German-American IT Security Forum

IT Security Association Germany (TeleTrusT) in cooperation with GACC – German American Chamber of Commerce

San Francisco, 06.06.2022

How to track down side channels you didn't even know exist

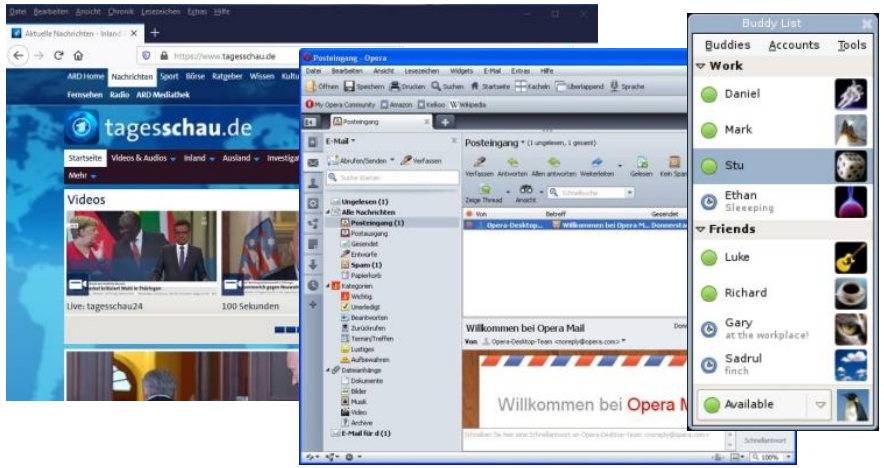
Dr. Claudia Priesterjahn, achelos GmbH

JOINT PROJECT „AUTOMATISCHE SCHWACHSTELLENANALYSE VON KRYPTOGRAPHISCHEN PROTOKOLLEN“ (AUTOSCA)

(AUTOMATIC DETECTION OF SIDE CHANNELS IN CRYPTOGRAPHIC PROTOCOLS)

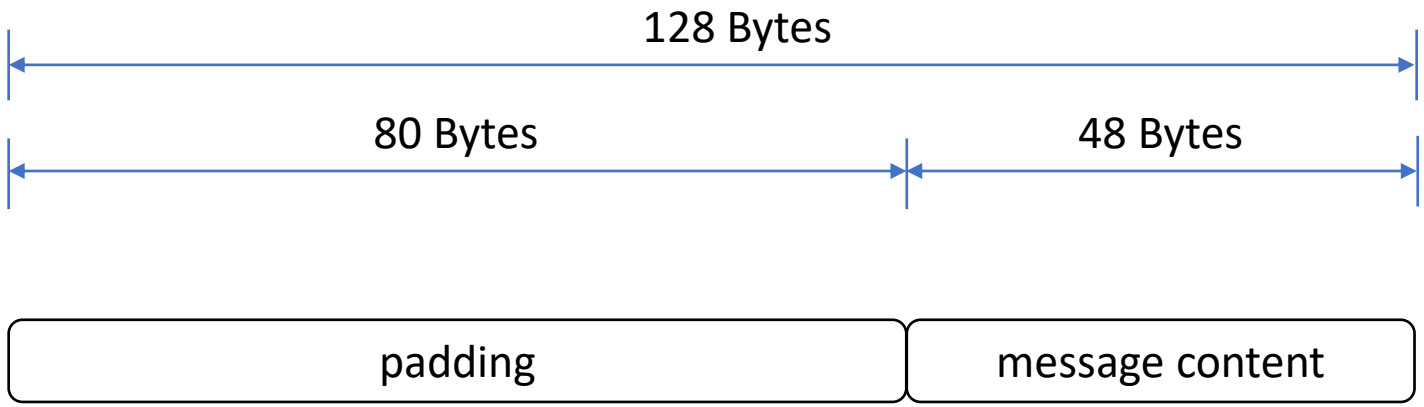
Secure Communication in Everyday Life

TLS – Transport Layer Security



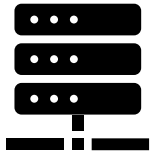
- Constantly new vulnerabilities and side channels
- Every change to the implementation may open new side channels

