

Reflections on the Motorola Canopy WMAN Product

Joshua Wright

<http://802.11ninja.net/~jwright/canopy.ppt>

Casual Observations

- Security White Paper:
http://www.motorola.com/Enterprise/contentdir/en_US/Enterprise/Files/White%20Papers/Canopy%20Security%20White%20Paper.pdf
 - Google "Canopy Security White Paper"

CANOPY'S PROPRIETARY PROTOCOL

"Canopy's proprietary air interface provides a strong foundation against attacks by invaders. First of all, because the Canopy system is based on a proprietary protocol, there are no published specifications for the product by which sniffer radios could be built."

Stream or Block Cipher?

"Third, data transmitted over the air is scrambled into 64-byte data packages thus providing an additional obstacle to unauthorized decoding."

Authentication

Unlike many fixed wireless broadband products, the Canopy system does not use clear text transmissions but rather a proprietary protocol for transmissions. When this protocol is combined with the Canopy Bandwidth and Authentication Manager (BAM), an added level of security is achieved for the operator and the network.

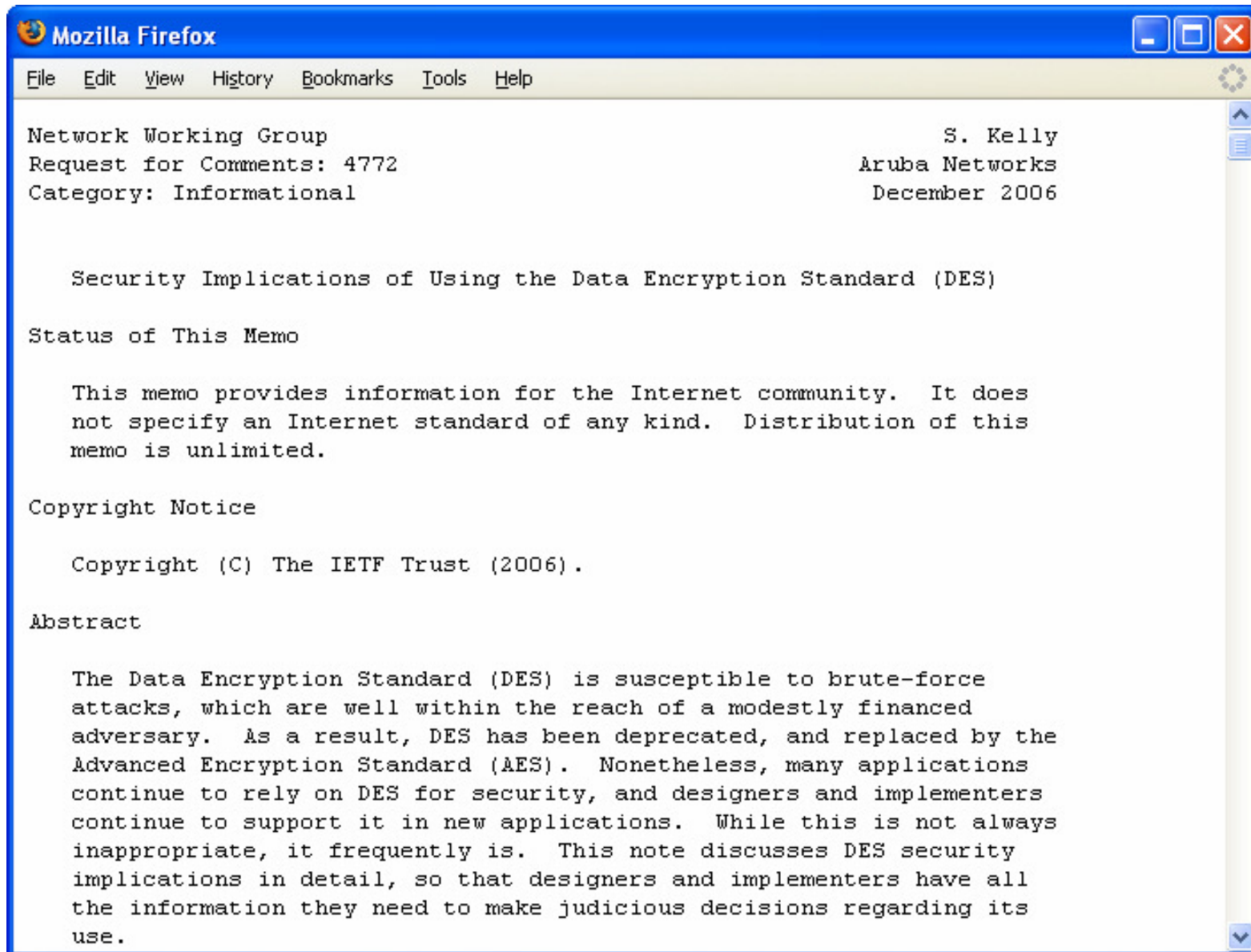
<i>Step</i>	<i>Description of Task</i>
1	When an SM attempts to enter the Canopy network it sends a registration request to the AP.
2	The AP then sends an authentication request to the BAM.
3	The BAM generates a 128 bit random number that is sent to the SM as a challenge.
4	The SM calculates a response using either its factory set key or the Authentication key if it has been assigned by the network operator.
5	This challenge response is sent to the BAM through the AP.
6	The BAM compares the challenge response to what it calculated using the same random number and the Authentication key from the BAM SQL database.
7	If the results agree, the BAM sends the AP a message authenticating the SM and sends the SM and AP QoS information.
	If the results do not agree or the SM is not in the database the BAM sends the AP a message denying authentication and the AP sends the SM a message to lock itself out from that AP for 15 minutes before retrying.

