Instructor Notes for the "Identity Management" Scenario
September 15, 2008

The Identity Management scenario illustrates several issues related to maintaining information about the identity of users. The scenario is built around authorized user and visitor access to a physical military base. Several identity management issues are explored, including the establishment of access policies, different mechanisms for identifying people, and risks associated with using computers to manage identity information.

Phase One: Basic identity-based physical access control

- Costs of compromises are relatively low, as are costs of false positives or other denial of service.
- Users queue up outside the base, approach the guard checkpoint and attempt to gain entry to the base.
- Initially, no users are authorized to enter the base – so the guard turns all users away. The player must add user's to the base access list – or simply add the "Command" group of which each authorized user is a member.
- If the player does not permit "escorted visitors", a user continues to complain and play does not progress until visitors are permitted.
- If the player allows "public" into the base, a wall gets defaced and the users each again queue up to enter the base until "public" is no longer allowed in.
- Player has insufficient funds to purchase scanners or card readers during this phase.
- After the last user enters the base, if the player had not selected "ID Badges", a wall is defaced and remains defaced until the player selects "ID Badges". If the player had selected ID Badges, then one of the users looses a badge and requires an escort. In either event, the player progresses to phase two.

Phase Two: Keeping track of users via identity information.

- Costs of compromises are relatively low, as are costs of false positives or other denial of service.
- Users again queue up for entry just as in Phase I.
- Player is informed the commander wants to know whether a given user has entered or not.
- Users keep queuing (and player loses money) until player selects to log entries.
- If player selected to log entries, but does not automate the process, the guard complains about managing manual lists and play cycles until player automates logging by purchasing a scanner or card reader and connecting it to a computer with a database.
- Simply buying and connecting an ID Device is not enough: player must also establish the corresponding zone policy, e.g., "Hand Scanner".
- Player has insufficient money to purchase an Authorization card reader or a combination scanner and card reader.

- If player just hooks the ID Device to the local LAN, the ID database is created on the Server and is manipulated from the Internet – allowing an attacker to enter the base. Player must configure router filter – or disconnect server from the LAN to complete this phase.
- Disconnecting the LAN from the Internet causes user to complain, and objective will not complete.
- Feedback based on device selection as follows:
    - Just eye scanner; pink eye prevents user from entering, needs escort.
    - Just hand scanner – 3rd degree poison oak wraps hands in gauze
    - Just identity card reader, lost card. Stolen card. Attacker enters base using someone else's card.

Phase III Authorized and Questionable Strangers

- Costs of compromise are now very high, as are costs of preventing authorized users from entering the base.
- Players must enable access by authorized users who are not assigned to or known by the base. These visiting users are authorized by a central authority that is recognized by the base.
    - Starts with Joe, Floats and Sanders outside
    - After Floats and Sanders enter once, the Internet goes down.
    - Recognize Strangers done when Floats and Sanders enter twice
- If the player had just an "authorization card reader", then the goal of permitting authorized strangers is met because it is assumed the cards are encoded by the central authority to reflect user authorizations. No network link is needed to continue – though one is helpful for logging of entry. However, lost and stolen cards result in unauthorized entry to the base.
- Use of a plain identity card reader or a hand or eye scanners require connection to the centralized database via the Internet. Player must deploy VPN gateways to protect the data in transit. Otherwise data is compromised leading to unauthorized entry and perhaps disclosure of identity data.
- Reliance on Internet to gain access to base results in blocked access and great loss when network goes down.
- Expensive card/hand card/iris scanners eliminate the need for a internet connection logging. If network is connected, then a VPN is needed to keep the authorization system from being hacked.

SECOND OBJECTIVE [does not appear until first objective complete]

- Base work is outsourced and a lot of new contractors start showing up on the base.
- Player encouraged to biometrically scan and check "strangers" against centralized databases – possible legal/ethical issues.
- Contractors and authorized visitors keep cycling in and bad things happen until player elects to check biometrics data against a national database
    - Selection of eye scanner not adequate because of a sparse database
    - If player deploys a "dna scanner" the Admiral's daughter comes for a visit, is scanned and the guard learns she is not related to the Admiral.

And the playeris later reminded that such devices do not exist in a form that can be used for real-time authentication.