**Usability and Security**

**Wofür wird der Benutzer benötigt?**

* Authentifikation des menschlichen Benutzers
* Entscheidungen bezüglich der Security Policy
* Automatisierung ist zu schwer und kostspielig

**objektive Maßstäbe von Benutzbarkeit:**

* Schritte, die man benötigt, um eine bestimmte Aufgabe zu vollenden
* entspricht das Design bestimmten Benutzbarkeitskriterien?
* Unterschied zwischen Neulingen und Experten
* Begriffe werden konsistent genutzt
* Benutzer bekommt Feedback
* Benutzer werden die Konsequenzen einer Aktion verdeutlicht
* Benutzer wird nicht mit bedeutungslosen Informationen überflutet
* "undo" oder andere Wiederherstellungsoperationen

**Wie lässt sich ein sicheres System benutzerfreundlicher machen?**

* Make it "just work"
* unsichtbare Sicherheit
* vom Benutzer kann nicht erwartet werden, dass er Entscheidungen trifft, welche er nicht treffen kann
* Make security/privacy understandable
* mache sie intuitiv
* mache sie sichtbar
* Train the user
* umsetzbare Ratschläge, welche der Benutzer versteht

**Guidelines for Secure Iteraction Design:**

* Risiken eingehen sollte teuer sein
* benutze sichere Defaulteinstellungen (Sicherheitseinstellungen dauern lange und sind schwer)
* vermeide Überraschungen und Unaufmerksamkeit bei Änderungen
* das mentale Modell des Systems und das wirkliche System sollten ähnlich sein
* Benutzer sollte Aktionen abbrechen und sich von Fehlern erholen können
* Aktionen sollten rückgängig gemacht werden können
* Benutzer sollte Möglichkeit haben den Zugriff anderer auf die eigenen Ressourcen zu reduzieren
* Vertrauenswürdige Pfade
* Kanäle des Benutzers vor der Manipulation anderer schützen
* die Sprache des Benutzers sprechen
* dem Benutzer die Konsequenzen einer Entscheidung klarmachen
* Benutzer sollte Sicherheit-Policies festlegen können, die zu seiner Aufgabe passen
* das Gedankenmodell des Benutzers respektieren

**Design-Strategien:**

* Security by Admonition (Mahnung)
* für das Erteilen von Rechten wird der Benutzer gefragt
* Security by Designation (Festlegung)
* Rechte werden vorher für Benutzeraktionen festgelegt
* User-assigned Identifiers
* ein einziges Namensschema für alle Ressourcen und Anwendungen