Encryption

The Canopy system also has provisions for the industry-accepted DES with key management via the Telecommunications Industry Association (TIA) standard BRAID cryptosystem. In addition, the Canopy system provides for AES for customers who require the most secure networks available.

Encryption	Bits in Key	Number of Possible Keys
DES	56	$2^{56} = 72,057,594,037,927,900$
AES	128	$2^{128} = 340,282,366,920,938,000,000,000,000,000,000,000,000,000$

RFC4772



The image shows a screenshot of a Mozilla Firefox browser window. The title bar reads "Mozilla Firefox" and the menu bar includes "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". The main content area displays the text of RFC 4772, which is a Request for Comments document. The text is formatted in a monospaced font and includes a header section with the author's name and affiliation, a title section, and several paragraphs of text.

Network Working Group S. Kelly
Request for Comments: 4772 Aruba Networks
Category: Informational December 2006

Security Implications of Using the Data Encryption Standard (DES)

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The IETF Trust (2006).

Abstract

The Data Encryption Standard (DES) is susceptible to brute-force attacks, which are well within the reach of a modestly financed adversary. As a result, DES has been deprecated, and replaced by the Advanced Encryption Standard (AES). Nonetheless, many applications continue to rely on DES for security, and designers and implementers continue to support it in new applications. While this is not always inappropriate, it frequently is. This note discusses DES security implications in detail, so that designers and implementers have all the information they need to make judicious decisions regarding its use.

