**One-time Pads**

**One-time pad** is a type of encryption which has been proven to be impossible to crack if used correctly.

* Each bit or character from the plaintext is with a character from a secret random key (or pad) of the same length as the plaintext, resulting in a coded message.
* If the key is truly random, with a **size >= than plaintext**, **never re-used in whole or part** and **kept secret**, the coded message will be impossible to decrypt or break without knowing the key.

**XOR: Exclusive-Or binary operator**

* It is something that can be done really fast with minimal computing power
* XOR jumbles things up
* If you XOR number A with number B, if either of the numbers are random then the output is random.

**One-Time Encryption**

* Encrypting “I love you” (8 characters) with 1, 5, 7, 13, 8, 2, 6, 4.
* ENCODED MESSAGE: J – Q – V – I – M – A – U – Y
* If **the key was thrown away (hence ONE-TIME PAD)**, it would be impossible to crypt-analyse this encoded message to get the plaintext
* Any cipher text can correspond to any plain text.
* Things like Entropy / English language patterns become completely irrelevant

**One-time pad problems**

* It’s based on a secret
* Key distribution / distributing the one-time pads
* Most of the time, they were eventually cracked because of the way the keys were being generated which allowed them to be crypt-analysed or just stupid / lazy ways to generated the keys which made it crackeable or re-using the same pads if they “ran out of ways” to generate keys.
* Problem with OTP: If you were ever able to know a plaintext corresponding to a ciphertext, you would know all the random numbers and if those random numbers were re-used again, you would be able to instantly crack that message.
* There were bugging rooms where the Russians were sending messages and using the sound of the keys to detect which were being done. As the random numbers were being generated, they were able to intercept them because of that.  
  **^ Side-channel attack example**

**Number stations**

* A shortwave radio station characterised by broadcasts of formatted numbers, which are believed to be addressed to intelligence officers operating in foreign countries.
* There are hundreds of real stations in different voices and have been running / used for decades and even being used by spies today still.

**Distributing OTP’s with other methods**

* Steganographically: E.g. YouTube distributes a large volume of 1’s and 0’s and you could just synchronise any YouTube video
  + **Steganography**: Practise of concealing a file, message, image or video within another file, message, image or video.
* There are a lot of interest channels and ways to distribute a large number of bits if you wanted to synchronised with other people. However, if you do this over an open channel, it is risky and you’re relying on security by obscurity and as soon as someone figures / works out your bits then your OTP is useless.

**Threats**

**Threats:** Attacks and attackers

**Threat Model:**

* A notion of who your attacker is
* What sort of attacker that you’re likely to have
* What sorts of attacks you’re trying to defend against

Threats are where attacks come from and the nature of possible attacks

**We need to be the sort of security engineers where we understand both the TALK and the TECH**

* It is important to understand what you are defending against

**Building a Threat Model Intro**

* Threat mode: When someone says you need to defend this, you try to work out “do I need to defend this against the NSA?” or “do I need to defend this against the Russian mafia?” or “do I need to defend this against a random little kid?”
* **WHO IS IT THAT I AM DEFENDING AGAINST?**
* This is worth noting because I want to know how much money to spend and go to different degrees of trouble depending on the attacker.
* Pentesters may say: “threat modelling is a waste of time, who cares where threats come from? We just need to know what weaknesses a system has. Our job is to find ALL weaknesses”
  + This is true to a certain degree as Pentesters find weaknesses and the don’t care what attacker they’re up against, they just care what weaknesses a system has
  + However, suppose you have a system and you’re a defender and the system is riddled with weaknesses. If you have a pentester come in, they’ll find a hundred of your zillion weaknesses.
  + However, you **cannot defend and patch every single weakness unless you have an infinite amount of resources at the time**.
  + So you have to make a really hard decision to **determine which weaknesses to focus on**.

