Embedded Automotive Security, Winter 2015

COURSE WEBSITE:	CLEW AT HTTP://WWW.UWINDSOR.CA/CLEW
Time & Location:	1:00pm-2:20pm, Tuesday and Thursday, 2100 CEI
Professor:	Dr. Huapeng Wu
	Phone: ext 2568, Email: hwu@uwindsor.ca, Office: CE3049
Office hours:	2:30pm-3:30pm, Wednesday and Thursday
Midterm exam:	Thur. Feb 26, 2015 at 2100 CEI (in class)
Final exam:	Tue. Apr 21, 2015 (location TBA)

Objective:
The objectives of this course are to make students 1). Understand modern cryptographic primitives, such as symmetric key and public key systems, hash functions, and cryptographic protocols. 2). Understand security requirements for vehicular electronics and software, such as hardware protection, software protection, and secure communication of in-vehicle, vehicle-to-vehicle, and vehicle-to-infrastructure. 3). Learn how to utilize cryptographic techniques to provide mechanisms and services for vehicular security needs. 4). Design and test simple security schemes for certain security critical vehicular applications, such as electronic immobilizer and keyless entry.

Contents:
The course contents include the following: Introductions to cryptographic primitives, such as symmetric key scheme (AES), public-key system (ECC), and the security services they provide; A review of automotive attacks and security objectives; Cryptography-based security module and mechanisms to provide vehicular hardware and software protection and various vehicular communications; Certain security critical vehicular applications.

Textbook & Reference Book:

- Embedded Security in Cars -- Securing Current and Future Automotive IT Applications, Lemke, Kerstin; Paar, Christof; Wolf, Marko (Eds.), Springer-Verlag, 2006. (Ebook: ISBN 978-3-540-28428-4; Hardcopy: ISBN 978-3-540-28384-3)
- Introduction to Cryptography with Coding Theory, 2nd Edition, (hardcover), by Wade Trappe and Lawrence C. Washington, Pearson/Prentice Hall, New Jersey, 2006. ISBN: 0-13-186239-1

Grading:

Assignments:	10%
Midterm exam:	20%
Projects:	30%
Final exam:	40%

Other Important Messages:

- Students taking this course should have certain programming skill with a major computer language.
- Assignments and project reports are submitted electronically through Clew website. No email submission or hardcopy submission is allowed. Late submissions will be deducted 10% per day up to 3 days (after which no submission will be accepted). If you submit late or miss a submission due to medical or other reason please contact the professor as soon as possible.
- Students are welcomed to visit the professor's office during office hours. Visit during non-office hours should be pre-arranged through email. Email anytime is welcomed. I will reply your email within 24 hours during work days if not immediately. Please use your UWind email account and add [88590-04] to your email subject, otherwise response could be delayed.
- Both midterm and final exams are closed-book, but two pages (single-sided, letter size) of formula sheets are allowed for midterm, and four pages of formula sheets are allowed for the final.

Automotive Security