Sichere Datenübertragung von Formulardaten im Web

Formulare sind im WWW sehr beliebt, stellen sie doch eine Möglichkeit dar, ein Feedback von den Nutzern der eigenen Site zu bekommen. Zudem sind sie eine zusätzliche Möglichkeit, Tagungsanmeldungen, Materialanforderungen usw. papierlos abzuhandeln. Die bisherigen Möglichkeiten wurden bereits beschrieben und lassen sich unter *http://www.hu-berlin.de/rz/comm/www/formmail.html* nachlesen. Für den Einsatz des genannten Skriptes gab es jedoch bisher einige Einschränkungen, denn kein Autor kann es verantworten, wenn auf einer WWW-Seite abgefragte persönliche Angaben wie etwa die Kreditkartennummer unverschlüsselt über nicht abhörsichere Leitungen versandt werden.

Aus diesem Grund wurde das formmail-Skript nun so weiterentwickelt, dass es für den Benutzer der Web-Seite ohne zusätzlichen Aufwand auch für vertrauliche Angaben geeignet ist.

Wie kann das Skript genutzt werden?

1. Zuerst muss der Autor eines Formulars einen PGP-Schlüssel erwerben.
   Wie kommt man zu einem solchen Schlüssel? Die Software zum Erstellen eines Schlüsselpaares (man benötigt immer ein Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel, dem „public key“, und einem nichtöffentlichen Schlüssel, dem „private key“) kann man sich als Freeware von der International PGP Homepage (www.pgpi.com) downloaden. Nach der Installation der Software kann man sich ein oder mehrere Schlüsselpaare erstellen. Wichtig dabei ist die Angabe für „Key Pair Type“, hier bitte unbedingt „RSA“ angeben. Als Mailadresse muss die Adresse verwendet werden, die später im Formular als Empfänger („recipient“) angegeben werden soll. Da die Schlüssel in separaten Dateien gespeichert werden, kann man sie zur Sicherung anschließend kopieren, weitergeben sollte man jedoch immer nur den öffentlichen Schlüssel, der von Fremden zur Verschlüsselung einer Mail und zur Signaturprüfung verwendet werden kann. Zum Lesen einer verschlüsselten Mail und zum Signieren benötigt man seinen eigenen privaten Schlüssel. Wer noch einen Schritt weitergehen möchte, kann sein Schlüsselpaar auch noch bei der Zertifizierungsinstanz der Humboldt-Universität beglaubigen lassen. Detaillierte Informationen findet man auf der HU-CA-Seite: *http://ca.hu-berlin.de.*
   Bevor das Formular genutzt werden kann, muss der Autor seinen öffentlichen Schlüssel bekanntmachen, indem er ihn an webadm@rz.hu-berlin.de sendet, der ihn dann im Webserver hinterlegt.
2. Als nächstes muss eine Web-Seite erstellt werden, die ein Formular enthält. Als „action“ muss diesem Formular die folgende URL übergeben werden: *https://www.hu-berlin.de/cgi-bin/encformmail.pl.*
   Die Zugriffsmethode https stellt eine abhörsichere Verbindung zwischen Webbrowser und -server her. Das Perl-Skript encformmail.pl nimmt die eingegebenen Daten entgegen und verschlüsselt diese mit dem öffentlichen Schlüssel des Empfängers, bevor es sie per Mail über eine unsichere Verbindung weiterleitet.
   Dem Formular muss ein „recipient“ übergeben werden, eine Mailadresse also, an die die Daten des Formulars versandt werden.
3. Um das erstellte Formular in eine Web-Site einzugliedern, genügt ein Link derart: *https://www.hu-berlin.de/mein_verzeichnis/mein_formular.html*. (Konsequenterweise sollte man auch hier mit https arbeiten!) Darüber hinaus empfiehlt es sich, den Nutzer über die Vorgehensweise kurz zu informieren. Das erhöht das Vertrauen und die Bereitschaft, ein solches Formular zu nutzen. Wenn ein Nutzer nun den angegebenen Link aufrufen will, wird er aufgefordert, das Zertifikat des Web-Servers anzuerkennen. Tut er dies nicht, etwa weil er unserer Zertifizierungsinstanz misstraut, kann er die Seite nicht öffnen. Wenn der Link nicht mit https, sondern mit http versehen wird, erscheint die Aufforderung beim Auslösen der Formular-Aktion, also beim Drücken des Submit-Buttons.
4. Mails, die über ein solches Formular versandt werden, kommen verschlüsselt an und müssen vor dem Lesen entschlüsselt werden. Dazu gibt es für einige Mailprogramme komfortable Plugins, z. B. für Eudora und Outlook. Für Elm und Pine existieren Erweiterungsskripte. Wer mit anderen Programmen arbeitet, kann sich den Mailinhalt entschlüsseln lassen, indem er den Inhalt in die Zwischenablage kopiert und dann von PGP entschlüsseln lässt.

Katrin Lányi
katrin.lányi@rz.hu-berlin.de

Daniel Rohde
d.rohde@rz.hu-berlin.de