NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: **Spoofing Attacks for Voice Biometrics**

Speaker: Dr. Pavel Korshunov
Postdoctoral Researcher
Idiap Research Institute
Switzerland

Date/Time: 19 February 2016, Friday, 10:30 AM to 11:30 AM

Venue: MR1, COM1-03-19

Chaired by: Dr Ooi Wei Tsang, Associate Professor, School of Computing (ooiwt@comp.nus.edu.sg)

Abstract:

Despite the growing usage and the increasing reliability of the speaker verification systems, they are shown to be vulnerable to spoofing attacks. In a spoofing attack, an invalid user attempts to gain access to the system by presenting counterfeit or 'fake' speech sample(s) as the evidence of a valid user. Counterfeit speech can be synthesized from text, converted using speech of another person (e.g., an attacker), or simply replayed using some playback device such as a mobile phone. It was shown that such attacks are very successful in spoofing the state of the art verification systems with false acceptance rates reaching higher than 90%. To detect spoofing attacks, one needs an extensive dataset that has both genuine and spoofed data, a system that would successfully detect such attacks, a reliable measure of the detection performance, and a way to integrate (fuse) attack detection into existing biometric systems.

In this talk, I present the first publicly available dataset (AVspoof: https://www.idiap.ch/dataset/avspoof) that contains presentation attacks (aka replay attacks) for speech data. The dataset can be used to train and evaluate verification, anti-spoofing, and fused systems. I discuss several state of the art approaches for detecting audio spoofing attacks and compare their performances on the data from AVspoof dataset. I also show some demos using open source toolbox Bob (http://idiap.github.io/bob/) and explain how one can create a verification or an anti-spoofing detection system with reproducible results.

Biodata:

Pavel Korshunov is a postdoctoral researcher in Biometrics group at Idiap Research Institute

(Martigny, Switzerland), currently working on the problem of speaker anti-spoofing detection. Originally from Saint-Petersburg, Russia, he received a Ph.D. in Computer Science from School of Computing, National University of Singapore in 2011 and was a postdoctoral researcher at EPFL (Lausanne, Switzerland) from 2011 till 2015. He is a recipient of ACM TOMM Nicolas D. Georganas Best Paper Award in 2011, two top 10% best paper awards in MMSP 2014, and top 10% best paper award in ICIP 2014. He has over 50 research publications and is a co-editor of the new JPEG XT standard for HDR images. His research interests span many areas, including computer vision, video analysis, quality assessment, crowdsourcing, high dynamic range imaging, privacy protection, and, also lately, speech analysis, speaker recognition, speaker anti-spoofing, and machine learning. He is one of the current contributors to the signal processing and machine learning open source toolbox "Bob" (http://idiap.github.io/bob/).