**STEP 1: Building a Threat Model**:

* A Threat Model is a systematic approach to list out the possible sources of attacks / problems and where they may come from.
* Consider the **motives** of the possible adversaries (even though pentesters says otherwise)
* Think about **what the adversaries can gain** from the asset that is protected
* **SYSTEMATIC APPROACHES**
  + **Prioritising** your sources of attack and categorising your list.
  + **Threat Tree / Attack Tree**:
    - Assets are nodes
    - Threats are branches
    - Causes for those threats can be sub-branches
    - Used for enumerating the threat
    - Need to think of the boring sources of threat as well as **Hollywood-Style attacks**  
      (to avoid focusing too much attention on one threat and ignoring the others)

**STEP 2: Enumerate Threats (Analysing, Understanding)**

* Start with the assets at the top level.
* Look at attacks / threats on the assets.
* Start with broad categories and then slowly become more specific.

You keep drawing more and more trees out, not to be exhaustive, but you’ll think of more breakdowns and branches that you haven’t thought of previously. You’re doing it just to get as many ideas as possible, of ways something can be attacked.

**If you don’t do this, you’ll just think of only the OBVIOUS source of attack and you will only focus on those.**  
(**Hollywood Scenarios:** worry about things that they always worry about in Hollywood, but forget about the boring things)

Find Written Combination (I)

Install Improperly (I)

Cut Open Safe (P)

Pick Lock (I)

Get Combination from Target

Open Safe

Learn Combo

P = Possible

I = Impossible

Get Target to State Combo (I)

Listen to Conversation (P)

Bribe (P)

Eavesdrop

Blackmail (I)

Threaten (I)

Work out things in advance.

Try to work out sources of attack coming at us and the best way of dealing with them.

Dealing with them when we are actually IN the situation = it is unlikely that we’ll do the optimal thing.

We want to think of all our attacks in advance before we spend out money and before we allocate our resources.

If you’re a soldier and you walk into the middle of a minefield and you suddenly realise this, what should you do?

* You shouldn’t start think about this when you’re standing in the middle of the minefield
* You’ll always think of better solutions and think about things more carefully / analytically / wisely if you **think about things in advance**.
* The army has worked out standard ways of dealing with problems and soldiers know it.
* If you walk through a minefield and suddenly someone realises that they’re in a minefield, you stay still and you re-trace the steps, as closely as possible back to where you came from.

What if you’re a soldier and you suddenly get ambushed?

* You run towards the people ambushing you rather than running away, because ambushes are set up to wait for you to run away into a perfect position so that they can get maximum shooting time.

What do you do if you’re ambushed in a minefield?

**Let ideas flourish during a brainstorm (suppress the critical part, where you deny ideas / say no to them) so that you can generate a lot of ideas**. **Killing ideas too soon is a bad thing**. **Criticise once you have completed brainstorming.**

* The reason for Possible and Impossible tags in the tree above, is that you still want to insert the idea into the tree and tag it rather than take it out entirely which can be bad.

**Incidence Response**: What do people do when an attack happens?

* 9/11 attacks: After the first plane crash, there was still time to act before the second plane crashed
* The president had the power to take down civilian aircraft, but he was still reading to the children.
* The fault doesn’t lie with him, but lies with the people who set up the system.
* There was a failure of design
* Our job as security engineers is to design some sort of system.
* If the president needs to act at a moments notice to do something:
  + There needs to be someone with him at all times OR
  + We give other people power to take action etc.
* Having a single point of failure can be bad. If you have a single bottleneck on a failure you work really hard to make sure that it won’t fail.

**Sources of attack**

**Exam: WHAT IS THE THREAT MODEL OF A PARTICULAR SITUATION? (Practise doing threat models on examples)**

* **What this means, is that Richard wants us to tell him what sorts of threats are they up against and what sorts of attackers are they up against?**
* **Examples of things in an answer:**

**Common Threat Classes / Sources of Threats (THESE ARE JUST CATEGORIES. IN EXAM, WE NEED TO BE SPECIFIC)**

This is a non-comprehensive list of some of the common threat classes not a thorough checklist. Your threat model should include (but is not limited to) the following classes of attacks.

