SECURITY

Assignment 1, Friday, September 15, 2017

S1013793 Carlo Jessurun

S1013792 Tony Lopar

Radboud University

Teaching assistant

Assignment 1

For every assignment we send in we'll try to also include the questions so that you won't have to keep two papers side by side. We will always start with the question, followed by our solutions in the same structure as the assignment.

1. **(30 points)** A basic case of information security appears in your everyday life on your (smart) phone. Imagine Alice sending instant messages to Bob using a free message service like WhatsApp or Signal. The assets to protect are easily identified: The messages transmitted by Alice and Bob and then stored on their phones. Consider the security goals of confidentiality, authenticity and availability in this specific context.

   For each of these three security goals, briefly describe:
   a. what it means for Bob in this context;
   b. an attack that compromises that security goal;
   c. an example of a basic countermeasure against that attack.

Solutions are on the next page.

Solutions 1

1. Below are our solutions to assignment 1.
    a. **For Bob this means that:**
        i. **Confidentiality**: that no outside actor can read the content of what Alice and Bob are communicating.
        ii. **Authenticity**: he's certain about the identity of Alice. In particular, Bob is not talking to any outside actors, while he thinks he is talking to Alice.
        iii. **Availability**: the communication services that Bob is using are readily available. An outside actor cannot prevent the communication between Alice and Bob.
    b. **An attack vector that breaks:**
        i. **Confidentiality** could be a state actor that has the same keys Alice and Bob agreed upon while initiating their chat session. Giving it the opportunity to snoop in on the message.
        ii. **Authenticity** could for instance be a man in the middle attack where a hacker uses a MITM wifi hotspot to pose himself as Alice.
        iii. **Availability** could simply be a DDOS attack that inhibits Bob from talking to Alice.
    c. **A basic countermeasure to ensure:**
        i. **Confidentiality** would be a peer to peer based chat session (using Signal for example) where keys are agreed upon upfront and used to encrypt the traffic between the two devices.
        ii. **Authenticity** using the above technique of peer to peer traffic, MITM won't work since the attacker doesn't have the keys and therefore cannot decrypt the content.
        iii. **Availability** using a peer to peer based technique makes it more difficult to be DDOSed. Since YOU are connecting to the other person's device, the DDOS has to be targeted against you specifically and not against the service. A possible solution would be to only use your mobile network to make sure you can't be found easily or if really paranoid use multiple anonymous simcards.

Assignment 2

2. **(14 points)** Somehow we've all been taught to access all sorts of systems or gain some form of trust by using passwords and entry codes. There are more ways to achieve the same goal, though. Rather than using 'something you know' (like a password), systems may rely on 'something you own' or 'something you are', or a combination of these (often called 'multiple factors').
    a. In each of the following scenarios, explain which (possibly multiple) of the above methods are used (i.e. something you own, know, or are). Explicitly list the 'factors'.
        i. withdrawing money from an ATM
        ii. making a payment using online banking
        iii. password recovery using security question
        iv. logging on to a website with password and email confirmation
        v. unlocking your phone with your fingerprint
        vi. passing through customs at the border
        vii. entering a CAPTCHA code
        viii. calling a friend by telephone
    b. Which security goal does all of this mainly concern?

Solutions are on the next page.

Solutions 2

2. we simply looked at what we do in our daily lives to solve these solutions.
    a. **In each of the following scenarios, explain which (possibly multiple) of the above methods are used (i.e. something you own, know, or are). Explicitly list the 'factors'**.
        i. withdrawing money from an ATM
            1. **Know**: Your pin passcode to the ATM as something you know.
            2. **Own**: Your ATM card as something you own.
        ii. making a payment using online banking
            1. **Know**: Your password as something you know.
            2. **Own:** Your SMS based token id to your phone or identifier from the bank.
            3. **Are:** Your fingerprint scan as something you are.
        iii. password recovery using security question
            1. **Know**: The answer to the security question.
        iv. logging on to a website with password and email confirmation
            1. **Know**: your password to login to the website.
            2. **Own**: Your email address.
        v. unlocking your phone with your fingerprint
            1. **Are**: You are your fingerprint.
        vi. passing through customs at the border
            1. **Know**: As you have to verify yourself to the security guard, he might ask trick questions that only you know based on for instance your ESTA approval.
            2. **Own**: Your passport for instance.
            3. **Are**: Often you'll need to leave your fingerprints behind.
        vii. entering a CAPTCHA code
            1. **Know**: You interpret the code and verify by writing it down.
        viii. calling a friend by telephone
            1. Know: You know the number as you've just called it.
            2. Own: To call your phone needs to have a SIM card inside it.
    b. Which security goal does all of this mainly concern?
        i. Authenticity

