The Effects of Authentication on AX.25 Packet Radio Data Transmission Time

Paul D. Wiedemeier, Ph.D., KE5LKY
Digital Communication Research Laboratory

The University of Louisiana at Monroe
College of Business Administration
Computer Science and CIS Department

My special thanks to ...

- TAPR and ARRL
- Local conference coordinators
- Steve Bible (N7HPR)
- Mark Thompson (WB9QZB)
- Ed Mellnik (WB2QHS)
- Mark Walker (W7CLU)
- Dennis Bourassa (W7IME)
- Jeremy McDermond (NH6Z)
- Ken Konechy (W6HHC)
- Robbie Robinson (KB6CJZ)
- Nick Luther (K9NL)
- Tim Salo (AB0DO)

Introduction

Introduction

- Problem
  - Call sign “spoofing” is trivial within AX.25 packet radio networks.
    - Configure a computer to place a bogus FCC call sign in all AX.25 packets transmitted.
  - It is often difficult for the recipient of a message to determine whether the message has been “spoofed”.

Introduction

- In 2004, Paul Toth (NA4AR) and the ARRL High-Speed Multimedia & Network Workgroup published a report title "*Security & Data Integrity on a Modern Amateur Radio Network"* that requested …

> "… the support of the ARRL Board of Directors for development and filing of a 'Notice of Proposed Rulemaking' permitting the use of encryption and strong security protocols on domestic transmissions above 50 MHz".

Digital Communication Research Laboratory

Introduction

- The authors' claimed that ...

> "… licensees in the Amateur Radio Service need to be free to utilize ... industry-standard security and authentication tools to protect the integrity of their stations".

Introduction

- FCC Part 97.113 rule

> *"(a) No amateur station shall transmit … (4) … ; messages encoded for the purpose of obscuring their meaning, except as otherwise provide herein;"*

Introduction

- Encryption is …
  - A process by which the bits of a message are modified (i.e. scrambled) such a way that only the intended recipient can extract information.
- An individual that intercepts a copy of an encrypted message will not be able to extract information.

Introduction

- Authentication refers to the ability of an individual or station to determine whether …
  1. The sender of a received message is who they assert they are.
  2. The message received is what was transmitted.
- I can authenticate a message without encrypting it.

Introduction

- Solution
  - **Use authentication software!**
  - The message recipient is now able to determine whether …
    - The message was actually transmitted by the source.
    - The received message was the one actually transmitted.

Introduction

- The research presented here, and discussed in the paper, explores the use of the following authentication software when transmitting messages.
  - Gnu Privacy Guard (GPG)
  - Secure Socket Layer and Transport Layer Security (SSL/TLS)
  - Internet Protocol Security (IPsec)

Introduction

- Specifically, we compare the time required to transmit messages over a 2-meter AX.25 packet radio network using “no authentication”, GPG, SSL/TLS, and IPsec.

Introduction

- I will discuss the following topics during this presentation.
  1. Materials
  2. Methods
  3. Results
  4. Conclusions
  5. Future Research?

Materials

Materials

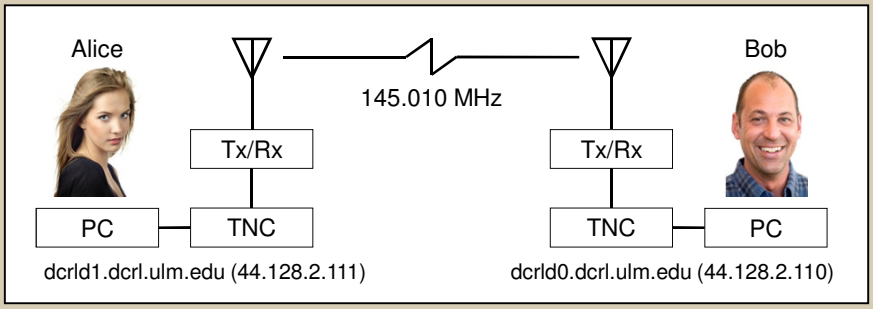

Figure 1: The logical hardware configuration of our AX.25 packet radio stations dcrld0 and dcrld1.

