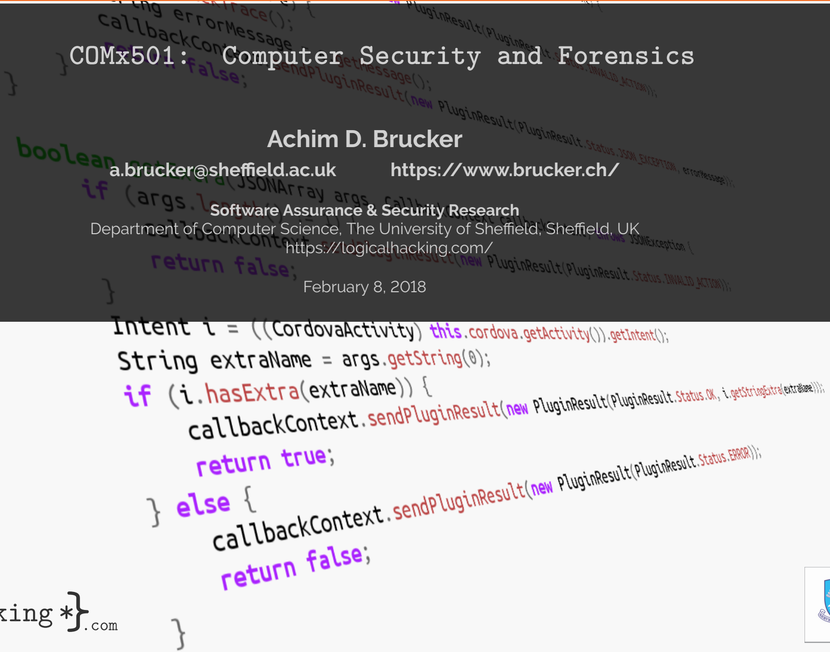
COMx501: Computer Security and Forensics

Achim D. Brucker

a.brucker@sheffield.ac.uk **https://www.brucker.ch/**

Software Assurance & Security Research
Department of Computer Science, The University of Sheffield, Sheffield, UK
https://logicalhacking.com/

February 8, 2018



```
Intent i = ((CordovaActivity) this.cordova.getActivity()).getIntent();
String extraName = args.getString(0);
if (i.hasExtra(extraName)) {
    callbackContext.sendPluginResult(new PluginResult(PluginResult.Status.OK, i.getStringExtra(extraName)));
    return true;
} else {
    callbackContext.sendPluginResult(new PluginResult(PluginResult.Status.ERROR));
    return false;
}
```

{* LogicalHacking *}.com

The University Of Sheffield.

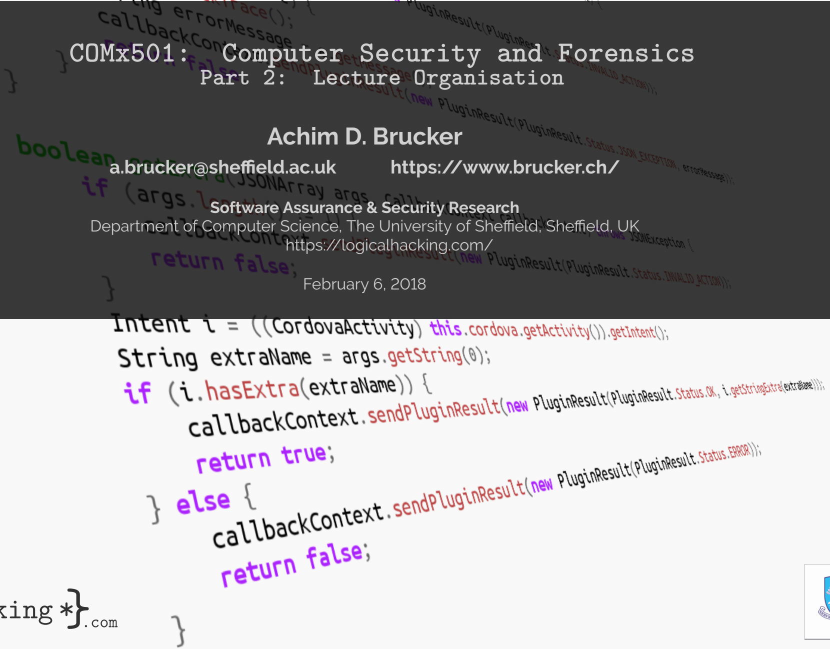
COMx501: Computer Security and Forensics
Part 2: Lecture Organisation

Achim D. Brucker

a.brucker@sheffield.ac.uk **https://www.brucker.ch/**

Software Assurance & Security Research
Department of Computer Science, The University of Sheffield, Sheffield, UK
https://logicalhacking.com/

February 6, 2018



```
Intent i = ((CordovaActivity) this.cordova.getActivity()).getIntent();
String extraName = args.getString(0);
if (i.hasExtra(extraName)) {
    callbackContext.sendPluginResult(new PluginResult(PluginResult.Status.OK, i.getStringExtra(extraName)));
    return true;
} else {
    callbackContext.sendPluginResult(new PluginResult(PluginResult.Status.ERROR));
    return false;
}
}
```

{* LogicalHacking *}.com

The University Of Sheffield.

