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.

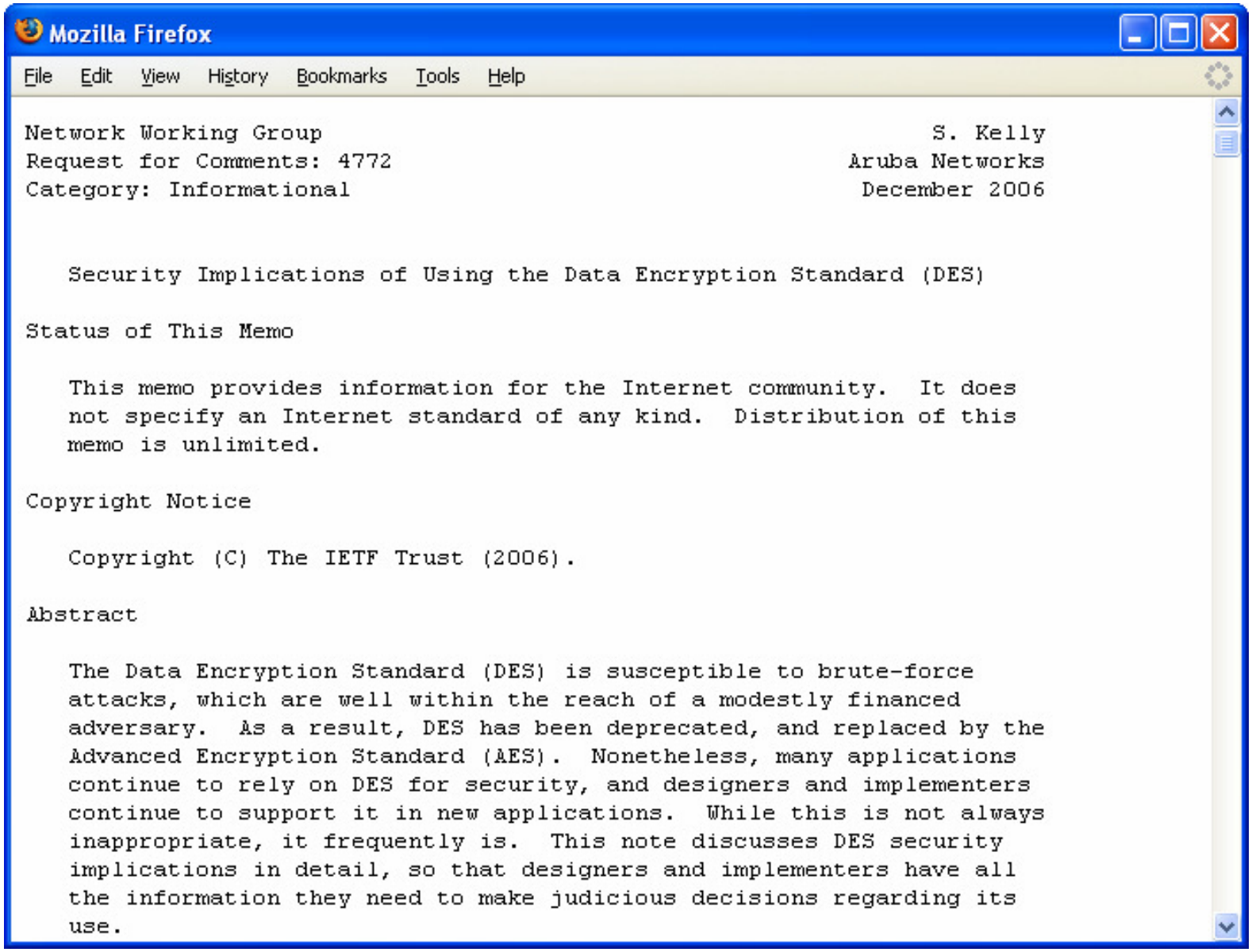
Step	*Description of Task*
1	When an SM attempts to enter the Canopy network it sends a registration request to the AP.
2	The AP then sends an authentication request to the BAM.
3	The BAM generates a 128 bit r[illegible] number th[illegible] sent to the SM as a cha[illegible]ng
4	The SM calculate[illegible] respo[illegible]e using ei[illegible]r its factory set key or th[illegible] A[illegible]hor[illegible]ation key i[illegible]as be[illegible] assigned by the n[illegible]vo[illegible]erator.
5	This [illegible]e[illegible]ge respons[illegible]is ent[illegible]o the BAM through [illegible]he AP
6	[illegible]he BAM com[illegible]ares [illegible]he challenge response to what it calcul[illegible]ed [illegible] the same random number and the Au[illegible]he[illegible]icatio[illegible] key from the BAM SQL database.
7	[illegible]f [illegible]re[illegible]ults agree, the BAM sends the AP a [illegible]ssage authenticating the SM and sends the SM and AP QoS information.
[illegible]	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

