Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEKTION 9
E-MAIL SICHERHEIT

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Informationen zur Nutzungslizenz

Die folgenden Lektionen und Arbeitsmaterialien sind öffentlich verfügbar unter den folgenden Bedingungen seitens ISECOM:

Alle Materialien der Hacker Highschool werden für den nicht-kommerziellen Einsatz in Grund-, Haupt-, Realschulen und Gymnasien zur Verfügung gestellt, sowohl für öffentliche und private Bildungseinrichtungen, als auch für Privatunterricht zu Hause. Die Materialien dürfen in keiner Form für den Wiederverkauf reproduziert werden. Der kommerzielle Einsatz der Materialien, welche käuflich erworben werden können, in jeglicher Form von Schulstunde, Unterricht, Training, Meeting, Kongress, Vorlesung, Fortbildung, Sommer- oder Abendschulen ist ohne vorigen Erwerb einer Lizenz explizit untersagt. Um eine Lizenz zu erwerben, besuchen Sie bitte http://www.hackerhighschool.org/license.

Das Hacker Highschool (HHS) Projekt ist ein Unterrichtswerkzeug. Der Einfluss auf die Lernenden liegt beim Lehrer, nicht jedoch beim Werkzeug. Aus diesem Grund erkärt sich ISECOM nicht für Schäden verantwortlich, welche aus einem eventuellen Missbrauch der hier publizierten Informationen hervorgehen.

Das HHS Projekt ist die Arbeit einer offenen Gemeinschaft. Wir hoffen, dass die Lesenden Nutzen in unsem Projekt finden werden und bitten um Unterstützung unserer Arbeit, sei es durch den Erwerb einer Lizenz, durch eine Spende, Sponsoring oder in anderer Form.

Für das gesamte Material © ISECOM 2004

Inhalt

Mitwirkende

Stephen F. Smith, Lockdown Networks

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

ÜBERSETZUNG

Georg Berky

Karl Pausch

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura

Universitat Ramon Llull

9.1 Einführung

Jeder nutzt E-Mail. Es ist neben Deinem Webbrowser die am zweitmeisten genutzte Anwendung im Internet. Was Du aber wahrscheinlich noch nicht weißt ist, dass eine nicht zu unterschätzende Anzahl von Netzwerkangriffen und Sicherheitsrisiken durch E-Mail entsteht. Hinsichtlich Deiner Privatsphäre birgt der Missbrauch von E-Mails sowohl die Gefahr, den Inhalt Deiner Nachrichten zu enthüllen, als auch das Risiko, einem Spammer Informationen über Dich preiszugeben. Der Zweck dieses Moduls ist es, Dir Informationen darüber zu geben, wie E-Mail arbeitet, wie E-Mail sicher genutzt wird, wie E-Mail-basierte Angriffe funktionieren, und wie eine Sicherheitsstrategie für E-Mails aussehen kann.

9.2 Wie E-Mail funktioniert

Wie Luftpost durch die Luft versendet wird, wird 'E'-Mail durch das 'E' versendet, das 'E' ist in diesem Fall ein Netz von elektronischen Verbindungen in und zwischen den Netzwerken welche das Internet ausmachen. Wenn Du eine E-Mail von Deinem Computer verschickst, werden die Daten von Deinem Computer zu einem SMTP Server geschickt. Der SMTP Server ist dann entweder selbst für die Domäne der E-Mail zuständig und leitet die Post an seinen eigenen Posteingangsserver weiter – oder er sucht nach dem korrekten SMTP Server. Im zweiten Fall sendet er Deine E-Mail an seinen „Kollegen" von der korrekten Domäne, der sie dann wiederum an den Posteingangsserver zugestellt. Dort wartet Deine E-Mail dann darauf, dass sie der vorhergesehene Empfänger abruft.

9.2.1 E-Mail Konten

E-Mail Konten sind über viele unterschiedliche Quellen verfügbar. Du kannst ein Konto über Deine Schule bekommen, über Deine Arbeitsstelle oder über Deinen Internetanbieter. Wenn Du ein E-Mail Konto bekommst, wirst Du auch eine zweiteilige E-Mail Adresse in der Form: **Benutzername@Domänen.name** bekommen. Der erste Teil, der *Benutzername*, identifiziert Dich im Netzwerk, und unterscheidet Dich dort von allen anderen Benutzern. Der zweite Teil, *Domänen.name* wird benutzt, um das spezifische Netzwerk zu identifizieren. Der Benutzername muss einzigartig in Deinem Netzwerk sein, genauso wie der Domänenname einzigartig über alle Netzwerke im Internet sein muss. Benutzernamen sind jedoch über die Grenzen Deines Netzwerks hinaus nicht einzigartig. Es ist also möglich das zwei Benutzer in zwei unterschiedlichen Netzwerken den selben Benutzernamen besitzen. Zum Beispiel wenn im Netzwerk bignetwork.net ein Benutzer mit der Adresse **bill@bignetwork.net** existiert, dann wird es dort keinen witeren Benutzer mit der Adresse **bill@bignetwork.net** geben. Trotzdem sind **bill@bignetwork.net** und **bill@smallnetwork.net** beide gültige E-Mailadressen, die auf unterschiedliche Benutzer verweisen.

Eines der ersten Dinge, die Du tun wirst wenn Du Deine E-Mail-Programm einrichtest, ist die Eingabe Deiner E-Mailadresse. Dein E-Mail Client ist das Programm das Du zum senden und Empfangen von E-Mails benutzen wirst. Microsoft Outlook ist wohl das meistbekannteste (seit es kostenlos mit jedem Microsoft Betriebssystem ausgeliefert wird), es sind aber noch viele andere gute Clients für Windows und Linux verfügbar, wie Mozilla, Eudora, Mozilla Thunderbird und Pine.