Changes & Updates

Compared to last year:

- no changes in the learning objectives
- changes based on student feedback
  - two MOLE quizzes (weight: 15% each)
  - weight of exam reduced to 70% (and less time)
  - update of content
  - problem sheets contain repetition of material from the preliminaries

General recommendations

  - Do the problem sheets – they are a collection of mock exam questions!
  - Prepare the tutorial-style sessions!
  - Do the labs – they help you to understand the theory!
  - Do ask questions (in the lecture, forums, or personal)!

How this module is taught

- Three types of “events”
  - **Lectures:** presenting new content, i.e., extending your knowledge
    - usually a two hours block on Tuesdays
    - usually contains a small practical demonstration
  - **Tutorials:** deepen your knowledge by discussing problems from the problem sheets
    - usually a one hour block on Thursdays
    - you will only benefit, if you tried to solve some problems yourself!
  - **Labs:** deepen your knowledge doing practical exercises
    - two sessions of two hours on Monday
    - planned dates for COM3501: weeks 6 and 10
    - planned dates for COM4501/601: weeks 7 and 9
- Again: problem sheets are important!
- MOLE discussion boards for
  - general questions about the lecture
  - discussing homework
  - discussing emerging security topics
  - suggesting improvements

Lecture slides

Lecture slides for the week

- Will be uploaded to MOLE on Tuesday morning 9am (latest)
- May contain [1] ________ words (cloze-style)

Problem Sheets

- Problem sheets serve several purposes:
  1. extend and deepen your knowledge of the subject
  2. provide a set of “mock” questions similar to the MOLE quizzes (multiple choice) and exam
  3. provide detailed references (reading list) on a per-chapter level
     (I tried my best to only refer to freely available material/books)
  4. help you to catch up on preliminaries
- Exercises carry one of the following labels:
  - **COM[346]501:** relevant to exam/quizzes for COM3501, COM4501, and COM6501
  - **COM[46]501:** relevant to exam/quizzes for COM4501, and COM6501
  - **Repetition:** exercises discussing preliminaries
    (You might know this already, if not, these exercises will help you to catch up.)
  - **no exam:** exercises that cover areas that will not be asked in MOLE quizzes or exams. Usually, they contain practical exercises that you can do on your computer. While they help you to deepen your knowledge, they are not suitable for examination.
- Problem sheets will be uploaded to MOLE on Friday morning
- Solutions (not necessarily for all questions/problems)
  - will usually be presented the following Thursday
  - should be discussed in MOLE
- Remember: Problem sheets are important!

Labs

Two labs

- Two labs:
  - formal (logic-based) analysis of security protocols
  - secure programming and security testing

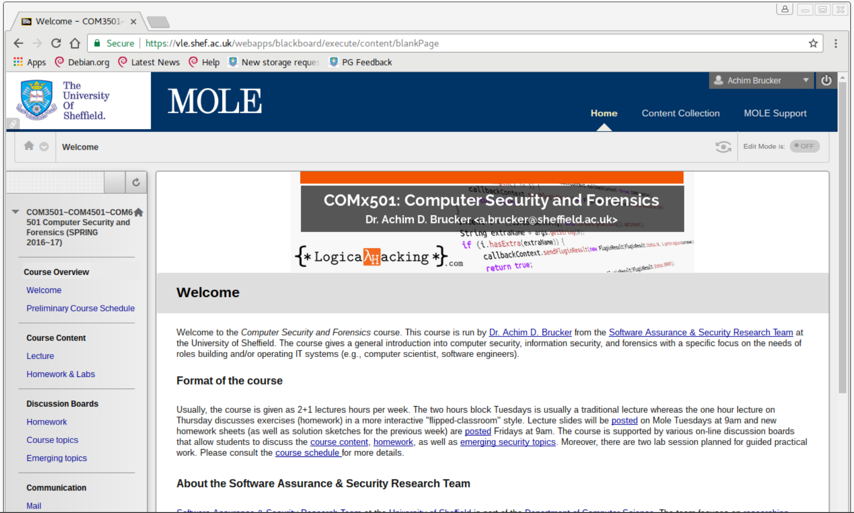
  Labs will be offered in two groups (COM3501 and COM[46]501) to provide more individual help/feedback
- each lab will be a 2 hours block (Monday)
- topic will be prepared in lectures and homework
- lab in the computer room to develop practical experience
  (and get direct feedback/help from lecturer/demonstrator)