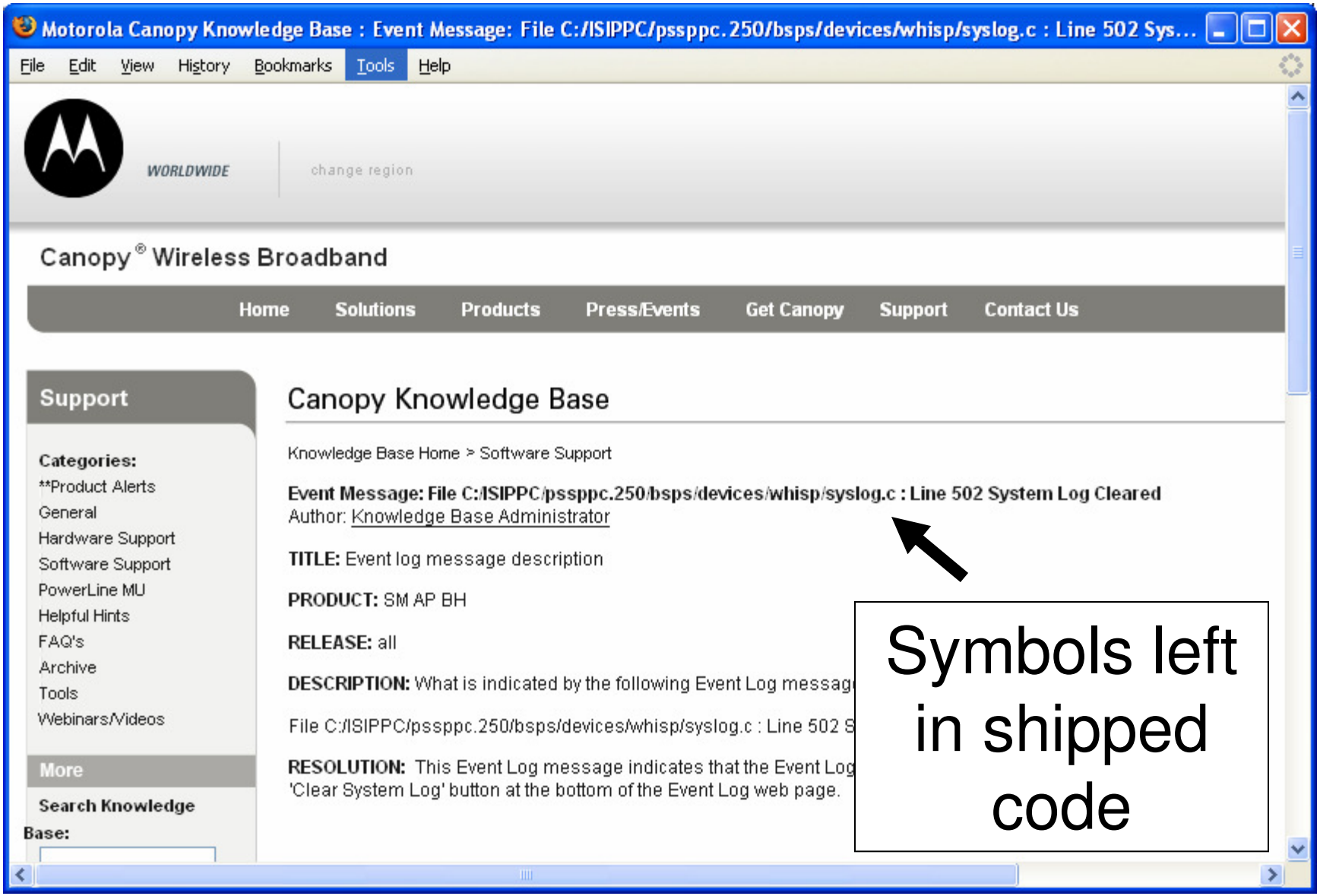
The Canopy system also has provisions for the industry-accepted DES with key management via the Telecommunications Industry Association (TIA) standard BRAID cryptosystem. In addition, the Canopy system provides for AES for customers who require the most secure networks available.

