COMPGA11:
Research in Information Security

Steven Murdoch
University College London

based on a course by Tony Morton

Term 2 – 2014/15

Course summary

- “To develop an understanding of what research in information security is about, how to identify a contribution, what the quality standards in scientific publications are, and to study selected technical sub-topics in depth”
- “Students will be exposed to research on information security, by reading quality technical research papers in information security”
- Why?
  - Understand how to interpret and write papers
  - Read some important work in the field

Aims and outcomes

- “To develop an understanding of what research in information security is about,…
  - Understand different **research approaches** and the idea of scientific method
    - Recognise if a paper follows the principles of **scientific method**
    - If not, is there a justifiable reason
      - Not all topics naturally follow the scientific method e.g. papers describing frameworks
- Be able to read and **critically review** research literature in information security

Aims and outcomes

- ...how to identify a contribution,...
  - Be able to recognise, contextualise and evaluate a **contribution** to a field of work
- ...what the quality standards in scientific publications are,...
  - Able to identify a good (or bad) piece of scientific research and explain why
  - Understand what makes a good (or bad) academic paper

Aims and outcomes

- ...and to study selected technical sub-topics in depth.”

- Be able to carry out – independently - a literature review of a chosen topic in information security

Structure of course

- Week 21 (this lecture)
  - Introduction
  - Dissertation project presentations (1)
- Week 22
  - The scientific process
  - Dissertation project presentations (2)
- Weeks 23–31, excluding weeks 26 and 29
  - Student presentations and discussion
- Week 26
  - Reading week
- Week 29
  - Ethics (Courtois and Sasse)

Assessment

- Two information security paper reviews (20%) – 10% each
- Presentation in class (20%)
  - Including active participation in class
  - You are expected to attend all presentations and be able to discuss papers
- First iteration of literature review for MSc dissertation (60%)
- More details later…

Types of publication venue

- Journal
  - No presentations, no meetings, just article
- Symposium/conference
  - Published proceedings, presentation at event
- Pre-print
  - Little or no peer review, just article
- Book
  - Reviewed by publisher that it will sell, but not necessarily peer review
- Workshop
  - Presentation at event, perhaps no publication

Ranking of research

- There is a desire for an objective way to decide whether research is important
- Very difficult to do reliably but you will encounter such metrics in practice
- Mostly based around bibliometrics
  - Some legitimate reason for this
  - Though mostly because it can be processed automatically

Ranking publications

- Number of citations (per year)
- Why might this not reliably represent the importance of a paper?
- Why do people cite papers?
- How might people increase their citation count?

Ranking publication venue

- Thomson Reuters impact factor = A/B where
  - A: number of citations to articles published in previous two years
  - B: number of articles published
- Many problems with bibliometrics
- Venues do have a reputation, which is somewhat consistent

Ranking researchers

- "A scientist has index *h* if *h* of his/her N_p papers have at least h citations each, and the other (N_p – h) papers have no more than *h* citations each."
[An index to quantify an individual's scientific research output, J. E. Hirsch]

Steven J. Murdoch

Department of Computer Science, University College London
Security, Privacy, Anonymous Communications, Chip and PIN, EMV

Google Scholar		
Citation indices	All	Since 2010
Citations	1949	1397
h-index	19	16
i10-index	25	23

Title 1–20	Cited by	Year
Low-cost traffic analysis of Tor SJ Murdoch, G Danezis Security and Privacy, 2005 IEEE Symposium on, 183-195	413	2005
Embedding covert channels into TCP/IP S Murdoch, S Lewis Information Hiding, 247-261	238	2005
Hot or not: Revealing hidden services by their clock skew SJ Murdoch Proceedings of the 13th ACM conference on Computer and communications ...	159	2006
Keep your enemies close: distance bounding against smartcard relay attacks S Drimer, SJ Murdoch USENIX Security Symposium, 87-102	149	2007
Ignoring the great firewall of china R Clayton, SJ Murdoch, RNM Watson Privacy Enhancing Technologies, 20-35	126	2006
Sampled traffic analysis by internet-exchange-level adversaries SJ Murdoch, P Zieliński Privacy Enhancing Technologies, 167-183	120	2007
Chip and PIN is Broken SJ Murdoch, S Drimer, R Anderson, M Bond Security and Privacy (SP), 2010 IEEE Symposium on, 433-446	101	2010
Optimised to fail: Card readers for online banking S Drimer, S Murdoch, R Anderson Financial Cryptography and Data Security, 184-200	64 *	2009
Metrics for security and performance in low-latency anonymity systems SJ Murdoch, RNM Watson Privacy Enhancing Technologies, 115-132	57	2008
Thinking inside the box: system-level failures of tamper proofing S Drimer, SJ Murdoch, R Anderson Security and Privacy, 2008. SP 2008. IEEE Symposium on, 281-295	51	2008
Performance Improvements on Tor or, Why Tor is slow and what we're going to do about it R Dingledine, SJ Murdoch Online: http://www. torproject. org/press/presskit/2009-03-11-performance. pdf	49	2009

