Homework 3: IPsec & PKI
Due at 11:59PM on March 20 as a PDF via websubmit (HW3).

March 6, 2013

Exercise 1 (Reductions.)**.** Suppose we have an CPA secure symmetric-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$. Consider the following encryption scheme: $(\mathsf{Gen}^+, \mathsf{Enc}^+, \mathsf{Dec}^+)$ where

Algorithm Gen^+:	**Algorithm** $\mathsf{Enc}^+(k, m)$:	**Algorithm** $\mathsf{Dec}(k, (c, m))$:
$k \leftarrow \mathsf{Gen}$	$c \leftarrow \mathsf{Enc}(k, m)$	Return m
Return k_1	Return (c, m)	

- This $(\mathsf{Gen}^+, \mathsf{Enc}^+, \mathsf{Dec}^+)$ scheme is obviously not CPA secure. Explain why.
- Explain why you **cannot** do a reduction that prove that if $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is CPA-secure then $(\mathsf{Gen}^+, \mathsf{Enc}^+, \mathsf{Dec}^+)$ is also secure. Where does the reduction fail?

Exercise 2 (Authenticated encryption.)**.** Suppose we have an CPA secure symmetric-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ and a secure message authentication code $\mathcal{MAC} = (\mathsf{Gen}', \mathsf{Sign}, \mathsf{Ver})$. We wish to construct a new symmetric encryption scheme that provides *both* authenticity and CCA security.(Recall that CPA = chosen plaintext security, and CCA = chosen ciphertext security). Such a scheme is usually called *authenticated encryption scheme*. Consider the following suggestion $(\mathsf{Gen}^+, \mathsf{Enc}^+, \mathsf{Dec}^+)$:

Algorithm Gen^+:	**Algorithm** $\mathsf{Enc}^+((k_1, k_2), m)$:
$k_1 \leftarrow \mathsf{Gen}$	$c \leftarrow \mathsf{Enc}(k_1, m)$
$k_2 \leftarrow \mathsf{Gen}'$	$\sigma \leftarrow \mathsf{Sign}(k_2, c)$
Return (k_1, k_2)	Return (c, σ)

1. Write down the decryption algorithm, Dec^+.
2. Scheme $(\mathsf{Gen}^+, \mathsf{Enc}^+, \mathsf{Dec}^+)$ can be shown to provide *authenticity* of messages due to UF-CMA security of $\mathcal{MAC}$. Use a reduction to prove that it also provides CCA security. (Hint; this reduction is a classic. Feel free to search online to see how it is done. I only require that your explanation is clear, correct, in your own words, and that you properly cite your sources.)
3. Now, consider the following encrypt-and-authenticate scheme $(\mathsf{Gen}^*, \mathsf{Enc}^*, \mathsf{Dec}^*)$:

Algorithm Gen^*:	**Algorithm** $\mathsf{Enc}^*((k_1,k_2),m)$:	**Algorithm** $\mathsf{Dec}^*((k_1,k_2),(c,\sigma))$:
$k_1 \leftarrow \mathsf{Gen}$	$c \leftarrow \mathsf{Enc}(k_1,m)$	$m' \leftarrow \mathsf{Dec}(k_1,c)$
$k_2 \leftarrow \mathsf{Gen}'$	$\sigma \leftarrow \mathsf{Sign}(k_2,m)$	If $\mathsf{Ver}(k_2,m',\sigma)=1$ then return m'
Return (k_1,k_2)	Return (c,σ)	Else return "fail".

This scheme is not CPA secure.

(a) To show this, come up with a contrived example of a message authentication code $\mathcal{MAC}$ that is secure, but completely breaks the confidentiality (*e.g.,* CPA security) of this scheme. (Hint. Think of ex1 in the last problem set.)

(b) What does this example suggest about the difficulties of combining cryptographic primitives?

Exercise 3 (MAC vs checksum)**.** Authenticated IPsec packets contain both a MAC (keyed with a symmetric key) and a checksum (unkeyed).

1. Why does an IPsec packet need both?
2. Show that a checksum is not a secure MAC. To do this, show that an adversary playing the MAC security game where
$$MAC_k(m) = CRC32(m)$$
can win with probability 1. (Check wikipedia for the definition of CRC32.)
3. Does your attack still work if the checksum output is made to be longer? (For example, instead of 32 bits for CRC32, we use a CRC with 128 bits of output.)

Exercise 4 (Key exchange.)**.** We consider the key exchange protocols discussed in Krawcyzk's slides.

1. Consider the "SIGMA-I:active protection of Initiators id" protocol on slide 35 of Krawcyzk. Krawcyzk claims that with this protocol, an active adversary E (a man-in-the-middle between A and B) cannot learn the identity of the initiator A.
   (a) Explain why E cannot learn A's identity.
   (b) Show how E can learn B's identity.
   (c) Explain why E cannot cause A and B to agree on a key that is different from g^{xy}.
2. Now consider the "SIGMA-R:active protection of Responders id" protocol on slide 36 of Krawcyzk. Krawcyzk claims that with this protocol, an active adversary E (a man-in-the-middle between A and B) cannot learn the identity of the responder B.
   (a) Explain why E cannot learn B's identity.
   (b) Show how E can learn A's identity.
3. Consider the "SIGMA: Basic Version" protocol on Slide 34, and suppose we modify it by getting rid of the "$MAC_{K_m}(B)$" part of the message B sends to A. Can a man-in-the-middle E mount an identity misbinding attack on this modified protocol? If yes, describe the attack.

Exercise 5. (Readings) For each of the following items, provide a response of no more than 300 words, and remember to properly cite your sources.

1. Read Ellison & Schneier's paper on the 10 risks of PKI at `http://www.schneier.com/paper-pki.pdf`. Then, look online for an incident that made the news that highlights on of the ten risks described in this paper. The incident can impact a PKI used any system of interest. Describe the system, the PKI, the incident and explain how it relates to one of the risks described in the paper.

2. Recently, TURKTRUST, a Turkish certificate authority, created a false certificate for Google. Do some research online and explain what happened; how the "attack" was carried out, what was the motivated, who instigated it, and how technically it was executed. What PKI risk(s) does this event highlight?

3. A "web-of-trust" public key infrastructure model is often suggested as an alternate to the a PKI. Briefly describe 2 advantages and 2 disadvantages that "web of trust" has over an hierarchical PKI. You can refer to excerpt about public key infrastructures from Katz and Lindell (page 446-453) or any other online sources you find.

Submission policy.

Every submitted assignment MUST include the following information:

1. List of collaborators

2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)

3. Number of late days used on this assignment

4. Total number of late days used thus far in the entire semester

If any of this information is missing, at least 20% of the points for the assignment will automatically be deducted from your assignment. See also discussion on plagiarism on the course syllabus.