622.755 – Crypto Engineering Winter Term, 2020/21

Project: SuperSAM Security Analysis

Firstname Lastname

1 Executive Summary

Please write a general overview explaining the major issues that you found. This should be fairly succinct and must not exceed 2 pages.

2 Specific points

Each subsection should cover one weakness/mistake. You must look at both the Implementation Note and the AES implementation. Every analysis must at least identify two problems in each of the two components and for at least one (per component) I would like you to make a serious effort to demonstrate a problem and suggest a fix.

For each problem that you identify give a name and a clear reference to where it occurs as part of the subsection title. Then have paragraph that describes the problem; followed by further paragraphs detailing how to exploit it and how to fix it.

Here is one example.

2.1 Implementation Note: Wrong Generator, Section 2.3. on Page 3

Problem Description: Wrong Generator Value. The given DH Parameters are from RFC 3526; the prime was verbatim copied from the RFC, but upon double checking it turns out that the generator value in the RFC is given as 2 rather than the value 3.

Demonstrating this as a vulnerability: A generator g has the special property that it will generate the entire prime group, this means that for different x, g^x will (eventually) generate all $p-1$ elements. This is important because it makes the DL problem in this group computationally infeasible (for any p large enough). If an element r is chosen that is not a generator, it is possible that it generates only a much smaller subgroup. In the worst case with very few (even just two) elements. In this subgroup, the DH problem is no longer difficult to solve.

Proposed Improvement: Use the standardised generator value of 2.

Example application of the marking scheme

Clearly a problem has been spotted here correctly: (1 mark out of 1 mark).
There is a relatively clear description of the problem. Perhaps the biggest shortcoming in the description is that it is not specific enough w.r.t. the RFC (which page, section): (4 marks out of 5 marks).
The demonstration of the problem is rather hand waving. A good demonstration could have been to consider if the value 3 indeed has a low order using some maths tool package: (5 marks out of 10 marks).
The improvement/fix is really super trivial in this case: (1 mark out of 10 marks).