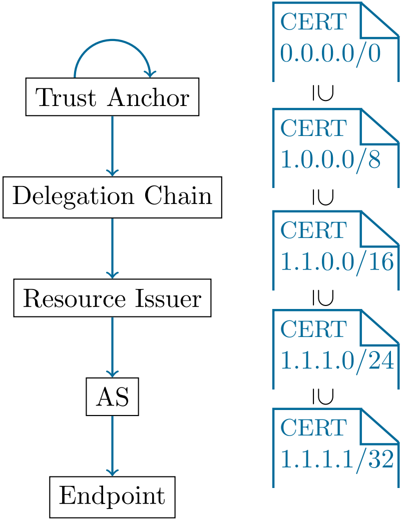
RPKI as Trust Root

- IANA/RIRs as trust anchor



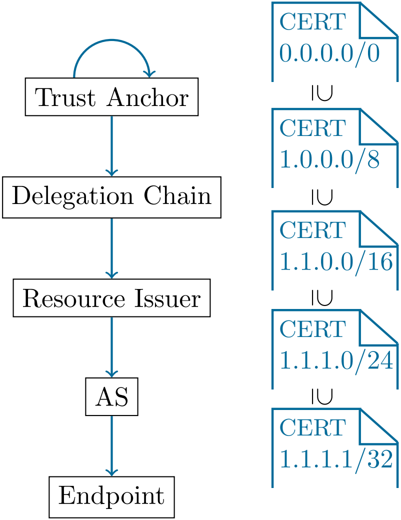
RPKI as Trust Root

- IANA/RIRs as trust anchor
- AS issues short-lived certificates for an IP address to endpoints



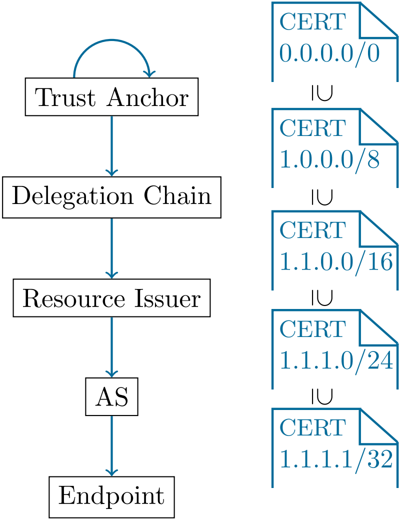
RPKI as Trust Root

- IANA/RIRs as trust anchor
- AS issues short-lived certificates for an IP address to endpoints
- AS misbehavior (i.e., equivocation) is detectable and cryptographically provable



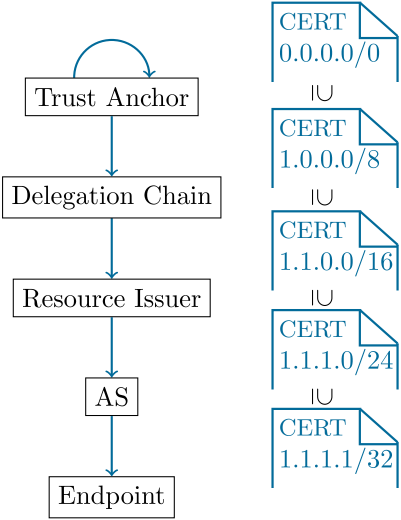
RPKI as Trust Root

- IANA/RIRs as trust anchor
- AS issues short-lived certificates for an IP address to endpoints
- AS misbehavior (i.e., equivocation) is detectable and cryptographically provable
- ASes are curious but cautious



RPKI as Trust Root

- IANA/RIRs as trust anchor
- AS issues short-lived certificates for an IP address to endpoints
- AS misbehavior (i.e., equivocation) is detectable and cryptographically provable
- ASes are curious but cautious
- Flexible PKI choice (e.g., control-plane PKI in SCION)

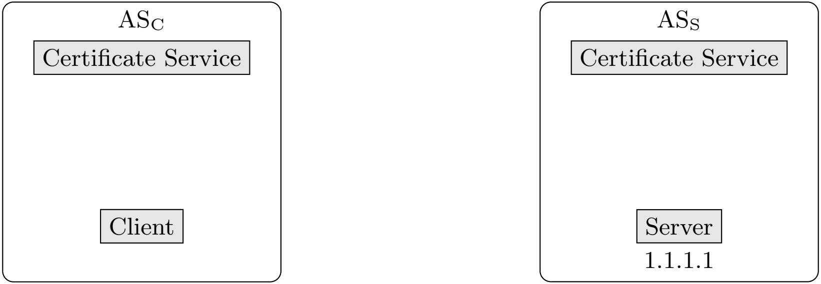


Use Cases

- Remote Login (SSH)
- Secure Session-Establishment (TLS)
- Query-Response (DNS)

