COMP6441 Lecture 8

Youhan Cheery

24 April 2017

1 Introduction

- You can never prove something is secure - you can only prove the algebra is secure!
- Need to formalise the right properties, the right axioms from which we can build a proof.
- Can never trust "top men" but you can trust the process, the thoroughness of the system and the foundations upon which the system is built and so on.
- Everything needs openness and scrutiny.

2 Points of Security

- How much work does a person need to do to beat the system, measured in points.
- A system worth 50 points is harder to break into through brute force than a system with 20 points of security.
- Logarithmic scale only cares about the number of digits of work. Allows insensitivity to the actual number.
- 50 questions to ask on average to break a system. As a binary (logarithmic) number this is 6 (the number of binary digits needed to express 50).

3 RSA

- Two ways to introduce complexity:
  1. AES does a lot of complicated things in a very systematic way. With all the mixing it is very difficult to un-mix
  2. Piggy-backing on an existing system that is already exceptionally complex, such as the prime numbers in mathematics

- In RSA we use the difficult to break down large numbers into their prime counterparts as a means of encrypting a system.
- We first pick a number, and raise it to some prime power and modulo it by some prime number.
- How do you prevent collisions? If the power you're raising to is co-prime with the number you are modulating by. The number you're modulating must also be a prime. It can be a non-prime, but as long as the power we're raising to has to have no common factors with its prime composites minus 1.
- If the number modding is not a prime, then we can go backwards using the Chinese Remainder Theorem.
- We start by picking 2 prime numbers, multiplying them and creating the number n.
- To go back, we simply raise it again to some power.
- Breaking down n is exceptionally hard. This is what makes RSA so difficult to crack.
- To get decryption key, use $\phi(n) = (p-1)(q-1) = m$. We need a number such that e (that you raise to the power) multiplied by that number gives you m.
- e is chosen such that $gcd(e, \phi(n)) = 1$. That is, they share no common factor.

4 Misdirection

- Misdirection is the art of making people not look where they should be looking when they should be looking at it. This is what social engineering is built upon.