Verified Time Balancing of Security Protocols (A Case Study)

Dirk Pattinson, RSCS ANU

September 30, 2018

1 Project Summary

The aim of the protocol is to conduct a case study on the time balancing of security protocols. In the abstract, we deem a protocol to be secure, if an eavesdropper or intruder cannot infer new knowledge, based on the observation they can make during the runs of a protocol. While nearly all security protocols are proved "secure" in the abstract, their implementation adds new observations that are not captured in an abstract model. Examples are the use of random numbers to generate nonces, measurable energy consumption during the run of a protocol, and the observation of execution times during the run of a protocol.

This project focuses on the latter, and analyses time balancing of a security protocol based on a formal model. We implement, in a theorem prover, a translation from the abstract protocol into executable code, where the executable code is supplemented with timing annotations. The formal property that we aim to prove is that "an eavesdropper cannot infer any information based on timing observations during the execution of a protocol". While we cannot conduct an real-scale, industrial scale analysis (as for instance done for the TLS and other protocols in Athanasiou et. al., SideTrail: Verifying Time-Balancing of Cryptosystems, Proc. VSTTE 2018, in the context of the Amazon Web Services), our case study will be extensible to a real world setting, for example in the context of a follow-on project, by further enriching the machine model of execution.

The project outcomes are: (i) a formal specification of the protocol, (ii) a provably correct translation into a model of executable code, (iii) a timing analysis based on this model, (iv) a modification of the executable code that provably guarantees non-observability of timing, and (v) an analysis that clearly delineates the scope of our results. We will use the ZRTP protocol for this case study.

2 Project Student: Donovan Chrichton

Donovan is an Australian citizen, currently in the Honours year of a Bachelor of Information Technology at Griffith University. Within the Honours programme, his current GPA stands at 6.75 / 7. He has won an award for academic excellence in 2015, a best graduate prize in 2017, and a second award for academic excellence for his honours year in 2017/2018.

I have been in constant communication with Donovan for the past six weeks (starting mid August 2018) in the context of his Honours project on "Type Correct Genetic Programming" for which he was looking to academic guidance on theorem proving and dependently typed programming that was not available at his home institution. Our interactions did cover both abstract approaches to the representation and manipulation of Syntax (such as Higher-Order Abstract Syntax, the locally nameless representation) as well as very concrete topics of representation of formal theories in a theorem prover.

From my interactions with Donovan, I can confirm that he would be ideally placed to take up the summer research scholarship, in particular because of the following:

- Mechanics of Theorem Proving. Donovan is already familiar with both the Idris dependently typed programming environment, and the Coq theorem prover. This is a steep learning curve for most, and Donovan can start on the project immediately.

- Representation and Translation of Syntax. Within his Honours project, Donovan investigates translation of syntactical representations of programs with a view of implementing aspects of genetic programming in a theorem prover. This gives him both the abstract understanding, and the hands-on experience, to implement the envisaged translation of the abstract protocol to (a model of) executable code.

Clearly his awards and Honours GPA also commend him very highly.

3 Student Contact Details

Name	Donovan Crichton
Address	122 Kent Rd Wooloowin, Brisbane, QLD, 4030
Mobile	+61 439 542 143
Email	donovan.crichton@griffithuni.edu.au

4 Alignment with ASD Interests

This project is closely aligned with the (much larger) project "Runtime Monitoring and Verified Implementations of Security Protocols" that was considered in the first round of project proposals for ASD. The project was deemed to be of interest and recommended for re-submission and merging with a project on the analysis of security protocols in the abstract.

5 Attachments

The following are attached to this project proposal:

- Donovan's academic transcript
- Donovan's current curriculum vitae.

Donovan Crichton

Curriculum Vitae

122 Kent Rd, Wooloowin
Brisbane, QLD 4030
☎ *(+61) 439 542 143*
✉ *donovan.crichton@griffithuni.edu.au*

Education

2017–Present **Bachelor of Information Technology (Honours)**, *Griffith University*, *GPA – 6.75 ABD*.

2015–2017 **Bachelor of Information Technology**, *Griffith University*, *GPA – 5.89*.
No Major - A strong focus on computer science and artificial intelligence.

2014 **Diploma of Software Development**, *Gold Coast TAFE*.

Awards and Prizes

2017-2018 Griffith Award for Academic Excellence

2017 Griffith School of ICT Graduand of the Year

2015 Griffith Institute of Integrated and Intelligent Systems Summer Vacation Scholarship - $2000

2015 Griffith Award for Academic Excellence

Relevant Experience

Education / Instruction

2018 Tri 2 **Lab Demonstrator/Tutor**, *Griffith University*, Work Integrated Learning.
WIL is the capstone course for the Griffith Bachelor of Information Technology - This course requires engaging with students to assist them in the completion of a real information system, project management, or software development projects for an external client.