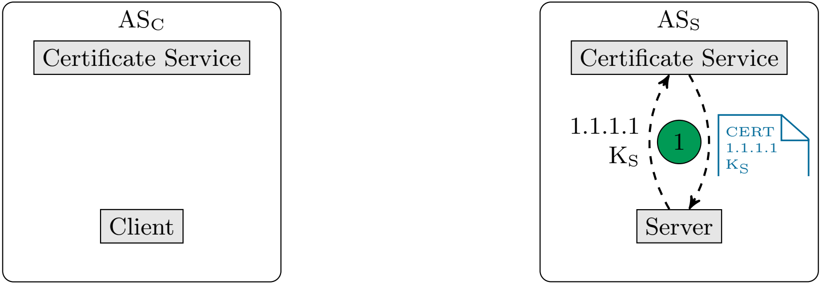
SSH PILA

Server at **1.1.1.1** wants to authenticate itself to the client



SSH PILA

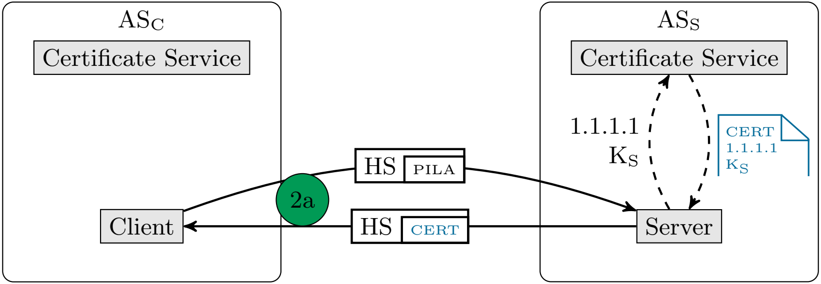
Server periodically fetches short-lived certificate from its local certificate service



SSH PILA

In parallel:

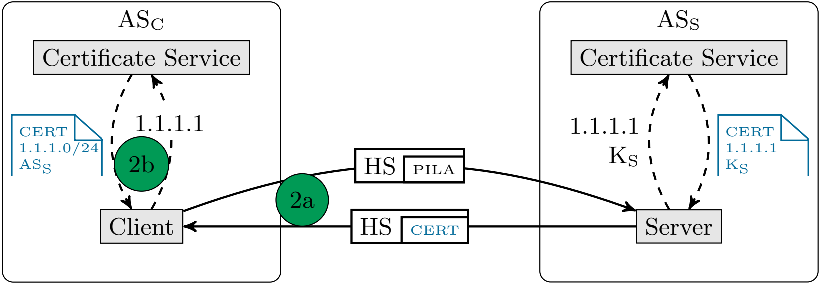
- SSH_{PILA} Handshake (reply contains the certificate)



SSH PILA

In parallel:

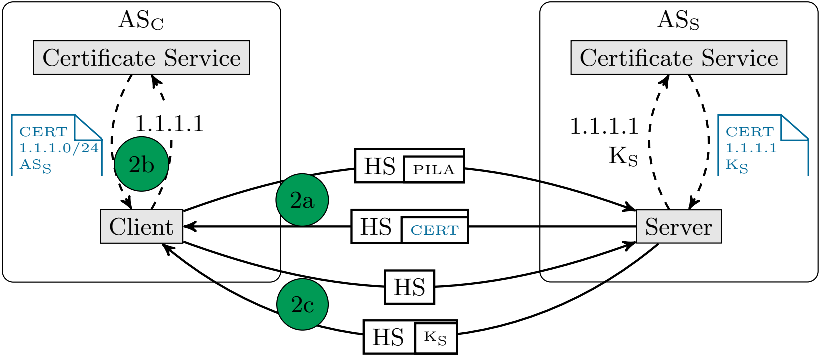
- SSH_{PILA} Handshake (reply contains the certificate)
- Client fetches AS certificate for 1.1.1.1



SSH PILA

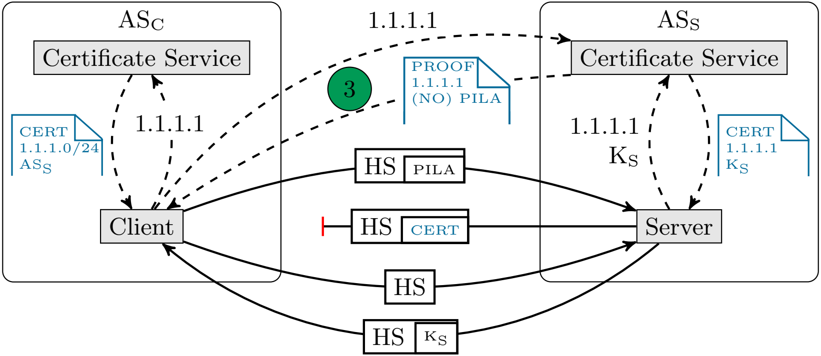
In parallel:

- SSH_{PILA} Handshake (reply contains the certificate)
- Client fetches AS certificate for 1.1.1.1
- Regular SSH Handshake (reply contains the public key)



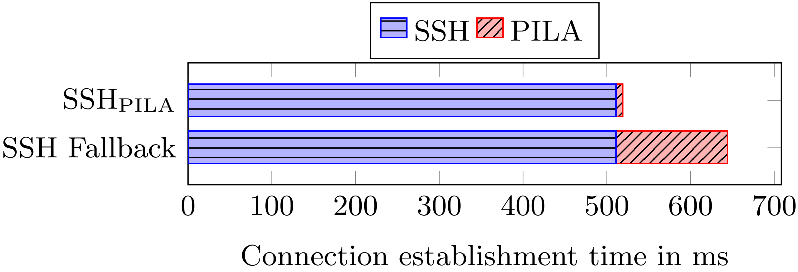
SSH PILA

If the SSH_{PILA} handshake fails, the client requests a proof that the server does not support PILA



SSH PILA

Latency Overhead



SSH PILA

Processing Delay

Average processing times of SSH_{PILA} operations in ms at the client, server, and certificate service:

	Client	Server	Certificate Service
Handshake Overhead	0.8	0.1	-
`GetEPCert`	-	1.0	17.0
`GetASCert`	4.3	-	8.3
`GetProof`	0.6	-	5.1

Conclusion

- Increase security through trust amplification
- PILA offers a new minimum level for fully automatic low latency key establishment
- Implementation and evaluation of PILA in combination with SSH, TLS, and DNS

Thank you!

Cyrill Krähenbühl
Network Security Group
Department of Computer Science
ETH Zürich

cyrill.kraehenbuehl@inf.ethz.ch