



4 AppArmor-Geschichte

AppArmor wurde ursprünglich von der Firma *Wirex Communications, Inc.* (<http://www.wirex.com>) unter dem Namen *SubDomain* entwickelt. Wirex Communications wurde 1998 von Crispian Cowan gegründet. Die Firma beschäftigte sich mit der Entwicklung von freien und kommerziellen Sicherheitslösungen, die als *Immunix* bezeichnet wurden. Das erste Produkt in dieser Reihe war StackGuard. Bei *StackGuard* handelt es sich um einen modifizierten GNU C-Compiler (gcc), der den kompilierten Code so modifiziert, dass die resultierenden Applikationen immun gegen das Einschleusen und Ausführen von Code durch Buffer-Overflow-Angriffe sind. Der StackGuard wurde auf der Immunix-Homepage (<http://www.immunix.org>) veröffentlicht. Dort stellte Wirex unter dem Namen *ImmunixOS* auch eine von der Red Hat Linux 5.1-Distribution abgeleitete Distribution zur Verfügung, die komplett mit dem StackGuard Compiler übersetzt worden war.

Im Jahr 2000 stellte Wirex mit *FormatGuard* ein weiteres Werkzeug zur Abwehr zur Verfügung und reagierte damit auf die neuartigen Angriffe, die Formatstring-Schwächen ausnutzen. FormatGuard ist eine Erweiterung der Glibc-Bibliothek. Um diesen Schutz nutzen zu können, ist ebenfalls eine erneute Übersetzung der Programme erforderlich. Basierend auf Red Hat Linux 7.0 wurde mit ImmunixOS 7.0 eine Distribution zur Verfügung gestellt, die entsprechend übersetzt worden war.

Ebenfalls wurde die Kernel-Erweiterung *SubDomain* erstmals der Öffentlichkeit vorgestellt (<http://archives.neohapsis.com/archives/linux/immunix/2000-q4/0014.html>). *Subdomain* war ein Kernel-Patch für den Linux-Kernel 2.2.17 und modifizierte die System-Calls. Dadurch konnte *SubDomain* das Lesen und Schreiben von Dateien und das Ausführen weiterer Prozesse überwachen. Die Überwachung erfolgte mit Hilfe von Profilen, die bereits eine AppArmor-ähnliche Syntax verwenden:

```
foo {
  /etc/readme r,
  /etc/writeme w,
  /usr/bin/bar x {
    /usr/lib/otherread r,
    /usr/opt/otherwrite w,
  },
}
```

Ein wesentlicher Vorteil von *SubDomain* war die schlanke Implementierung. Die erste Version bestand aus 4500 Zeilen C-Code. Der Parser benötigte 825 Zeilen

C-Code. Die Firma Wirex Communications war maßgeblich an der Entwicklung der Linux-Security-Module-Schnittstelle (*LSM*) im Kernel beteiligt. SubDomain wurde daher im Weiteren auf diese Schnittstelle portiert. Im Jahr 2003 benannte sich Wirex Communications, Inc. nach seinem Hauptprodukt in Immunix, Inc., um. Im Jahr 2004 wurde SubDomain an die *SUSE*-Distribution angepasst. Anfang 2005 wurde SubDomain in *AppArmor* umbenannt und unter dem neuen Namen beworben. Im Mai 2005 erwarb *Novell Inc.* die Firma Immunix Inc. Das Produkt AppArmor wurde erstmals mit dem ServicePack 3 für den SUSE Linux Enterprise Server (SLES) 9 von Novell veröffentlicht. Im Januar 2006 stellte Novell AppArmor unter der GNU General Public License (GPL) zur Verfügung und gründete das AppArmor-Projekt auf <http://www.opensuse.org/Apparmor>, wo die weitere Entwicklung stattfindet.