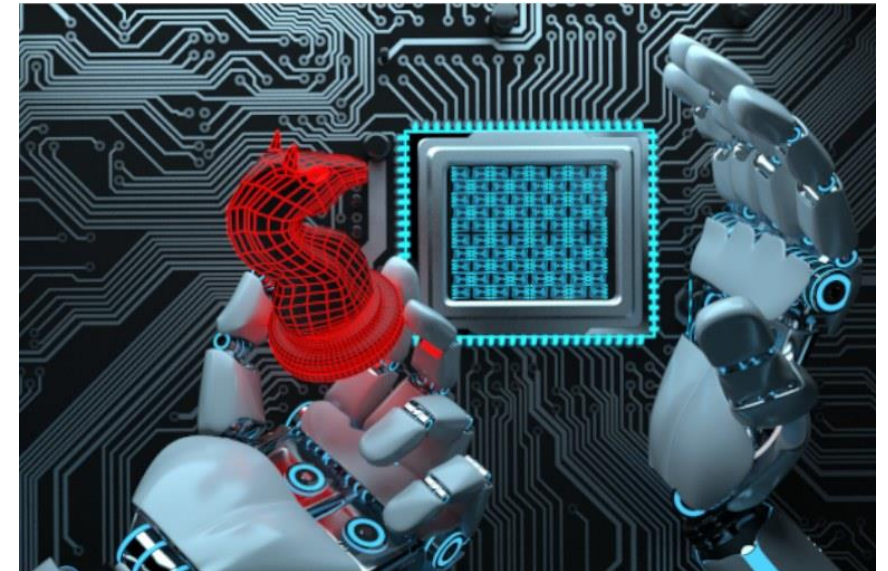


MASCHINELLES LERNEN FÜR DIE AUTOMATISCHE SEITENKANALANALYSE

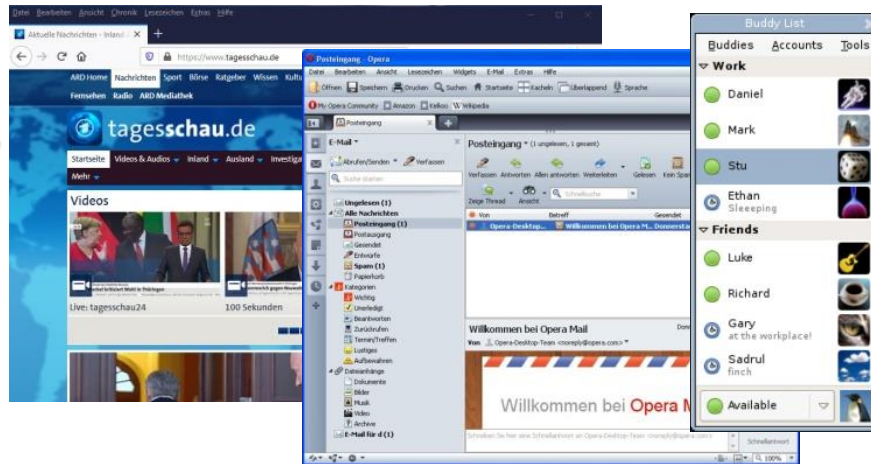
Dr. Claudia Priesterjahn
achelos GmbH



VERBUNDPROJEKT „AUTOMATISCHE SCHWACHSTELLENANALYSE VON KRYPTOGRAPHISCHEN PROTOKOLLEN“ (AUTOSCA)

