***The University of Queensland***
***School of Information Technology and Electrical Engineering***

***COMS3000***
***Semester 2, 2018***

# Assignment 2 (Weighting 13%)

This Assignment is due **12:00 NOON (MIDDAY) Thursday, 4/10/2018**

## *Cooperative and Automated Vehicles (CAV) Message Security*

### [COMS3000: 13%, 13 marks (total)]

Stuart Allen-Keeling, Queensland Transport and Main Roads, describes the current situation:

"Co-operative Intelligent Transport Systems (C-ITS) and Automated Vehicles (AV) represent a significant step forward in technology for the land transport industry. The new technology will enable equipped vehicles to relay and process their position, speed and direction with each other (C-ITS), and in conjunction with environmental sensors they will also be able to autonomously react to that information in real time (AV). Not only will vehicles be able to warn each other of impending dangers – traffic authorities will have direct, real time communication to and from vehicles, allowing for a level of traffic management and optimisation that has not been seen to date. Such a rich data and feature set is not only attractive to road authorities and Original Equipment Manufacturers (OEMs); it may also have appeal to those with less authority, such as criminals, hacktivists, and even terrorists.

European (EU) and American (US) standards both propose that one of the controls that will reduce the risk of misuse is the implementation of a 'Security Credential Management System' (SCMS). Essentially, this is an identity management system originating from the Information Technology world using Public Key Infrastructure (PKI) that was designed for conducting secure operations over a hostile network."

The SCMS uses two types of credentials. Enrollment Certificates (EC) that certify the public keys of legitimate stations and anonymous Authorisation Tickets (AT) (also PKI certificates) that certify the anonymous public keys that stations use to sign anonymous, but trusted, messages. Anonymous message validation is a requirement for privacy and anti-tracking.

REVIEW the current literature in Information Security in Co-operative Intelligent Transport Systems (C-ITS), C-ITS objectives and goals and the purpose of CAM and DENM messages. **Provide a concise (1500-2000 words) report** that includes the following.

- DESCRIBE THREE of the many THREATS to **C-ITS communications** (communications such as CAMs and DENMs) (explain ***why*** each is a threat).
- DESCRIBE THREE VULNERABILITIES you see in C-ITS communications that your described threats may be able to exploit (explain ***how*** those VULVERABILITIES may be EXPLOITED).
- DESCRIBE THREE CONTROLS that should be considered to mitigate the RISKS of these THREATS being realised (explain ***how*** your CONTROL reduces the RISK).
- PROPOSE How Australia can achieve **immediate AT certificate revocation**, while still complying with the EU standard certificate and message formats as much as possible?

The EU SCMS and US SCMS have different ways of handling the threat of misbehaving vehicles (either deliberately or by fault) in the system. The EU system provides vehicles with short-lived anonymous authorisation tickets (certificates) and refuses to provide replacement ATs for vehicles identified as misbehaving. Thus, when the existing ATs expire, the misbehaving vehicle will no longer be able to send valid signed messages. The US system proposes a complex method of linking ATs to a vehicle, while still maintaining backward privacy, so that the current AT certificates of a misbehaving vehicle can be revoked.

Australia follows the EU certificate standards (ETSI TS 102 941 and related standards) which do not support AT revocation. However, Australia wants to be able to immediately revoke AT certificates, rather than waiting for them to expire, while still complying with the EU standard certificate and message formats as much as possible.

How can Australia achieve **immediate AT certificate revocation**, while still complying with the EU standard certificate and message formats as much as possible? There is no "correct" answer. It is a measure of your understanding of the problem and "*evidence of originality and insight in identifying, generating and communicating competing arguments, perspectives or problem solving approaches; critically evaluating problems, their solutions and implications*".

## References:

This assignment includes is a review of current literature. Every statement you make must be backed up with the evidence (citation) of where you found the information. But remember, this is YOUR report – YOU interpret the information and present it in your own words.
Do NOT just present a series of quotations!

## Assessment – Marking Scheme:

**Threats (max 2 marks):** [core assessment]

Some **relevant** threats are explained and no vulnerabilities are identified as threats – 1

Relevant threats cited from quality sources with no vulnerabilities identified as threats – 2

**Vulnerabilities (max 2 marks):** [core assessment]

Some **relevant** vulnerabilities are explained and no threats are identified as vulnerabilities – 1

Relevant vulnerabilities cited from quality sources with no threats called vulnerabilities – 2

**Controls (max 3 marks):** [core assessment]

Some relevant controls are explained (how they reduce the risk) – 1

All three threats have relevant controls – 2

All three threats have relevant controls and are practical for the current state of C-ITS – 3

**Revocation (max 3 marks):** [extension: distinction, high distinction]

Proposal is practical for the current state of C-ITS for Australia – 1

Proposal is practical and shows good understanding of the problem for Australia – 2

Proposal also has evidence of substantial originality & insight in the solution & implications – 3

**Communication (max 3 marks):** [core assessment]

Readable English & mostly correct reference formats – 1

Acceptable university English, mostly correct reference formats, good linkage and flow – 2

High quality English, correct reference formats, excellent layout and compelling argument – 3

## Further Guidelines

### Report Length

The recommended length of the report is 1500 – 2000 words.
The word count suggestion is not an absolute "hard limit". It is expected that you stay within these word limits, with a margin of +/- 200 words. For this report, you should include the abstract in the word count, but NOT the title and references.

### Report Structure

The structure of the report should follow the following outline. The structure of the main content, e.g. the number of sections, headings etc. is up to you. Please use meaningful headings. It is important that the report has a logical flow and is easy to read. Professional and consistent formatting is expected.

- **Abstract** (maximum 100 word summary of report)
- **Introduction**
- … (main content, headings as appropriate)
- …
- …
- **Conclusions**
- **References**

### Information Sources

A significant part of the information in the report should be based on quality sources of information, i.e. peer-reviewed scholarly journal or conference papers. Given the focus of this assignment, you might also consider some relevant quality online sources of information.

It is expected that you will find, read, understand and summarise information from relevant sources. In addition to summarising information, you need to provide your own critical discussion and analysis of the information.

You need to express the concepts and ideas in your own words. You are allowed to quote small parts of text from different sources, but this needs to be clearly identified via quotation marks, accompanied by the relevant reference.

### Referencing Style

For this assignment, you are required to use the IEEE referencing style, which is simple and widely used, in particular in the areas of Electrical Engineering and Computer Science.

### Academic Merit, Plagiarism, Collusion and Other Misconduct

You should read and understand the statement on academic merit, plagiarism, collusion and other misconduct contained within the course profile and the document referenced in that course profile. Work without academic merit will be awarded a mark of 0.

### Submission Instructions

The following items need to be submitted:

- A hard-copy of the assignment is to be submitted through the Faculty of EAIT (Hawken Building 50) assignment chute and requires a **signed assignment cover sheet**.

- You also need to submit an **electronic version** of your assignment in PDF format via Blackboard.

The submission deadline is **12:00 NOON (MIDDAY) Thursday, 4th October 2018 – both copies must be submitted**. The hardcopy will be returned to you before the revision period at the end of semester.