CO331: Network and Web Security

Tutorial 1: Threat Modeling[*]

January 19, 2018

Question 1: Identifying risks

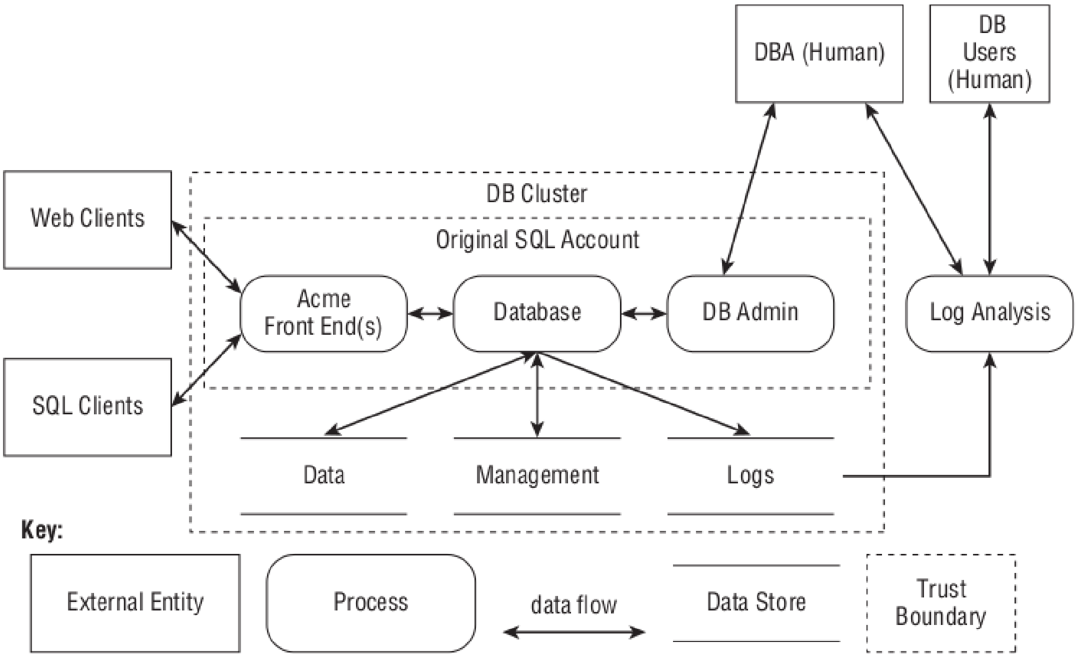
Below is a data flow diagram for Acme, an online retailer.

(a) From this diagram, identify three risks that Acme might face. (Hint: risks occur when data crosses trust boundaries.)

(b) Assign each of the risks you have identified to appropriate **STRIDE** categories:

Spoofing	**T**ampering	**R**epudiation
Information disclosure	**D**enial of service	**E**levation of privilege

(c) Propose two methods of addressing each risk you have identified.



Adam Shostack, *"Threat Modeling: Designing for Security"*, Wiley, 2014.

[*]Thanks to Chris Novakovic `c.novakovic@imperial.ac.uk` for preparing this material.

Question 2: Attack trees

Your goal is to gain access to a building. Draw an attack tree for achieving this goal.

A good attack tree should list a comprehensive range of actions that directly or indirectly contribute to achieving the goal. To get started, you may want to structure your attack tree in the following way:

- Your goal is to gain access to the building. This should be the root element in your attack tree.
- Identify the ingress points of the building. Gaining access to the building via any of these could be the first tier of your attack tree.
- For each ingress point in the first tier, identify the states that the ingress point could be in (if appropriate); they might be secure states, or insecure states. Gaining access to the building while the ingress point is in one of these states could be the second tier of your attack tree.
- For each of the states in the second tier, consider how the ingress point being in this state helps you achieve your goal: if the ingress point is in a secure state, how can you put it into an *insecure* state? If it's already in an insecure state, under what circumstances could it be in that insecure state? The actions necessary to ensure the ingress point is in the given state could form the third tier of your attack tree.
- Keep going! For each tier, create new child tiers for conditions that need to be met in order to achieve the goal in the parent tier.