Materials

- Software Requirements
  1. We wanted to investigate how application layer, transport layer, and network layer authentication software influence data transmissions over AX.25 packet radio networks.
  2. We required the use of data transmission server software (e.g. FTP server or web server) that would allow us to evaluate each authentication software independently.

Materials

- Software Requirements Continued
  3. We required the use of command line oriented client software that would allow us to retrieve data from the data transmission server software we chose to use.
  4. We required the use of network protocol analyzer software to inspect every packet transmitted between the client and server.
  5. We required open source software that could be installed on the Fedora Linux operating system.

Materials

Table 1: Specific software used to conduct our research.

Software	Associated Website or RFC
Apache Web Server	http://www.apache.org/
cURL	http://curl.haxx.se/
UNIX time command	http://www.kernel.org/doc/man-pages/online/pages/man1/time.1.html
Wireshark	http://www.wireshark.org/
Gnu Privacy Guard	http://www.gnupg.org/
Secure Socket Layer/Transport Layer Security	http://datatracker.ietf.org/doc/rfc5246/
Internet Protocol Security	http://datatracker.ietf.org/doc/rfc4301/

Materials

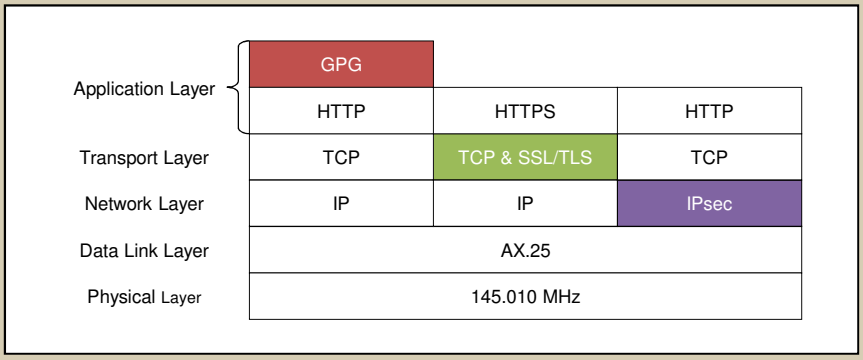

Figure 2: An "authentication enabled" generic data communication protocol stack.

Digital Communication Research Laboratory

Materials

- Three text files
  - text4KB.txt, text8KB.txt, and text16KB.txt
  - Comprised of text data. E.g. "`01234567890123 …`"

Methods

Methods

- Alice installs and configures a standard Apache web server on dcrld1.
  - She places the three text files within the Apache web server's home directory.
- Bob installs and configures Wireshark on dcrld0.
  - He starts Wireshark before each file transmission.

No (i.e. “None”) Authentication

Digital Communication Research Laboratory

No (i.e. “None”) Authentication

- Bob uses the cURL client on dcrld0 to retrieve each of the three text files on dcrld1 twenty times.
  - `time curl http://dcrld1.cs.ulm.edu/text#KB.txt > /tmp/text#KB.txt`

No (i.e. “None”) Authentication

- Bob records transmission times in a Microsoft Excel spreadsheet.
- Bob computes the average transmission time for each text file.

GPG Authentication

GPG Authentication

- Alice and Bob install and configure GPG on both dcrld1 and dcrld0 respectively.
- They create GPG public and private keys.
- They exchange their GPG public keys in a secure manner.
- They add the others GPG public key to their key ring.
- They GPG sign the others GPG public key with their GPG private key.

GPG Authentication

- Alice GPG clearsigns the three text files and places the GPG clearsigned versions within the Apache web server's home directory.

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

01234567890123456789012345678901234567890123456789012345678901234567890 …
01234567890123456789012345678901234567890123456789012345678901234567890 …
  :
  :
01234567890123456789012345678901234567890123456789012345678901234567890 …
01234567890123456789012345678901234567890123456789012345678901234567890 …

