Security

Assignment 1, Friday, September 9, 2016

Handing in your answers: For the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2016/exercises.html`

To summarize:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Hans or Joost). When working together, include **both** your names and student numbers.
- Submit one single **pdf** file – when working together, only hand in **once**.
- Hand in via Blackboard, before the deadline.

Deadline: Monday, September 19, 09:00 sharp!

Goals: After completing these exercises successfully you should be able to

- analyze systems using the fundamental security goals;
- identify assets and identify by what means they can be protected.

Marks: You can score a total of 100 points.

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:

   - what it means for Bob in this context;
   - an attack that compromises that security goal;
   - an example of a basic countermeasure against that attack.

2. **(24 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 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 3 'facts'.

   (b) Every day when you're traveling home from university by bus, you're scrolling 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 3 'facts'. Briefly explain how, – think broad.

   (c) Can you think of others that learn things in one or both of the above scenarios? Name at least two parties and describe what they learn. Keep in mind that very little information is still information!

3. **(22 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[1], 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.

4. **(24 points)** Last June it became known that the Democratic Party has allegedly been attacked by hackers associated with the Russian government[2]. This gave the hackers access to e-mails, memos, research data about the Republican opposition and to all kinds of internal documents.

   Describe what further damage the attackers can now do to the Democratic Party; what security goals can they breach? List at least three attacks, and for each attack describe which of the security goals (confidentiality, integrity, authenticity and availability) is violated.

[1] For the energy company, at least.
[2] `http://wapo.st/1tuiAUt`