Tools and technology of Internet filtering SJ Murdoch, R Anderson Access Denied: The Practice and Policy of Global Internet Filtering, ed ...	45	2008
Verified by visa and mastercard securecode: or, how not to design authentication SJ Murdoch, R Anderson Financial Cryptography and Data Security, 336-342	41	2010
A case study on measuring statistical data in the tor anonymity network K Loesing, S Murdoch, R Dingledine Financial Cryptography and Data Security, 203-215	35	2010
Chip and spin R Anderson, M Bond, SJ Murdoch Computer Security Journal 22 (2), 1-6	34 *	2006
An Improved Clock-skew Measurement Technique for Revealing Hidden Services. S Zander, SJ Murdoch USENIX Security Symposium, 211-226	32	2008
Covert channel vulnerabilities in anonymity systems SJ Murdoch PDF Document	27	2007
Covert channels for collusion in online computer games S Murdoch, P Zieliński Information Hiding, 419-429	24	2005
Phish and Chips B Adida, M Bond, J Clulow, A Lin, S Murdoch, R Anderson, R Rivest Security Protocols, 40-48	22 *	2009
Chip and Skim: cloning EMV cards with the pre-play attack M Bond, O Choudary, SJ Murdoch, S Skorobogatov, R Anderson arXiv preprint arXiv:1209.2531	16	2012

Dates and citation counts are estimated and are determined automatically by a computer program.

Peer review

- An expert in the field reads the paper
- Time consuming, subjective and expensive
- Probably best way to achieve goals
- Used by Research Excellence Framework

Understanding a paper

- Have conclusions been properly drawn?
- Has data been collected and processed in an appropriate way?
- Were experiments done properly (if appropriate)?
- What assumptions were made?
- What other papers should you read to learn more?

Module Assessment

- You will choose a set of three papers
  - One for presentation in class
  - Two for review
- Choices are constrained for fairness and to give a diverse range of topics
- To maintain fairness, marks will be calibrated depending on:
  - Whether it is an early or a late (in the course) presentation/review
  - The difficulty of the paper

Presentations

- Presentation slides to be submitted on Moodle by **10am on day of presentation**, in PDF format

- As a minimum, you must present most important parts, principal strengths and weaknesses, ethical concerns (if any), and use (if appropriate) of the scientific method

- Maximum time: 25 minutes (will be enforced)

Presentations

- Critically engage with the paper you are presenting – Do not just summarise it
- Assume audience has taken Introduction to Cryptography and Computer Security I
- Try to present something new/interesting
- Make presentation easy to follow and engaging
- Practice alone, then practice in front of friends

Discussions

- After each presentation the class will be invited to ask the speaker questions and engage in a discussion, particularly those who reviewed the paper

- To be able to properly discuss the paper, read the abstract and conclusion of the papers being presented and skim other parts

- Say what was good about the presentations and what could be improved

Paper review

- One page (form and instructions will be on Moodle)
  - Summary of the problem and description of the contribution.
  - The best about the paper for instance new ideas, proofs, simplifications, formalizations,implementation, performance improvement, new insight, expected impact of paper on society, etc.
  - Weaknesses of the paper for instance lack of originality, small increment over previous work, unsubstantiated claims, bad presentation, insufficient discussion of relation with prior work, etc.
  - Grade (should it be accepted for publication)
- Due at 10am on day of presentation (same as slides)

Assignment of papers

		Presentations			Summaries					
	Topic	Paper 1	Paper 2	Paper 3	Paper 1	Paper 1	Paper 2	Paper 2	Paper 3	Paper 3
21										
22										
23	Crypto	1	2	3	16	17	18	10	11	12
24	General	4	5	6	19	20	15	7	8	9
25										
26	Privacy	7	8	9	1	2	3	16	17	18
27	Language	10	11	12	4	5	6	13	14	15
28	Crypto	13	14	15	7	8	9	19	20	5
29										
30	General	16	17	18	10	11	12	1	2	3
31	Privacy	19	20		13	14	6	4		

- You must do one presentation and two paper summaries
- All must be on different topics
- Choose a number and select from Doodle poll, available Tuesday 2pm

Literature survey

- The aim of a literature review (sometimes called a literature survey) is to demonstrate to the reader that you have read and understood the main published work concerning a particular topic, and can summarise it, and objectively and critically review it.

Literature survey

- Due Thursday April 30th 2015 at 5pm (but remember exam preparation)
- Can be about topic of your MSc Information Security dissertation
    - Cannot be copied into your dissertation, but will be a useful foundation
    - If dissertation is done by a pair, so can your survey
    - 20 pages (individual) or 35 pages (pair)
- Otherwise can be on topic of one paper presented in course

Dissertation projects

- You need to **choose your project topic by 30 January 2015**

- Submit dissertation by 1 September 2015 (but don't forget exams)

- Details on COMPGA99 Moodle, along with list of proposed projects

- Today and next week there will be presentations from some potential supervisors