-----BEGIN PGP SIGNATURE-----: GnuPG v1.4.7 (GNU/Linux)

iQIVAwUBS2pEdvTJW9l7crFSAQJePw//YG97nwpNKXS9NPgpZQblq3/ualwDlrN2
Ss9fPkV78SRtXUBzNF6GVf07B3K2tlAF7K8YKU38c9vlTE95UgAE4UBaqM5n4Hal
SWfFEb04TAw4/6tuwVgNZxSIb7jvAPolRXAjJgHN5HEi6Fus/mjs/rsU8E4atbuZ
HufYrDoolFSu8rDDZ8sFvdATqlwghPvQJwCfQn+CkLpKFg32A+mATcmlZ8gfPo2h
HI+cig8vxaztcjOEC42Scq/erm80Hde5u4+0MUp1D6UuhGPRpTXw82+GHE7W3RzL
jzFTvWwbpsFiY79wvZN7DcbJs/gRDMtpSaKm5q7MmVB12lixifXfIZXLR6cGX/6/
HZ46Xln0/7o60I83yWC91XP0CUqbaJs9BrVYDNAPWbK2vhh2F2kYMEzrF1nUUv42
D0QE0yqj6/0VmJIrGjiAxgKPw9cfGAdxM9S3FoxiLJYhBdqZhcT0Nhfb04zbod5s
aZn/aK+OZmd8vqVvyD07ufwml6ttq8MeKiHtwm09tY7Zyp9bwew92VneAIPEFLQ5
oGBc431KX1SXYqEQB1IBOwUmIMBOuDXm6vSRpOmYhPkfYPDjfISj69f0Wg85k5Ez
NtzlBz0ldDNwLtZxrk3ETdq0lvLsZYhVNYXHGF0oJzObiuiPZiyPFvp4RUT9dc6L
gmijwab0u8E=
=/y0r
-----END PGP SIGNATURE-----
```

Unencrypted Data

GPG Signature

Figure 3: An example GPG "clearsigned" file.

GPG Authentication

- Bob uses the cURL client on dcrld0 to retrieve each of the three GPG clearsigned text files on dcrld1 twenty times.
  - `time curl http://dcrld1.cs.ulm.edu/text#KB.txt.dcrld1.asc > /tmp/text#KB.txt.dcrld1.asc`
- Bob GPG verifies the authenticity of each GPG clearsigned text file retrieved.

GPG Authentication

- Bob records transmission times in a Microsoft Excel spreadsheet.
- Bob computes the average transmission time for each GPG clearsigned text file.

SSL/TLS Authentication

SSL/TLS Authentication

- Alice installs and configures a secure Apache web server on dcrld1.
  - The standard and secure Apache web servers use the same home directory.
- In a secure manner, Alice provides Bob with a copy of her secure Apache web server's self signed SSL/TLS certificate.

SSL/TLS Authentication

- Bob configures dcrld0 to recognize dcrld1's self signed SSL/TLS certificate as authentic.
- Bob uses the cURL client on dcrld0 to retrieve each of the three text files on dcrld1 twenty times.
  - `time curl --ciphers rsa_null_md5 https://dcrld1.dcrl.ulm.edu/text#KB.txt > /tmp/text#KB.txt`

SSL/TLS Authentication

- Bob records transmission times in a Microsoft Excel spreadsheet.
- Bob computes the average transmission time for each text file.

IPsec Authentication

IPsec Authentication

- Alice creates an IP layer “Host to Host” encrypted communication channel between dcrld1 and dcrld0 using the `system-config-network` Linux command on dcrld1.