9.2.2 POP und SMTP

Nachdem Dein E-Mail Client Deine E-Mail Adresse kennt, muss er noch wissen wo er nach Deinen eintreffenden E-Mails sehen muss und wo er Deine ausgehenden E-Mails hinschicken soll.

Deine eintreffenden E-Mails gehen zuerst auf einen Computer, der POP Server (ein Posteingangsserver) genannt wird. Der POP Server, gewöhnlich wird er pop.smallnetwork.net

oder mail.smallnetwork.net genannt, hat eine Datei, die mit Deiner E-Mailadresse assoziiert ist, und welche die E-Mails beinhaltet, die Dir von irgendjemanden zugesandt wurden. POP steht für „Post Office Protocol".

Deine ausgehenden E-Mails werden an einen Computer, der SMTP Server genannt wird gesendet. Dieser Server, der meistens smtp.smallnetwork.net genannt wird, schaut nach dem Domänennamen der in den E-Mailadressen, aller E-Mails die Du sendest, steht und führt dann eine DNS Anfrage durch um den anderen SMTP Server zu ermitteln, an den die E-Mails gesendet werden sollen. Trifft die Mail beim zuständigen Server ein, leitet er sie an den Posteingangsserver weiter. SMTP steht für „Simple Mail Transfer Protocol".

Wenn Du Deinen E-Mail Client startest passiert eine Anzahl von Dingen:

1. Der Client öffnet eine Netzwerkverbindung zum POP Server
2. Der Client sendet Dein geheimes Passwort zum POP Server
3. Der POP Server sendet Dir Deine ankommenden E-Mails auf Deinen lokalen Computer
4. Der Client sendet Deine ausgehenden E-Mails zum SMTP Server

Das erste was Du bedenken musst ist dass Du kein Passwort zum SMTP Server sendest. SMTP ist ein altes Protokoll, das in den ersten Tagen der E-Mail entwickelt wurde - in einer Zeit als im Internet noch jeder jeden persönlich kannte. Das Protokoll wurde mit dem Hintergrund geschrieben das jeder, der es nutzt, vertrauenswürdig ist. Deswegen überprüft SMTP auch nicht, ob Du auch Du bist. Viele SMTP Server benutzen andere Methoden um Benutzer zu authentifizieren, aber theoretisch kann jeder einen SMTP Server zum Versenden von E-Mails benutzen. (Für mehr Informationen darüber schau Dir Abschnitt **9.2.4 Gefälschte Headers** an).

Die zweite wichtige Sache ist, dass dein geheimes Passwort im Klartextformat gesendet wird, wenn Du eine Verbindung zum POP Server aufbaust, um deine Mails abzuholen. Es kann zwar durch kleine Sternchen in Deiner Eingabemaske versteckt werden, aber es wird in einem leicht lesbaren Format über das Netzwerk übertragen. Jeder, der den Netzwerkverkehr überwacht - zum Beispiel mit einem Packet Sniffer - ist in der Lage Dein Kennwort zu sehen. Du kannst Dich in Deinem Netzwerk sicher fühlen, aber Du hast wenig Einfluss darauf, was in möglichen anderen Netzen passiert, durch das Deine Daten übertragen werden.

Die dritte und vielleicht wichtigste Sache, die Du über Deine E-mails wissen musst, ist, dass sie – genauso wie Dein Kennwort – im Klartextformat übertragen und gespeichert werden. Es ist möglich, dass die E-Mails bei der Übertragung vom Server auf Deinen Computer jederzeit mitgelesen werden können.

Dieses alles summiert sich zu einer Wahrheit auf: E-Mail ist keine sichere Methode zum Übertragen von Informationen. Sicher, E-Mail ist in Ordnung zum Weiterleiten von Witzen und zum Versenden von spunkball Warnungen, aber wenn Du Dich unwohl fühlst etwas aus Deinem Fenster zum Nachbarn hinüber zu rufen dann solltest Du es Dir vielleicht zweimal überlegen ob Du das selbe auch in eine E-Mail schreiben willst.

Hört sich das paranoid an? Gut, ja, es ist paranoid aber das macht es nicht zwangsläufig unwahr. In vielem in unserer E-Mail Kommunikation geht es um unbedeutende Einzelheiten. Keiner außer Dir, Bob und Alice interessiert sich für die Pläne zum Mittagessen nächsten

Dienstag. Und selbst wenn Carol unbedingt wissen möchte wo Du und Bob und Alice nächsten Dienstag essen werdet, ist die Möglichkeit ziemlich gering das Carol einen Paket-Sniffer in einem Netzwerk laufen hat durch das Deine E-Mail übertragen wird. Aber, wenn eine Firma dafür bekannt ist, dass Sie E-Mails dazu nutzt, um Kreditkartendaten zu übertragen, ist es nicht unwahrscheinlich anzunehmen, dass jemand eine Vorrichtung installieren- oder zumindest versuchen wird, die Kreditkartennummern im Netzwerkverkehr aufzuspüren.

9.2.3 Web Mail

Eine zweite Möglichkeit, E-Mail zu versenden, ist die Nutzung eines Webbasierten E-Mail Zugangs. Dies erlaubt Dir die Benutzung eines Webbrowsers um Deine E-Mails abzurufen. Und weil die E-Mail bei Dieser Nutzung normalerweise auf dem Webmail Server gespeichert werden, und nicht auf Deinem lokalen Computer, ist es sehr angenehm diesen Service auf vielen verschiedenen Computern zu nutzen. Es ist auch möglich das Dir Dein Internet Anbieter Zugang zu Deinen E-Mail über beides, POP und Web, ermöglicht.

Du musst Dich jedoch daran erinnern das Webseiten auf lokalen Computern gecached oder gespeichert werden, und das manchmal für eine bedeutende Zeitspanne. Wenn Du Deine E-Mails über ein Web basiertes System auf dem Computer eines anderen abrufst, ist es möglich das Deine E-Mails für andere, die diesen Computer auch benutzen, ebenfalls zugänglich sind.

