Authenticating on a Ham Internet

The FCC regulations for amateur radio, part 97, rule that encryption cannot be used to obscure the meaning of communications. Many read the rules and assume that there is no way to use authenticated communications, for example using a user name and password, without the FCC rules being updated. Fortunately, there are means by which authentication can be achieved without obscuring the meaning of a transition.

This article will touch on two method by which authentication can be achieved without obscuring the transaction, which is critical for remaining compatible with the FCC rules for ham radio, and without a third-party being able to later reuse information, gleaned by monitoring, in order to spoof a ham network user. The first method, Cram-MD5, allows passwords to be used over the air and the second, cryptographic signatures, allow for very flexible authentication to be achieved.

In April, I gave a presentation on the topic to the Atlanta Radio Club meeting and received encouragement from some club members and have decided to put together this article.

What Does Part 97 Say?

> Section 97.113 (4) "...messages in codes or ciphers intended to *obscure the meaning* thereof, except as otherwise provided herein..." (emphasis added).

Based on the above quote, we can use any method at our disposal to provide for secure authentication which does not obscure the meaning of communications. As we start using more computing environments and bring the Internet to ham radio, we have to make sure that service is not provided to non-licensed users. In voice space, it is generally easy to spot a non-ham, but when everyone is using the same software there is not a similarly intuitive way to distinguish between the licensed user and the unlicensed user.

Same Tools, Different Rules

Most networks and the Internet are not regulated by similarly restrictive rules as ham radio so generally strong encryption is used to hide the content of all transition from third-parties. Protocols such as SSL, SSH, and VPN Tunnels are commonly used and are highly appropriate for those networks. However, on the air we have to abide by restrictive rules that enforce that all communications must be readily monitored and understood by all third-parties. However, many of the protocols used on the traditional networks can be used with little modification on the air.

Imagine connecting to the Internet through a amateur radio gateway. One can browse the web since it is normally not encrypted, but cannot buy something on line because the order form uses an SSL connection, which is encrypted. One can send and receive e-mail, which is not business related, because the connection can usually by made through non-encrypted channels. Most e-mail clients will actually not even reveal the password when checking e-mail because they implement the Cram-MD5 authentication protocol.

Amazingly, this protocol prevents a password from being monitored by not ever sending it!

Many people make daily usage of the SSH protocol, which allows people to securely connect to other computers across the network. SSH keys can be used to securely connect without even using a password. Normally SSH would not be allowed because it is encrypted, but there is a non-default option which caused SSH to connect without encrypting the data – though one can still login without using a password. SSH uses public key infrastructure, PKI, which can be applied to amateur radio digital communications.

Cram-MD5 Password Hashes

Among the many authentication mechanisms used in computing today, password authentication is the most universally recognized. Cram-MD5 can be used to authenticate over the air without obscuring the communication and without a third-party being able to determine the password.

MD5 is a one-way-hash, a mathematical function, that converts any text into a number. Running the a piece of text through the MD5 process will always return the same number, but the number cannot be used to determine the text (this property is called one-way). Password authentication purposes, one takes a password and runs it through the MD5 function to generate a unique number which the server uses to confirm that the password is correct.

Cram-MD5 is an authentication method that makes use of the MD5 function and used by e-mail clients, such as Eudora or Outlook, to authenticate with a server without sending the password plain text. Unlike SSL connections, in which all information is encrypted, the message content in a Cram-MD5 session is plain text that can be monitored by third-parties.

Cram-MD5 manages to not reveal the password by not sending it at all. Instead, it uses a known mathematical function called MD5, which is a one-way-hash, to encode the password in such a way as to create an identifiable, non-reproducible token to be used in the place of the password.

The following illustration shows roughly how the authentication process works:

1. KI4AWF: Hello, I am KI4AWF.
2. SERVER: Hello KI4AWF, use 1234567 to authenticate.
3. KI4AWF: Using 1234567, my token is 8e638a158374d2caba6a5fec5274b3db.
4. SERVER: Token accepted, please go ahead with your message.
5. KI4AWF: Hey mother, traffic is pretty bad and I will not be able to make it on time...

Be sure to note the session number transmitted by the server on line 2. And the authentication token returned by the client on line 3. The most important thing to notice is that the content, that is the meaning, of the communication remains clearly copyable at

all times during the transition.

The authentication token is generated by the client by incorporating information that is already known to the server, that is the the user name, password, and the session number.

Compare Signed vs. Encrypted Messages

While passwords are very convenient and hashes can be used to authenticate over the air without encrypting the traffic, digital signatures provide a very powerful means of authenticating entire messages and streams of data.

Digital signatures generally use the RSA or Diffie-Hellman algorithms, which are asymmetric ciphers, making use of a public key and a private key. To send an encrypted message to a particular person, one uses the recipient's public key to encode the message in such a way that only the private key can unlock the message. However, the same algorithms can be used to produce a clear text signature. To sign a message, one uses his own private key to create a mathematical wrapper for the text. Anyone can then use the text and the sender's public key to verify that the signature is correct.

