

18739A: Foundations of Security and Privacy
Midterm Exam
(Due: Oct 25 before class)

October 20, 2011

Problem 1 (3.0 points)

Shown below is the initiation part of the Public Key Kerberos protocol in which the client obtains a “ticket granting ticket” (TGT) from the Kerberos Authentication Server (KAS), and also a key AK that the client uses later to communicate with the Ticket Granting Server (TGS). AK is also contained in TGT, and the TGT is encrypted with a long-term key shared between KAS and TGT.

$$\begin{aligned} C \rightarrow K & : \text{Cert}_C, \text{SIG}_C\{t_C, n_1\}, C, T, n_2 \\ K \rightarrow C & : \text{ENC}_{pk_C}\{\text{Cert}_K, \text{SIG}_K\{k, n_1\}\}, C, \text{ENC}_{k_{KT}}\{\text{TGT}\}, \text{ENC}_k\{AK, n_2, t_K, T\} \end{aligned}$$

Figure 1: The AS exchange protocol in Public Key Kerberos

Here C is the client and K is the KAS. We abbreviate by $\text{SIG}_C\{m\}$ the message m , $\text{SIG}_C\{m\}$. n_1, n_2 are nonces, t_C, t_K are timestamps, T is the name of the TGS. $\text{Cert}_C, \text{Cert}_K$ are certificates of the client and KAS respectively. pk_C is the public key of the Client, k is a fresh key generated by KAS and k_{KT} is a long-term key shared between KAS and TGT.

Part a (1.0 point)

State informally the authentication requirement for the above protocol.

Part b (1.0 point)

In 3-4 sentences argue informally whether the authentication requirement from Part a is satisfied by the protocol. If the protocol does not satisfy this requirement, demonstrate an attack and suggest a fix.

Part c (1.0 point)

Briefly explain the security guarantee you get if the Murphi model checker finds no errors in this protocol. Clearly list the simplifications made in constructing the model and how these assumptions can fail in the presence of a more powerful adversary.

Problem 2 (3.0 points)

The Q_{DL} protocol shown below hides the nonce generated by the initiator. The initiator's and responder's program are given below:

$$\mathbf{Init}_{DL} \equiv [\mathbf{new } x; gx := \mathbf{exp}_g x]_X(gx) \quad \mathbf{Resp}_{DL} \equiv []_X$$

We can prove the following for this protocol

$$\Gamma_1 \vdash \mathbf{Start}(X)[\mathbf{Init}_{DL}]_X \mathbf{Fresh}(X, gx)$$

where Γ_1 is empty.

The one-way authentication protocol Q_{CR} is shown below. The initiator does not generate the nonce but it is provided as a parameter to the initiator. The authentication property of the protocol depends on the nonce parameter being fresh. The initiator's and responder's program are given below:

$$\begin{array}{ll} \mathbf{Init}_{CR} \equiv (\hat{Y}, m_1)[& \mathbf{Resp}_{CR} \equiv ()[\\ \text{send } \hat{X}, \hat{Y}, m_1; & \text{receive } \hat{X}, \hat{Y}, x; \\ \text{receive } \hat{Y}, \hat{X}, s; & r := \mathbf{sign}(x, \hat{X}), \hat{Y}; \\ \text{verify } s, (m_1, \hat{X}), \hat{Y}; & \text{send } \hat{Y}, \hat{X}, r; \\]_X() &]_Y() \end{array}$$

We can prove the following for this protocol

$$\begin{aligned} \Gamma_2 \vdash_{Q_{CR}} \mathbf{Fresh}(X, m_1)[\mathbf{Init}_{CR}]_X \mathbf{Honest}(\hat{Y}) \wedge \hat{Y} \neq \hat{X} \supset \phi_{auth}. \\ \phi_{auth} \equiv \exists Y. (\mathbf{Receive}(Y, (\hat{X}, \hat{Y}, m_1)) < \mathbf{Send}(Y, (\hat{Y}, \hat{X}, \mathbf{SIG}_{\hat{Y}}\{m_1, \hat{X}\}))) \end{aligned}$$

A modified version of the invariant used in proving the above is given below. You can use this invariant in Part c of this problem.

