ASVspoof: World-leading Research Institutes and IT Companies are Joining Forces to Combat Voice Spoofs

Sophia Antipolis, FR -- 6 February 2019 -- Continually evolving in unpredictable ways, fake data present a key concern in today's society. Besides fake news, multimedia data such as video, image and voice data has become increasingly easier to generate or manipulate, opening up potential for its misuse, especially in fields of information security and user privacy. In 2018, so-called **DeepFakes** - realistic-looking, yet fake videos portraying celebrities - drew particular attention. This work showed how deep learning technologies can be used to generate illicit videos or audio recordings of specific target persons. The threat is not confined to the media, however. Anyone who uses biometrics technology of any kind, including voice, could also be concerned.

Together with a large team of international collaborators, **EURECOM,** a world-class French academic research center in the fields of data science and digital security, is working to fight the abuse of voice-based technologies and develop preventive strategies. Pooling efforts and expertise, the **ASVspoof 2019 challenge** (www.asvspoof.org) is currently underway, representing the largest and most comprehensive evaluation of spoofing and countermeasures to date.

The initiative's overriding objectives are to promote the development of reliable countermeasures that are able to distinguish between bona fide/genuine and spoofed speech. It aims specifically to encourage the design of generalized countermeasures, i.e., countermeasures that perform well when faced with spoofing attacks of unpredictable nature. As with the preceding 2015 and 2017 editions, the 2019 evaluation dataset contains training/development and evaluation partitions generated with different technologies, i.e. text-to-speech (TTS) and voice conversion (VC) algorithms, and replay scenarios.

"It is important to understand that, in future, we may no longer be able to judge by ourselves whether what we are watching or what we are listening to is genuine or not. Society is in urgent need of new tools, perhaps similar to today's anti-virus systems that will alert us to fake media, i.e. artificially generated or manipulated video or voice data," said Professor Nicholas Evans, Head of Audio Security and Privacy Group within EURECOM's department of Digital Security.

Used in smart home assistants, audio books, healthcare, public announcement systems and a plethora of other applications, artificial intelligence and machine learning technology is intended to facilitate many routine tasks of daily life. Google's 2016 introduction of 'WaveNet' technology showed the ease by which speech synthesis solutions can generate natural-sounding speech - the widely reported case of Google's hair salon appointment booking is probably still fresh in

everyone's mind. However, most of us are unable to distinguish fake speech from genuine speech produced by a human. Apart from the very real risk of mass manipulation via fake videos featuring politicians or celebrities, this also presents major security risks, for instance if someone's voice and speech pattern are imitated to fool a telephone banking service into believing the caller is the bank account holder. The ability of TTS and VC to put words in someone else's mouth or to clone someone's voice raises obvious concerns.

In a recent blog post, Google said that the technological progress was exciting but "*…we're keenly aware of the risks this technology can pose if used with the intent to cause harm. Malicious actors may synthesize speech to try to fool voice authentication systems, or they may create forged audio recordings to defame public figures. Perhaps equally concerning, public awareness of "deep fakes" (audio or video clips generated by deep learning models) can be exploited to manipulate trust in media: as it becomes harder to distinguish real from tampered content, bad actors can more credibly claim that authentic data is fake."*

The ASVspoof initiative is today one of the most successful of all anti-spoofing initiatives within the entire biometrics community. Over 150 registrations from around the world have been received for the 2019 edition including both academic and industrial participation.

Planning for ASVspoof 2019 started almost one year ago. While ASVspoof remains **mostly an academically-led initiative**, co-organised by EURECOM and INRIA in France, the National Institute of Informatics (NII) and NEC in Japan, the University of Eastern Finland and the University of Edinburgh in the UK, **the 2019 edition involves substantial data contributions from an impressive array of external partners from both academia and industry:** Aalto University (Finland), Academia Sinica (Taiwan), the Adapt Centre (Ireland), DFKI (Germany), HOYA (Japan), iFlytek (China), Google (UK), Nagoya University (Japan), Saarland University (Germany), Trinity College Dublin (Ireland), NTT Communication Science Laboratories (Japan), the Laboratoire Informatique d'Avignon (France) and the University of Science and Technology of China.

The initiative is supported by the Academy of Finland, the French national research-funding agency (ANR) and the Japan Science and Technology Agency.

For further information, contact Nicholas Evans at (evans at eurecom dot fr)

###

About EURECOM

EURECOM is a Graduate school and Research Centre in Digital Sciences located in the Sophia Antipolis (French Riviera), Europe's leading international science and technology park.

Founded in 1991 as a consortium, EURECOM has to build a large network of renowned academic and industrial partners. The "Institut Mines Telecom" is a founding member of EURECOM consortium. EURECOM research teams are made up of international experts, recruited at the highest level, whose work is regularly honored and has earned international recognition.

EURECOM is particularly active in research in its areas of excellence while also training a large number of doctoral candidates. Its contractual research is recognized across Europe and contributes largely to its budget.

Based on the close ties it has developed with industry, EURECOM can direct an essential part of its research activities towards areas of interest for its industrial partners. One of our challenges is to fill the gap between fundamental research and the more business oriented one in our partner companies. From the beginning, the main objective set by our members was excellence on an international level. In research this excellence results in a high number of publications and patents, in the active participation to international scientific events and organizations and of course in getting many important European contracts in the European framework. Given its size, EURECOM chose to focus its research activities on three main areas: networking and security, multimedia communications and mobile communications.

The largest department, Mobile Communications, focuses on digital signal processing for mobile communications applications that include current generation 4G and next generation 5G cellular radio systems, wireless protocols, information theory, and networking. Funding for research activities comes from private industry, European and national level sources in field of wireless communications.

To learn more about EURECOM, visit http://www.eurecom.fr/en/eurecom/strategy

#spoof #eurecom #google #asvspoof2019 #deepfake #fakedata #sophiaantipolis #research #technology #