Assessment

Two components:

- Two homework-style MOLE quizzes (each contributes 15%)
- Exam (contributes 70%)
  - $1\frac{1}{2}$ hours for COM3501
  - 2 hours for COM4501 & COM6501
- Questions will be similar to questions on problem sheets

MOLE



Welcome

Welcome to the *Computer Security and Forensics* course. This course is run by Dr. Achim D. Brucker from the Software Assurance & Security Research Team at the University of Sheffield. The course gives a general introduction into computer security, information security, and forensics with a specific focus on the needs of roles building and/or operating IT systems (e.g., computer scientist, software engineers).

Format of the course

Usually, the course is given as 2+1 lectures hours per week. The two hours block Tuesdays is usually a traditional lecture whereas the one hour lecture on Thursday discusses exercises (homework) in a more interactive "flipped-classroom" style. Lecture slides will be posted on Mole Tuesdays at 9am and new homework sheets (as well as solution sketches for the previous week) are posted Fridays at 9am. The course is supported by various on-line discussion boards that allow students to discuss the course content, homework, as well as emerging security topics. Moreover, there are two lab session planned for guided practical work. Please consult the course schedule for more details.

About the Software Assurance & Security Research Team

Software Assurance & Security Research Team at the University of Sheffield is part of the Department of Computer Science. The team focuses on researching

I Have a Question (How to Get Feedback)

Please ask

- During the lecture/tutorials/labs:
  - raise your hand or contact me in the break!
- During the week:
  - Check the MOLE boards, the question might already be answered
  - If not, post a new question on MOLE
    - while you there, check if you can help a fellow student
    - I will check MOLE at least once a day
  - If you feel you question is personal/confidential
    - Catch me after the lecture (or in a break)
    - Send me an email
      (if the question is of general interest, I will ask you to post it on MOLE)

Disclaimer: Module Content

This module is about **Computer Security** (not Cyber Security):

- Computer Security $\subseteq$ Cyber Security
- You will need to work with
  - Set theory and logic
    - $x = \{x \mid x \in Y \wedge \exists z > x.\, z \bmod 3 = 0\}$
    - $x \oplus y = x \wedge \neg y \vee \neg x \wedge y$
  - Natural deduction:

$$\frac{\{m\}_k \in \mathcal{DY}(M) \quad \mathrm{inv}(k) \in \mathcal{DY}(M)}{m \in \mathcal{DY}(M)}\,\mathrm{DecAsym}$$

  - Basic algebra
    $a^{n+m} = a^n \cdot a^m$
- Solid knowledge of one programming language
  we will use Ruby (lab) and Java (exam, problem sheets)

Tips:

- Work on the problem sheets (note the repetition exercises)
- Check last years exam and the mock exam

Legal Disclaimer

You need to be aware that

- applying security analysis or security testing techniques may harm the system under test (e.g., its availability, stability, security)
- only test your own systems or systems for which you have an explicit a written permission from the system owner and the owner of all intermediate infrastructure (i.e., network operator)
- what you are allowed to do, is limited in many ways, e.g., by laws, industrial regulations, user agreements
- any form of offensive security analysis (i.e., attacking systems)
  - within (e.g., system that are part of the university network) or
  - from (e.g., systems outside the university network) the university network

  is strictly forbidden.

Thank you for your attention!
Any questions or remarks?

Contact:

Dr. Achim D. Brucker
Department of Computer Science
University of Sheffield
Regent Court
211 Portobello St.
Sheffield S1 4DP, UK

a.brucker@sheffield.ac.uk
@adbrucker
https://de.linkedin.com/in/adbrucker/
https://www.brucker.ch/
https://logicalhacking.com/blog/

Cloze Solutions

1. missing

Document Classification and License Information

- This presentation is classified as *Student (COMx501 – 2017/18)*:
  Except where otherwise noted, this presentation is classified "*Student (COMx501 – 2017/18)*" and only available to students of the University of Sheffield that are registered to the module "COMx501: Computer Security and Forensics" in the academic year 2017/2018. Disclosure to third parties only after a confidentiality agreement has been signed.