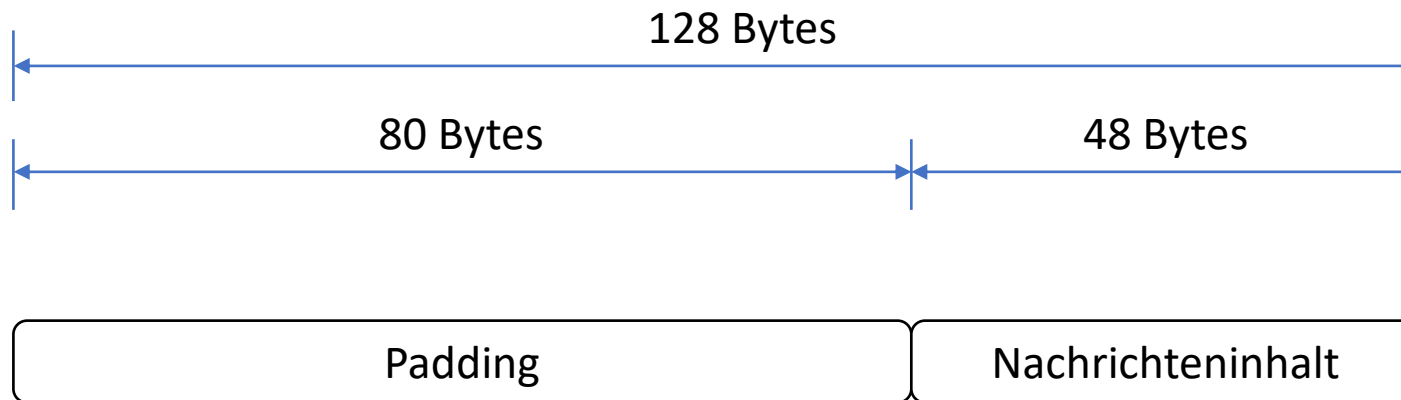
Sichere Netzwerkkommunikation aus dem Alltag

TLS – Transport Layer Security



- Ständig neue Schwachstellen und Seitenkanäle
- Jede Änderung an der Implementierung kann neue Seitenkanäle öffnen

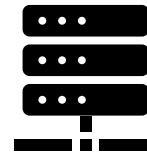
Padding



Bleichenbacher Angriff



Manipulierter
TLS Client



TLS Server

Verschlüsselte Nachricht
korrektes Padding
fehlerhafte Nachricht

Fehlernachricht 20

Verschlüsselte Nachricht
fehlerhaftes Padding
fehlerhafte Nachricht

Fehlernachricht 40

- Nutzt ein **Padding-Orakel**, um eine RSA Entschlüsselungsfunktion zu berechnen.
- Konstruktion des Orakels möglich auf der Grundlage von **Fehlermeldungen**, die von einer TLS-Serverimplementierung zurückgegeben werden.

Automatisierte Seitenkanalanalyse von kryptographischen Protokollen

- Automatisches Erkennen von Padding-Orakel Seitenkanälen
- Für TLS Protokoll
- Analyse auf Protokollebene – anwendbar auf alle TLS-Implementierungen

**Kann beliebige Orakel finden,
sogar unbekannte**

1. Erzeugen von Netzwerktraces

Automatisiertes
Testen

Maschinelles
Lernen

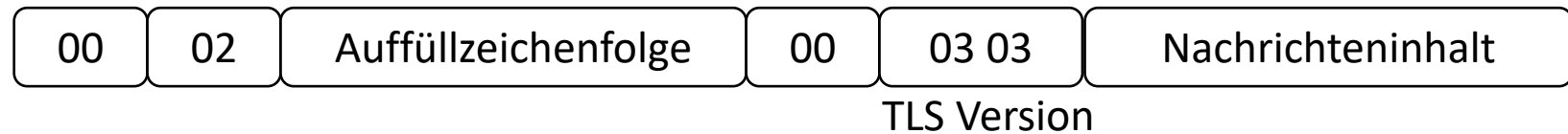
2. Suche nach Klassifikator für
korrektes und fehlerhaftes
Padding

