Introduction

Advanced Topics in Cybersecurity (7CCSMATC)

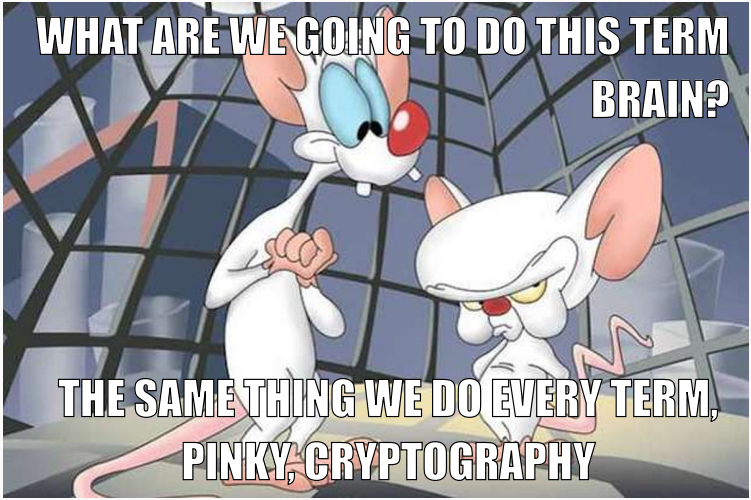
Martin R. Albrecht

Learning Aims & Outcomes (Formal / Every Year)

To engage with advanced topics in cybersecurity through contemporary academic literature and practice, with, for example, a focus on specific areas in cryptography, systems security, formal methods or usable security and key application domains that make use of these areas.

1. Describe and explain foundational concepts and definitions of an advanced, emerging area in cybersecurity.
2. Analyse and critique cutting edge research in an emerging area of cybersecurity.
3. Apply the key concepts and definitions of this area of cybersecurity in the solution of problems within that area.
4. Describe and explain open problems and existing challenges related to this area of cybersecurity.

This Year


WHAT ARE WE GOING TO DO THIS TERM BRAIN?
THE SAME THING WE DO EVERY TERM, PINKY, CRYPTOGRAPHY

Introduction

Advanced Topics in ~~Cybersecurity~~Cryptography (7CCSMATC)

Martin R. Albrecht

Learning Aims & Outcomes (Informal) I

Introduce you to “how cryptographers think”: how we reason about computational and communication security to build the foundations of information security.

Learning Aims & Outcomes (Informal) II

Modern cryptography, dating back to the mid 80s, brought with it a paradigm shift:

- away from common attack-then-repair cycles where attackers test if a system is secure and give up after a while,
- towards formal definitions of security, models of adversaries and security proofs.

Learning Aims & Outcomes (Informal) III

- What does it even mean for some scheme to be secure?
  - What does it mean for a block cipher to be secure?
  - What does it mean for an encryption scheme to be secure and are they the same thing?
  - Is there such a thing as a correct definition of security?
  - Is "post-compromise security" the thing you expect it to be?
  - How do cryptographers decide on these security notions?
- Cryptography is full of wonderful and sometimes wild ideas on how to reason about security.
  - We will cover the "Random Oracle Model", a model that is obviously not true, we even have a formal proof that it is false, yet it underpins the security of the Internet.
- We will talk about cryptography in light of the threat of quantum computing.
  - We will discuss how quantum devices are not faster but different to classical computers.
  - So different, in fact, that even our definitions of what it means to be secure will need to change, not just the algorithms we use to protect communication.

Practicalities

Level	7 (CS MSci)
Credits	15
Assessement	2x coursework (50% each)
Office hour	Mondays, 3pm, arrange via e-mail
Office	Bush House BH(N)7.02
E-mail	martin.albrecht@kcl.ac.uk

Keats

- links to slides,
- references to reading material,
- announcements
- discussion forum

Lunch / Schedule

This lecture is awkwardly scheduled. I suggest we work with this as:

- Block 1: 12:00 to 13:15
- Lunch break
- Block 2: 13:45 to 14:50

Any counter proposals?

The Whiteboard

- I might and hopefully will jump the whiteboard to discuss questions, proofs etc.
- The whiteboard is not captured by the recording
- You should bring something to write to note down the contents of the whiteboard

These Slides

If we find typos/mistakes in these slides I aim to uploaded corrected slides soon after the lecture.

Prerequisites: Content

- This is an **advanced module**,
  so I will assume you took 6CCS3CIS (Cryptography)
- This is an **module on advanced topics in cryptography**,
  so I will casually use concepts from mathematics and theoretical computer science

Mathematical Prerequisites I

You should be comfortable with material that is standard in a introduction module on discrete mathematics, including:

basic discrete objects functions (injective/surjective), sets and set operations (union, intersection, Cartesian product), tuples, strings, concatenation;

simple combinatorics counting objects as 2^n, $\binom{n}{2}$, ...;

discrete probability union bound, principles of multiplication & addition, conditional probabilities;

logic boolean operators, implications, contrapositive, quantifiers;

induction and recursive definitions of functions;

rules of exponents and logarithms $2^x \cdot 2^y = 2^{x+y}$ etc;

linear algebra vector spaces, matrices, determinants, etc;

basic modular arithmetic addition, subtraction, multiplication, idempotence of modular reduction: e.g. $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$.

basic number theory multiplicative modular inverses, Chinese remainder theorem, finite fields, etc.

$\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{Z}_N$, $\mathbb{R}$, $\mathbb{C}$ ...

Computer Science Prerequisites

flow control if/while/foreach constructs;

variables types and scope, especially the idea of scopes that are inaccessible from certain blocks of code;

information dependency when does one value/variable influence another?

simple data structures sets, arrays, associative arrays, strings;

subroutines calling principles, factoring out lines of code into a subroutine, inlining subroutine calls, recursion.

complexity theory polynomial-time vs NP, ...

abstract thinking about computation theory of computing, algorithms, etc.

Prerequisites: Perspective

- This is an **optional module**,
  so I will assume you want to be here.
- This is advanced topics in **cryptography** and not fundamentals of computing.
  - I will expect that you reach for a textbook to learn/recap fundamental concepts you are not/no longer familiar with.
- This is an **advanced topics** module,
  so you will be required to read research papers to fully understand some of the ideas discussed here.
  - Indeed, if I get you to be able to read cryptographic research papers, I consider this module a success.

Prerequisites: Approach

- I will routinely give you literature to read in preparation for a lecture.
  - This will be announced on KEATS.
- I will assume that literature as read.
- But I will not assume that literature as understood.
  - That's what the lectures/sessions/seminars are for.
- I will give you references to the literature and usually neither links nor PDF copies on KEATS.
  - A point of this module is for you to be able to digest the literature, being able to find it is a trivial first step.

Prerequisites: Assessment

- I have published the assignments, take a look to understand what this module expects.
- You are welcome to crack on with these relying on textbooks and research papers.
- If you show up to the lectures, I assume you want to be here.
- I will try to make it clear if a lecture/session is particularly relevant to the assignments.

Level, Feedback & Help

- This is the first time this module is running, it is meant to be **advanced** and thus challenging, but not a pointless **grind**.
- I will rely on your regular and timely feedback to adjust the level of the module as we go along.
- Help me out here!
  1. Ask questions/give feedback during the lectures
  2. Ask questions/give feedback on the discussion forums
  3. Ask questions/give feedback in an e-mail to me
  4. Ask questions/give feedback in my office hours

Speed

- I tend to assume that my audience follows along and I speak quite fast.
- This is bad!
- Help me to slow down, ask questions, ask me to repeat, rephrase
- Let’s make this interactive.

Let's go!