$$\begin{aligned} \Gamma_2 \equiv \mathbf{Honest}(\hat{Y}) \supset \forall \hat{X}, t, m. (\mathbf{Send}(Y, t) \wedge \mathbf{Contains}(t, \mathbf{SIG}_{\hat{Y}}\{m, \hat{X}\}) \supset \\ (\mathbf{Receive}(Y, (\hat{X}, \hat{Y}, m)) < \mathbf{Send}(Y, (\hat{Y}, \hat{X}, \mathbf{SIG}_{\hat{Y}}\{m, \hat{X}\})))) \end{aligned}$$

A sequential composition Q_{COM} of the protocols is shown below

$$\begin{array}{l}
 \mathbf{Init}_{COM} \equiv (\hat{Y})[\\
 \quad \mathbf{new} \ m_1; \\
 \quad gm_1 := \mathbf{exp}_g \ m_1; \\
 \quad \mathbf{send} \ \hat{X}, \hat{Y}, gm_1; \\
 \quad \mathbf{receive} \ \hat{Y}, \hat{X}, s; \\
 \quad \mathbf{verify} \ s, (gm_1, \hat{X}), \hat{Y}; \\
]_X() \\
 \mathbf{Resp}_{COM} \equiv ()[\\
 \quad \mathbf{receive} \ \hat{X}, \hat{Y}, x; \\
 \quad r := \mathbf{sign} \ (x, \hat{X}), \hat{Y}; \\
 \quad \mathbf{send} \ \hat{Y}, \hat{X}, r; \\
]_Y()
 \end{array}$$

Part a (0.5 point)

State in the syntax of PCL the authentication property of Q_{COM} .

Part b (1.0 point)

Argue informally how the properties of Q_{DL} and Q_{CR} can be combined to derive the property of Q_{COM} from Part a.

Part c (1.5 point)

Now provide a formal proof of the property from Part a that follows the structure of the informal argument in Part b using the sequential composition theorem of PCL.

Problem 3 (0.5 × 3 = 1.5 points)

In this problem, we consider an active network adversary who can perform arbitrary probabilistic polynomial time (PPT) computation. Consider the following three scenarios. For each scenario, state the weakest notion of security (among IND-CPA and IND-CCA) that the encryption scheme needs to satisfy in order to guarantee secrecy of the specified payload in the presence of the adversary. Briefly justify the choice of the security notion.

1. Using SSL, honest parties A and B have already established a shared key k . A sends message m to B encrypted with k . B decrypts the ciphertext, re-encrypts it with k and sends it back to A . The payload is the message m and the adversary is an active network adversary.
2. A spaceship S sends data encrypted with the public key of a space station SS to SS that then relays this data to earth using a long term shared key k . An alien A from Mars has learnt k . A tries to fool S into sending the message “Do not attack Mars” to SS , but is not sure at this point if it succeeded, i.e. A is not sure if the message m sent by S to SS is “Do not attack Mars” or some other text. SS realizes that k has been compromised and so it forwards the message m to earth with an alternate shared key k' that is not known to A . The payload is the message m and the adversary is the alien A .

3. Nations X and Y are at war, and they have warships WX and WY out at sea. WX knows that any message it sends to its base station in the clear will be intercepted by WY , then encrypted with a shared key k_Y and sent to WY 's base station. WY sends a message m encrypted with key k_Y where m is not sent by WX that was intercepted by WY . The payload is the message m and the adversary is WX .

Problem 4 (2.5 points)

This question requires you to understand the proof of optimality of δ for privacy in the analysis of Voting protocols, as discussed in class on Sep 22, 2011.

Part a (1.25 points)

Explain why equation 4 in the proof of Theorem 2 on Page 30 of ‘Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study’ by Kuesters et al ¹ holds true. Explain the definitions you refer to, in your explanation.

Part b (1.25 points)

Justify why the value of δ in the proof of Theorem 2 on Page 31 of ‘Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study’ is optimal. Specifically, you only need to explain why the last part of the proof holds, after having derived that the difference in the probabilities involved is δ - bounded (You need to explain the part starting with ‘It remains to show that δ is optimal.’). Explain the definitions you refer to, in your justification.

¹<http://www.infsec.uni-trier.de/publications/paper/KuestersTruderungVogt-TR-2011.pdf>