Stefan Schumacher
<stefan@net-tex.de>
PGP: 0xB3FBAE33

Magdeburg, 17. Januar 2004

Kurzpaper zum eingereichten Vortrag:

Anwendung kryptographischer Programme am Beispiel von NetBSD

Warum ist dieses Thema fuer die Besucher interessant?
Kryptographie ist z. Zt. das wohl einzige Mittel um zuverlässig die Privatsphäre zu schützen oder die Integrität von Daten sicherzustellen.
Kryptographische Methoden sind außerdem auch hervorragende Mittel um Rechnersysteme vor Manipulation und Einbruch zu schützen bzw. diesen nachzuweisen.

Warum beschaeftigen Sie sich mit diesem Thema?
Die Anwendung kryptographischer Methoden ist sowohl von privatem Interesse, da so der Schutz der eigenen Privatsphäre erleichtert werden kann, desweiteren sind eben diese Programme (bspw. `cgd`, AIDE oder `verified exec`) auch sehr gut geeignet um Rechnersysteme abzusichern und zu schützen.
Weiterhin befindet sich die Kryptographie zwar in der öffentlichen Diskussion (u. a. mit RFID, Onlinebanking, Krankenkarte oder digitaler Signatur), ist aber bei einem sehr großen Teil der Bevölkerung im Detail leider völlig unbekannt, was zum Teil sicherlich auch auf die sehr anspruchsvollen mathematischen Grundlagen zurückzuführen ist, zum anderen aber auch auf fehlende Aufklärungsarbeit, die an den gewöhnlichen Otto Normaluser gerichtet ist.

Welche Struktur/Gliederung soll der Vortrag bzw. Workshop haben?
Der Vortrag soll sukzessive eine Einführung in die praktischen Grundlagen und Anwendung der Kryptographie geben.
Zuerst werde ich Prüfsummenverfahren (wie EAN13 und MD5) einführen und erklären, wobei ich hier keinen Mathematikunterricht halten will sondern nur die für die Anwendung notwendigen Grundlagen erläutere, dazu gebe ich einige Anwendungsbeispiele.
Die Anwendungen sind zum größten Teil im Userland implementiert, also auf verschiedenen Unixiimplementierungen einsetzbar (z.B. `md5`, `cfs` oder `gpg`), einige sind aber spezielle NetBSD-Anwendungen.
Nach den Prüfsummen möchte ich die symmetrischen Verschlüsselungsverfahren erläutern und ebenfalls in Anwendungen (Cryptographic Filesystem, `mcrypt`) demonstrieren. Zusätzlich ist ein kurzer Exkurs zum Thema Datenvernichtung (`wiper`) geplant.
Aufbauend auf die symmetrischen Verfahren werden abschließend asymmetrische Verfahren dargelegt, hierbei werde ich das Grundverfahren der Schlüsselpaare anhand der bekannten *Alice* & *Bob* Beispiele erklären und praktisch mit GnuPG begleiten. Desweiteren wird hierbei noch die kryptographische Signatur erläutert.

Planen Sie auch eine praktische Vorfuehrung im Rahmen des Beitrages?
Größere Vorführungen habe ich nicht geplant, ich bin aber durchaus bereit bzw. in der Lage parallel zum Vortrag einige kleinere Programmbeispiele (wie sha1, md5 oder GnuPG) zu zeigen.
Soweit ich bisher weiß sind weitere Veranstaltungen zu `silc` von Christian Horchert und zu PGP/GnuPG von der CLUG geplant. Es wäre meiner Meinung nach von Vorteil wenn ich meinen Vortrag vor diesen Beiden halten könnte, da ich mehr auf die Grundlagen eingehe uns so auch vielleicht ein paar mehr Interessenten für diese Veranstaltungen anwerben kann :-)
Zusätzlich zu meinem Vortrag werde ich mit Hubert Feyrer am NetBSD-Stand sein und es ist kein Problem dort zusätzlich Installparties oder kleinere Workshops abzuhalten.

Welche einschlaegigen Webseiten gibt es zum Thema?
Ich richte zur Zeit eine Seite zu dem Vortrag auf meiner eigenen Homepage ein, darauf werden die Vortragsunterlagen zu finden sein, sowie Links zu den angesprochenen Programmen und weitere Howtos bzw. Unterlagen.
Die Seite lautet http://www.net-tex.de/krypt/
meine Folien: (Entwurfsversion!) http://www.uni-magdeburg.de/steschum/krypt.pdf