Bell-LaPadula Modell

Das Bell-LaPadula-Modell ist ein mathematisches Modell für die Sicherheitspolitik in Computersystemen, das 1973 von den US-amerikanischen Informatikern David Elliott Bell und Leonard J. LaPadula entwickelt wurde. Das Modell basiert auf dem Konzept der Mandatory Access Controls (MAC) und ist besonders relevant für sicherheitskritische Umgebungen wie Regierungs- und Militärsysteme.

Das Bell-LaPadula-Modell konzentriert sich auf die Vertraulichkeit von Informationen und stellt sicher, dass keine nicht autorisierte Freigabe von Informationen stattfindet. Es basiert auf zwei Hauptprinzipien:

1. **No Read Up (NRU)**: Dieses Prinzip besagt, dass ein Subjekt auf keine Weise auf Informationen zugreifen kann, die sich auf einer höheren Sicherheitsstufe befinden als das Subjekt selbst. Mit anderen Worten, ein Subjekt auf einer niedrigeren Sicherheitsstufe darf keine Informationen von einer höheren Sicherheitsstufe lesen.

2. **No Write Down (NWD)**: Dieses Prinzip besagt, dass ein Subjekt keine Informationen auf einem niedrigeren Sicherheitsniveau schreiben oder weitergeben kann als das Sicherheitsniveau des Subjekts selbst. Mit anderen Worten, ein Subjekt auf einer höheren Sicherheitsstufe darf keine Informationen auf einer niedrigeren Sicherheitsstufe schreiben.

Zusätzlich zu diesen beiden Hauptprinzipien umfasst das Bell-LaPadula-Modell auch eine Struktur von Sicherheitsklassen und -niveaus, die den Zugriff auf Ressourcen steuern. Diese Klassifizierungen basieren oft auf Etiketten wie "Top Secret", "Secret", "Confidential" usw.

Das Bell-LaPadula-Modell bietet eine formale Methode zur Überprüfung und Durchsetzung von Sicherheitsrichtlinien in Computersystemen, die auf der Vertraulichkeit von Informationen basieren. Es hat jedoch seine Grenzen und berücksichtigt nicht andere wichtige Sicherheitsaspekte wie Integrität und Verfügbarkeit von Informationen.

Das Konzept der **Nicht-Interferenz**, auch bekannt als "Noninterference" oder "Non-interference Security Model", wurde 1982 von Kenneth J. Biba in seinem Artikel "Integrity Considerations for Secure Computer Systems" eingeführt. Es handelt sich um ein Sicherheitsmodell, das sich auf die Integrität von Informationen konzentriert.

Das Grundprinzip der Nicht-Interferenz besteht darin, sicherzustellen, dass das Verhalten eines Subjekts auf einem höheren Sicherheitsniveau die Integrität der Informationen auf einem niedrigeren Sicherheitsniveau nicht beeinträchtigen kann. Anders ausgedrückt, ein Subjekt mit höherem Zugriffsprivileg darf keine unerwünschten Änderungen an Informationen vornehmen, auf die Subjekte mit niedrigeren Zugriffsprivilegien zugreifen können.

Das Modell der Nicht-Interferenz kann in zwei Kategorien unterteilt werden:

1. **Starke Nicht-Interferenz**: Unter starkem Nicht-Interferenzprinzip dürfen Änderungen, die von Subjekten auf einem höheren Sicherheitsniveau vorgenommen werden, die Sichtbarkeit oder Integrität der Informationen auf einem niedrigeren Sicherheitsniveau nicht beeinträchtigen.

2. **Schwache Nicht-Interferenz**: Unter schwachem Nicht-Interferenzprinzip dürfen Änderungen, die von Subjekten auf einem höheren Sicherheitsniveau vorgenommen werden, die Sichtbarkeit der Informationen auf einem niedrigeren Sicherheitsniveau beeinträchtigen, dürfen jedoch deren Integrität nicht beeinträchtigen.

Das Konzept der Nicht-Interferenz ist besonders wichtig für Systeme, in denen die Integrität von Informationen von entscheidender Bedeutung ist, wie beispielsweise Finanz- oder Gesundheitsinformationssysteme. Es bietet eine formale Methode zur Überprüfung und Durchsetzung von Integritätsrichtlinien und hilft, unerwünschte Änderungen oder Manipulationen an kritischen Daten zu verhindern.

Die Nichtableitbarkeit (englisch: "Non-Deducibility") ist ein Sicherheitskonzept, das von Dorothy E. Denning und Peter J. Denning im Jahr 1986 in ihrem Artikel "Certification of Programs for Secure Information Flow" vorgestellt wurde. Es ist eine Erweiterung des Konzepts der Nicht-Interferenz und konzentriert sich auf den Schutz sensitiver Informationen vor unautorisierten Ableitungen.

