Kurzfassung der Dissertation

Sichere E-Mail-Kommunikation mit XML-basierten Technologien

Dipl.-Ing. Lijun Liao
Lehrstuhl für Netz- und Datensicherheit
Ruhr-Universität Bochum

E-Mail ist heutzutage eine der erfolgreichsten Anwendungen des Internets. Das aktuelle E-Mail Format ist im Standard RFC 822 der Internet Engineering Task Force (IETF) spezifiziert, jedoch sind einige Teile der Spezifikation für den täglichen Gebrauch nicht zufriedenstellend.

Erstens, die Datenstruktur ist sehr kompliziert. Header-Felder, die die Darstellung einer E-Mail beschreiben, werden mit Header-Feldern für die Adressierung, die Verwaltung und den Transport gemischt. Darüber hinaus erhöht die Komplexität der Struktur eines E-Mail-Body deutlich, wenn die E-Mail signiert oder verschlüsselt ist. Zweitens, das E-Mail Format ist für die Speicherung großer Datenmenge ungeeignet. Drittens, individuelle Informationen können nicht an einzelne Empfänger zugestellt werden, wenn diese als „Bcc“ adressiert werden. In diesem Fall reagieren E-Mail-Clients auf zwei unterschiedliche Arten. Entweder verwirft der E-Mail-Client alle verborgenen Empfänger, oder er erzeugt für jeden Eintrag im Bcc-Feld eine Kopie der E-Mail, die dann ausschließlich an diesen Empfänger versandt wird. Beide Lösungen sind nicht zufriedenstellend. Entweder kann der Empfänger nicht überprüfen, ob er tatsächlich der intendierte Empfänger ist, oder es werden wertvolle Berechnungs- und Kommunikationsressourcen verschwendet. Viertens, die Absicherung durch digitale Signaturen und Verschlüsselungsfunktionen betrifft stets den gesamten E-Mail-Body. Dies führt ebenfalls zu unnötigem Einsatz von Ressourcen. Der bisherige Standard zur Bearbeitung signierter bzw. verschlüsselter Multipart E-Mails sieht vor, dass die E-Mail immer vollständig eingelesen wird. Auch wenn nur einzelne Teile der E-Mail verwendet werden sollen, muss die gesamte E-Mail zuerst heruntergeladen und verifiziert bzw. entschlüsselt werden. Entsprechend werden auch hier wertvolle Berechnungs- und Kommunikationsressourcen verschwendet. Fünftens, eine E-Mail Signatur gewährleistet nicht die Integrität der Header-Felder, obwohl durch die Manipulation bestimmter Header-Felder Phishing-Angriffe möglich werden.

Um diese Probleme zu lösen, wird in dieser Arbeit ein neues E-Mail-Format namens XMail vorgeschlagen. In XMail werden Nachrichten in Form von XML Dokumenten transportiert. Zum Verschlüsseln und Signieren wird auf die für XML definierten Standards XML-Encryption und XML-Signature zurückgegriffen. Diese Lösung bietet mehrere Vorteile. In XMail können einzelne Teile einer E-Mail gelesen, verifiziert und entschlüsselt werden, ohne dass die E-Mail im Ganzen vorliegen muss. Den verborgenen Empfängern können nun individuelle Informationen zugestellt werden, so dass unabhängig von ihrer Anzahl stets nur eine E-Mail versendet werden muss. Weiterhin wird durch das sorgfältiges Design von XMail gewährleistet, dass XMail-Nachrichten sehr effizient verarbeitet und gespeichert werden können. Ein weiter großer Vorteil von XMail ist, dass existierende Schlüsselmanagementtechniken wie PGP und X.509 unterstützt werden.

Auch für E-Mails nach RFC 822 werden Lösungsansätze für obige Probleme diskutiert. Wir schlagen ein verlustfreies und einfaches Speicherungsformat vor. Teile der für XMail entwickelten Sicherheitsmechanismen können darüber hinaus auch für einen Sicherheitsmechanismus für unterschiedliche Schlüsselmanagementtechnologien wie PGP und X.509 verwendet werden.