Web basierende E-Mail Zugänge sind oft kostenlos und einfach zu bekommen. Das heißt, dass diese Dir die Möglichkeit geben, mit mehreren Identitäten online zu sein. Du kannst zum Beispiel eine E-Mail Adresse nur für Deine Freunde haben und eine andere nur für Deine Verwandten. Dies wird auch als zulässig betrachtet solange Du nicht absichtlich jemanden damit betrügen willst.

Übungen:

1. Du kannst eine Menge darüber lernen, wie POP E-Mails überträgt, indem Du das telnet Programm benutzt. Wenn Du telnet anstelle eines E-Mail Clients verwendest, musst Du alle Befehle von Hand eingeben (Befehle, die das E-Mail Client Programm gewöhnlich automatisch übergibt). Finde über eine Suchmaschine die Anweisungen und Befehle die nötig sind um auf einen E-Mail Zugang über ein Telnet Programm zugreifen zu können. Was sind die Nachteile, wenn Du diese Methode zum Übertragen von E-Mails benutzt? Was sind einige mögliche Vorteile?
2. Finde drei Anbieter von Web basierten E-Mail Services. Welche, wenn Sie es überhaupt tun, Versprechungen geben Sie bezüglich der Sicherheit beim Versenden und Abrufen von E-Mails über Ihren Service? Gibt es irgendwelche Bestrebungen der Anbieter um Ihre Benutzer zu authentifizieren?
3. (freiwillige Hausaufgabe) Ermittle den SMTP Server für Deine E-Mail Adresse, den Du am häufigsten benutzt.

9.3 Sichere E-Mail Benutzung Teil 1: Empfang

Jeder nutzt E-Mail, und zur Überraschung von einigen Menschen, kann Deine E-Mail auch gegen Dich benutzt werden. E-Mail sollte wie eine Postkarte behandelt werden, bei der jeder, wenn er darauf schaut, den Inhalt sehen kann. Du solltest niemals etwas in eine einfache E-Mail schreiben von dem Du nicht willst das es gelesen wird. Diese Tatsache sagt uns das es Strategien geben muss, um unsere E-Mails abzusichern. In diesem Abschnitt wollen wir die sichere und normale Nutzung von E-Mail behandeln und untersuchen, wie wir unsere Privatsphäre online schützen können.

9.3.1 Spam, Phising und Betrug

Jeder möchte E-Mail haben. Vor langer Zeit in einer weit, weit entfernten Galaxie war es so das Du nur Mails von Leuten bekommen hast, die Du auch gekannt hast, und es gab nicht viele Dinge um die Du Dir Gedanken machen musstest. Jetzt bekommst Du Mail von Leuten, von denen Du noch nie etwas gehört hast und die Dich fragen, ob Du Software, Medikamente und Immobilien kaufen möchtest und dabei nicht erwähnen das Du Ihnen damit hilfst 24 Millionen Euro aus Nigeria zu erwerben ???HÄÄÄ?????????. Diese Art von unerwünschten Angeboten nennt man Spam. Es ist für viele Menschen überraschend, dass die E-Mails, die Sie empfangen eine Menge an Informationen über den Absender enthalten, wie zum Beispiel wann die E-Mail geöffnet wurde, wie viele Male sie gelesen wurde, ob sie weitergeleitet wurde etc. Diese Technologie, Web Bugs („Defekt", „Wanze im Web") genannt, wird sowohl von Spammern als auch von rechtmäßigen Absendern genutzt. Ebenso verrät das Antworten auf eine E-Mail oder der Klick auf einen Link zum „Abbestellen" eines Mailservices dem Sender das er eine genutzte E-Mail Adresse erreicht hat. Ein weiterer Angriff gegen die Privatsphäre sind die zunehmenden „Phishing" Attacken. Hast Du jemals eine E-Mail bekommen, in der Du aufgefordert wirst, Dich irgendwo anzumelden um Deine Bank- oder Ebay Zugangsinformationen zu überprüfen? Sei achtsam, denn das ist ein Trick um Deine Zugangsdaten zu stehlen. Um Dich vor dieser Art von Angriffen zu schützen gibt es ein paar einfache Strategien, die nachfolgend erklärt werden.

9.3.2 HTML E-Mail

Ein Besorgnisfaktor hinsichtlich Sicherheit von HTML-basierter E-Mail ist die Nutzung von *Web Bugs*. Web Bugs sind versteckte Bilder in Deiner E-Mail, die auf den Web Server des Absenders verweisen, und den Absender benachrichtigen, dass Du die E-Mail bekommen oder geöffnet hast. Eine andere Schwachstelle in HTML E-Mail ist das der Absender Links in die E-Mail einbauen kann welche die Person identifiziert, die den Link anklickt. Dies kann dem Absender Informationen über den Status einer Nachricht geben. Du solltest also grundsätzlich einen E-Mail Client benutzen, bei dem man das automatische Herunterladens von angehängten oder eingebundenen Bildern verbieten kann. Ein anderes Problem stellen Skripten in E-Mails dar, die eine Anwendung starten können, wenn Dein Browser nicht gegen diese Sicherheitslücken gepatcht wurde.

Bei Web basierten E-Mail Clients kannst Du eine Option haben mit der Du das automatische Herunterladen von Bilder deaktivieren kannst, oder mit der Du die Nachricht als reinen Text ansehen kannst. Beides sind gute Sicherheitspraktiken. Der beste Weg, Dich gegen HTML-Mail basierte Angriffe auf Sicherheit und Privatsphäre zu schützen, ist, textbasierte E-Mail zu nutzen. Wenn Du unbedingt HTML-Mails benutzen musst, sei vorsichtig!

