CS342 Computer Security **Handout # 6**
Profs. Daniel Bilar and Lyn Turbak **September 24, 2006**
Wellesley College

Problem Set 2

Due: Midnight Monday, October 2

Overview:

In this assignment you will investigate security protocols in three paper-and-pencil problems. There is no lab component to this assignment. However, there will be a PS3 lab assignment (posted later this week and due on Friday, October 6) that will overlap with PS2.

Working Together:

All problems on this assignment are individual problem that you must solve on your own.

Submission:

Each student should submit a hardcopy containing solutions of all three problems by sliding it under Daniel's door.

Notational Conventions:

The notational conventions used on this assignment are somewhat different than those used in the class and handouts but often seen in the literature:

Principals: A (Alice), B (Bob), M (Mallory). $M(A)$ means "M acting as A".

Keys: $\{M\}_{K_{AB}}$ is a message encrypted with a key shared between A and B.

Encryption: $\{M\}_K$. Example: Encryption with A's public key: $\{M\}_{K_A}$.

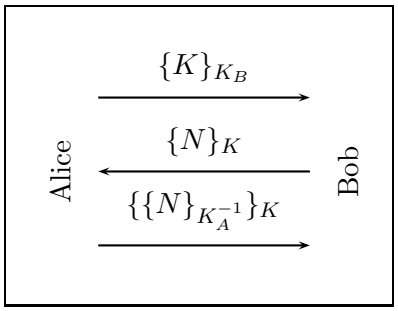
Signing: $\{M\}_{K^{-1}}$. Example: Signing with A's private key: $\{M\}_{K_A{}^{-1}}$

Nonces: N. Fresh data items used for challenge/response.

Message concatenation: $\{M1, M2\}$.

Protocol Representation: Protocols will be represented using a notation illustrated below to the left, which is an alternative representation of the notation on the right:

M1. $A \rightarrow B$: $\{K\}_{K_B}$
M2. $B \rightarrow A$: $\{N\}_K$
M3. $A \rightarrow B$: $\{\{N\}_{K_A^{-1}}\}_K$



Individual Problem [20]: Password Sniffing It's Alice's well-deserved coffee break, and she finds herself at *Starbucks*®, sipping on a latte, busily typing away on her laptop. Mallory, laptop in tow as well, walks down the street, and happens to see Alice through the window. Mallory, feeling mischievous today, and having failed his introductory ethics class, decides that it would be a lark to eavesdrop on Alice.

a. What opportunities for password sniffing (gaining access to Alice's password) does Mallory have in this scenario? Remember that security is a system, and that there are many components to it (social, hardware, software, networks, etc.) and that you are allowed to make reasonable assumptions for Alice's behaviour and habits. Describe at least five ways.

b. Mallory, having strategically placed himself next to Alice, learns that she is enjoying the free Wireless Internet to surf, checking her `POP`-based Wellesley email account and accessing a `.htaccess` protected website on `cs.wellesley.edu`. What additional opportunities avail themselves now to Mallory? Describe three more. Again, you can make reasonable assumptions about Mallory's capabilities and mischievousness.

Individual Problem [40]: Reading a Protocol

Consider the following protocol:

M1.	$A \rightarrow B$:	$\{K\}_{K_B}$
M2.	$B \rightarrow A$:	$\{N\}_K$
M3.	$A \rightarrow B$:	$\{\{N\}_{K_A^{-1}}\}_K$

Table 1: A protocol

a. Give a brief description of the protocol and what it seems to try to accomplish, e.g its goal.

b. Show that the protocol admits a *masquerading* attack. A masquerading attack occurs when someone pretends to be somebody else (masquerading is part of the man-in-the-middle attack). Discuss the reasons for the attack.

c. Modify the protocol in table 1 to prevent the masquerading attack.

Individual Problem [40]: A Type-flaw Attack

Consider the *Yahalom* protocol (table 2), a key distribution/authentication protocol. There are three principals involved; A,B and and key distribution server S. A and B share a key with S. The aim of the protocol is key generation by S of a new session key K_{AB} for principals A and B (in addition to authenticating them for the purpose of the exchange). Assume N_x are 8-bit nonces, and keys K are 16 bits long.

M1.	$A \rightarrow B$:	A, N_1
M2.	$B \rightarrow S$:	$B, \{A, N_1, N_2\}_{K_{BS}}$
M3.	$S \rightarrow A$:	$\{B, K_{AB}, N_1, N_2\}_{K_{AS}}, \{A, K_{AB}\}_{K_{BS}}$
M4.	$A \rightarrow B$:	$\{A, K_{AB}\}_{K_{BS}}, \{N_2\}_{K_{AB}}$

Table 2: Yahalom protocol

a. Describe in English what each step of the Yahalom protocol (table 2) does.

b. Alas, this protocol is susceptible to a *type-flaw* attack, which is formally described below in table 3. A type-flaw attack on a security protocol is an attack in which a field in a message that was originally intended to be of one type is subsequently interpreted as another type. Again, an assumption is violated: A field is assumed to hold one type of value, but it holds another.

M1.	$M \rightarrow B$:	M, N_1
M2.1	$B \rightarrow M(S)$:	$B, \{M, N_1, N_2\}_{K_{BS}}$
M2.2	$M(B) \rightarrow S$:	$B, \{M, N_1, N_2\}_{K_{BS}}$
M3.	$S \rightarrow M$:	$\{B, K_{BM}, N_1, N_2\}_{K_{MS}}, \{M, K_{BM}\}_{K_{BS}}$
M4.	$M \rightarrow B$:	$\{M, \{N_1, N_2\}\}_{K_{BS}}, \{N_2\}_{\{N_1, N_2\}}$

Table 3: Yahalom Type-Flaw Attack

Describe in English what the attack protocol (table 3) does.

c. Describe where the type-flaw attacks takes place and what M gains as a result of the attack (Hint: Suppose Mallory is in cahoots with Ophelia, another nefarious character. M wants to give O access to his communication with B without sending O the session key. How does the type-flaw attack help?).