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

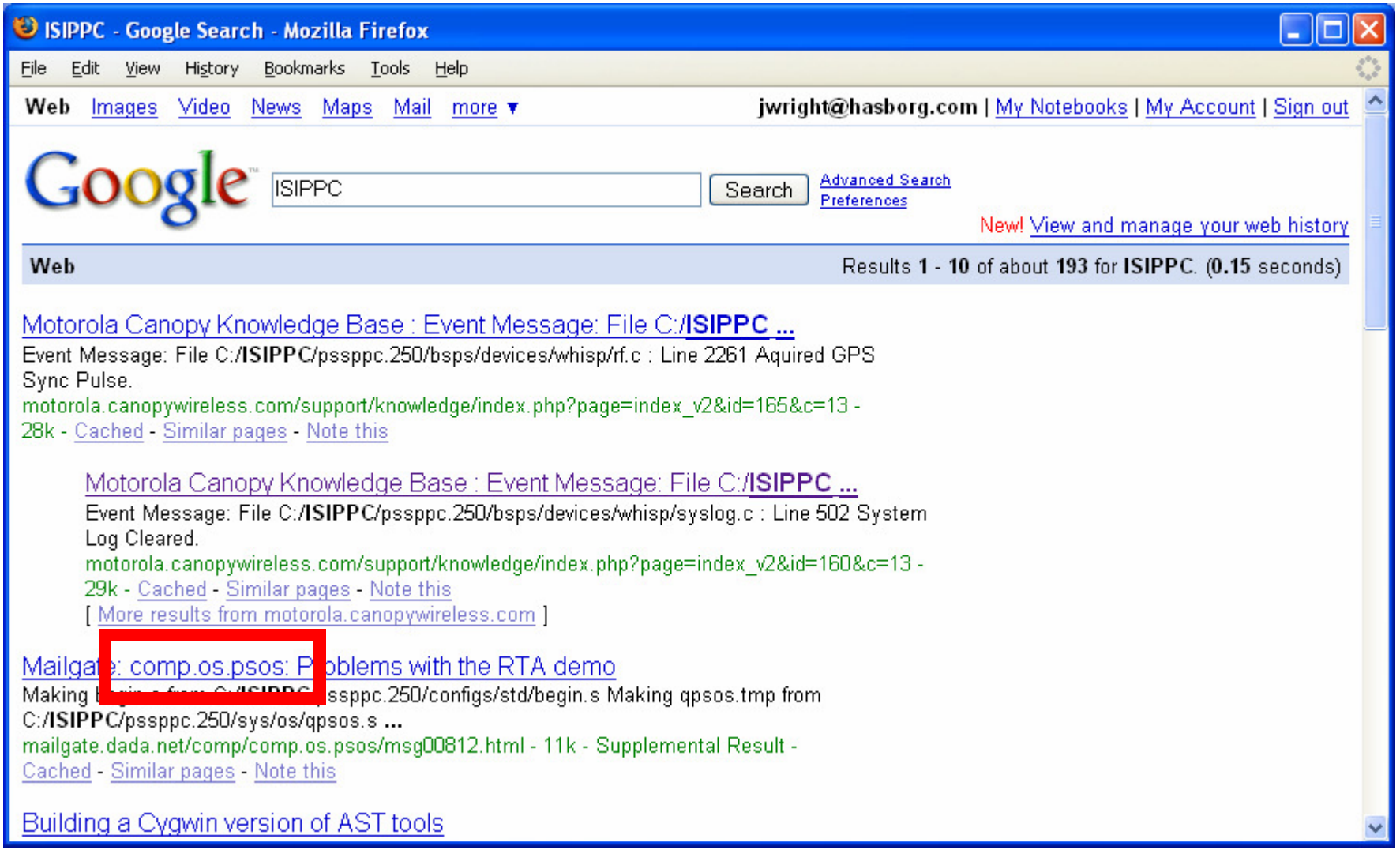
RFC4772


Mozilla Firefox
File Edit View History Bookmarks Tools Help
Network Working Group
Request for Comments: 4772
Category: Informational
S. Kelly
Aruba Networks
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



ISPPC?


ISIPPC - Google Search - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Web Images Video News Maps Mail more ▼
jwright@hasborg.com | My Notebooks | My Account | Sign out
Google
ISIPPC
Search
Advanced Search
Preferences
New! View and manage your web history
Web
Results 1 - 10 of about 193 for ISIPPC. (0.15 seconds)
Motorola Canopy Knowledge Base : Event Message: File C:/ISIPPC ...
Event Message: File C:/ISIPPC/pssppc.250/bsps/devices/whisp/rf.c : Line 2261 Aquired GPS Sync Pulse.
motorola.canopywireless.com/support/knowledge/index.php?page=index_v2&id=165&c=13 - 28k - Cached - Similar pages - Note this
Motorola Canopy Knowledge Base : Event Message: File C:/ISIPPC ...
Event Message: File C:/ISIPPC/pssppc.250/bsps/devices/whisp/syslog.c : Line 502 System Log Cleared.
motorola.canopywireless.com/support/knowledge/index.php?page=index_v2&id=160&c=13 - 29k - Cached - Similar pages - Note this
[More results from motorola.canopywireless.com]
Mailgate: comp.os.psos: Problems with the RTA demo
Making begin.s from C:/ISIPPC/pssppc.250/configs/std/begin.s Making qpsos.tmp from C:/ISIPPC/pssppc.250/sys/os/qpsos.s ...
mailgate.dada.net/comp/comp.os.psos/msg00812.html - 11k - Supplemental Result - Cached - Similar pages - Note this
Building a Cygwin version of AST tools

pSOS


pSOS - Wikipedia, the free encyclopedia - Mozilla Firefox
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
WIKIPEDIA
The Free Encyclopedia
navigation
Main page
Contents
Featured content
Current events
Random article
interaction
About Wikipedia
Community portal
Recent changes
Done