9.3.3 Sicherheit von E-Mail-Anhängen

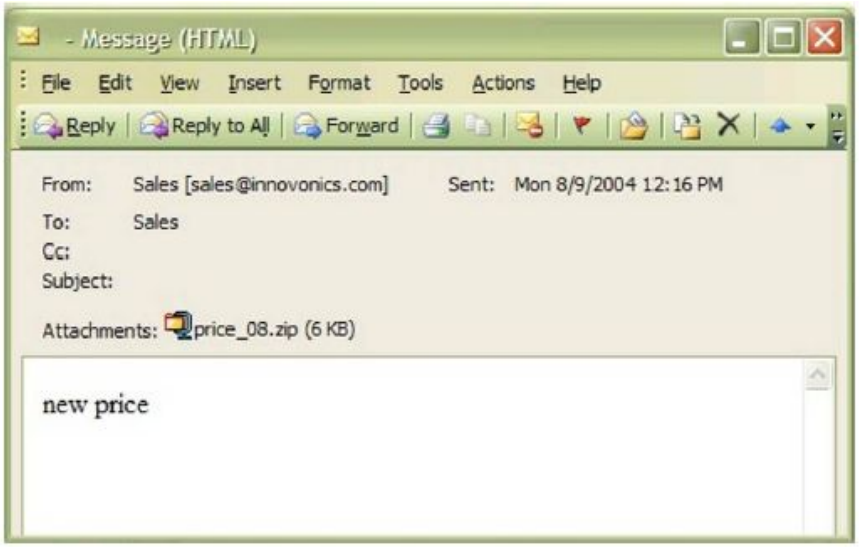
Ein anderes besorgniserregendes Sicherheitsproblem von empfangenen E-Mails sind Anhänge. Angreifer können Dir schadhafte Software („Malware"), Viren, Trojanische Pferde und alle möglichen Arten von unangenehmen Programmen zusenden. Die beste Verteidigung gegen schadhafte Software in E-Mail-Anhängen ist, keine Nachrichten zu öffnen die von jemandem kommen, den oder die Du nicht kennst. Öffne niemals eine Datei mit der Erweiterung .exe, .bat, .com, .pif oder .scr, weil diese Dateinamenserweiterungen zu ausführbaren Dateien gehören, die Deinen Computer mit einem Virus infizieren können. Als gute Gegenmaßnahme solltest Du alle Dateien, die Du empfängst, zuerst auf Deine Festplatte speichern und mit einem Antivirenprogramm untersuchen. Sei vorsichtig mit Dateien die wie bekannte Dateitypen aussehen, wie zip Dateien. Manchmal tarnen Angreifer Dateien indem sie das Symbol verändern oder Dateierweiterung verstecken, so das Du nicht weißt, dass es sich um eine ausführbare Datei handelt.

9.3.4 Gefälschte Header

Gelegentlich kannst Du E-Mails empfangen die aussehen als wenn sie von jemanden wären den Du kennst, oder vom „Administrator“ oder „Postmaster“ oder „Sicherheitsteam“ Deiner Schule oder Deines Internetanbieters. Der Betreff kann „Returned Mail“ oder „Hacking Aktivität“ oder andere interessante Betreffzeilen sein. Oftmals ist da auch ein Anhang. Das Problem ist, dass man kein technisches Wissen benötigt und allenfalls 10 Sekunden an Arbeit, um eine E-Mail Adresse zu fälschen. (Es ist auch - abhängig davon, wo Du lebst - sehr illegal).

Um das zu tun, musst Du nur eine einfache Änderung in den Einstellungen Deiner E-Mail Client Software vornehmen. Dort wo Du danach gefragt wirst Deine E-Mail Adresse einzugeben (unter Optionen, Einstellungen oder Präferenzen) gibst Du einfach irgend etwas anderes an. Ab da an werden alle Deine Nachrichten eine falsche Rückadresse haben. Bedeutet das Du sicher sein kannst nicht identifiziert zu werden? Nein, nicht wirklich. Jeder, der in der Lage ist, einen E-Mail Header zu lesen und sich einen Durchsuchungsbefehl beschaffen kann, ist vermutlich in der Lage Deine Identität aus den Informationen, die der Header beinhaltet zu rekonstruieren. Folglich kann ein Spammer sich als der ausgeben, der er gerade sein möchte. Also wenn Fannie Gyotoku [telecommunicatecreatures@cox.net] Dir eine magische Handy Antenne verkauft die sich als Frühstücksflockenpackung in Stanniolpapier verpackt herausstellt, kannst Du das bei cox.net reklamieren, aber sei nicht überrascht, wenn sie Dir erzählen, dass es dort keinen Mitarbeiter mit diesem Namen gibt.

Die meisten Internetanbieter authentifizieren den Absender und schützen so vor der Weiterleitung, das heißt das Du auch der sein musst, für den Du Dich ausgibst, um E-Mails über deren SMTP Server zu versenden. Das Problem ist, dass Spammer oft einen SMTP Server auf Ihrem PC laufen haben, und sich auf diesem nicht authentifizieren müssen, um eine E-Mail zu verschicken, deshalb können sie dort auftreten wie sie möchten. Der einzige sichere Weg zu erfahren ob eine verdächtige E-Mail echt ist, ist es, den Absender anzurufen, wenn man ihn kennt. Antworte niemals auf eine E-Mail, bei der Du vermutest, dass sie gefälscht ist, da das dem Absender mitteilt das er eine gültige und aktuelle Adresse erreicht hat. Du kannst Dir auch die Informationen im Header anschauen um zu ermitteln wo die Mail herkommt wie im folgenden Beispiel aufgezeigt:



Das ist eine E-Mail von jemanden den ich nicht kenne, mit einem verdächtigen Anhang. Normalerweise würde ich sie einfach löschen, aber ich möchte wissen, wo sie herkommt. Deshalb werde ich mir den Header der Nachricht ansehen. Ich benutze Outlook 2003 als meinen E-Mail Client, und um den Header anzusehen gehst Du nach Anzeige>Optionen und Du wirst die Header Informationen wie unten dargestellt sehen:

```
Microsoft Mail Internet Headers Version 2.0
Received: from srv1.mycompany.com ([192.168.10.53]) by mx1.mycompany.com
over TLS secured channel with Microsoft SMTPSVC(6.0.3790.0);
       Mon, 9 Aug 2004 11:20:18 -0700
Received: from [10.10.205.241] (helo=www.mycompany.com)
      by srv1.mycompany.com with esmtp (Exim 4.30)
      id 1BuEgL-0001OU-8a; Mon, 09 Aug 2004 11:15:37 -0700
Received: from kara.org (67.108.219.194.ptr.us.xo.net [67.108.219.194])
      by www.mycompany.com (8.12.10/8.12.10) with SMTP id i79IBYUr030082
      for <sales@mycompany.com>; Mon, 9 Aug 2004 11:11:34 -0700
Date: Mon, 09 Aug 2004 14:15:35 -0500
To: "Sales" <sales@mycompany.com>
From: "Sales" <sales@innovonics.com>
Subject:
Message-ID: <cdkdabgurdgefupfhnt@mycompany.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
       boundary="--------cfwriebwwbnnfkkmojga"
X-Scan-Signature: 178bfa9974a422508674b1924a9c2835
Return-Path: sales@innovonics.com
X-OriginalArrivalTime: 09 Aug 2004 18:20:18.0890 (UTC) FILETIME=
[868FEAA0:01C47E3D]
----------cfwriebwwbnnfkkmojga
Content-Type: text/html; charset="us-ascii"
Content-Transfer-Encoding: 7bit
----------cfwriebwwbnnfkkmojga
Content-Type: application/octet-stream; name="price_08.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="price_08.zip"
----------cfwriebwwbnnfkkmojga--
```

Nun, der Teil der mich interessiert ist gelb unterlegt. Beachte dass das „Received from kara.org“ mit einer IP Adresse versehen ist, die scheinbar zu einem xo.net DSL Zugang gehört. Das stimmt nicht mit innovonics.com überein, der behauptet der Absender zu sein.

Auch wenn ich mir innovonics.com's Mail Server mit nslookup anschaue, kommt seine Adresse wie folgt zurück:

```
C:\>nslookup innovonics.com
Server:  dc.mycompany.com
Address:  192.168.10.54
Non-authoritative answer:
Name:    innovonics.com
Address:  64.143.90.9
```

Also war mein Verdacht korrekt, und die E-Mail beinhaltet sehr wahrscheinlich schadhafte Software in einer ausführbaren Datei, die sich als zip Datei darstellt. Die schadhafte Software hat den Computer der Person mit dem DSL Zugang infiziert, der jetzt ein Zombie ist, und Kopien der schadhaften Software an jeden schickt, der in seinem infizierten Adressbuch steht. Ich bin froh darüber das ich das überprüft habe!

Übungen:

4. Citibank und PayPal sind die zwei meist verbreiteten Ziele von Phising E-Mails. Erforsche was die Citibank oder PayPal unternimmt um Phising zu bekämpfen/kontrollieren.
5. Recherchiere ob Deine Bank oder Deine Kreditkartenfirma eine veröffentlichte Stellungsnahme über den Gebrauch von E-Mail und persönlichen Informationen hat.
6. (freiwillige Hausaufgabe) Untersuche eine Spam Mail die Du empfangen hast und schau ob Du die echte Quelle der Nachricht ermitteln kannst.

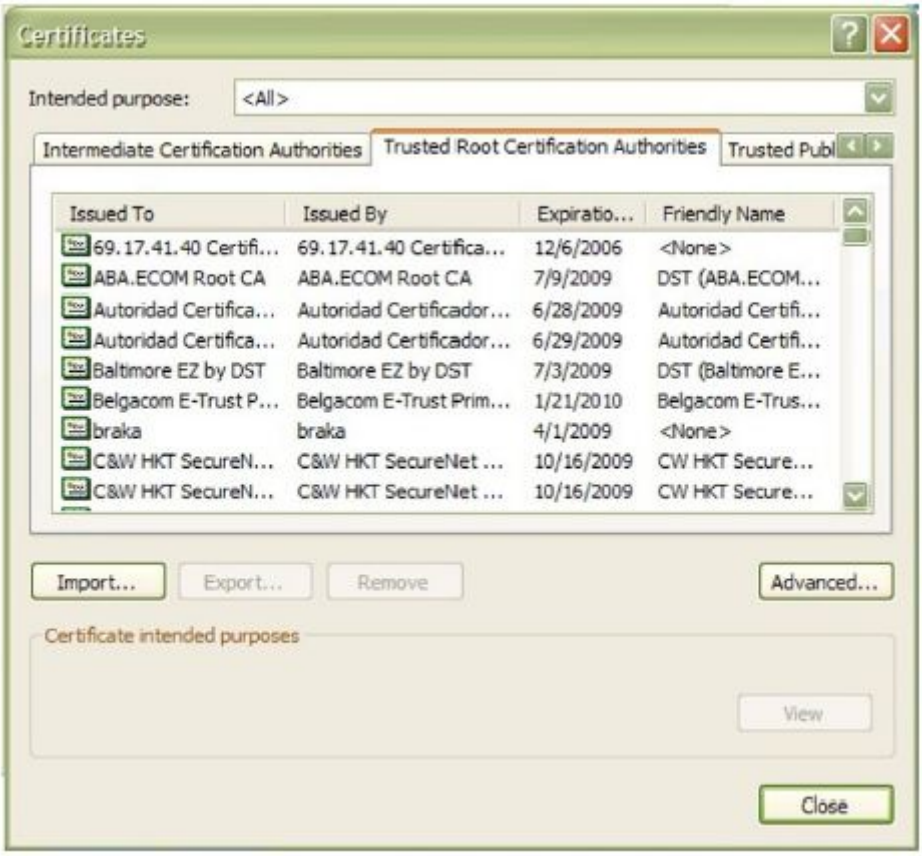
9.4 Sichere E-Mail Benutzung Teil 2: Senden