Assignment 3

3. **(31 points)** After the Snowden revelations of 2013, it should not be news to anybody that there's always someone listening. Depending on the situation, however, what they 'hear' might vary. Consider the following scenarios (assume no extra privacy precautions).

    a. A friend sends you a link to a political blog post, recommending the contents as something you'd appreciate. You're using Gmail to read the email; your friend is using a mail server at @yourfriendsname.com, which he hosts on a rented server in 'the cloud'. What does Google learn about you and your friend based on this interaction? Name at least 4 'facts'.
    b. Every day when you're traveling home from university by bus, you're scrolling through Facebook on your phone. Sometimes you stop scrolling for a closer look, you like a photo or a post, you click a few links. When you're traveling with others, you put your phone away and talk, instead. What could Facebook learn about you? Again, name at least 4 'facts'. Briefly explain how – think broad.
    c. Can you think of three others that learn things in one or both of the above scenarios? Name at least three parties and describe what they learn. Keep in mind that very little information is still information!

Solutions are on the next page.

Solutions 3

3. Below are our solutions to assignment 3.
    a. **Google will learn the following things based on the interaction:**
        i. The IP address of the ‘rented’ server.
        ii. Based on automatic whois lookup it will also learn about:
            1. Registrant Name
            2. Registrant Organization:
            3. Registrant Street
            4. Registrant City
            5. Registrant Country: NL
            6. Registrant Phone: +31.629159265
            7. Etc etc.
        iii. Your political preference
        iv. That you communicate with your friend by mail
    b. **Facebook will learn the following things based on your behaviour**
        i. Since you started the Facebook app, Face will know the exact route you took by bus.
        ii. What you may be interested to see. For instance, because you often stop scrolling when pictures of dogs appear.
        iii. What you like to read, because you clicked some links to articles to read them
    c. **Three other parties could include:**
        i. Advertisement companies.
        ii. The NSA.
        iii. If using a blogging framework, the frameworks analytical system.

Assignment 4

4. (**25 points**) ‘Smart’ energy meters are becoming more and more common in Dutch homes. The manual (and annual) meter measurement is slowly becoming history: instead, energy companies simply read out the energy meter remotely (e.g. every 15 minutes). While it is undeniably convenient , it is not without risks**.**

    a. Name an asset of the energy company, and an asset of the home owner.
    b. For each asset, describe at least one threat.
    c. Describe at least one technical measure, one organizational measure and one legal measure, and indicate which threat(s) listed in (b) they counteract.

Solutions 4

4. Below are our solutions to assignment 4.
    - **a. The assets can be listed as**
        - i. **Energy company**: customer data.
        - ii. **Home owner**: personal data.
    - **b. Based on the above assets threats can be defined as**
        - i. **Energy company**: confidentiality, integrity, Authenticity, Availability, Non-repudiation and Accountability of the incoming data supplied by the 'Smart' energy meters. Especially integrity is very important as the data supplied by the 'Smart' meters defines the bill that the customer has to eventually pay.
        - ii. **Home owner**: Contrary to the energy company, the main concern for individual homeowners will be confidentiality. Say for instance that a burglar can hack into content of the 'Smart' meter. He could then easily identify patterns in when the homeowners come home and leave so he'll know when to break into the home and steal valuables.
    - **c. Measures to prevent threats**
        - i. Technical measure
            1. Properly encrypting the data and the communication, counteracts both threats.
        - ii. Organizational measure
            1. Checking the measures regularly to detect possible incorrect values in order to detect possible fraud, counteracts the threat for the energy company(maybe also the threat for the home owner by early detection)
        - iii. Legal measure
            1. Prosecution of any fraud, counteracts both threats