PKCS#1v1.5 Padding

Korrektes Padding

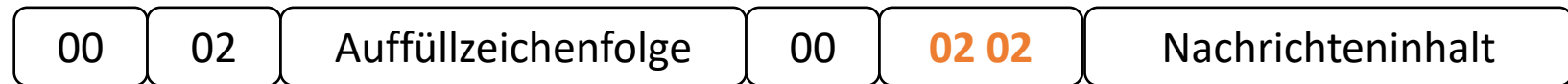
Startbytes

Trennbyte



Manipuliertes Padding

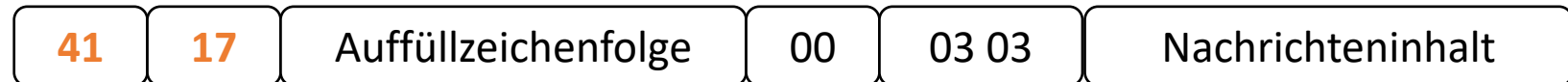
(1) Falsche TLS Versionsnummer



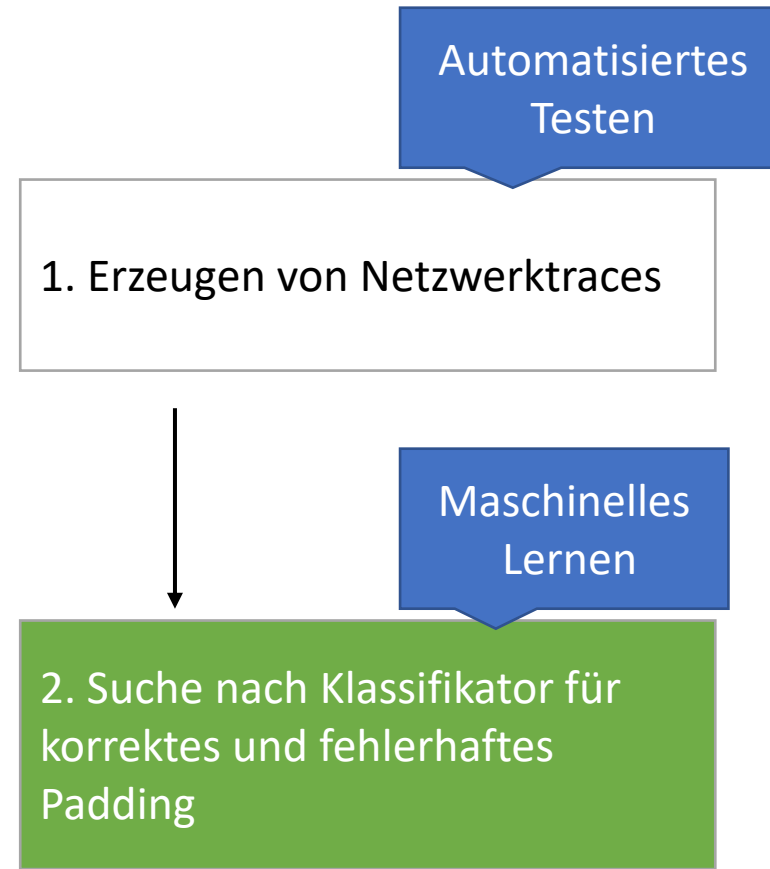
(2) Fehlender Separator



(3) Falscher Padding Start



Automatisierte Seitenkanalanalyse von kryptographischen Protokollen

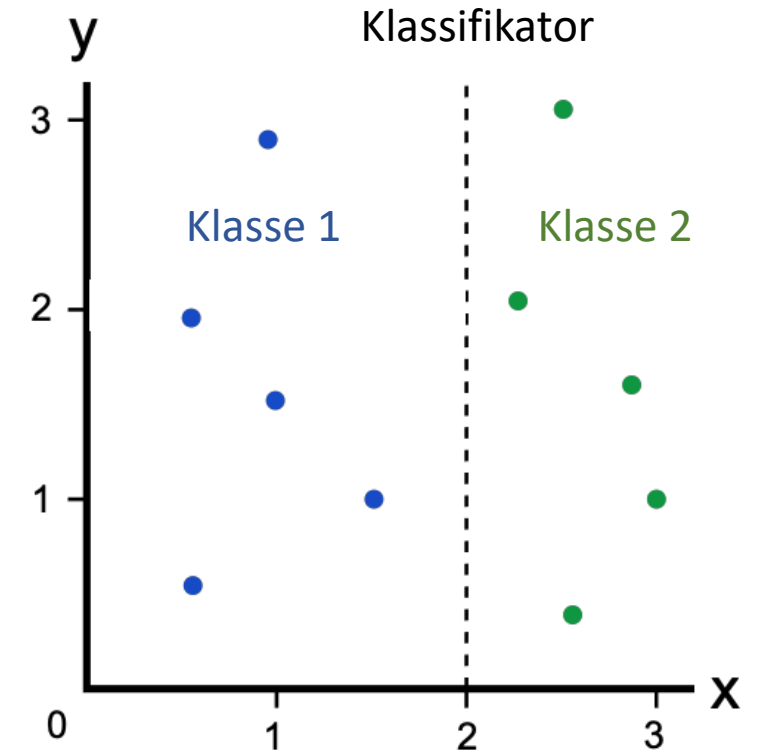


Maschineller Lernansatz

- Detektion eines Padding-Orakels:

Lernbarkeit eines binären Klassifikators:
erkennt auf Netzwerktrace aus TLS und TCP
Nachrichten, ob ein Padding korrekt oder
falsch ist

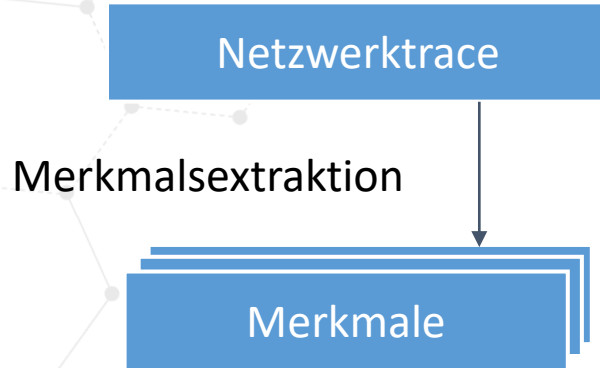
Klassifikator = Padding-Orakel



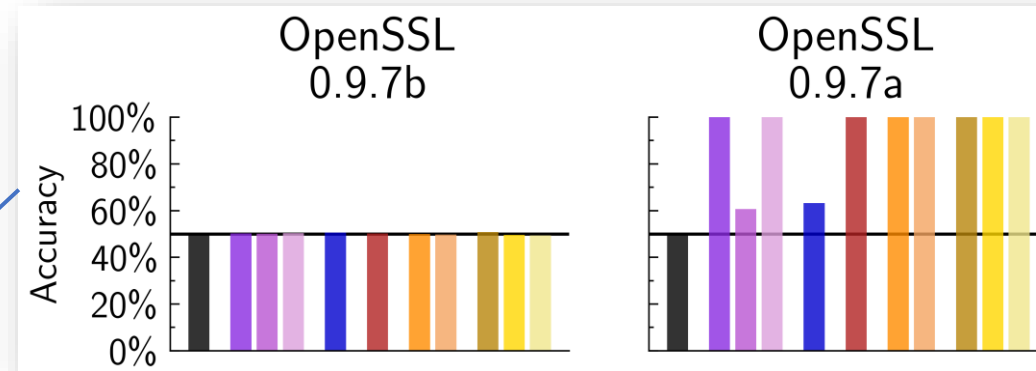
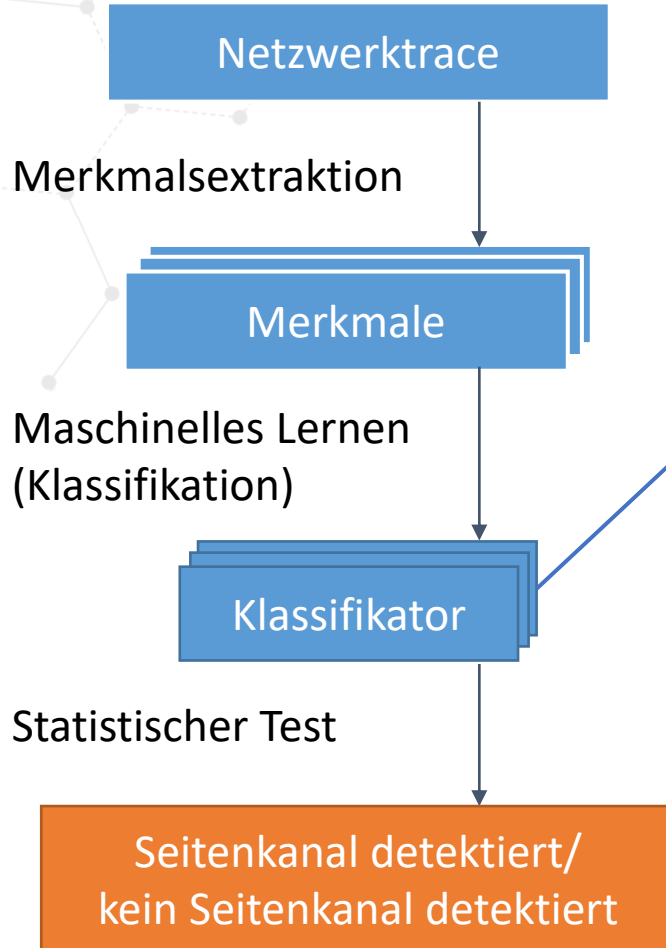
Umsetzung des Maschinellen Lernens