Das Senden von E-Mail ist ein bisschen sorgenfreier. Es gibt ein paar Dinge die Du tun kannst um sicherzugehen das Deine Unterhaltung sicher ist. Das erste ist zu gewährleisten das die Verbindung sicher ist (schau Dir den Abschnitt 9.4 Verbindungssicherheit für mehr Informationen an). Es gibt auch Möglichkeiten die Dir erlauben Deine Nachrichten digital zu signieren, was garantiert, dass die Nachricht von Dir ist und auf der Route dorthin nicht verfälscht wurde. Für ein Maximum an Sicherheit kannst Du Deine Nachricht verschlüsseln um sicherzugehen dass sie niemand liest.

Digitale Zertifikate weisen nach wo E-Mails herkommen, und das sie nicht beim Durchgang geändert worden sind. Wenn Du Dir die Nutzung von digitalen Signaturen zu einer Gewohnheit für wichtige E-Mails machst, hast Du eine Menge Glaubwürdigkeit wenn Du jemals in die Lage kommst eine gefälschte E-Mail, die angeblich von Dir sein soll, als solche identifizieren zu müssen. Du kannst Deine E-Mails auch so verschlüsseln, dass sie kein anderer lesen kann außer dem Empfänger. Speziell PGP bietet einen hohen Grad an Verschlüsselung, und um die zu brechen wird eine extreme Computerleistung benötigt.

9.4.1 Digitale Zertifikate

Ein digitales Zertifikat ist einzigartig für eine einzelne Person, etwa so wie ein Führerschein oder ein Pass, und besteht aus zwei Teilen. Diese Teile sind ein öffentlicher und ein privater Schlüssel. Das Zertifikat wird üblicherweise von einer vertrauenswürdigen Certificate Authority oder CA ausgestellt. Die Liste mit Certificate Authorities denen Du vertraust, wird automatisch durch das Windows Update verteilt (wenn Du ein Microsoft Windows Benutzer bist) und du kannst sie in Deinem Browser unter Werkzeuge>Internet Optionen>Inhalte>Zertifikate ansehen. Du kannst dort auch hingehen, um Zertifikate anzusehen, die auf Deiner Maschine installiert sind (Deine und andere), und um andere Certificate Authorities anzusehen denen Du vertraust.



Du kannst den automatischen Update von CAs deaktivieren, und Du kannst auch das Entfernen aller CAs von der Liste auswählen wenngleich das nicht zu empfehlen ist. Eine Anleitung wie das zu tun ist befindet sich auf der Microsoft Webseite.

9.4.2 Digitale Signaturen

Eine Digitale Signatur wird durch Deine E-Mail Software erstellt zusammen mit Deinem privaten Schlüssel der die Echtheit Deiner E-Mail garantiert. Der Zweck der Signatur ist ein zweifacher. Der erste ist, zu bestätigen das es von Dir kommt. Das nennt man Unleugbarkeit. Der zweite ist, sicherzustellen dass der Inhalt nicht verändert wurde. Das nennt man Unversehrtheit oder Integrität der Daten. Der Art und Weise, mit der ein E-Mail Programm das bewerkstelligt, ist dass der Inhalt der Nachricht durch eine Einweg-Hashfunktion läuft. Diese produziert eine Ausgabe fester Größe Deiner E-Mail, den man Message Digest nennt. Das ist ein eindeutiger und einzigartiger Wert, und wenn der mathematische Algorithmus, der ihn produziert stark ist, hat der Message Digest folgende Eigenschaften:

- Die Originalnachricht kann nicht anhand des Digest zurückgerechnet werden.
- Jeder Digest ist einzigartig.

Nachdem der Digest erstellt wurde, wird er mit Deinem privaten Schlüssel verschlüsselt. Der verschlüsselte Digest wird an Deine Originalnachricht zusammen mit Deinem öffentlichen Schlüssel angehängt. Der Empfänger öffnet dann die Nachricht und der Digest wird mit

Deinem öffentlichen Schlüssel entschlüsselt. Der Digest wird mit einem identischen Digest, der vom Mail Programm des Empfängers erstellt wurde verglichen. Wenn sie übereinstimmen bist Du fertig. Wenn nicht lässt Dich Dein Mail Client wissen das die Nachricht geändert wurde. Es gibt zwei Arten von Signierungs-/Verschlüsselungsfunktionen S/MIME und PGP. S/MIME wird als die erste Wahl für Unternehmen und Staat betrachtet, vielleicht weil es ein weniger Arbeit verursachendes Certificate Authority Modell zur Authentifizierung benutzt und weil es durch Microsofts Outlook Express E-Mail Programm leichter zu implementieren ist. PGP ist öfter die Wahl der Computernutzer Gemeinde, weil es auf einem dezentralen Vertrauensnetz zur Authentifizierung basiert, in dem die Vertrauenswürdigkeit eines Benutzers durch das „Freund von einem Freund" System bestätigt wird, in dem Du Dich bereit erklärst, das wenn Du mir vertraust kannst Du auch allen Personen vertrauen denen ich vertraue. Ebenso betrachtet es die Computergemeinde als Herausforderung und eine Art der Entspannung, solche zusätzlichen Features in Thunderbird einzubauen.