* **Users**
  + Unintentional attacks (by frustrated or stupid users)
  + Malicious attacks
* **Attackers** **(external)**
  + Casual attackers
    - Does not target this victim specifically
    - Attacks the victim while scanning many other attackers
  + Determined attackers
    - Targets the victim
    - Has motive against the victim
    - Tries to find vulnerabilities of the victim
  + Funded attackers (NSA, CIA, MOSSAD – Someone with deep pockets)
    - Like determined attackers, but also:
    - Performs reconnaissance
    - Hires people and purchases equipment to perform the attack

^THESE DIFFERENT ATTACKERS ALL POSE DIFFERENT THREATS AND YOU NEED TO RESPOND TO THEM DIFFERENTLY

* **Natural Disasters / Accidents**
* **Movie plot threats**
  + The crazy things we see in movies.
  + Sometimes these can really happen so we need to defend against them
* **Error and failures**
  + Mechanical
  + Human

**Example question**: Imagine you are operating an internet café. What is the threat model that you’re going to be defending against?

**1. List out all the assets that you’re trying to protect.**

* You have hardware that can be stolen
* Someone can go into your internet café and launch an attack and get you in trouble.
* Someone can screw up your bandwidth and make everything slow / horrible so people don’t want to use you
* You might have software in the café and they can steal it.
* They may corrupt your software, so that you need to re-install everything (competing businesses / malicious users)
* Your customer database

**2. List out all the potential threats against the assets that you’re trying to protect.**

*(IN THE EXAM, YOU SHOULD BE BRAINSTORMING A LIST OF THREATS, THEN REWRITE THE LIST WITH MORE COMMON THREATS)*

Below is a brainstorm (not listed in order of importance)

* Internet café customers
  + How serious is the threat of customers?
  + They have complete access to your entire building / physical hardware
  + People accidentally putting malware on your computers
* Internet café suppliers
  + Why would the suppliers attack you if you’re an internet café?
* Employees / insiders
  + Employees have everything
  + ‘Why are they a big threat?
    - Employees have all the access that customers have
    - They’re there for a projected period of time
    - They’re often supervising themselves, so they don’t have other people watching
  + Employees stealing a customer database
  + Disgruntled employees with the technical skills and access to physical / software systems
* External attackers
  + Store malicious software on there, such as sniffers, and then when foreign tourists come in to do money transfers etc. they get all their credentials.
  + Your store may be liable for the losses taken from affected customers at your internet café
  + This would be a very serious threat
  + People stealing your processing power

**3. Sort out all the ideas in order of importance**

It is unlikely that you will be up against: Funded / state sponsored attacks (NSA, CIA etc.)

* When you defend, you have to defend appropriately to the level.

Most naïve businesses are concerned with movie scenario plots

* The mafia attacking me, hackers out to get me etc.

**Insider Attacks (ALWAYS CONSIDER INSIDER ATTACKS IN A THREAT MODEL)**

* Most organisations underrate the danger of **insider attacks**, unless they are banks who have learnt that insiders will always be there and that you can’t get rid of them.
* Insiders are people that know the password, have access to things and may even be the people that monitor / manages the security system.
* Companies never want to think about insiders / talk about them and when you’re pen-testing, they’ll normally want to put an I (impossible) next to insiders.
* We know from banks that people/staff just go bad randomly and you can’t predict it.

Suppose an attack is happening / a threat is being carried out.

* You don’t want to deal with it ONLY when it is actually happening.
* Don’t attack when everyone is calm and ready and waiting for you to attack.
* Attackers will attack when **no one is ready to attack**.

**When is it a good time to attack?**

* When there is change
  + Environmental (e.g. bank keycards, online apps)
  + Organisational (e.g. new systems, merger or takeover)
  + Requirements (e.g. Millenium bug)
* Should you rank threats?
  + Are all threats as equally likely and should be ranked the same?
  + Even if the smallest threat is executed and successful, it can cascade into more serious threats.