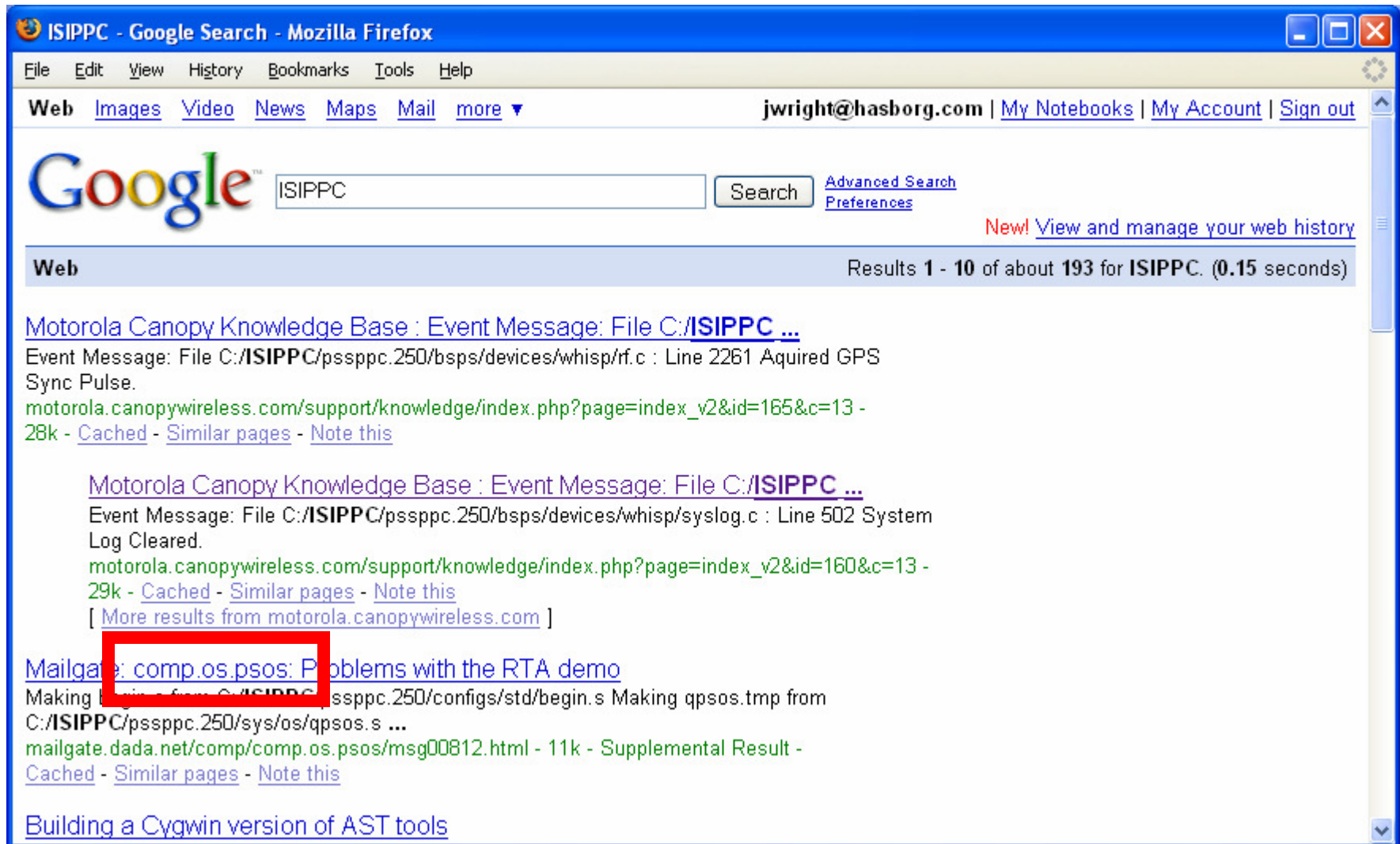
Error Messages are your Friend

The screenshot shows a web browser window titled "Motorola Canopy Knowledge Base : Event Message: File C:/ISIPPC/pssppc.250/bsps/devices/whisp/syslog.c : Line 502 Sys...". The browser's address bar and menu bar are visible. The page content includes the Motorola logo, navigation links (Home, Solutions, Products, Press/Events, Get Canopy, Support, Contact Us), and a "Support" sidebar. The main content area displays an event message with the following details:

- Event Message:** File C:/ISIPPC/pssppc.250/bsps/devices/whisp/syslog.c : Line 502 System Log Cleared
- Author:** Knowledge Base Administrator
- TITLE:** Event log message description
- PRODUCT:** SM AP BH
- RELEASE:** all
- DESCRIPTION:** What is indicated by the following Event Log message
File C:/ISIPPC/pssppc.250/bsps/devices/whisp/syslog.c : Line 502 S
- RESOLUTION:** This Event Log message indicates that the Event Log
'Clear System Log' button at the bottom of the Event Log web page.