9.4.3 Erwerb eines Zertifikats

Wenn Du daran interessiert bist, ein Digitales Zertifikat oder eine Digitale ID zu erwerben, musst Du mit einer Certificate Authority (Verisign und thatwe sind die Bekanntesten, wenngleich Du über eine Websuche auch weitere finden wirst) Kontakt aufnehmen. Beide verlangen, dass Du eine Identifikation bereitstellst um zu überprüfen das Du der bist der Du angibst zu sein. Du kannst ein kostenloses Zertifikat von thatwe bekommen, aber sie brauchen dazu eine bedeutende Menge an persönlichen Informationen, eingeschlossen eine Identifizierungsnummer von der Regierung (wie sie in einem Pass oder einem Personalausweis steht). Verisign berechnet eine Gebühr für Ihre Zertifikate und benötigt eine Kreditkarte zur Bezahlung, dafür fragen sie nach weniger persönlichen Informationen. (Wahrscheinlich verlässt sich Verisign auf die Kreditkartenfirma um Deine persönlichen Informationen zu bestätigen). Diese Nachfrage nach Informationen kann aufdringlich erscheinen, aber denke daran, dass Du diese Firmen danach fragst, dass sie sich für Deine Vertrauenswürdigkeit verbürgen. Und, wie immer, sprich es mit Deinen Erziehungsberechtigten ab, bevor Du irgendwelche persönliche Informationen herausgibst.

Der größte Nachteil bei der Benutzung einer Certificate Authority ist, das Dein privater Schlüssel für jemand anderen verfügbar ist, nämlich für die Certificate Authority. Wenn die Certificate Authority gefährdet ist, dann ist auch Deine digitale ID gefährdet.

9.4.4 Verschlüsselung

Als eine zusätzliche Ebene der Sicherheit, kannst Du Deine E-Mails verschlüsseln. Verschlüsselung ersetzt Deinen E-Mail Text durch ein wildes Durcheinander von Nummern und Buchstaben, das nur der beabsichtigte Empfänger lesen kann. Deine tiefsten Geheimnisse und die Stilblüten deiner schlechtesten Dichtkunst werden so vor allen versteckt, denen du nicht sehr stark verstraust.

Dennoch musst Du bedenken dass, obwohl es sich gut für Dich anhört (und auch für alle die sich nicht wirklich wünschen unserer schlechten Poesie ausgesetzt zu sein), einige Regierungen Cryptographie nicht erlauben. Die Argumente dagegen können stichhaltig sein oder nicht (ihr könnt das unter Euch diskutieren), aber Stichhaltigkeit ist nicht der Punkt. Der Punkt ist, dass - abhängig von den Gesetzen deines Landes - das Versenden von verschlüsselten E-Mails ein Verbrechen sein kann, unabhängig vom Inhalt.

9.4.5 Wie funktioniert es?

Verschlüsselung ist ziemlich schwer zu verstehen (es gibt ganze Zweige der Mathematik, die sich nur damit beschäftigen), darum versuche ich es auf einem weniger technischen Weg zu erklären.
Jason möchte eine verschlüsselte Nachricht versenden. Darum ist das erste was Jason tun wird, zu einer Certificate Authority zu gehen um ein Digitales Zertifikat zu bekommen. Dieses Zertifikat hat zwei Teile, einen öffentlichen und einen privaten Schlüssel.

Wenn Jason verschlüsselte Nachrichten mit seiner Freundin Kira austauschen möchte, müssen sie vorher die öffentlichen Schlüssel austauschen. Wenn Du einen öffentlichen Schlüssel von einer Certficatione Authority, die Du als vertrauenswürdig ausgewählt hast, abrufst, kann der Schlüssel automatisch durch die zertifizierenden Autorität verifiziert werden (erinnere dich an deinen Ausweis, den du vorzeigen musstest). Das bedeutet, dass Dein E-Mail Programm überprüft, ob das Zertifikat gültig ist und nicht widerrufen worden ist. Wenn das Zertifikat nicht von einer Autorität kommt der Du vertraust, oder es ein PGP Schlüssel ist, dann musst Du den Fingerabdruck des Schlüssels überprüfen. Typischerweise wird dies getrennt getan, entweder durch einen Austausch des Schlüssels von Angesicht zu Angesicht oder über die Daten des Fingerabdrucks.

Nun nehmen wir an dass Kira und Jason passende Verschlüsselungsschemata benutzen, und signierte Nachrichten ausgetauscht haben, dann hat jeder den öffentlichen Schlüssel des anderen.

Wenn jetzt Jason eine verschlüsselte Nachricht versenden möchte, beginnt der Verschlüsselungsprozess mit der Umwandlung des Texts von Jasons Nachricht zu einem prehash Code. Dieser Code wird generiert durch Benutzung einer mathematischen Formel die Verschlüsselungsalgorithmus genannt wird. Es gibt viele Arten von Algorithmen, aber für E-Mail sind S/MIME und PGP die gebräuchlichsten.

Der Hash Code von Jasons Nachricht wird vom E-Mail Programm verschlüsselt, das dazu Jasons privaten Schlüssel benutzt. Jason benutzt dann Kiras öffentlichen Schlüssel um die Nachricht zu verschlüsseln, so das nur Kira sie mit Ihrem privaten Schlüssel entschlüsseln kann, und das vervollständigt den Verschlüsselungsprozess.

9.4.6 Entschlüsselung

Kira hat also eine verschlüsselte Nachricht von Jason empfangen. Das wird typischerweise durch ein Schlossbildchen an der Nachricht in Ihrem Eingang angezeigt. Den Prozess der Entschlüsselung übernimmt die E-Mail Software, aber was hinter der Bühne passiert ist etwas folgendes: Kiras E-Mail Programm benutzt Ihren privaten Schlüssel um den verschlüsselten Pre Hash Code und die verschlüsselte Nachricht zu entschlüsseln. Dann ruft Kiras E-Mail Programm Jasons öffentlichen Schlüssel von der Festplatte ab (erinnere Dich daran das wir die Schlüssel schon ausgetauscht hatten). Der öffentliche Schlüssel wird zum entschlüsseln des Pre Hash Codes benutzt und um zu überprüfen ob die Nachricht auch von Jason kam. Kiras E-Mail Programm generiert dann einen Post Hash Code aus der Nachricht. Wenn der Post Hash Code mit dem Pre Hash Code übereinstimmt wurde die Nachricht auf dem Weg zu Kira nicht verändert.