Padding



Bleichenbacher Attack

manipulated
TLS Client



TLS Server

encrypted message
valid padding
invalid message

error code 20

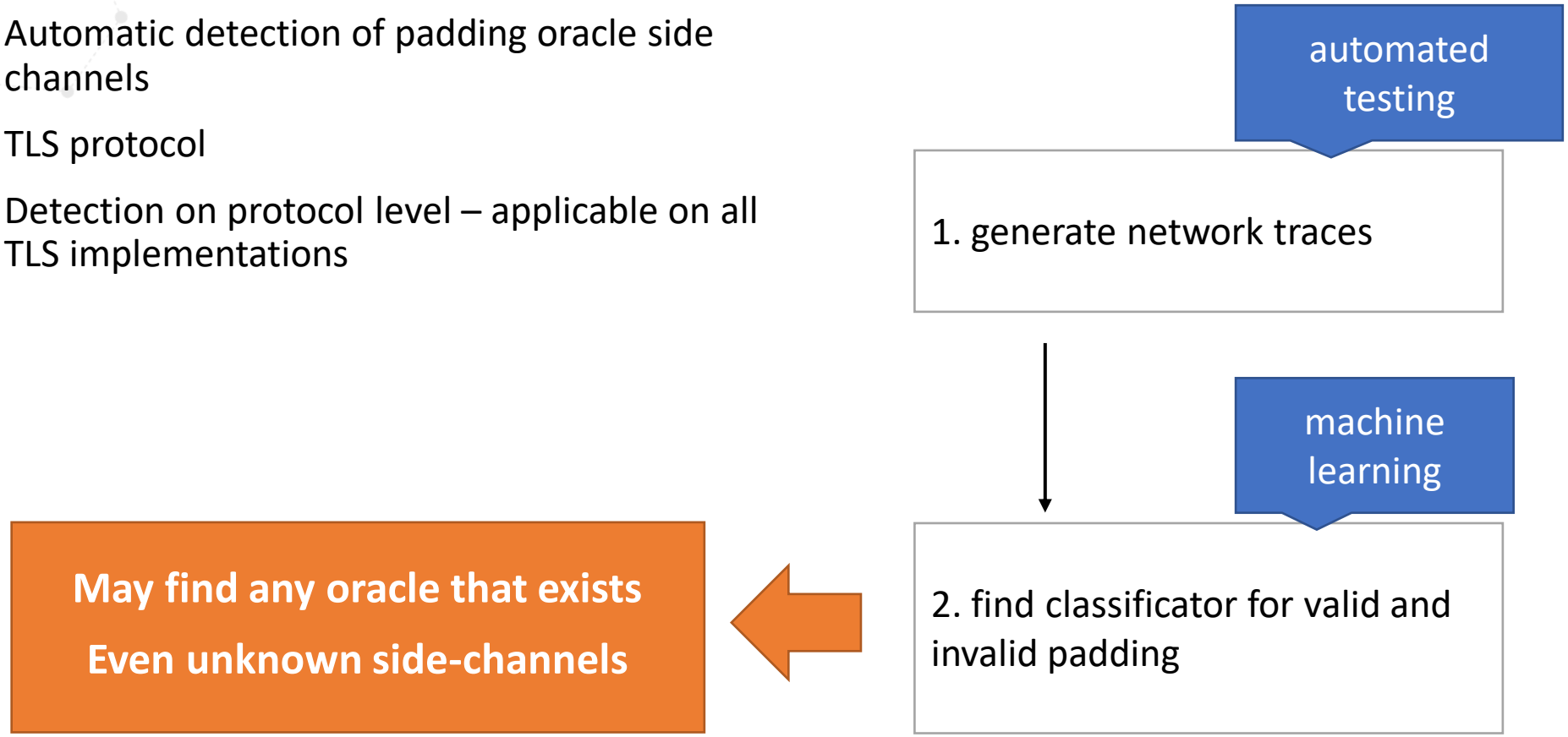
encrypted message
invalid padding
invalid message

error code 40

- uses a **padding oracle** to compute an RSA decryption function
- oracle can be contructed from **error messages** sent by the TLS server

