# 1 Course Number, CRN and Title

Course Number: CS 59000
CRN: 063
Title: Privacy Preserving Biomt Auth.
(Since the character limit of the course title is 30, the actual title: "Privacy Preserving Biometrics Authentication from Mobile Devices" was shortened during the registration time.)

# 2 Course Objectives

- To implement the privacy preserving biometrics based authentication approach proposed in [1], in the mobile device platform.
- To evaluate the performance of the aforementioned approach when used in the mobile device platform, to identify any bottlenecks and to do the required improvements to avoid them.
- To extend the aforementioned approach to support multi-model biometrics.

# 3 Course Description

Biometrics represents a strong authentication factor. Most of the existing biometrics based authentication solutions focus on how to authenticate to a personal device using one's biometrics. In [1], we have proposed a novel approach to authenticate to a remote service provider using biometrics, in a privacy preserving manner. So far, it has been evaluated only in personal computer (PC) platform. In order for this approach to be widely used, it must be implemented and evaluated in the mobile devive platform as well. I anticipate that there will be several challenges when porting the solution to the mobile device platform. One of the key objectives of this study is to identify and address such challenges in order for the solution to be successfully ported to the mobile device plaform.
Furthermore, the solution in [1] is based on unimodal biometrics (i.e: only one biometric trait of the individual is used as the authentication factor), which suffers from high error rates caused by noise in sensed data, intra-class variation, inter-class similarities, and vulnerability to attacks such as artificial fingerprints. Multimodal biometrics has been identified as a better solution which improves the authentication accuracy and enhances the security against spoofing attacks. The second objective of this study is to extend the approach in [1] to support multimodal biometrics. It will be first designed, implemented and evaluated in the PC platform. If the time permits, it will also be ported to mobile device platform during Spring 2016, otherwise it will be completed during Summer 2016.

# 4 Course Outline

- Porting the client side implementations of the enrollment protocol and the authentication protocol proposed in [1] to mobile device platform, which includes:
  - securely recieving and storing the artifacts: identity token, SVM classifier and error corrected biometrics feature vector in the mobile device.
  - implementng the key components of the authetication software: PHash computation, error correction decoding, SVM prediction, Pedersen commitment generation, Zero Knowledge Proof of Knowledge of protocol runner, in the mobile device.
- Carrying out performance tests (in terms of accuracy and computation time) based on the implementation of the solution in the mobile device.
- Designing an extension to the solution in [1] order to support multimodal biometrics. Implement it in PC platform and evaluate its performance.

# References

[1] H. Gunasinghe and E. Bertino, "Privacy Preserving Biometrics-Based and User Centric Authentication Protocol," in *Network and System Security - 8th International Conference, NSS 2014*, 2014, pp. 15–17.