ALERTE MÉDIA

ASVspoof 2019 : Des instituts de recherche et des leaders de technologie mondiaux s'unissent pour lutter contre le spoofing de la voix

Sophia Antipolis, FR -- 21 février 2019 -- Les fausses données – une préoccupation majeure dans la société d'aujourd'hui – évoluent continuellement et de façon imprévisible. Outre les fausses nouvelles, les données multimédias telles que les vidéos, les images et les données vocales sont de plus en plus faciles à générer ou à manipuler, ce qui ouvre des possibilités d'utilisation abusive, en particulier dans les domaines de la sécurité de l'information et de la vie privée des utilisateurs. En 2018, DeepFakes – des vidéos réalistes mais fausses représentant des célébrités – a particulièrement attiré l'attention. Ces trucages ont montré comment les technologies d'apprentissage en profondeur peuvent être utilisées pour générer des vidéos ou des enregistrements audio illicites de personnes ciblées. Mais la menace ne se limite pas aux médias. Quiconque utilise la technologie biométrique, quelle qu'elle soit, y compris la voix, devrait s'en inquiéter.

EURECOM, centre de recherche français de renommée mondiale spécialisé dans le Data Science et la sécurité numérique, s'emploie à lutter contre l'abus des technologies vocales et à développer des stratégies de prévention en collaboration avec une vaste équipe de collaborateurs internationaux. Le défi ASVspoof 2019 (www.asvspoof.org) représente à ce jour l'évaluation la plus large et la plus complète de l'usurpation d'identité et des contre-mesures.

L'initiative a pour principaux objectifs de promouvoir la mise au point de contre-mesures fiables capables de faire la distinction entre un discours authentique et un discours usurpé. Elle vise spécifiquement à encourager la conception de contre-mesures généralisées, qui sont performantes lorsqu'elles sont confrontées à des attaques par spoofing de nature imprévisible. Comme pour les éditions précédentes de 2015 et 2017, l'ensemble des données d'évaluation de 2019 contient des partitions de formation/développement et d'évaluation générées avec différentes technologies, c'est-à-dire des algorithmes de synthèse vocale (ASV) et de conversion vocale (ACV), ainsi que des scénarios de rediffusion.

« Il faut comprendre que, dans le futur, nous ne serons peut-être plus en mesure de juger par nous-mêmes si ce que nous regardons ou écoutons est authentique. La société a un besoin

urgent de nouveaux outils, peut-être similaires aux systèmes antivirus d'aujourd'hui, qui nous avertiront de la présence de faux médias, c'est-à-dire de données vidéo ou vocales générées ou manipulées artificiellement », explique Nicholas Evans, professeur et responsable du groupe Sécurité audio et confidentialité au sein du département Sécurité numérique d'EURECOM.

Utilisées dans les assistants à domicile intelligents, les livres audio, les soins de santé, les systèmes d'annonces publiques et une pléthore d'autres applications, l'intelligence artificielle et la technologie d'apprentissage machine sont destinées à faciliter de nombreuses tâches quotidiennes de la vie courante. L'introduction en 2016 de la technologie « WaveNet » par Google a montré la facilité avec laquelle les solutions de synthèse vocale peuvent générer des sons naturels ; le cas largement rapporté de la prise de rendez-vous dans un salon de coiffure sur Google est probablement encore frais dans l'esprit de tous. Mais la plupart d'entre nous est incapable de distinguer un faux d'un vrai discours produit par un humain. Au risque très réel de manipulation de masse par le biais de fausses vidéos mettant en scène des politiciens ou des célébrités s'ajoute celui pour la sécurité, par exemple si la voix et le discours d'une personne sont imités pour faire croire à un service bancaire téléphonique que l'appelant est le titulaire du compte. La capacité des algorithmes de synthèse et de conversion vocales à mettre des mots dans la bouche d'une personne ou de cloner sa voix soulève des préoccupations évidentes.

Dans un récent article de blog, Google a déclaré que le progrès technologique était passionnant mais « *... nous sommes très conscients des risques que cette technologie peut poser si elle est utilisée pour nuire intentionnellement. Des acteurs malveillants peuvent synthétiser la parole pour essayer de tromper les systèmes d'authentification vocale ou créer de faux enregistrements audio pour diffamer des personnalités publiques. Tout aussi inquiétante peut-être, la sensibilisation du public aux « DeepFakes » (clips audio ou vidéo générés par les modèles d'apprentissage en profondeur) peut être exploitée pour manipuler la confiance dans les médias : plus il devient difficile de faire la distinction entre contenu réel et contenu falsifié, plus les mauvais acteurs peuvent affirmer de manière crédible que les données authentiques sont fausses.* »

ASVspoof est aujourd'hui l'une des initiatives d'anti-spoofing les plus réussies de la communauté biométrique. Plus de 150 inscriptions en provenance du monde entier ont déjà été reçues, y compris d'établissements universitaires et d'industriels.

La planification d'ASVspoof 2019 a commencé il y a presque un an. Bien qu'elle reste une initiative essentiellement dirigée par des universitaires, organisée conjointement par EURECOM et l'INRIA en France, le National Institute of Informatics (NII) et le NEC au Japon, l'Université de Finlande orientale et l'Université d'Edimbourg au Royaume-Uni, l'édition 2019 réunit des contributions importantes de données provenant d'un nombre impressionnant de partenaires extérieurs au milieu universitaire et industriel : Université d'Aalto (Finlande), Academia Sinica (Taiwan), le Centre Adapt (Irlande), DFKI (Allemagne), HOYA (Japon), iFlytek (Chine), Google (Royaume-Uni), Nagoya University (Japon), Saarland University (Allemagne), Trinity College Dublin (Irlande), NTT Communication Science Laboratories (Japon), Laboratoire informatique d'Avignon (France) et l'Université des sciences et techniques de Chine.

L'initiative est soutenue par l'Académie de Finlande, l'Agence Nationale française de financement de la Recherche (ANR) et la Japan Science and Technology Agency.

Pour de plus amples informations, contactez Nicholas Evans Nick.Evans@eurecom.fr

###

Contact média : Natja Igney, media@eurecom.fr , tél. +33 (0)7 52 52 52 04
Pour en savoir plus sur EURECOM, visitez le site http://www.eurecom.fr/en/eurecom/strategy