Netzwerktrace

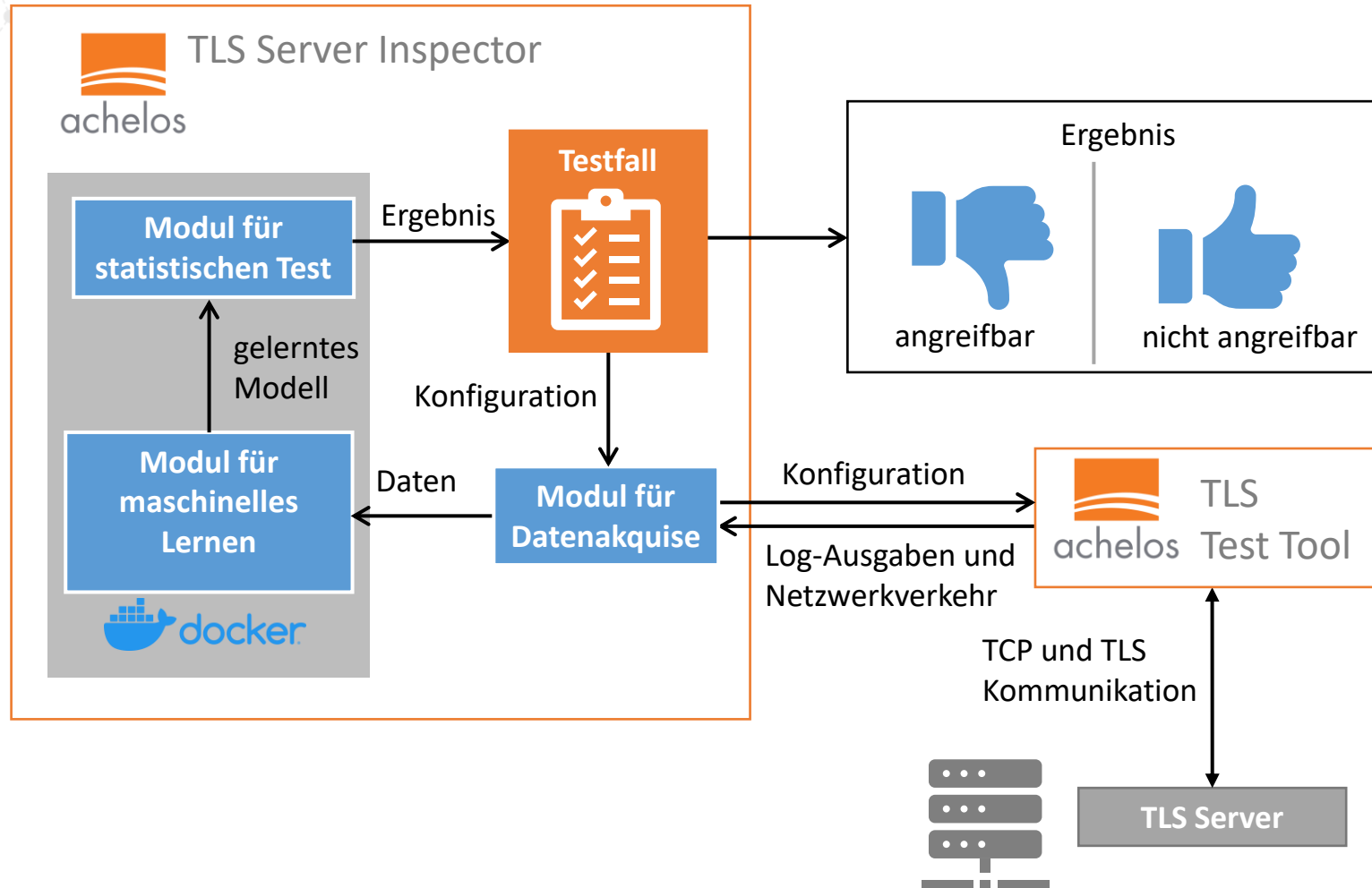
Umsetzung des Maschinellen Lernens



Umsetzung des Maschinellen Lernens

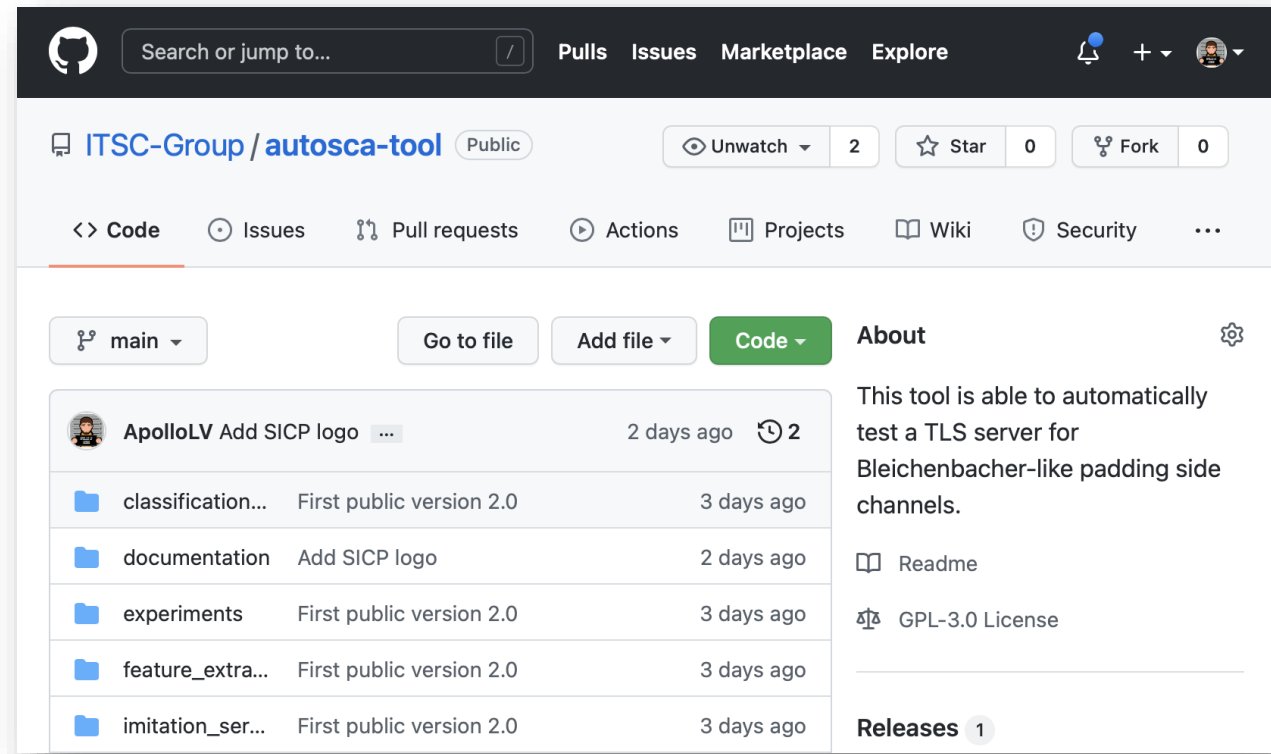


Technische Umsetzung



Verfügbarkeit

Verfügbar Open Source unter
<https://github.com/ITSC-Group/autosca-tool>





Vielen Dank! | Thank you!

achelos GmbH

Vattmannstraße 1 | 33100 Paderborn | GERMANY

T +49 5251 14212-0 | info@achelos.de

achelos.de | IoT.achelos.com