- Alice edits the file `/etc/raccoon/raccoon.conf` and adds support for RSA authentication and NULL encryption.

IPsec Authentication

- Bob creates an IP layer “Host to Host” encrypted communication channel between dcrld0 and dcrld1 using the `system-config-network` Linux command on dcrld0.
- Bob edits the file `/etc/raccoon/raccoon.conf` and adds support for RSA authentication and NULL encryption.

IPsec Authentication

- Bob uses the cURL client on dcrld0 to retrieve each of the three text files on dcrld1 twenty times.
  - `time curl http://dcrld1.cs.ulm.edu/text#KB.txt > /tmp/text#KB.txt`

IPsec Authentication

- Bob records transmission times in a Microsoft Excel spreadsheet.
- Bob computes the average transmission time for each text file.

Results

Digital Communication Research Laboratory

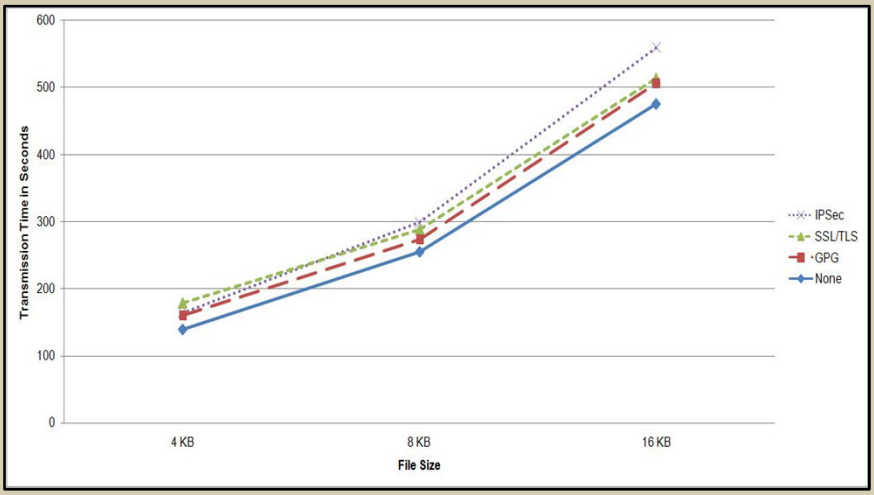

Figure 4: GPG, SSL/TLS, IPsec, and No (i.e. “None”) Authentication Data Transmission Time.

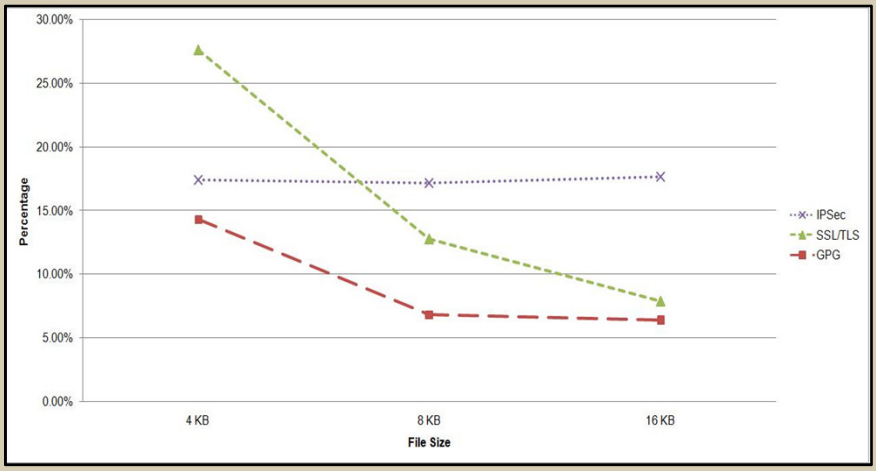

Figure 5: GPG, SSL/TLS, and IPsec Authentication Data Transmission Time as a Percentage of No (i.e. "None") Authentication Data Transmission Time.

Conclusions

Conclusions

- With regards to the three authentication methods we evaluated, GPG performs the best.
- The paper lists the steps required to install and configure each of the authentication methods.

Future Research?

Future Research?

- I recommend that the ARRL consider offering the following services to the amateur radio community.
  - Act as a “clearing house” for GPG public keys.
  - Act as a SSL/TLS certificate authority (CA).

Acknowledgements

- The ULM Digital Communication Research Laboratory
- The ULM College of Business Administration
- The ULM Computer Science and CIS Department
- Allison M.D. Wiedemeier, Ph.D.

Questions?

Contact Information

Paul D. Wiedemeier, Ph.D.
Assistant Professor of Computer Science
ULM Digital Communication Research Laboratory Principal Investigator

Address: The University of Louisiana at Monroe
Computer Science and CIS Department
College of Business Administration
700 University Avenue
Administration Building, Room 2-37
Monroe, Louisiana, 71209

Phone: 318-342-1856
FAX: 318-342-1857
Email: wiedemeier AT ulm DOT edu, wiedemeierp AT gmail DOT com
WWW: http://www.cs.ulm.edu/~pdw/
Office: Hemphill Airway and Computer Science Building, Room 348