Sample answers for Question 1

These are just some suggestions: there's no definitive list of correct answers. There are many more risks than the examples listed below, and there are more than two possible ways of addressing each of them.

- Vulnerability in front end exposes customer order data to an attacker (STRIDE: **I**nformation disclosure)
  1. Require front end code changes to be signed off by a co-worker and tested before being deployed to a production server
  2. Don't write sensitive payment information (e.g. full credit card numbers, PINs) to order DB table, to limit damage caused by disclosure
- Attacker emails malware to DB user, who opens it on an internal Acme workstation, granting backdoor access to Acme to the attacker (STRIDE: **E**levation of privilege)
  1. Install anti-virus software on Acme workstations
  2. Give DB users the lowest level of privilege necessary for them to do their work on Acme workstations, to limit the damage malware can do to the OS
- Passive network attacker steals session details of logged-in customer while in transit and uses them to pose as customer (STRIDE: **S**poofing)
  1. Tie customer session details to a particular IP address
  2. Use HTTPS for web client/front end communication (thus guaranteeing the confidentiality of the session details)
- Active network attacker modifies admin request to front end (STRIDE: **T**ampering)
  1. Only allow administrative connections over HTTPS (thus guaranteeing the request's integrity)
  2. Restrict administrative access to the internal Acme network
- Attacker edits log files after attack to make an innocent party appear responsible for it (STRIDE: **R**epudiation)
  1. Make log files append-only on logging file system
  2. Automatically send logs of critical actions to a printer
- Attacker floods Acme with bogus orders, filling the database server's disk and preventing new orders from being placed (STRIDE: **D**enial of service)
  1. Buy more database servers/disks, to make a denial of service less likely in this scenario
  2. Rate-limit orders from users (e.g. maximum of n orders per hour per user)
- DBA is a human, and is therefore susceptible to coercion (STRIDE: **E**levation of privilege)
  1. Pay them more money (and hopefully make them less susceptible to coercion)
  2. Require more than one DBA (or manager) to perform certain privileged functions, thus requiring successful coercion of more than one person

Sample answer for Question 2

- Gain access to a building
    - Go through an external door
        - Go through an unlocked external door
            - Go through a door with a malfunctioning lock mechanism
            - Enter during business hours, when the door is unlocked
            - Put sticky tape over the latch while the door is unlocked, and come back later
        - Go through a locked external door with an ID card reader
            - Disengage the electromagnet/latch
            - Social-engineer your way inside
                - Tailgate an authorised person
                - Befriend an authorised person and convince them to let you in
                - Approach the door with your hands full
            - Use an ID card
                - Find an authorised person's ID card
                - Steal an authorised person's ID card
                - Clone the magnetic strip/RFID tag on an authorised person's ID card
                - Social-engineer an authorised person into giving you their ID card
        - Go through a locked external door with a keyhole
            - Disengage the electromagnet/latch
            - Social-engineer your way inside
                - Tailgate an authorised person
                - Befriend an authorised person and convince them to let you in
                - Approach the door with your hands full
            - Use a key
                - Find an authorised person's key
                - Steal an authorised person's key
                - Photograph and cut a copy of an authorised person's key
                - Social-engineer an authorised person into giving you their key
            - Pick the lock
            - Drill through the lock
    - Go through an external window
        - Go through an unlocked external window
            - Climb through an unlocked ground-floor window
            - Use a ladder to climb through an unlocked higher-storey window
        - Go through a locked external window
            - Crowbar open a ground-floor window and climb through
            - Throw a brick through a ground-floor window and climb through
    - Gain access to an attached building and enter the target building via an internal door
    - Go through a HVAC shaft
        - Gain access to a HVAC shaft at ground level
            - Unscrew an external HVAC exhaust at ground level and crawl in
        - Gain access to a HVAC shaft on the roof
            - Gain access to the roof, unscrew an external HVAC exhaust and crawl in
                - Gain access to the roof by jumping onto it from an adjacent building
                - Gain access to the roof by landing a helicopter on it
    - Go through an external wall
        - Make a hole in the wall with a sledgehammer
        - Make a hole in the wall with a Jeep