Seminar on Security Protocols and Applications
Final Exam

30th June 2005

- ⋆ The exam duration is 1h45'.
- ⋆ All documents and electronic devices (except wireless communication devices) are allowed.
- ⋆ If you do not have enough space on the sheet please use a separate page with your name on and clear references: use two different sheets for the different exercises as they will be corrected separately.

LAST NAME: ....

First Name: ....

Section: ....

1 IPSec and IKE

1.1 Security Associations

1. Describe all the security associations that are necessary to allow a machine to successfully ping another machine over an IPSec protected network.

2. How many Diffie-Hellman operations have to be carried out to establish these associations?

1.2 Cookies and Nonces

IKE makes use of cookies and nonces.

1. Use the main mode exchange to explain the attacks that cookies and nonces should prevent.

2. Are cookies and nonces still efficient if aggressive mode is used?

1.3 IPSec Authentication

The following three methods of authentication are specified in IPSec:

- Pre-Shared Key: provide the same key to all parties
- Digital Signature: provide each party with the public key of the other
- Public Key Cryptography: provide each party with a certificate of its public key.

For each authentication method find a scenario where that particular method would be specially recommended.

1.4 PSK attack on IKE Main Mode

In the seminar we have seen an attack against IKE aggressive mode with PSK authentication which allows a passive attacker to retrieve the pre-shared key just by listening to the exchange.

1. Explain why this attack does not work with main mode.

2. Modify the attack so that it works in main mode for an attacker located between the two parties. Describe the packets that are exchanged and the operations that are carried out.

3. What should be done to prevent these attacks against the PSK.

LAST NAME: ....

First Name: ....

Section: ....

2 Forging X.509 Certificates

We consider X.509 certificates signed by using `md5WithRSAEncryption`. We want to submit an RSA public key (N_1, e_1) to the certificate authority for certification such that we can infer a fake certificate for another RSA public key (N_2, e_2). RSA moduli are assumed to be 2048-bit long. We also assume that $e_1 = e_2 = 65537$ and that all fields except the moduli parts in both certificates will be completely identical.

We assume that we have filled all fields of the X.509 form, except the RSA modulus part (and the signature to be appended by the certificate authority). We assume that the length of the form (represented as a string) from the beginning of the form to the beginning of the modulus field is a multiple of 512 bits.

2.1 Preliminaries

We recall the Merkle-Damgård scheme for the $\mathsf{MD5}$ hash function. $\mathsf{MD5}$ is an iterative hash function which proceeds by first padding the message with a string which only depends on its length so that the padded string has a length multiple of 512 bits, then splitting it in a sequence of 512-bit blocks. Every block is then iteratively hashed by using a compression function C. More precisely, we define a sequence H by $H_0 = \mathsf{IV}$ where IV is a standard initial vector and $H_i = C(H_{i-1}, X_i)$ where X_i is the ith block to be hashed. The last H_i value is the hash of the message.

1. We denote by $\mathsf{MD5}'$ the hash function obtained from $\mathsf{MD5}$ by removing the padding scheme and replacing the standard initial vector IV by an arbitrary 128-bit string IV'. Show that there exists a vector IV' such that for any N_1 and N_2 such that $\mathsf{MD5}'(N_1) = \mathsf{MD5}'(N_2)$, the strings to be signed in both certificates produce identical $\mathsf{MD5}$ hash values.

2. We recall that strings are signed using `md5WithRSAEncryption` by first hashing using $\mathsf{MD5}$, then putting the hash in a specific format, and finally signing by using the plain RSA signature scheme.

   With the above IV' and $\mathsf{MD5}'$, deduce that if $\mathsf{MD5}'(N_1) = \mathsf{MD5}'(N_2)$, a valid signature for the certificate with N_1 is also a valid signature for the certificate with N_2.

3. We assume that we can find two different 1024-bit blocks b_1 and b_2 such that $\mathsf{MD5}'(b_1) = \mathsf{MD5}'(b_2)$. (We actually can, very efficiently!)

   Show that for any 1024-bit string b, we have $\mathsf{MD5}'(b_1||b) = \mathsf{MD5}'(b_2||b)$.

2.2 Constructing N_1 and N_2

By using the previous notations, it remains to find b such that $N_1 = b_1||b$ and $N_2 = b_2||b$ are valid RSA moduli for which we know the factorization.

1. We recall that a valid RSA modulus is a product of two different large prime integers. Let p_1 and p_2 be two (different) random 512-bit prime numbers. Show that we can compute and integer b_0 between 0 and p_1p_2 by using the Chinese Remainder Theorem such that p_1 divides $b_1 2^{1024} + b_0$ and p_2 divides $b_2 2^{1024} + b_0$.

2. By taking $b = b_0 + kp_1p_2$ for $k = 0, 1, 2, \ldots$, (heuristically) show that we are likely to find k such that $(b_1 2^{1024} + b)/p_1$ and $(b_2 2^{1024} + b)/p_2$ are both primes. Conclude.

2.3 Discussion

1. To what extend is the above attack devastating?

2. We now assume that given two vectors IV' and IV'' defining $\mathsf{MD5}'$ and $\mathsf{MD5}''$ we can find two 1024-bit blocks b_1 and b_2 such that $\mathsf{MD5}'(b_1) = \mathsf{MD5}''(b_2)$. Can we now derive a more dangerous attack?

3. We now assume that given a vector IV' defining $\mathsf{MD5}'$ and a 1024-bit block b_1 we can find another 1024-bit block b_2 such that $\mathsf{MD5}'(b_1) = \mathsf{MD5}'(b_2)$. Can we now derive an even more dangerous attack?