



Eine Security Policy Engine für Virtuelle Private Netze

Motivation

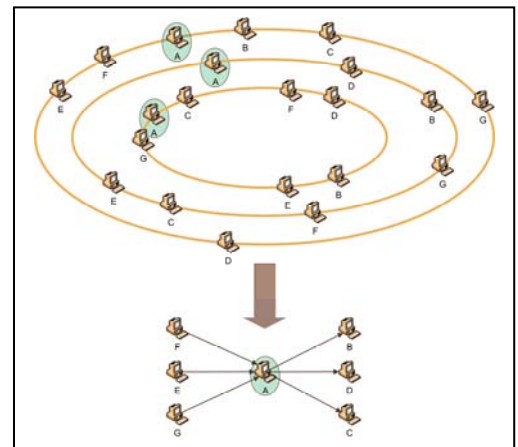
Virtuelle Private Netze sind Overlay-Netze, die von einem bestimmten Nutzerkreis gebildet werden und nur diesem zur Verfügung stehen. Sie werden von einem Initiator „gegründet“ und können einem bestimmten Zweck dienen – z. B. Videospiele, Telefonie, Distributed Computing, File Sharing ... – oder auch eher allgemeine Ziele verfolgen. Es stellt sich aber die Frage, wie Sicherheitsziele in einem solchen Netz kooperativ erreicht werden können.

Als möglicher Weg, die Sicherheit eines solchen Netzwerks zu verbessern, wurde am Lehrstuhl ein flexibler Mechanismus entworfen, der Policies (Richtlinien) zur Steuerung der Sicherheit im Netzwerk vorsieht. Am Netz beteiligte Knoten evaluieren diese Policies und treffen Entscheidungen wie die Aufnahme neuer Knoten ins Netz anhand der in den Policies definierten Regeln.

Aufgabenstellung

In dieser Arbeit bauen wir auf der bereits erfolgten formalen Definition unseres Policy-Mechanismus auf. Ziel ist es eine Policy Engine zu entwerfen und zu implementieren, die Beitrittsvorgänge kontrollieren kann und für weitere Zwecke erweiterbar bleibt. Dabei muss insbesondere gelöst werden:

- Umsetzung von Policies in entsprechenden Datenstrukturen
- Ausführung von Policy-Kombinationen
- Implementierung von 1-2 sog. „Kontrollmethoden“



Kontrollmethoden werden von der Policy Engine ausgeführt und liefern als Ergebnis wahr oder falsch. Beispiele für solche Methoden sind:

- Access Control Lists (ACL)
- Signaturverifizierung (z. B. mit PGP/GPG)
- Auswertung bestimmter Messwerte
(Hierfür gibt es ein fertiges, am Lehrstuhl entwickeltes Framework)

Voraussetzungen

Engagement und Freude an der Arbeit; Kenntnisse in Python oder Java; Kenntnisse in Netzsicherheit sind hilfreich

Stichworte

Policies, Sicherheit in privaten Netzen, Kryptographie

