Foundations of Computer Security
Lecture 79: Security Target Example

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin
Sun Java System Identity Manager is a product for managing user access privileges stored in directory services. Evaluation to EAL2 performed by Cygnacom in summer 2005.

**Assumptions**

- OE.NoUntrusted: no untrusted users on the system
- OE.Time: the OS has reliable time stamps

**Threats**

- T.BadPasswords: users may have selected guessable passwords
- T.Abuse: authorized users perform bad actions
- T.Mismanage: administrators don’t manage security well
- T.Privil: unauthorized user gains access
- T.Undetect: attack attempts go undetected
- T.Walkaway: a user leaves workstation without logging out
Security Objectives for the TOE

- O.ManagedData: store properties of users
- O.PasswordGen: support automatic generation of passwords
- O.PasswordQual: specify password quality parameters

Security Objectives for the Environment

- OE.Time: the underlying OS provides reliable time
- ON.NoUntrusted: the administrator assures no untrusted users or software on the host
Security Requirements

- (21 requirements from CC relevant to this type of product)

TOE Summary

- Mapping of security requirements to subfunctions
- Assurance measures provided by the vendor (CVS listings, product documentation, vulnerability assessment)

Rationale: how threats are countered

- e.g., T.BadPassword is countered by O.PasswordGen and O.PasswordQual
A Security Target is a specific system or class of systems submitted for evaluation.

The policy may be specified “fresh” or as previously evaluated protection profiles.

The idea is to specify what security means for this product and how the product enforces that notion of security.

Next lecture: Common Criteria Evaluation