COMPGA11: Research in Information Security

Steven Murdoch
University College London

based on a course by Tony Morton
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 Friday (this lecture)
  - Introduction
  - Dissertation project presentations (1)
- Week 22 Monday
  - The scientific process
  - Dissertation project presentations (2)
- Weeks 22–29 Fridays, excluding weeks 25 and 29
  - Student presentations and discussion
- Week 25 Friday
  - Reading week – no lecture
- Week 29 Friday
  - Ethics (Courtois)
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

<table>
<thead>
<tr>
<th>Title</th>
<th>Cited by</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low-cost traffic analysis of Tor</td>
<td>413</td>
<td>2005</td>
</tr>
<tr>
<td>Embedding covert channels into TCP/IP</td>
<td>238</td>
<td>2005</td>
</tr>
<tr>
<td>Hot or not: Revealing hidden services by their clock skew</td>
<td>159</td>
<td>2006</td>
</tr>
<tr>
<td>Keep your enemies close: distance bounding against smartcard relay attacks</td>
<td>149</td>
<td>2007</td>
</tr>
<tr>
<td>Ignoring the great firewall of china</td>
<td>126</td>
<td>2006</td>
</tr>
<tr>
<td>Sampled traffic analysis by internet-exchange-level adversaries</td>
<td>120</td>
<td>2007</td>
</tr>
<tr>
<td>Chip and PIN is Broken</td>
<td>101</td>
<td>2010</td>
</tr>
<tr>
<td>Optimised to fail: Card readers for online banking</td>
<td>64*</td>
<td>2009</td>
</tr>
<tr>
<td>Metrics for security and performance in low-latency anonymity systems</td>
<td>57</td>
<td>2008</td>
</tr>
<tr>
<td>Thinking inside the box: system-level failures of tamper proofing</td>
<td>51</td>
<td>2008</td>
</tr>
<tr>
<td>Performance Improvements on Tor or, Why Tor is slow and what we're going to do about it</td>
<td>49</td>
<td>2009</td>
</tr>
</tbody>
</table>

Tools and technology of Internet filtering
SJ Murdoch, R Anderson
Access Denied: The Practice and Policy of Global Internet Filtering, ed ...

Verified by visa and mastercard securecode: or, how not to design authentication
SJ Murdoch, R Anderson
Financial Cryptography and Data Security, 336-342

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

Chip and spin
R Anderson, M Bond, SJ Murdoch
Computer Security Journal 22 (2), 1-6

An Improved Clock-skew Measurement Technique for Revealing Hidden Services.
S Zander, SJ Murdoch
USENIX Security Symposium, 211-226

Covert channel vulnerabilities in anonymity systems
SJ Murdoch
PDF Document

Covert channels for collusion in online computer games
SJ Murdoch, P Zieliński
Information Hiding, 419-429

Phish and Chips
B Adda, M Bond, J Clulow, A Lin, S Murdoch, R Anderson, R Rivest
Security Protocols, 40-48

Chip and Skim: cloning EMV cards with the pre-play attack
M Bond, O Choudary, SJ Murdoch, S Skorobogatov, R Anderson

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: 10 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

- You must do one presentation and two paper summaries
- All must be on different topics
- Choose a number and select from Doodle poll, available tomorrow (Saturday 16th) at 6:30pm; Please complete by 6pm Monday 18th
- [http://sec.cs.ucl.ac.uk/users/smurodch/teaching/compga11allocation.html](http://sec.cs.ucl.ac.uk/users/smurodch/teaching/compga11allocation.html)

<table>
<thead>
<tr>
<th>Date</th>
<th>Week</th>
<th>Presentation</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>22-Jan</td>
<td>21</td>
<td>1 2 3 4 5 6</td>
<td>7 8 9 10 11 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13 14 15 16 17 18</td>
<td></td>
</tr>
<tr>
<td>29-Jan</td>
<td>22</td>
<td>19 20 21 22 23 24</td>
<td>25 26 27 28 29 30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>31 32 33 34 35 36</td>
<td></td>
</tr>
<tr>
<td>05-Feb</td>
<td>23</td>
<td>37 38 39 40 7 8</td>
<td>1 2 3 4 5 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 10 11 12 13 14</td>
<td></td>
</tr>
<tr>
<td>12-Feb</td>
<td>24</td>
<td>15 16 17 18 25 26</td>
<td>19 20 21 22 23 24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>37 38 39 40 41 42</td>
<td></td>
</tr>
<tr>
<td>19-Feb</td>
<td>25</td>
<td>Reading week</td>
<td>15 1 2 3 4 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 7 8 16 18 19</td>
<td></td>
</tr>
<tr>
<td>26-Feb</td>
<td>26</td>
<td>9 10 11 12 13 14</td>
<td>20 21 22 23 24 25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>33 34 35 36 41 42</td>
<td></td>
</tr>
<tr>
<td>04-Mar</td>
<td>27</td>
<td>27 28 29 30 31 32</td>
<td>17 26 27 28 29 30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>31 32 39 40 37 38</td>
<td></td>
</tr>
<tr>
<td>11-Mar</td>
<td>28</td>
<td>33 34 35 36 41 42</td>
<td>17 26 27 28 29 30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>31 32 39 40 37 38</td>
<td></td>
</tr>
<tr>
<td>18-Mar</td>
<td>29</td>
<td>Ethics</td>
<td>15 1 2 3 4 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 7 8 16 18 19</td>
<td></td>
</tr>
</tbody>
</table>
To select which papers you will present and review, choose a number between 1 and 42 from the allocation spreadsheet.

**Week 21: 22/01/2016**

**Integral Cryptanalysis on Full MISTY1**  Yosuke Todo


Blocking-resistant communication through domain fronting  David Fifield*, Chang Lan, Rod Hymers

Wu, Zhenyu, Zhang Xu, and Haining Wang. Whispers in the Hyper-space: High-speed Covert Communication

A Human Capital Model for Mitigating Security Analyst Burnout  Sathya Chandran Sundaramurthy, Ou, and Michael Wesch, Kansas State University; John McHugh, RedJack, LLC.; S. Raj Rajagopalan

Geambasu, Roxana, et al. Vanish: Increasing Data Privacy with Self-Destructing Data. USENIX Security Assessing Deceptive Advertisement Modifications Kurt Thomas (Google), Elie Bursztein (Google), Oded McCray (Science Institute, Databricks), Grant Ho (UC Berkeley), Nav Jagpal (Google), Alexandros Kapravelos (UC McCoy (International Computer Science Institute, George Mason University), Antonio Nappa (International Computer Science Institute, UC Berkeley), Paul Pearce (UC Berkeley), Niels Posegaard (Google)


Robust Authenticated-Encryption AEZ and the Problem that it Solves Viet Tung Hoang1,2 Ted Krovetz1,2


Crowdsourcing Attacks on Biometric Systems, Achintya Prakash
Week 26: 26/02/2016

Under-Constrained Symbolic Execution: Correctness Checking for Real Code


Phoneypot: Data-driven Understanding of Telephony Threats


Cryptanalysis of the Multilinear Map over the Integers

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 28th 2016 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 2016**
• Details on COMPGA99 Moodle from tomorrow, along with list of proposed projects
• Today and next week there will be presentations from some potential supervisors
• Next week you will submit preferences for topic and supervisor