INTERNE MITTEILUNG: GS-AG, 2011-03-23 (Apparmor)

Wie der "Zufall" so will, scheint auch Apparmor nicht zuverlässig zu sein - ein fundamentales Sicherheitswerkzeug. Da gepflegte Langzeit-Bugs fast schon selbstverständlich sind, sogar bei kernel-nahen Komponenten der OS-Basis, sollten hoffungsvolle Behauptungen überprüft werden, schon wegen der Open-Sauce und der Transpiranz ...

* Die Anweisung DENY NETWORK soll nicht zuverlässig sein (KONTROLLIEREN, siehe Bug-Reports).
* ATTRIB R soll nicht nur lesen, sondern gleich auch schreiben erlauben (KONTROLLIEREN, siehe Bug-Reports).

Gestern haben wir APPARMOR im aktuell installierten Ubuntu 10.04 LTS (Desktop und Workstations) getestet. Der Eintrag "audit deny /home/*/Desktop/Downloads/ rw," schützt bei "usr.bin.wine" weder vor dem Lesen noch vor dem Schreiben, er schützt auch nicht die Unterverzeichnisse, ist also vollkommen wirkungslos. Sämtliche Anwendungen von WINE haben Vollzugriff - auch ein zusätzliches Profil für die jeweilige Applikation löst dieses Problem nicht. Damit ist jedenfalls die Behauptung "Attrib R" als zutreffend bestätigt. ABER: Bei einem ebenso erstellten Profil "usr.bin.firefox" mit gleicher Anweisung funktioniert diese Sperre. Also befindet sich WINE außerhalb jeder zuverlässigen Apparmor-Kontrolle - Aktualisierung und ein Neustart des Systemes ändern daran nichts.

Der Eintrag "audit owner /home/*/.mozilla/firefox/*.default/bookmarkbackups/ r," im Profil "usr.bin.firefox" verhindert offensichtlich NICHT das Schreiben in /home/*/.mozilla/firefox/*.default/bookmarkbackups/bookmarks-*.* und wenn ansonsten KEINE Schreiberlaubnis (w) erteilt wurde, dann erfüllt APPARMOR seinen ureigenen Zweck nicht oder nicht zuverlässig. Wir haben an dieser Stelle den Schnell-Test beendet und ein weiteres Pseudo-Security-Tool finden können ...

Apparmor ist eiegntlich ein fundamentales Security-Management (ähnlich wie SELinux) und wenn uns derartige Fehler nach jeweils einem Testdurchlauf innerhalb einer Stunde auffallen, dann können Unzuverlässigkeiten solcher Dimension auch JEDEM professionellen Programmierer nicht entgangen sein. Reagiert das "heilige Experten-Team" darauf selbst nach mehreren Jahren mit Verschwiegenheit, dann wird dieser Zustand beabsichtigt ignoriert. Stellt man so ein Prüfergebnis den Welterklärern und medialen "Linux-Aposteln" gegenüber, dann ist ersichtlich, daß die nichtmal ihr eigenes Geschwätz seriös getestet haben. Dennoch wird überall und wiederholt behauptet Linux sei besonders sicherer, weil ..." und immer wieder pseudo-wissenschaftlich "erklärt" wie gut Apparmor mit dem Kernel verzahnt sei. Diese Kernel-Komponenten sind jedenfalls weder sicher noch zuverlässig.

EMPFEHLUNG: Eine gründliche Diagnose bezüglich der Zuverlässigkeit von Apparmor ist erforderlich, weil ansonsten fehlende System-Sicherheit zu einer realen Gefahr wird. Diese Check-Liste ist eine hilfreiche "Ergänzung" zum Test der fundamentalen Funktionen.

Was würde wohl ein Autofahrer sagen, wenn während der Fahrt das Lenkrad abbricht und anschließend die Fahrertüre herausfällt ? Würde er begeistert feststellen "der Motor läuft doch einwandfrei" und weiterhin den "genialen Konstruktions-Künsten" dieser Ingenieure vertrauen ? Und würden die "Experten" der Auto-Magazine weiterhin über das zuverlässigste Auto aller Zeiten "berichten" ?

A159 ### secur-2011-03-22-A159.htm -- (ref: toolrep_e01.htm)
