Security Engineering

Common Issues in SubmissionsWS 2022/23

Elisabeth Oswald

Overview

The assessment is very specific and tasks you to point out specific issues with a provided system specification. Quoting from Moodle:

> The mini project puts you in the shoes of an independent consultant who is given an initial specification/system design and associated embedded AES implementation for a secure access control system, called SuperSAM.
>
> Your job is to provide an assessment of what you are given: the "implementation note" describes the overall system in a semi-formal manner and provides some rational for some design choices. There is also an associated AES implementation that is meant to run on a hardware token that will be an essential part of the overall system. You are meant to point out flaws and offer solutions.

The main reason, why students lost points is that they provided generic discussions of security issues, which is **not** what the assessment asks for. It asks for an assessment of **exactly** the system that is given, and so to point out specific issues in the specification and associated source code. No points can be awarded for a generic discussion, e.g. of typical RFID security problems. No points can be awarded for discussing generic solutions either: the task is to fix the specific system, not to fix some system.

Another major issue seems to have been that the specification was insufficiently studied and thus weird/wrong conclusions/interpretations were drawn, and seemingly those spread among the student body, and were adopted (seemingly) by many without critical appraisal. I shall mention a few frequent"misunderstandings" below.

A third major issue was that, unlike in previous years, many students didn't engage with the meetings, and didn't hand in drafts for me to comment on.

AES as a "suggestion": AES is a specification, and whilst there are equivalent round functions, the AES encryption scheme is not open for interpretation.

RFID security issues: wireless communications in general are insecure when not encrypted. RFID specific attacks are problematic when communications are not encrypted and no authentication is provided. The specification is clear that only encrypted messages are communicated and authentication of tokens is foreseen. If

you want to argue that things like sniffing and skimming are still a threat, you must demonstrate an attack that works for the provided system.

Human error: is indeed always important to take into account. But to list generic issues around usability without describing a specific attack vector to the given system is insufficient.

DPA: requires to have known inputs with a fixed key. You must think if or not this can be applied to the different protocols in the given specification.

Size of IDs: there seems to be the idea that if an ID value can be out of a space of 2^{32} values, one must store somewhere 2^{32} values. This is nonsense; 32 bits would need to be stored on the token for the ID. Suggestions of x bits are sufficient should be considered carefully: if x is not a multiple of a native data type of the processor, then loading x will be expensive. Also if x is too small, this may cause problems if e.g. buildingIDs need to be revoked on a regular basis.

ECB mode: is clearly not a good choice, but how would an attack really look like in this concrete system?

Factoring: is not a concern when working withe prime numbers (if you still think that larger prime numbers are harder to factor you should consider re-taking Cryptography).

Several students thought that the core system design decision to keep readers as much as possible offline, by tokens having tickets is wrong. Fair enough: but then your analysis would need to consider what would be the potential issues when tokens are only used for authentication? What happens if readers go offline? Would this be possible for all companies/set ups/building locations?

Several students lifted pictures from sources and used text from published papers. This is a type of plagiarism that is called "bad academic practice". Don't do it. Any passage that contained lifted text or copied figures was given 0 points.