Automatisierte Testverfahren für TLS-Bibliotheken

Ben Swierzy

Das TLS-Protokoll ist verantwortlich für die Verschlüsselung und Authentifizierung der meisten Kommunikation im Internet. Anwendungen verwenden zur Nutzung von TLS in der Regel Bibliotheken, wodurch sich die Entwickler nicht mit den teils sehr komplexen Protokolldetails beschäftigen müssen. Die korrekte Funktionsweise der Bibliotheken wird dadurch essentiell für die Sicherheit von vielen Anwendungen. In diesem Vortrag werden verschiedene Techniken zum automatisierten Testen mit deren Stärken und Schwächen skizziert. Zum Abschluss gibt es einen Ausblick auf die Bedeutung der Techniken für automatisierte Bibliotheks- und Versionserkennung.