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

---

**Diagram:**

- Strong Authentication
- No Authentication
- TCPCrypt
- OWE
- TOFU
- Lowest Level of Security
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)

Strong Authentication

Web PKI
DANE

TCPCrypt
OWE

TOFU

Lowest Level of Security

No 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

Strong Authentication

No Authentication

TCPCrypt

OWE

Web PKI

DANE

TOFU

Lowest Level of Security

No 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?

Diagram:
- Strong Authentication
  - DANE
  - Web PKI
- No Authentication
  - OWE
  - TCPCrypt
  - TOFU
- Lowest Level of Security
- Motivation
  - Trust Amplification
  - PILA
  - Use Cases
  - Conclusion
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

Strong Authentication
- DANE
- Web PKI
- PILA
- OWE
- TCPCrypt

No Authentication
- TOFU
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 ... Authentication should ...
- uses IP-address–based authentication
- be widely applicable
- be low-latency
- require no user interaction
Goals

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

PILA ... Authentication should ...

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

**Trust Amplification**

**PILA**

**Use Cases**

**Conclusion**

---

**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

---

![Diagram](image-url)
**Motivation**

**Trust Amplification**

**PILA**

**Use Cases**

**Conclusion**

### 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
In parallel:
- SSH\textsubscript{PILA} Handshake (reply contains the certificate)
SSH PILA

In parallel:

- $\text{SSH}_{\text{PILA}}$ Handshake (reply contains the certificate)
- Client fetches AS certificate for 1.1.1.1
SSH PILA

In parallel:

- SSH\textsubscript{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\textsubscript{PILA} handshake fails, the client requests a proof that the server does not support PILA
SSH PILA
Latency Overhead

SSH PILA
SSH Fallback

Connection establishment time in ms

SSH PILA
SSH Fallback

PILA
Krähenbühl et al.

35
SSH PILA

Processing Delay

Average processing times of $\text{SSH}_{\text{PILA}}$ operations in ms at the client, server, and certificate service:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Client (ms)</th>
<th>Server (ms)</th>
<th>Certificate Service (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handshake Overhead</td>
<td>0.8</td>
<td>0.1</td>
<td>-</td>
</tr>
<tr>
<td>GetEPCert</td>
<td>-</td>
<td>1.0</td>
<td>17.0</td>
</tr>
<tr>
<td>GetASCert</td>
<td>4.3</td>
<td>-</td>
<td>8.3</td>
</tr>
<tr>
<td>GetProof</td>
<td>0.6</td>
<td>-</td>
<td>5.1</td>
</tr>
</tbody>
</table>
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