PGP is a free program that allows everyday computer users to use strong PKI cryptography for e-mail messages. It provides an excellent example of a signed message and an encrypted message.

First consider the message “Hello, this is KI4AWF doing a presentation on PKI,” encrypted with PGP:

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.2.3 (FreeBSD)
hQIOA26qQQhVmtQQEAf/ZYuA17TsGubUjNsrbY3kjBvvMpNUcEtMclkAKR7oDhNQ
Ts3xbrIQiOMLZP0GB42gwXqMdNIxVir1wLYszJxbipJLMI/yk5Awg27zrcYXjK3b
2SyTdbaUvReYlsT47ZOKJtxYBHJ3sjg0/vo+MAmDe8yVcU7t5+c0WiCHY5dALkgY
+4ZTIql+kJV4UjdZ9FriVcPhT+CMCez6z6bt+lMBvFxq4I++HojLA9TeAAE/ui5z
zQnIGTPAjKAIsAxFxSGog90/vMHsFcfZT90rXoENNzyEOp+201dZ6N68p1kNBoui
dEATsTQODN7fodIEv6IrWCmRW9PEXFgiVGMTgyxMuwgAjTlgW9rSUNGlbrGWVwsd
/jswPDHSIpSHyxl1gK6hz/LCBpfGzsddUJziyATtK2b/nl3eqPg2b+sQ49p5l236
myCun7dIkgP6imgmuZp2snEy92fJufKK92532zYfMzL5c1mrQJuk3sfVaXXslL3v
iWPtiqlBdBZsmflwiUtUqNza9HASeXCzW529ufpc3FknFNJZ/yYyrQFT5LEeapHq
lLTPF6XDHwXD0AorIPRNGyKXje0upBOAFXBQ8RNxDWRdQBgbGcTo4UqPNc3gUW0X
kP5OK15fAdaZhCQ6UMAekiYuiEebkBX1ooAFoUzCfFwFdFM2fRcDJwW+Wy41HqkO
5tJyAaBWz0emXSaNG6iAbaxu0R+JMxjyIcSE4rTcbZsMY8f8brChcjVJTnwE2gum
oaX51uX3GmexpJi+x9EqmssEsVqVOXe83kvlbtoiXIsXIgAxH15vcqjgi4NDvZmU
540IxIHBpSvIrthYRkIzwGQIUUTn
=ghjG
-----END PGP MESSAGE---
```

The result is an impressive garble of information. The message can be easily decrypted by the recipient with his private key, but everyone else is prevented to knowing anything about the contents of the message. While this might be useful for normal Internet or business communications, it is clearly off limits on the air.

In contrast to the encrypted message, consider the following clear text signed communication:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hello, this is KI4AWF doing a presentation on PKI.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.3 (FreeBSD)
iD8DBQFAWvVru9L44h+QFq8RAqNGAJ4pKiBtjMVMPP2Una+Gpvz1Ntp2NACgusOH
Ltg7340+wFoF2yEpHHMNN84=
=uhR/
-----END PGP SIGNATURE-----
```

The content, that is the meaning, of the message is clearly visible and is surrounded by mathematical information about the message. That information is used to verify, with absolute certainty, that the message has not be forged or corrupted in transit and that is was produced by the owner of a specific cryptographic key.

Digitally signed messages can be used in the place of passwords because the contents are always clearly visible and the authorship of the message can be verified. A digital station could have a list of the public keys of all authorized operators and promptly reject control instructions that are signed with any unknown key. The connections are not encrypted since the contents, including all of the commands, is clearly visible. An operator could simply connect through a signed-packet session to the remote station to control it. However, unauthorized instructions, those not signed with a known key, are ignored by the digital station.

IPSEC without Encryption

The IEEE IPSEC standard is a protocol implemented by all modern networked operating systems including, Linux, FreeBSD, MacOS, and Windows 2000 and newer. IPSEC provides for configurations that allow for messages to be signed, but not encrypted. This is the easiest way to implement widespread PKI for an amateur wireless network.

Concluding Remarks

Building access points allowing amateurs to connect to the Internet over long range

wireless links is a great opportunity to experiment with the exciting combination of radio and computer technologies. However, security methods must be put in place to keep third-parties from spoofing network hams and also to prevent non-licensed users from illegally accessing the amateur wireless network.

Cram-MD5 is the ideal method for implementing password authentication over ham links. It has been long proven by traditional e-mail systems and can be implemented in such a way that a ham must provide a user name and password to access to the network. A Java applet should be developed to allow hams to authenticate with an amateur gateway through his web browser.

In the long run, cryptographically signed and verifiable connections are the best way to provide for password-less security and to prevent non-licensed users from illegally accessing the wireless network. The IPSEC is the best way to implement this without becoming incompatible with existing networking hardware and software.