dat11gja@student.lu.se

Home exercises 1

by Gustav Jansson Ekstrand

1.1

As medical information, such as medical records, allergies, etc., is considered sensitive information, is it wise to keep this confidential.
By keeping this information in a locked database, we solve this problem. However, in medical situations and emergencies, medical personnel should be able to access this information. By implementing a login functionality for this system, said personnel can access this information when needed. This login functionality may be a simple one-step login, but a two-factor authentication model may be desirable for those, mainly the doctors, who have access to all medical information, especially the more delicate information, such as medical charts.
Information about allergies is very important to be known throughout the medical personnel, and should be accessible to all staff members, and maybe only a simple login method is required for the personnel with lower access, such as nurses.
When it comes to patient access, it is only necessary for a person to be able to access their own medical information. This is a no brainer.
However, the administrators access is a bit harder to determine. On one hand, the administrator does not need to know the medical information of patients, since they aren't treating them, and should thus only be able to maintain the system without the ability to read the information in clear text. This can be done by hashing the stored information in the database, making it impossible to read without deciphering it. On the other hand, it may not matter, and maybe could cause implications due to complicating the maintainability. Besides, it seems very likely that an administrator has the capacity to decrypt the hashed data. If i ever were to implement such a system, I would prefer an administrator with a master key, and the ability to access all the stored information in the database.

1.2

1. Select a prime q such that 20 < q < 100
   $q = 23$
2. Select a prime such that $(p-1) \bmod q = 0$
   $q = 47$
3. Select α such that 1 < α < p - 1, and calculate $g = \alpha^{(p-1)/q} \bmod p$
   $g = 2^{(47-1)/23} \bmod 47 = 4$
4. Select a such that 1 < a < q - 1
   $a = 6$
5. Calculate $y = g^a \bmod p$
   $y = 4^6 \bmod 47 = 7$

dat11gja@student.lu.se

The public key is packaged as such: (47, 23, 4, 7)
The private key is packaged as such: (47, 23, 4, 6)

6. Select an integer k such that $gcd(k,\ p-1) = 1$

$k = 5$ då $gcd(5,\ 46) = 1$

7. Calculate $r = (g^k\ mod\ p)\ mod\ q$

$r = (4^5\ mod\ 47)\ mod\ 23 = 14$

8. Calculate $s = k^{-1}(h(m) + ar)\ mod\ q$

$s = 14(17 + 6 * 14)\ mod\ 23 = 11$

The signature for m is: (14, 11)

Verification:

1. Calculate $w = s^{-1}\ mod\ q$

$w = 21\ mod\ 23 = 21$

2. Calculate $u_1 = w * h(m)\ mod\ 23$ och $u_2 = w * r\ mod\ 23$

$u_1 = 21 * 17\ mod\ 23 = 12$

$u_2 = 21 * 14\ mod\ 23 = 18$

3. Calculate $v = ((g^{u_1} * y^{u_2})\ mod\ p)\ mod\ q$

$v = ((4^{12} * 7^{18})\ mod\ 47)\ mod\ 23 = 14$

4. The signature is verified if and only if $v = r$

$v = 14$

$r = 14$

The signature is considered verified, since v and r is the same.

1.3

One example of a digital signature forgery is the *existential forgery* were an adversary, maybe with a malign intent, can create a valid m/s pair $(m,\ s)$. By producing a random signature and computing a message. However, this message is not specified by the adversary, and will thus maybe only will be good for recieving tokens or other similar things. In other words, this type of forgery is not very advanced, but will still cause problems.

1.4

ECB has drawbacks when it comes to blocks that are identical. When some words or phrases are reused often, repetetive blocks of ciphered text can occur, making it easy for codebook attacks, as patterns are recognisable. The confidentiality of the message is not serious, and the encryptions may be analysed and properties that are concidered secure can be deduced.

Cipher block chaining uses an initialisation vector that enhances the encryption, making it harder to recognise repetitions in patterns, and thus inhibits deciphering.

1.5

Security Target (ST): A security target is defined as “an implementation-dependent statement of security needs for a specific identified TOE.”[1], or, in other words, is the confines and specifications of a Target of Evaluation (TOE).
Target of Evaluation (TOE): A target of evaluation is, most commonly, a software, firmware or hardware, that is, as its name suggests, the targeted system that is evaluated with security as an outset.

The outline of a ST-document is defined as following:

- Introduction - with references and and overview of the TOE
- Conformance claims - identifies the conformance claims to Common Criteria
- Security problem definition - describing threats, policies and assumptions of the TOE
- Security objectives - statements with the intended solutions for the problems defined
- Extended components definition
- Security requirements
- TOE summary specifications - enables a general understanding of how the TOE is implemented

The penetration testing needed for EAL2 products is based on a vulnerability analysis, the resistance of “Basic Attack Potential”.

[1] http://www.fmv.se/Global/Dokument/Verksamhet/CSEC/SP-192.pdf,