2018 Tri 2 **Lab Demonstrator/Tutor**, *Griffith University*, Foundations of Systems Development.
This is a first year course covering introductory project management, systems design, and UML.

2018 Tri 2 **Lab Demonstrator/Tutor**, *Griffith University*, Software Technologies.
This second year programming course covers real-world use of software development skills in python. Covering concepts such as version control, testing, interfacing with SQL/Spreadsheets, and GUI design. Role requires demonstration of practical concepts to reinforce content covered in lectures as well as assisting students.

2018 Tri 1 **Lab Demonstrator/Tutor**, *Griffith University*, Work Integrated Learning.

2018 Tri 1 **Lab Demonstrator/Tutor**, *Griffith University*, Programming Principles.
This is a second year introductory programming course in Python. This role involves reinforcing programming concepts covered in lectures through practical demonstrations and answering student questions.

2017 Tri 2 **Lab Demonstrator/Tutor**, *Griffith University*, Foundations of Systems Development.

Vocational

2014–2015 **Contract Research Assistant**, Queensland University of Technology, Brisbane.
Employed to develop data-analytics research tools in Python, using a Django front-end and a heavy XML component. Role also provided Linux hosting and deployment support to the multi-disciplinary team.

Notable Projects

2018 Tri 1 **A purely functional task planner**.
This was a project to develop a task planner in Haskell to parse PDDL domain and world files, and then return the first plan found given a particular search strategy. This project required the implementation of parser combinators from scratch, as well as understanding of thunk build up when using lazy programming languages.

2017 Tri 3 **Dependently-Typed Zippers over Higher Order Abstract Syntax trees**.
This was a project to implement a dependently-typed zipper over a HOAS tree in Idris. This project served as an introduction to program representation via HOAS, Huet zippers, and dependently-typed functional programming in Idris.

2017 Tri 2 **A purely functional artificial neural network**.
Implemented as a final project in an introductory functional programming course, this was implemented in Haskell using the automatic differentiation library. A working artificial neural network was implemented that could learn simple arithmetic functions.

2016 Tri 2 **Detection and Tracking of Micro-Droplets in Real Time**, *QLD Micro- and Nanotechnology Centre*.
This capstone project required the implementation of computer vision detection and tracking algorithms to detect contaminated micro-droplets. This involved organising an interface between multiple kinds of hardware devices: A high-speed custom video camera, a data-acquisition device, and a waveform generator, all interfacing through C or C++ drivers.

Programming Languages

Markup Languages

HTML	**Basic**
CSS	**Basic**
Latex	**Intermediate**

Scripting Languages

Javascript	**Intermediate**
Python	**Intermediate**
VBA	**Basic**

Imperative and Object Oriented General-Purpose Languages

C	**Intermediate**
C++	**Intermediate**
C#	**Intermediate**
Java	**Intermediate**
Swift	**Fluent**

Functional Languages

Haskell	**Intermediate**
Idris	**Intermediate**
Coq	**Basic**
SML	**Basic**

Other Languages

SQL	**Basic**

Other Technology Skills

Basic	Web Hosting, Graphic Design, Web Design, Database Creation and Maintenance, Microsoft Windows, Various IDEs
Intermediate	BASH, Vim, non-Debian flavours of Linux
Advanced	Building from source, Debian-flavours of Linux

Research Interests

- Interactive Theorem Proving
- Dependently-Typed Functional Programming
- Linear Types
- Garbage Collection In Pure Functional Languages
- Reinforcement Learning
- Symbolic Regression
- Logic
- Automatic Programming
- Artificial Intelligence
- Bio-Inspired Meta-heuristics

Griffith UNIVERSITY

Academic Transcript

Name: Donovan Jeffrey Crichton **Griffith Identification Number: 2621188** **Page 1 of 3**

DEGREES AWARDED

Award	Bachelor of Information Technology
Conferral Date	19 July 2017
Testamur	235738
AQF Recognition	This award is recognised within the Australian Qualifications Framework

ACADEMIC RECORD

Undergraduate

Bachelor of Commerce

Award Major : Accounting

Semester 1 - 2007
Bachelor of Commerce

1001MGT	Management Concepts	0CP	Fail No Assessment Submitted
1101AFE	Accounting Principles	0CP	Fail No Assessment Submitted
	Total Credit	0CP	Cumulative GPA 0.00

