h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACULTY OF COMPUTER SCIENCE

CRISP
Center for Research
in Security and Privacy

– Master Thesis –

Machine Learning Algorithms for Attack Detection on Speaker Recognition Systems

da/sec

da/sec is the biometrics and internet security research group and is affiliated with University of Applied Sciences Darmstadt and the Center for Research in Security and Privacy (CRISP). It is led by Prof. Dr. Harald Baier and Prof. Dr. Christoph Busch. The focus of the group is on highly innovative and applied IT security research in the special fields of biometrics, internet security and digital forensics. Read more on www.dasec.h-da.de.

Motivation & Goal

Speaker recognition systems are already used for security relevant applications, e.g. telephone banking. Replay attacks, in particular unit-selection, pose a major thread to the performance of speaker recognition systems. For the specific attack with unit-selection Text-To-Speech-systems (TTS), speech samples of the attacked subject are captured, segmented into parts, called units, and replayed in different sequence to the Speaker Identification and Verification (SIV) system.

Current research provides multiple features for unit-selection detection. Goal of this thesis is to employ multiple machine learning algorithms analyzing different features in order to determine the performance of combinations of feature and machine learning algorithm.

Tasks

- Literature research for features utilized for unit-selection detection
- Train machine learning algorithms on different features
- Evaluate the performance of different machine learning algorithms on different features

Requirements

- Interest in biometrics/speaker recognition
- Basic knowledge in machine learning algorithms
- Programming skills (Matlab, Julia, Python)

By Date

- Immediately

Contact

Ulrich Scherhag
ulrich.scherhag@h-da.de

h_da
Faculty of Computer Science
CRISP - Center for Research in Security and Privacy
Schöfferstraße 8b
64295 Darmstadt