Elektrotechnisches Kolloquium

der Bergischen Universität Wuppertal

Die Fakultät für Elektrotechnik, Informationstechnik und Medientechnik lädt zur Teilnahme an folgender Vortragsveranstaltung mit anschließender Diskussion ein:

Es spricht Pascal Bemmann

Lehrstuhl für Lehrstuhl für IT-Sicherheit und Kryptographie
Prof. Dr.-Ing. Tibor Jager

über das Thema

On Practical Subversion-Resilience

Inhalt:

Die sichere Kommunikation über das Internet ist zu einem festen Bestandteil unseres Alltags geworden. Wir verlassen uns darauf, dass unsere Kreditkartendaten nicht kompromittiert werden, wenn wir im Internet einkaufen. Von modernen Instant-Messaging Apps wie WhatsApp und Signal erwarten wir, dass unsere privaten Gespräche mit Freunden und Familie vor dem Zugriff Dritter geschützt sind. All dies ist durch den Einsatz moderner Kryptographie möglich geworden. In den letzten Jahren wurde aufgedeckt, dass mächtige Angreifer diese Sicherheit, an die wir uns so lange gewöhnt haben, im großen Stil untergraben haben. Im Jahr 2013 wurde durch die Snowden-Enthüllungen die massenhafte und verdachtsunabhängige Überwachung der Telekommunikation auf globaler Ebene, vor allem durch die USA, bekannt. Insbesondere wurde festgestellt, dass die Sicherheit gängiger kryptographischer Protokolle durch die Verwendung von sogenannter Backdoors (deutsch „Hintertüren“) untergraben wurde. Diese Backdoors beschreiben Angriffe, bei denen die Implementierung kryptografischer Primitive unbemerkt verändert wird. Dadurch wurde es möglich, dass Geheimdienste unberechtigten Zugriff auf eine Kommunikation erhielten, die zuvor als sicher galt. Diese Enthüllungen stießen einer Reihe von wissenschaftlichen Arbeiten an, die diese Angriffe formal beschrieben sowie geeignete Gegenmaßnahmen entwickelten. Eine dieser Gegenmaßnahmen ist das so genannte „Watchdog“-Modell. Hierbei wird angenommen, dass ein vertrauenswürdiger Wächter (Watchdog) eine Implementierung, die mutmaßlich Backdoors enthält, gegen eine Spezifikation testet, bevor diese tatsächlich zum Einsatz kommt. Ein Angreifer ist nur dann erfolgreich, wenn er es schafft, die Tests des Watchdogs zu umgehen, und es ihm trotzdem gelingt, die Sicherheit einer Primitive zu brechen. Es wurden bereits beeindruckende Fortschritte beim Entwurf von sicheren Primitiven in diesem Modell erzielt. Dennoch gibt es nach wie vor eine Reihe von Aspekten in den bisher zur Verfügung stehenden Primitiven, welche die Anwendbarkeit einschränken. In diesem Vortrag werden Ansätze diskutiert, wie die Anwendbarkeit von Verfahren, die gegen Hintertüren geschützt sind, weiter verbessert werden kann.
Der Vortrag ist auf Englisch

T e r m i n : **20.12.2023, 14 Uhr**

O r t : **Online via Zoom** (Meeting ID: 695 6296 7570, Passcode: xb7RGe0u)
https://uni-wuppertal.zoom.us/j/69562967570?pwd=UGRCV3VmRnkwQ0Z2VmRzQXV4SURRdz09