Automatic Side-channel Detection in Cryptographic Protocols

- Automatic detection of padding oracle side channels
- TLS protocol
- Detection on protocol level – applicable on all TLS implementations



PKCS#1v1.5 Padding

valid padding

start bytes | | | separator | | |

00	02	padding string	00	03 03	message content
				TLS Version	

manipulated padding

(1) invalid TLS version

00	02	padding string	00	**02 02**	message content

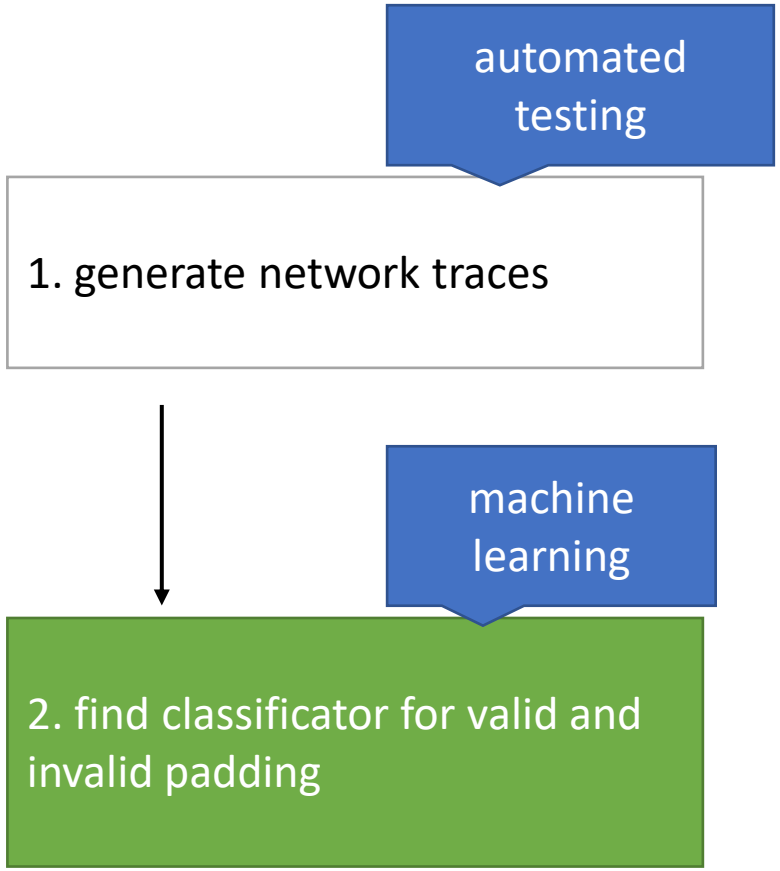
(2) missing separator

00	02	padding string	**37**	03 03	message content

(3) invalid start bytes

41	**17**	padding string	00	03 03	message content

