

**Offen gebliebene Frage:** Wie kann man sicherstellen, dass ein Grid System von unberechtigten Eingriffen geschützt wird. Konkreter gefragt: Wenn ein Hacker es schafft in das Grid System auf dem Grid-Knoten (Client) einzubrechen und Ergebnisdaten zu verfälschen, wie kann man dem Grid System trauen, richtige Ergebnisse vorzuweisen.

**Antwort:** Wir setzen an der Stelle mit der Beantwortung der Frage auf, an der die Ergebnisdaten vom Grid-Knoten (Client) an den Grid-Server geschickt werden. Davor kann ein Hacker in das Grid Rechenwerk auf dem Grid-Knoten mit verschiedenen Techniken (Schlüssen knacken, Kernel Modifikationen des Betriebs- oder Anwendungssoftware-Systems, Vortäuschen falscher Identifikationen etc.) das Ergebnis verfälscht haben.

Auf dem Grid-Server wird das Ergebnispaket des Grid-Knoten (Client) analysiert, ob die Ergebnisdaten syntaktisch, semantisch und Sicherheitskontext bezogen (Verschlüsselung) korrekt sind. Ist dies alles der Fall, geht der Grid-Server von einem gültigen Ergebnispaket aus und leitet es der Trust Komponente zur weiteren Analyse weiter, was im Folgenden ausgeführt wird.

Und hier kommt der Punkt, an dem man durch verschiedenste Mechanismen sicherstellen kann, dass das Ergebnis "mathematisch" korrekt ist. An Hand einiger Beispiele wird hier aufgezeigt, wie das in realen Grid Umgebungen implementiert worden ist:

- ◆ Jeder Grid-Knoten (Client) wird durch einen Trust-Index charakterisiert. Ist der Trust-Index hoch (was beispielsweise bei Rechnern der Fall ist, die man selber im Zugriff hat und selber betreut), wird diesem Rechner eine höhere Ergebnisqualität zugesprochen, als ein Grid-Knoten (Client), der neu einem Grid beigetreten ist und noch nie Ergebnispakete zurückgeliefert hat.
- ◆ Über die Laufzeit eines Grid-Knoten (Client) verändert sich der Trust-Index entsprechend den Analysen, ob Ergebnispakete "mathematisch" korrekt zurückgegeben worden sind. Sind die Ergebnisse ohne Beanstandung, steigt der Trust-Index, gab es Beanstandungen, wird der Trust-Index des Grid-Knoten (Client) auf den Wert eines neuen Grid-Knotens (Client) zurückgesetzt.
- ◆ Eine verschwenderische Möglichkeit die Richtigkeit der Ergebnisse zu überprüfen wäre, ein und dasselbe Aufgabenpaket an zwei Grid-Knoten (Client) zu verschicken. Wobei hier der Trust-Index des einen Grid-Knotens (Client) deutlich höher (Wert ist konfigurierbar) sein muss als der des anderen Grid-Knotens (Client). Sind beide Ergebnispakete empfangen worden, werden die Ergebnisse verglichen. Sind die beide gleich, liegt ein korrektes Ergebnis vor. Die Trust-Index Werte werden entsprechend erhöht. Sind die Ergebnisse unterschiedlich, liegt eine Fälschung vor. Als Grid Betreiber kann man sich nun überlegen, entweder dem Ergebnis des Grid-Knotens (Client) mit dem hohen Trust-Index zu vertrauen oder schickt das gleiche Aufgabenpaket noch einmal an einen Grid-Knoten (Client) mit einem hohen Trust-Index. Der Grid-Knoten (Client) mit dem geringeren Trust-Index wird darüber hinaus auch noch gesenkt.
- ◆ Fallen Grid-Knoten (Clients) unterhalb eines gewissen Trust-Index Werts, werden diese Grid-Knoten (Clients) aus dem Grid Verbund herausgenommen, um die Rechenleistung des Grids nicht zu verringern. Liegt die e-Mail Adresse des Grid-

## Ein sicheres Grid System kommt nicht von alleine

- Knotens (Client) vor, kann der Grid-Server eine Benachrichtigung an diesen zu dessen Information schicken.
- ◆ Da die eben beschriebene verschwenderische Möglichkeit die Rechenleistung eines Grids halbiert (jedes Aufgabenpaket wird zwei Mal berechnet), können hier verschiedene andere Mechanismen zur Optimierung herangezogen werden:
    - Die Aufgabenpakete werden überlappend vergeben, so dass jeder Grid-Knoten (Client) immer dazu beiträgt die Ergebnispakete des Vorgänger und Nachfolger Grid-Knotens (Client) mit zu überprüfen
    - Es werden vom Grid-Server durch Zufall bestimmte Ergebnisse des Ergebnispaketes auf dem Grid-Server zur Kontrolle noch einmal selber berechnet
    - Es werden vom Grid-Server per Zufall kleinere Intervalle als Kontroll-Aufgabenpakete an Grid-Knoten (Clients) verschickt und anschließend mit dem bereits vorliegenden Ergebnissen verglichen

**Zusammenfassung: Ein sicheres Grid System kommt nicht von alleine** und man muss dafür etwas tun. Die Ausführungen sind bewusst auf einem abstrakten Niveau gehalten worden, da es im Sinne des Betreibers eines Grids liegt, den für ihn persönlich zu vertretenden Aufwand zu tätigen, um seinen Ergebnissen Vertrauen zu schenken. Und Aufgrund unserer Erfahrungen sind wir in der Lage das in ein stimmiges Gesamtkonzept zu bringen.

