



Qumate.Security.TLS/IKE

Prüfen Sie die Sicherheit Ihrer Netzwerke

Wenn Server untereinander oder mit Clientsystemen kommunizieren, gehört die Absicherung dieser Verbindungen heute immer dazu. Man möchte wissen, wer mit wem verbunden ist und die übertragenen Daten verschlüsseln, damit Dritte diese nicht mitlesen oder verändern können. Diese Netzwerkverbindungen werden mit kryptographischen Mitteln gesichert.

Gehen Sie auf Nummer sicher! Finden Sie Fehler in der Implementierung und Konfiguration Ihrer sicheren Netzwerke, bevor es Hacker tun.

Transport Layer Security (TLS) und Internet Key Exchange (IKE)/Internet Protocol Security (IPsec) sind heute als Grundlage von sicheren Netzen anerkannte Standards. Dabei sind die Implementierung sowie der korrekte Einsatz bestehender Bibliotheken eine große Herausforderung. Die verfügbare Vielfalt an Konfigurationsoptionen ist derart riesig, dass sowohl bei der Integration als auch bei der späteren Konfiguration des Produktsystems Schlupflöcher für Angreifer entstehen können. achelos bietet Ihnen ein leistungsfähiges Testmittel, um diese Lücken und Fehler zu finden, damit Ihre Netzwerkverbindungen sicher werden.

achelos Testsuiten sichern Ihr Netzwerk

Qumate.Security.TLS und Qumate.Security.IKE untersuchen Ihr Produkt im Hinblick auf die sichere Umsetzung und das Verhalten gegen Fehler, die von Angreifern häufig verwendet werden, um Ihre schutzbedürftigen Datennetze zu betreten. Untersuchungsaspekte des BSI wurden in Zusammenarbeit mit den Experten einer akkreditierten Prüfstelle zu leistungsfähigen Testmitteln entwickelt.

Leistungsstarke Werkzeuge

Testziele sind die Prüfung des kompletten Aufbaus der TLS- oder IKE-Verbindung bis zur gegenseitigen Authentifizierung und die Reaktion auf fehlerhaftes Verhalten:

- fehlende oder falsche Kommunikationsteile
- fehlerhaftes Schlüsselmaterial
- fehlerhafte Zertifikate
- ungeeignete Cipher-Suiten
- fehlerhafte Reaktion auf Manipulationen

Im Rahmen der Zertifizierung von Netzwerkkomponenten benötigen Hersteller, Evaluatoren und Zertifizierer diese leistungsstarken Werkzeuge. Mit ihrer Hilfe können Sie die Implementierungen der Sicherheitsprotokolle detailliert untersuchen und die Ergebnisse angemessen protokollieren.

Optimieren Sie die Entwicklung Ihrer Netzwerkkomponente

Sie planen die Einführung einer innovativen neuen Netzwerkkomponente und möchten den Markteintritt so schnell wie möglich realisieren? Dann bieten wir Ihnen leistungsstarke Testsuiten, die Sie bereits parallel zur Entwicklung einsetzen können. Sie überprüfen automatisiert, kontinuierlich den jeweiligen Stand der Implementierung auf die Einhaltung kryptografischer Prozesse sowie das regelkonforme Verhalten Ihrer Komponente. Sichern Sie sich diesen Wettbewerbsvorteil und nutzen ein Produkt, das die Evaluation und Zertifizierung Ihrer neuen Netzwerkkomponente optimal unterstützt. Mit den Testsuiten von achelos können auch bereits im Markt eingesetzte Netzwerkkomponenten untersucht werden.

Vorteile für Hersteller:

- effiziente und qualitativ hochwertige Entwicklung durch entwicklungsbegleitende Testverfahren
- Zeitersparnis verschafft Wettbewerbsvorteil durch schnellere Markteinführung
- optimale Ergebnisse im Zertifizierungsprozess durch standardisierte Testverfahren mit aussagefähigen Prüfberichten
- individuelle Konfigurierbarkeit der gewünschten Tests

Automatisierte Testverfahren für Profis

Eine Vielzahl von Test- und Evaluierungshäusern nutzen bereits die Testsuiten aus der Qumate.World, um Tests im Rahmen akkreditierter Prüfverfahren durchzuführen. Die Testsuiten von achelos sind sehr flexibel und besitzen einen hohen Automatisierungsgrad. Anwender können sich ganz gezielt auf das Testen konzentrieren, eigene Testideen umsetzen sowie Testumfang und -tiefe mitbestimmen.

Die Qumate Produkte unterstützen Sie bei der Umsetzung Ihrer Softwareentwicklung im Sinne der ISO/ IEC 27000. Tests werden von der Anforderung bis zum Report durchgängig und nachvollziehbar dokumentiert. achelos hat bei der Architektur und Implementierung der Testsuiten systematisch auf einen modularen Aufbau geachtet. Auf Basis des Qumate.Testcenters lassen sich verschiedene Testsuiten, Werkzeuge und Simulationen integrieren. Ihr Entwicklungs- und Testteam nutzt die sehr komfortable Simulationsumgebung der Qumate.Security.World. Automatisierte Tests und ausführliche Testberichte weisen die Qualität von Produkten nach. Sie benötigen keinerlei weitere IT-Infrastruktur oder aufwendige Laborumgebung.

TLS-Implementierungen sicher testen



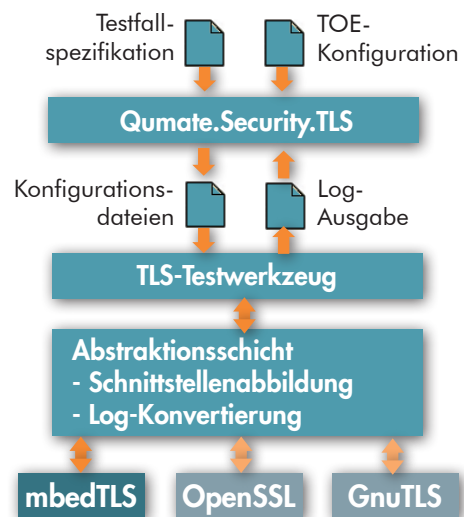
Für die Überprüfung der Eigenschaften der TLS-Implementierung von Clients und Servern wird eine Testumgebung in der Qumate.Security.World bereitgestellt. Auf Basis von Testaspekten, die von Prüflaboren auf eine angestrebte CC-Evaluierung einer Netzwerkkomponente ausgerichtet sind, hat achelos ein produktunabhängiges TLS-Testwerkzeug entwickelt. Dabei verhält sich Qumate.Security.TLS entweder als Client, um Ihre Server zu prüfen oder als Server, um das Clientverhalten zu untersuchen.



Prüfen Sie Ihre IKE/IPsec-Implementierung

Die Testsuite Qumate.Security.IKE hat achelos analog zu TLS entwickelt, sie prüft die Internet-Key-Exchange Implementierung. Das IKE-Werkzeug behandelt auch Testaspekte der IPsec-Ebene.

Architektur der Testumgebung



Architektur am Beispiel TLS (IKE analog)

Produktvarianten Testsuiten der Qumate.Security.World sind inkl. Testwerkzeuge einzeln verfügbar:

- Qumate.Security.TLS-Client
- Qumate.Security.TLS-Server
- Qumate.Security.IKE-IPsec

optional:

- Simulationsumgebung
- Software Development Kit