Bachelor of Information Technology

Semester 1 2015
Bachelor of Information Technology

Transfer Credit from TAFE Queensland Gold Coast

1001ICT	Introduction to Programming	10CP	
1004ICT	Foundations of Comp Systems	10CP	
1005ICT	Object Oriented Programming	10CP	
1007ICT	Computer Systems and Networks	10CP	
1012ICT	Communications for ICT	10CP	
1410ICT	Intro to Info Systems	10CP	
9999TRCR	Free Choice Elective	20CP	
1621ICT	Web Design and Development	10CP	6
2004ICT	System Analysis and Design	10CP	7
2402ICT	Discrete Mathematics	10CP	7
2501ICT	Programming Mobile Application	10CP	7

Semester 2 2015
Bachelor of Information Technology

1612ICT	Interactive App Develop	10CP	7
2001ICT	Project Management	10CP	6
2002ICT	Database Design	10CP	7
2508ICT	Principles of Intelligent Syst	10CP	7

Awarded Griffith Award for Academic Excellence 2015

Transcript produced on 26 September 2018

Semester 1 2016
Bachelor of Information Technology

1011SCG	Mathematics 1A	10CP	6
3530ICT	Scientific and Parallel Comput	0CP	1

Semester 2 2016
Bachelor of Information Technology

1012SCG	Mathematics 1B	10CP	6
3020ICT	Industry Affiliates Program	20CP	6
3410ICT	Professional Issues in IT	10CP	7

Trimester 1 2017
Bachelor of Information Technology

3420ICT	Systems Programming	20CP	7
3421ICT	Multiagent Systems	10CP	5

Total Credit	240CP	Program GPA	5.89

Successfully completed the requirements of the program.

Bachelor of Information Technology (Honours)

Trimester 2 2017
Bachelor of Information Technology (Honours)

6105ICT	Advanced Topics in Info Tech C	10CP	6
6106ICT	Advanced Topics in Info Tech D	10CP	7
6190ICT_P1	Honours Thesis	0CP	Continuing Grading
6190ICT_P2	Honours Thesis	0CP	Continuing Grading

Trimester 1 2018
Bachelor of Information Technology (Honours)

6112ICT	Research Methods in IT	10CP	7
6190ICT_P3	Honours Thesis	0CP	Continuing Grading
6205ICT	Advanced Topics in Info Tech A	10CP	7

Total Credit	40CP	Program GPA	6.75

Awarded Griffith Award for Academic Excellence 2017 - 2018

Undergraduate GPA 5.54

End of Transcript

GRADES AND NOTATIONS

PASSING GRADES	FAILING GRADES
Study Completed *from* 1 January 2013	Study Completed *from* 1 January 2013
7 – High Distinction 6 – Distinction 5 – Credit 4 – Pass	3 – Fail 2 – Fail 1 – Fail 0 – FNS (No assessment submitted) 0 – WF (Withdrew after final date)
Study Completed *prior* to 1 January 2013	Study Completed *prior* to 1 January 2013
High Distinction (HD) Distinction (D) Credit (C) Pass (P)	Fail Fail – No assessment submitted Withdrawn with Failure – Withdrew after final date

NOTATIONS	DESCRIPTION
CTG – Continuing Grading	To be graded in a subsequent semester/trimester
DEF – Deferred Examination	Grade to be finalised
RW – Result Withheld	Grade to be finalised
UNF – Unfinalised	Grade to be finalised
W – Withdraw	Withdrew without failure
WF – Withdrawn with failure	Withdrew after final date
NGP/NGF – Non-graded Pass/Non-graded Fail	These grades are used when the course is assessed on a Pass/Fail basis. No higher grades are awarded.
Study Completed *from* 1 January 2013	
SUP/SSP – Supplementary Assessment	Grade to be finalised
Study Completed *prior* to 1 January 2013	
SP/SS – Supplementary Assessment	Grade to be finalised
Pass Conceded (PC)	Not achieved a passing grade but demonstrated a level of performance close to that of a passing grade.

GRADE POINT AVERAGE	
To determine a Grade Point Average (GPA) calculation – see the Grade Point Average Policy. GPA's shown on an Official Academic Transcript may be recorded as:	
Career GPA	Summation over all attempts at all courses over all trimesters while the student has been enrolled at a particular career level (undergraduate or postgraduate). This summation is cumulative across programs if the student transfers between programs. The summation is cumulative when a student graduates from a program, and subsequently enrols in another program.
Program GPA	Summation over all attempts at all courses over all trimesters while the student has been enrolled in the particular program.