Automatic Side Channel Detection in Cryptographic Protocols

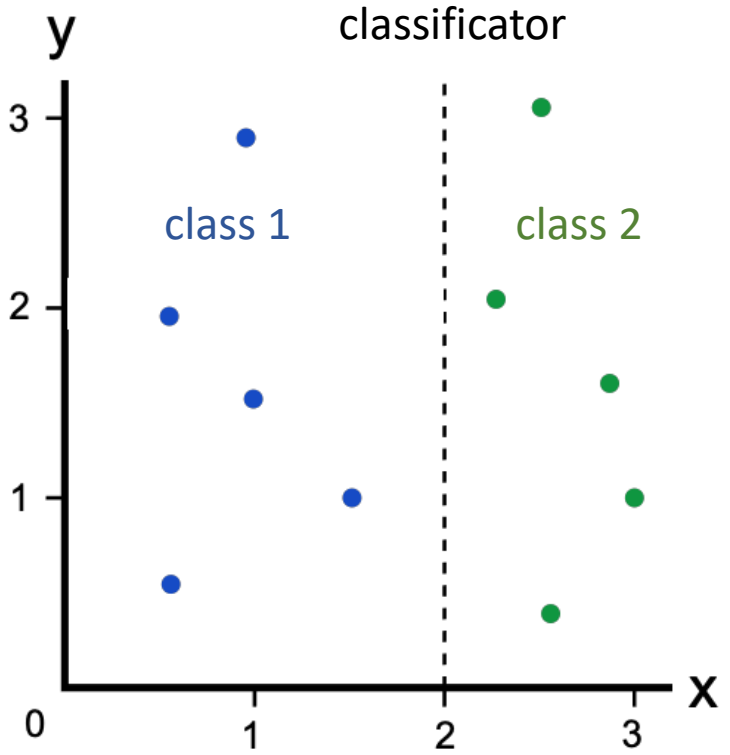


Machine Learning Approach

- Detect padding oracle

  Learnability of binary classifier:
  detects on network trace from TLS and TCP messages whether a padding is correct or incorrect

  classifier = padding oracle

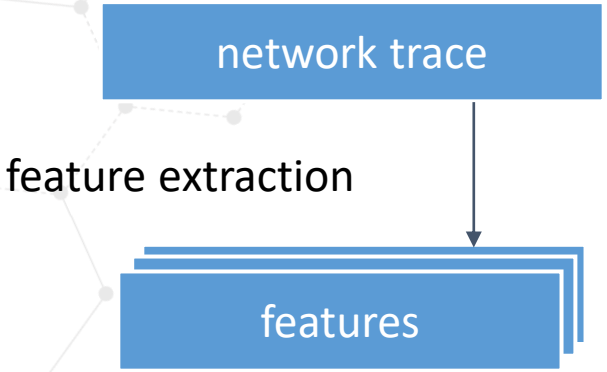


9

Implementation of Machine Learning Approach

network trace

Implementation of Machine Learning Approach



Machine Learning

network trace

feature extraction

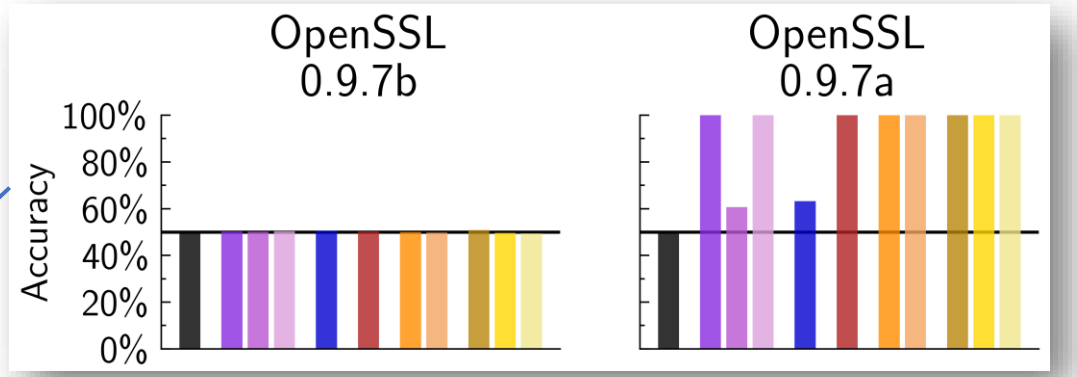
features

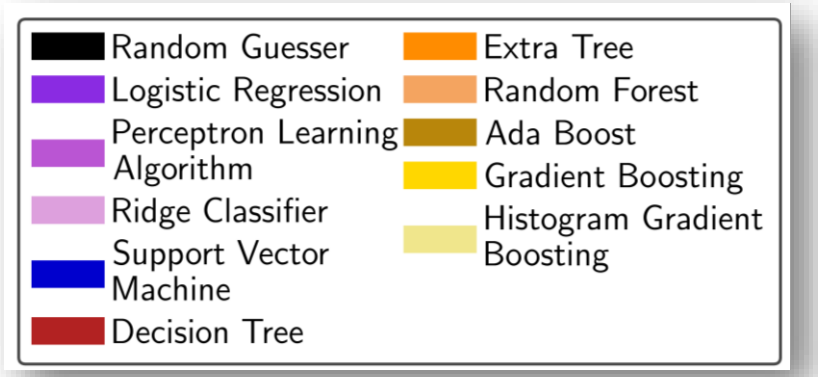
machine learning (classification)

