

# THE UNIVERSITY OF AUCKLAND

---

**SEMESTER TWO, 2017**

**Campus: City**

---

**COMPUTER SCIENCE**

**COMPSCI 725 Practice Exam**

**(Time allowed: TWO hours)**

**NOTE:** Do not write your name on your answer sheet.

The required readings for this course are listed on the back side of this question sheet.

1. (10 marks) Recall Lampson's 'restrict' strategy: "let the bad guys in, but keep them from doing damage."

Could this strategy be used to defend the password MiTM threat identified by Gelernter (2017)? Explain briefly. To receive full marks, you must identify the "bad guys", the secured area that the "bad guys" are allowed to enter, the "damage" which could be prevented, and a way in which this preventable damage could be prevented.

ATTACHMENT FOLLOWS

The following articles were on the assigned reading list this semester. They are listed in order of discussion.

- Lampson (2004) Computer security in the real world
- McReynolds (2017) Toys that listen: A study of parents, children, and internet-connected toys
- Guri (2016) SPEAKE(a)R: Turn speakers to microphones for fun and profit
- Mehrnezhad (2017) Stealing PINs via mobile sensors: Actual risk versus user perception
- Gelernter (2017) The password reset MitM attack
- Wu (2017) Automated inference on criminality using face images
- Yampolskiy (2016) Artificial intelligence safety and cybersecurity: A timeline of AI failures
- Brown (2017) Finding and preventing bugs in JavaScript bindings
- Liang (2016) An empirical validation of malicious insider characteristics
- Twyman (2015) Robustness of multiple indicators in automated screening systems for deception detection
- Baki (2017) Scaling and effectiveness of email masquerade attacks: Exploiting natural language generation
- Doty (2013) Privacy Design patterns and anti-patterns: Patterns misapplied and unintended consequences
- Jia (2016) The 'web/local boundary' is fuzzy: A security study of Chrome's process-based sandboxing
- Walker (2012) Contract cheating: a new challenge for academic honesty?