Das Konzept der Nichtableitbarkeit besagt, dass aus dem Verhalten eines Systems keine Schlüsse auf die sensiblen Informationen gezogen werden können, auf die ein Benutzer keinen Zugriff hat. Anders ausgedrückt, selbst wenn ein Benutzer nur Zugriff auf eine bestimmte Menge unklassifizierter Informationen hat, darf er aus dem Verhalten des Systems keine sensiblen oder klassifizierten Informationen ableiten können.

Das Ziel der Nichtableitbarkeit besteht darin, sicherzustellen, dass selbst wenn ein Benutzer Zugriff auf Informationen auf einem niedrigeren Sicherheitsniveau hat, er nicht in der Lage ist, durch Beobachtung des Verhaltens des Systems auf Informationen auf einem höheren Sicherheitsniveau zu schließen.

Das Konzept der Nichtableitbarkeit ist besonders relevant für sicherheitskritische Systeme, in denen die Vertraulichkeit von Informationen von entscheidender Bedeutung ist. Es bietet eine Methode zur Überprüfung und Gewährleistung des Schutzes sensitiver Informationen vor unautorisierten Ableitungen, auch wenn Benutzer Zugriff auf Teile der Informationen haben, aber nicht auf alle.

Ein verdeckter Kanal (englisch: "Covert Channel") ist ein Kommunikationsweg oder Mechanismus in einem Computersystem, der nicht für den offiziellen Informationsaustausch vorgesehen ist und normalerweise dazu verwendet wird, Informationen heimlich zu übertragen oder zu manipulieren. Diese Kanäle werden oft ausgenutzt, um Sicherheitsrichtlinien zu umgehen oder unbefugten Zugriff auf sensible Informationen zu ermöglichen.

Es gibt zwei Hauptarten von verdeckten Kanälen:

1. **Speicherkanäle**: Diese Kanäle nutzen die gemeinsame Nutzung von Speicherressourcen, um Informationen zwischen Prozessen zu übertragen. Beispielsweise können zwei Prozesse ihre gemeinsame Nutzung von Speicherbereichen verwenden, um Informationen durch das Setzen und Löschen von bestimmten Bits zu übertragen.

2. **Zeitkanäle**: Diese Kanäle basieren auf der Kontrolle der Systemressourcen, insbesondere der CPU-Zeit oder der Netzwerkbandbreite. Ein Prozess kann beispielsweise seine Ausführungsgeschwindigkeit so ändern, dass ein anderer Prozess, der diese Änderung überwacht, daraus Informationen ableiten kann.

Verdeckte Kanäle stellen eine ernsthafte Sicherheitsbedrohung dar, da sie dazu verwendet werden können, Informationen zu stehlen, Systeme zu kompromittieren oder Sicherheitsmaßnahmen zu umgehen. Die Erkennung und Verhinderung verdeckter Kanäle erfordert spezielle Sicherheitsmechanismen und Überwachungstechniken, um unautorisierte Kommunikationen zu identifizieren und zu unterbinden.

Das Beweisen von Informationsflusseigenschaften von Systemen und Programmen ist ein wichtiger Aspekt der Sicherheitsanalyse, insbesondere wenn es darum geht sicherzustellen, dass sensible Informationen nicht unerlaubt weitergegeben oder manipuliert werden können. Informationsflusseigenschaften beziehen sich auf die Art und Weise, wie Informationen innerhalb eines Systems oder Programms fließen und welche Sicherheitsgarantien bezüglich der Vertraulichkeit und Integrität dieser Informationen gelten.

Beim Beweisen von Informationsflusseigenschaften werden formale Methoden verwendet, um sicherzustellen, dass bestimmte Sicherheitsrichtlinien eingehalten werden. Dazu gehören beispielsweise:

1. **Vertraulichkeit**: Sicherstellen, dass sensible Informationen nur von autorisierten Benutzern oder Prozessen gelesen werden können und dass keine unautorisierte Weitergabe an nicht autorisierte Entitäten stattfindet.

2. **Integrität**: Sicherstellen, dass Informationen während ihrer Übertragung oder Verarbeitung nicht unerlaubt manipuliert oder verändert werden können.

3. **Abhängigkeiten zwischen Sensitivitätsstufen**: Sicherstellen, dass keine unerlaubte Informationsübertragung zwischen verschiedenen Sicherheitsstufen oder Klassifizierungen stattfindet. Zum Beispiel, dass Informationen auf einem höheren Sicherheitsniveau nicht auf ein niedrigeres Sicherheitsniveau durchsickern können.

Formale Methoden zum Beweisen von Informationsflusseigenschaften umfassen oft mathematische Modelle wie Lattice-basierte Zugriffskontrollen, Typsysteme oder Analyse von Flussgraphen. Diese Methoden ermöglichen es, Sicherheitsrichtlinien formal zu spezifizieren und zu überprüfen, ob ein System oder Programm diese Richtlinien einhält.

Das Beweisen von Informationsflusseigenschaften ist besonders wichtig in sicherheitskritischen Anwendungen wie Regierungssystemen, Finanzinstitutionen oder kritischen Infrastrukturen, wo der Schutz von sensiblen Informationen von größter Bedeutung ist.