Engineering von Protokollen zur sicheren Zweiparteienberechnung

Fortschritte im Entwurf, Optimierung und Anwendungen effizienter sicherer Funktionsauswertung

Dipl.-Inf. (Univ.) Thomas Schneider

Lehrstuhl für Systemsicherheit, Horst Görtz Institut für IT-Sicherheit,
Fakultät für Elektrotechnik und Informationstechnik an der Ruhr-Universität Bochum

Zusammenfassung. Sichere Zweiparteienberechnungen, auch bezeichnet als sichere Funktionsauswertungen (engl. Secure Function Evaluation, SFE), erlauben zwei sich gegenseitig misstrauenden Parteien (Client & Server), gemeinsam eine beliebige Funktion f auf ihren jeweiligen Eingabedaten x, y zu berechnen, ohne über die Ausgabe $z = f(x, y)$ hinausgehende Informationen preiszugeben. Für lange Zeit galten solche generischen Techniken als ineffizient. Durch die rasante Entwicklung von Computern und Kommunikationsnetzen, algorithmische Verbesserungen, automatische Generierung und Optimierung von SFE Protokollen sind sie jedoch mittlerweile auch für praktische Anwendungsszenarien nutzbar geworden. Diese Arbeit präsentiert die folgende fundamentale Fortschritte im Bereich des Entwurfs, der Optimierung und Anwendungen effizienter SFE.

Optimierungen und Konstruktionen von Schaltkreisen. Die Komplexität bekannter effizienter SFE Protokolle hängt linear von der Größe der zu berechnenden Funktion ab. Zudem ermöglichen moderne SFE Verfahren basierend auf verbesserten Garbled Circuit (GC) Konstruktionen die kostengünstige sichere Berechnung von XOR Gattern. Wir zeigen Transformationen, welche die Größe von booleschen Schaltkreisen erheblich reduzieren, wenn XOR Gatter deutlich weniger Kosten verursachen als andere Gatter. Die vorgestellten Optimierungen ermöglichen effizientere Schaltkreise für Standardfunktionalitäten wie Vergleichsoperationen und schnelle Multiplikation.

Hardwareunterstützte SFE Protokolle. Wir verbessern die Einsetzbarkeit von SFE Protokollen durch hardware-basierte Konstruktionen. Insbesondere können GCs von einer manipulationssicheren Hardware generiert werden, die der Server einem Client zur Verfügung stellt, ohne dass der Client dieser Hardware vertraut. Das vorgestellte hardwareunterstützte SFE Protokoll erlaubt erstmalig, daß die Kommunikation zwischen Client und Server unabhängig von der Größe der berechneten Funktion ist. Des Weiteren wird gezeigt, wie GCs in Hardware seitenkanalresistent ausgewertet werden können (engl. One-Time Programs).

Modulares Design effizienter SFE Protokolle. Die automatische Generierung von SFE Protokollen aus einer Spezifikation ermöglicht die verbesserte Benutzbarkeit für Anwendungsentwickler und weniger fehleranfällige Implementierungen. Wir stellen ein Framework vor, welches den modularen Entwurf effizienter SFE Protokolle als Sequenz von Operationen auf verschlüsselten Daten ermöglicht. Das Framework erlaubt die Kombination effizienter SFE Protokolle, basierend auf homomorpher Verschlüsselung sowie GCs, und abstrahiert von den zu Grunde liegenden kryptographischen Details. Unsere zugehörige Sprache und das Werkzeug TASTY (Tool for Automating Secure Two-partY computations) erlauben es, solche modularen und effizienten SFE Protokolle zu beschreiben, automatisch zu generieren, auszuführen und zu benchmarken.

Anwendungen. Die in dieser Arbeit vorgestellten Fortschritte wurden bei zahlreichen Anwendungen eingesetzt wie beispielsweise effizientere sichere Auktionen sowie sichere Gesichtserkennung, bei der die Eingabedaten geheim gehalten werden. Die Kombination von GCs und manipulationssicherer Hardware ermöglicht es erstmals, Daten sicher an einen nicht vertrauenswürdigen Anbieter Dienstanbieter ("Cloud") so auszulagern, dass beliebige Berechnungen auf den ausgelagerten Daten mit kurzer Antwortzeit sicher berechnet werden können.