Security

Assignment 1, Tuesday, September 9, 2015

Handing in your answers: For the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2015/exercises.html`

Briefly,

- submission via Blackboard (`http://blackboard.ru.nl`);
- one single pdf file;
- make sure to write all names and student numbers and the name of your teaching assistant (Brinda or Joost).

Deadline: Thursday, September 17, 24:00 (midnight) sharp!

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

- analyse systems using the fundamental security goals;
- identify assets and identify by what means they are protected.

Marks: You can score a total of 100 points.

1. **(30 points)** A basic case of information security appears in your everyday life when the information is exchanged; not only between people but also between personal electronic devices, for instance, a smart watch and a smart phone. Consider the scenario in which your smart watch is transmitting your fitness regime/health statistics to an application on your phone. The assets to protect are easily identified: The health data transmitted by the watch to the phone application and possibly stored on both watch and the phone. Consider the security goals of **confidentiality**, **authenticity** and **availability** in this specific context. For each of these three security goals

   (a) explain briefly what these mean in the specific context;

   (b) describe an attack that compromises each security goal; and

   (c) give an example of a basic countermeasure offered against each kind of attack.

2. **(40 points)** Imagine that you have a high-end car from a reputed car producer X and you come to know that some hackers have found out ways to remotely control some of your car parts (e.g. dashboard, digital radio, steering wheel, brakes etc.).

   (a) Specify two assets in the above attack scenario and briefly describe one threat for each of these two assets.

   (b) Give an example from each of the categories of protective measures that would prevent the above scenario: **Technical measures**, **Organisational measures** and **Legal measures** that are useful against at least one of the threats you identified in (a).

   (c) In response to the discovered vulnerability, car producer X decides to send out USB sticks with firmware updates to their customers (via physical mail). Is this a good idea? Explain your answer briefly in terms of security goals.

. . . . **The assignment continues on the next page!** . . . .

3. **(30 points)** The Dutch government has introduced DigiD (the Dutch electronic identity system) for an increasing number of services over the last few years. For most people, this is just one more password to remember. DigiD is not something a typical user needs every day, though, so this might not be as easy as it sounds.

   Consider a user who cannot quite remember their password, and decides to write it down on a post-it note. It is stuck to their monitor, conveniently in sight when needed. Then, one particularly unfortunate night, our user is the victim of a burglary. The burglar is about to head off with the computer, but then suddenly recognises the credentials on the screen as a DigiD login.

   (a) Describe three (or more) attacks that the burglar could now perform, and mention for each attack which of the security requirements (confidentiality, integrity, availability, authenticity) is violated.

   (b) If the burglar were to be indicted in the Netherlands for the attacks you found in (a), which computer crime laws would be violated in case of each of them, if any? (See slide 32 of the introductory lecture slides).