CS181S – Systems Security Fall 2020

Problem Session 1: Threats

Monday August 31, 2020

1. **Adversarial Thinking.** Let's imagine that I decide I need a new scheme to determine whether a student has attended all of the classes. The requirements for this scheme include:

   - There is a process to establish with high probability, at the end of semester, whether any given student has attended every lecture.
   - The costs are not unreasonable.
   - The mechanism is not disruptive.

   So the utility of a proposed scheme might be evaluated in terms of: (i) whether it has vulnerabilities that allow a student to miss lecture without being caught, (ii) the costs, and (iii) other issues.

   (a) Analyze each of the following proposed schemes, giving your assessment in terms of (i) through (iii). Assume that the scheme is implemented exactly as described.

   As an example of the kind of answer we are expecting, here's an example analysis for a scheme used in many classes where attendance is required.

   Scheme 0: Roll Call. At the start of class, the professor calls each student's name from a registration list. When a student's name is called, that student – if present – is expected to reply "present". The professor records those answers (or lack thereof) on the list, which is kept in the professor's office.

   ANSWER: (i) Vulnerabilities: One student might answer for another, so a student's absence can be hidden if a friend is willing to help. (ii) Costs: Time is lost at the start of lecture. If 6 names can be called per minute, then a class with 30 students would have 5 minutes lost at the start of each lecture. (iii) Other issues: The scheme does not gracefully handle students who arrive at lecture late.

   Scheme 1: Random Polling. A separate piece of paper with each student's name is printed and placed in a hat. Before the end of each class, I randomly select 6 of these slips from the hat; the name on each of those slips is read aloud. If a student whose name is read is present, then that student is expected to reply "present". I record the date and absence of an answer on a list. The slips that were removed are returned to the hat for possible selection next time.

   Scheme 2: Clickers. Each student is expected to have purchased a "clicker" and registered it, thereby establishing a binding between the "clicker" ID and the student's name. A student is expected to bring that "clicker" to class. During each class, I ask at least one multiple-choice question. Students are expected to respond by using the "clicker".

Scheme 3: Random Pop Quiz. At random points during the semester, I distribute a short quiz towards the end of class. Students write answers on the quiz and, at the end of class that day, submit their solution.

(b) Suggest a better scheme. It should have fewer vulnerabilities, reasonable costs, and no significant other issues. Analyze this proposed scheme, giving your assessment in terms of (i) through (iii).

2. **Threat Modeling.** Consider the following system: Users have an electricity meter installed outside their house; you may assume that the meter resists physical attacks. The meter is connected to a WiFi home area network, as are major appliances inside the house; assume that the home network is not bridged to the public Internet (i.e., the device cannot be accessed from outside the home network). The meter is also connected to a cellular (e.g., GSM) wide area network (WAN), which enables communication with the electrical utility service. Here are some functional requirements for this system:

   - The meter can report to the utility service the amount of electricity used each hour.
   - During periods of peak power usage, the utility service can send hints to the meter to conserve energy, which the meter relays to appliances on the HAN.
   - Upon receiving conservation hints, an appliance can choose to enter a lower-power mode.

   Your job is to perform a threat analysis and harm analysis on this system. This will involve three steps:

   (a) What are the assets of the system? Identify at least three core assets that are essential to stakeholders in the system, rather than ancillary assets that merely enable access to those core assets. You may exclude the hardware and software implementing clients and servers from your analysis, as well as the network itself.

   (b) What are the threats of concern? What are their motivations and capabilities? Are there any threats that are excluded? Make your threat analysis specific to the system under consideration, rather than being generic.

   (c) For each asset, what are the possible harms that could occur? For each harm, characterize whether it affects the confidentiality, integrity, or availability of the corresponding asset. If you can't come up with one of those three kinds of harms for a particular asset, write a sentence or two explaining why you believe that asset can't be harmed in that way.