classificators

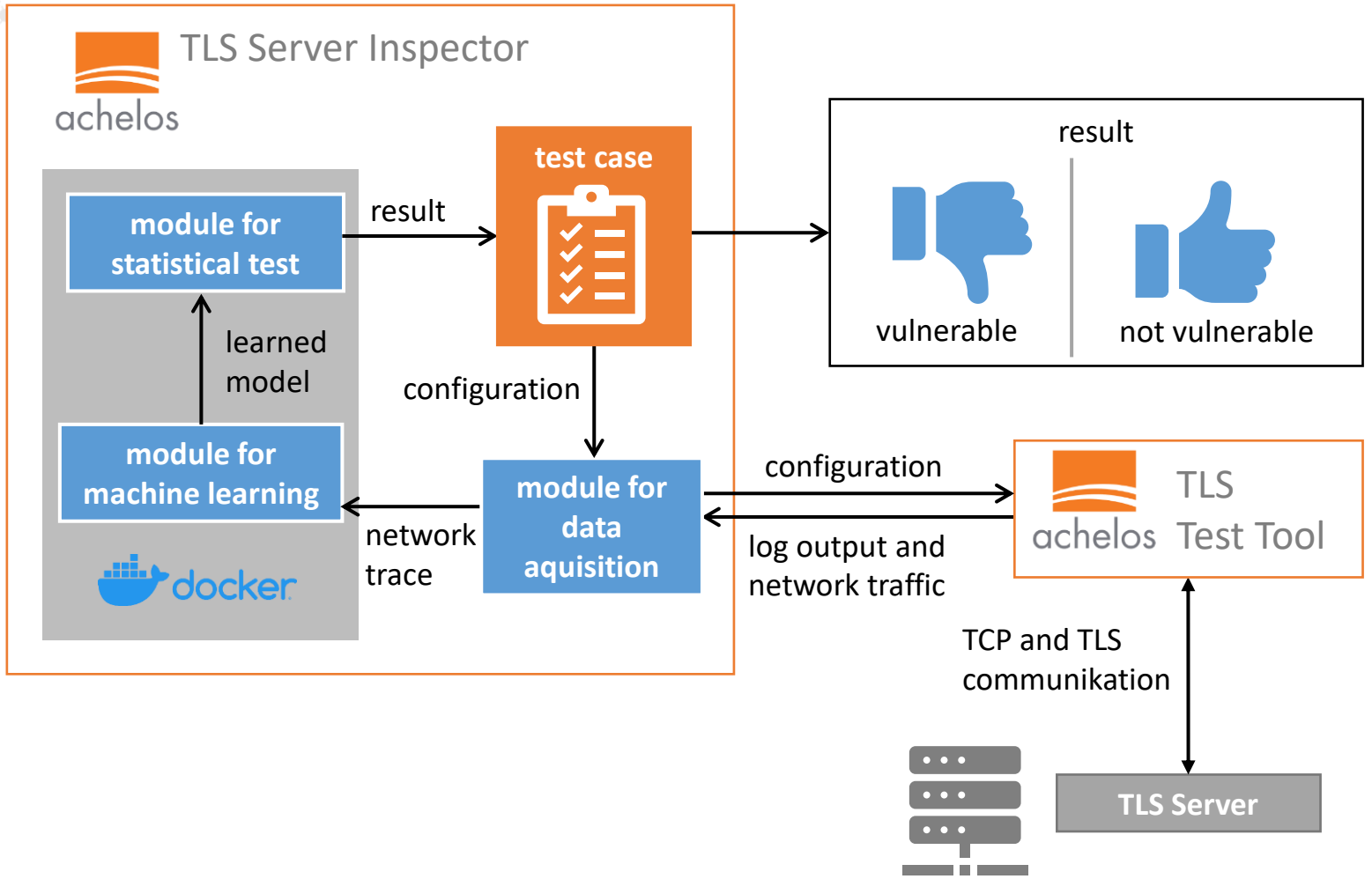
statistical test

side channel detected/ not detected



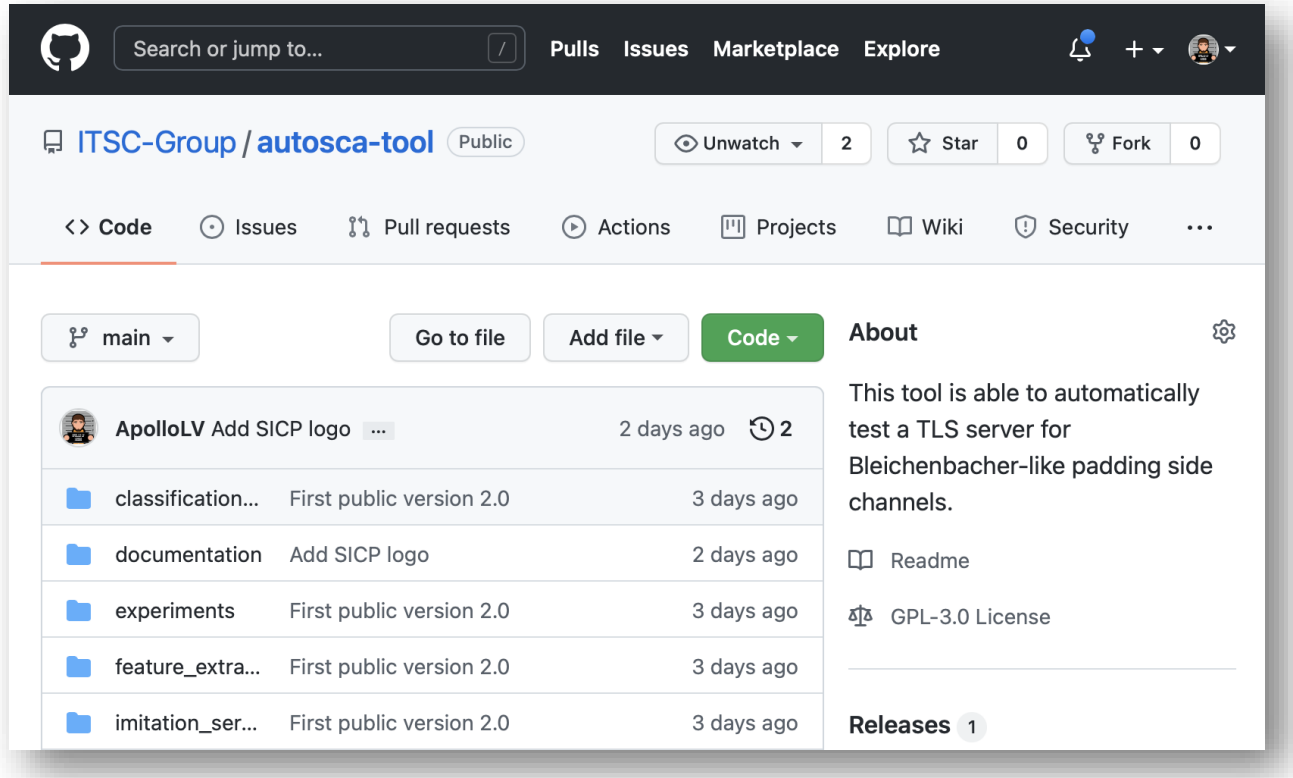


Prototype


TLS Server Inspector
achelos
module for statistical test
result
test case
learned model
module for machine learning
configuration
module for data aquisition
network trace
docker
result
vulnerable
not vulnerable
configuration
log output and network traffic
TLS
achelos Test Tool
TCP and TLS communikation
TLS Server

Availability

available open source at
https://github.com/ITSC-Group/autosca-tool



achelos

Vielen Dank! | Thank you!

achelos GmbH
Vattmannstraße 1 | 33100 Paderborn | GERMANY
T +49 5251 14212-0 | info@achelos.de
achelos.de | IoT.achelos.com