Morning:

Sharing a secret for future communication

* **Diffie Hellman:** how can you and I establish a secret that no-one else knows if we are on the other side of the world?
  + How to share a secret: (5^3)^7 = …..125
    - (5^7)^3 = ……125 since (a^b)^c = a^(bc) = (a^c)^b
    - Mod 1000
  + Share a base. Each choose a base. Each raise the base to your power and share the result. Take the others raised number and raise it to your power and mod it. The result is your key.
  + Eavesdroppers know a^b and a^c. But not b or c. When you use large enough numbers, you can’t simply work out b and c by observation. The picture explains it well

Back to Vulnerabilities and Exploits:

**Memory Corruption:**

* Stack -> working memory, LIFO
* Heap -> less controlled, more dynamic memory
* Instruction pointers return address are stored on the stack
* Buffer overflow and integer overflow
* Format strings:

Evening:

Bug Bounties:

* Bug bounties are when you look for bugs in code and notify the relevant company about them in return for a reward. You submit a detailed report.
* Tips:
  + Whenever there’s a big software update -> integration errors and more chance to find bugs
  + Looking through prior reports for a bug -> ^ chance of recurring problem
* ‘Fuzzing’ – to help detect your bugs
* How to fuck a Mac: hold command + S while booting & remove the user file. Then create a new super user account from which you can change the password of other users.
* Slides Tutorial for Fuzzing. (software – AFL)

Penetration Testing:

* Authorised attack on a system to evaluate security risks
* Involved in a holistic risk assessment
* E.g. let someone try to break into your house
* For discovering vulnerabilities, test existing defence controls (firewalls, etc), exposing weaknesses
* Pen-testing tools: prevent you from writing all the tests someone else has already done
  + NMAP – what ports are open on your system, network probing tool
    - Open ports may be vulnerable to listening to attacks
  + KALI – includes tools for pretty much every kind of attack
  + METASPLOIT – installing this will make your anti-virus upset since it’s a kit of hacking tools
  + GOBUSTER
* CTF websites on the slides

Content:

* Read about the homework from Richards lecture slides
* Diffie Hellman doesn’t give us authentication – only 1 person in the world will know how to securely communicate with me, but I don’t know who it is
* How can we do authentication on the internet without any per-shared secrets
  + Shop publishes a public key -> in the message I send them a key
    - 1 sided authentication
  + But then a hacker can just make a fake website with the fake public key -> how do we know that the public key on the website is the real public key of the company and wasn’t put there by a hacker
  + Man in the middle: I have the MIM’s public key and MIM has mine and the Shops. The shop has the MIM’s who is distributing and intercepting and encrypting and re-encrypting.
  + Protocol for how to prevent man in the middling:
    - PgP – to read about (web of trust)
    - PKI;

(Public Key Infrastructure): solves the man in the middle problem but not much else

* SSL/TLS: Bruce Schneider’s paper
* Links your public key to something (like a passport linking a photo with a name) that is certified by something the everyone trusts
  + X509 certificates -> link your public key to a webdomain
    - Certificates are signed for integrity
      * Easier to know the relatively small number of public keys of legitimate signers
    - Check the signature on the certificate with that on the browser
* Problem: computer doesn’t know anything about the real world - > only that it’s the correct domain name. People often set up fraudulent websites with similar names to the real one’s
* Lots of examples of problems on the lecture slides
* Padlocked only means the person who owns this website is the person with that domain, not that it’s the person in the real world
* Extended verification – extra required information from the applicant to get a certificate
* Self-signed: not checked by root certificate.
* Formal homework:
  + TLS HANDSHAKE
  + Fraudulent certificates being issued examples