CS 1653: Applied Cryptography and Network Security
Term Project, Phase 3

Lindsey Bieda leb35@pitt.edu Tucker Trainor tmt33@pitt.edu

March 2, 2012

Introduction: Cryptographic Techniques

(an introductory paragraph or two that broadly surveys the types of cryptographic techniques that your group has decided to use to address threats T1-T4)

Threat 1: Unauthorized Token Issuance

Threat Description

Begin by describing the threat treated in this section. This may include describing examples of the threat being exploited by an adversary, a short discussion of why this threat is problematic and needs to be addressed, and/or diagrams showing how the threat might manifest in your groups current (insecure) implementation.

Mechanism Description

Next, provide a short description of the mechanism that you chose to implement to protect against this threat. For interactive protocols, it would be helpful to provide a diagram explaining the messages exchanged between participating principals. (See the notes from Lecture 10 for example diagrams.) Be sure to explain any cryptographic choices that your group makes: What types of algorithms, modes of operation, and/or key lengths did you chose? Why? If shared keys are needed, how are they exchanged?

Correctness and Security of Mechanism

Lastly, provide a short argument addressing why your proposed mechanism sufficiently addresses this particular threat. This argument should address the correctness of your approach, as well as its overall security. For example, if your mechanism involves a key agreement or key exchange protocol, you should argue that both parties agree on the same key (correctness) and that no other party can figure out the key (security).

Threat 2: Token Modification/Forgery

Threat Description

Mechanism Description

Correctness and Security of Mechanism

Threat 3: Unauthorized File Servers

Threat Description

Mechanism Description

Correctness and Security of Mechanism

Threat 4: Information Leakage via Passive Monitoring

Threat Description

Suppose Eve can listen to an information exchange between Alice and Bob. Even without being able to interrupt or modify the exchange, Eve can still glean enough information to perform malicious acts. If insufficient security is in place, Eve may be able to gather enough data to

- know the contents of the exchanges;
- to impersonate Alice or Bob;
- use offline password guessing to discover passwords or other secret information.

Eve does not need to be an active participant in a conversation to illicitly benefit from it, and thus exchanges between Alice and Bob must be kept secure.

Mechanism Description

Shared key/session key to encrypt messages between Alice and Bob.

Correctness and Security of Mechanism

Summary and Errata

(conclude with a paragraph or two discussing the interplay between your proposed mechanisms, and commenting on the design process that your group followed. Did you discuss other ideas that didnt pan out before settling on the above-documented approach? Did you end up designing a really interesting protocol suite that addresses multiple threats at once? Use this space to show off your hard work!)