An arrow points from a text box to the file path in the event message title. The text box contains the text "Symbols left in shipped code".

ISPPC?



The screenshot shows a Mozilla Firefox browser window with the title "ISPPC - Google Search - Mozilla Firefox". The address bar contains "jwright@hasborg.com | My Notebooks | My Account | Sign out". The search bar has "ISPPC" entered, and the search button is visible. The search results are displayed under the heading "Web" and show "Results 1 - 10 of about 193 for ISPPC. (0.15 seconds)".

The first result is from Motorola Canopy Knowledge Base, titled "Event Message: File C:/ISPPC ...". The snippet reads: "Event Message: File C:/ISPPC/pssppc.250/bps/devices/whisp/rf.c : Line 2261 Aquired GPS Sync Pulse." The URL is "motorola.canopywireless.com/support/knowledge/index.php?page=index_v2&id=165&c=13 - 28k - Cached - Similar pages - Note this".

The second result is also from Motorola Canopy Knowledge Base, titled "Event Message: File C:/ISPPC ...". The snippet reads: "Event Message: File C:/ISPPC/pssppc.250/bps/devices/whisp/syslog.c : Line 502 System Log Cleared." The URL is "motorola.canopywireless.com/support/knowledge/index.php?page=index_v2&id=160&c=13 - 29k - Cached - Similar pages - Note this". A link "[More results from motorola.canopywireless.com]" is provided.

The third result is from Mailgate, titled "comp.os.psos: Problems with the RTA demo". The snippet reads: "Making ... from C:/ISPPC/pssppc.250/configs/std/begin.s Making qpsos.tmp from C:/ISPPC/pssppc.250/sys/os/qpsos.s ...". The URL is "mailgate.dada.net/comp/comp.os.psos/msg00812.html - 11k - Supplemental Result - Cached - Similar pages - Note this".

The fourth result is "Building a Cygwin version of AST tools".

pSOS

The screenshot shows a Mozilla Firefox browser window with the title "pSOS - Wikipedia, the free encyclopedia". The address bar contains the URL "http://en.wikipedia.org/wiki/PSOS". The browser's menu bar includes "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". The page content features the Wikipedia logo on the left and the article title "pSOS" in the center. Below the title, it says "From Wikipedia, the free encyclopedia". The main text of the article begins with "According to some industry insiders, **pSOS** stands for **plug-in Silicon Operating System** but the official stance is that it is not an abbreviation, just a made-up word. (The original authors will not divulge the origin of the term.)" followed by a paragraph about its development in 1982 by Alfred Chao and its use as an RTOS for Motorola 68000 architecture.

File Edit View History Bookmarks Tools Help

http://en.wikipedia.org/wiki/PSOS

Google

site:motorola.can... http://w...4772.txt Motorola Canopy ... ISIPPC - Google S... pSOS - Wikipedi...

Sign in / create account

article discussion edit this page history

Your continued donations keep Wikipedia running!

pSOS

From Wikipedia, the free encyclopedia

According to some industry insiders, **pSOS** stands for **plug-in Silicon Operating System** but the official stance is that it is not an abbreviation, just a made-up word. (The original authors will not divulge the origin of the term.)

This [real time operating system](#) (RTOS) was created in about 1982 by Alfred Chao, and developed/marketed for the first part of its life by his company Software Components Group. In the 1980s pSOS rapidly became the RTOS of choice for all embedded systems based on the [Motorola 68000](#) family architecture, because it was written in 68000 assembler and was highly optimised from the start. It was also modularised, with early support for OS-aware debugging, plug-in device drivers, [TCP/IP](#) stacks, language libraries and disk subsystems. Later came source-level debugging, multi-processor support and further networking extensions.

navigation

- [Main page](#)
- [Contents](#)
- [Featured content](#)
- [Current events](#)
- [Random article](#)

interaction

- [About Wikipedia](#)
- [Community portal](#)
- [Recent changes](#)

Done