Beachte: Wenn Du Deinen privaten Schlüssel verlierst, werden Deine verschlüsselten Dateien nutzlos, darum ist es wichtig das Du eine Methode hast um Deine privaten und öffentlichen Schlüssel zu sichern.

9.4.7 Ist Verschlüsselung unbrechbar?

Entsprechend den Nummern und der Ebene der Verschlüsselung die zum Beispiel von PGP angeboten wird ist die Verschlüsselung unbrechbar. Sicher, wenn eine Million Computer daran arbeiten würden wären sie mit Sicherheit erfolgreich, aber nicht bevor die Millionen von Affen Ihr Manuskript für Romeo und Julia fertiggestellt haben. Die Zahlentheorie die hinter dieser Art von Verschlüsselung liegt, beinhaltet die Faktorzerlegung der Produkte von sehr großen Primzahlen und trotz der Tatsache das Mathematiker die Primzahlen über Jahre studiert haben gibt es keinen einfachen Weg diese zu brechen.

Aber Verschlüsselung und Privatsphäre sind etwas mehr als nur Nummern. Denn sollte jemand anderes Zugang zu Deinem privaten Schlüssel bekommen dann hat er auch Zugriff auf alle Deine verschlüsselten Dateien. Verschlüsselung funktioniert nur, wenn sie Teil eines größeren Umfeldes ist, welches Schutz für beides bietet, sowohl für den privaten Schlüssel wie auch für die Pass-Phrase.

Übungen:

1. Ist Verschlüsselung legal in dem Land in dem Du Dich aufhältst? Finde ein Land in dem es legal ist E-Mail zu verschlüsseln und ein Land in dem es illegal ist.
2. Science Fiction Autoren stellen sich zwei Arten von Zukunft vor, eine in der das Leben der Menschen durchsichtig ist, das heißt, das sie keine Geheimnisse haben und eine in der jedermanns Gedanken und deren Kommunikation vollkommen persönlich sind. Phil Zimmermann der Entwickler von PGP glaubt an die Privatsphäre als eine Quelle der Freiheit. Lies seine Gedanken darüber, warum Du PGP brauchst auf der Seite **http://www.pgpi.org/doc/whypgp/en/**. Wenn Du die englische Sprache beherrscht, dann schau Dir den Artikel ‚A Parable about openness' von dem Science Fiction Autor David Brins auf **http://www.davidbrin.com/akademos.html** an, in dem er einige Punkte anführt in denen er Offenheit als Quelle für die Freiheit verteidigt. Ansonsten stellen die vier Artikel von Peter Mühlbauer unter **http://www.heise.de/tp/r4/artikel/4/4221/1.html** eine gute Lektüre zu diesem Thema dar. Diskutiere diese beiden unterschiedlichen Standpunkte. Welchen bevorzugst Du? Welcher, denkst Du wird erfolgreicher sein? Wie denkst Du wird die Zukunft der Privatsphäre aussehen?

9.5 Sicherheit von Verbindungen

Nicht zuletzt kommen wir zur Sicherheit von Verbindungen. Stelle für Web Mail immer sicher das Du eine SSL Verbindung zum Web-Mailsystem deines Internetanbieters benutzt. Ein kleines Schloss wird dann unten in der Statusleiste Deines Browsers erscheinen. Wenn Du POP und einen E-Mail Client benutzt, stelle sicher dass Du Deinen E-Mail Client so konfigurierst dass er SSL für POP auf Port 995 und für SMTP auf Port 465 benutzt. Das verschlüsselt die Mail von Dir zum Server, und schützt auch Deinen POP/SMTP Benutzernamen und Dein Passwort. Dein Internetanbieter sollte eine Anleitung, wie so etwas konfiguriert wird, auf seiner Webseite haben. Wenn er keine sichere POP/SMTP Verbindung zur Verfügung stellt, dann tust Du gut daran den Internetanbieter zu wechseln!

Übung:
Wenn Du einen E-Mail Zugang hast dann finde heraus ob Dein Zugang SSL für die Verbindung benutzt. Wie überprüfst Du das bei Deinem E-Mail Client? Stellt Dein Internetanbieter Informationen bezüglich SSL-Verbindungen bereit?

Weitere Informationen

Kann jemand anderes meine E-Mail lesen?
http://www.research.att.com/~smb/securemail.html
MIT's PGP freeware Seite
http://web.mit.edu/network/pgp.html

Allgemeine Neuigkeiten zum Thema Privatsphäre im Internet:
Electronic Privacy Information Center
http://www.epic.org/
und
Electronic Frontier Foundation
http://www.eff.org/
Mehr über PGP
http://www.openpgp.org/index.shtml
Wie das lesen einer E-Mail Deine Privatsphäre gefährden kann
http://email.about.com/od/staysecureandprivate/a/webbug_privacy.htm
Vermeidung von E-Mail Viren
http://www.ethanwiner.com/virus.html
Ein kurzer Überblick an Fragen zum Thema E-Mail Sicherheit
http://www.zzee.com/email-security/
Ein kurzer Überblick an Fragen zum Thema E-Mail Sicherheit
http://www.claymania.com/safe-hex.html
Windows basierte E-Mail Vorsichtsmassnahmen
http://www.windowsecurity.com/articles/Protecting_Email_Viruses_Malware.html
http://computer-techs.home.att.net/email_safety.htm
Unterschiede zwischen Linux und Windows Viren (mit Informationen darüber warum die meisten Linux E-Mail Programme sicherer sind)
http://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses/