hp e3000

webwise porting

# hp webwise secure web server porting case study

presented by Mark Bixby
mark_bixby@hp.com

Solution Symposium 2001

# webwise components

- Apache 1.3.9
  - vanilla web server
- mod_ssl 2.4.9-1.3.9
  - adds SSL support and other enhancements to Apache
- OpenSSL 0.9.4
  - SSL protocol, crypto algorithms, PKI utilities
- MM 1.0.12
  - platform independent shared memory library
- RSA BSAFE Crypto-C 4.2
  - legal implementations of RSA, RC2, and RC4

# the porting process

- configure
- compile
- install
- load (unresolved externals)
- run
- repeat until successful
- submit your changes back to the public source tree
    - diff -ru virginsourcedir mpesourcedir >patch.txt

# apache configure issues

- resulting NMPRG needs chmod 755 permissions
- new src/os/mpeix subdirectory required for DSO support and other things
- workaround needed for shell variable problem
  - bad: `foo=$foo ./some/script`
  - good: `foo="$foo"; export foo; ./some/script`
- ld linker parameters for creating shared libraries
  - `-b -a archive`
- detecting unresolved exernals without executing the code
  - `callci run testprog\;stdin=\*bogus 2>&1 | grep ^UNRESOLVED`

# apache compile issues

- src/os/mpeix/Makefile.tmpl
  - copy and modify src/os/unix/Makefile.tmpl
- src/os/mpeix/os-inline.c
  - clone from src/os/unix/os-inline.c
- src/os/mpeix/os.c
  - clone from src/os/unix/os.c
- src/os/mpeix/os.h
  - copy and modify src/os/unix/os.h
  - WebWise version string

# apache compile issues (cont.)

- src/support/ab.c

```
#ifndef MPE
#  include <sys/time.h>
#endif
```

# apache install issues

- temporary installation file names contain # characters
  - bad: `dsttmp=$dstdir/#inst.$$#`
  - good: `dsttmp=$dstdir/inst.$$`

# apache load issues

- getpass()
  - Richard Stevens' Advanced Programming in the Unix Environment
  - http://www.kohala.com/start/apue.html
- dlopen()/dlsym()/dlerror()/dlclose()
  - code from scratch using HPGETPROCPLABEL() and hpunload()
  - good enough for Apache, but not a 100% implementation
- gettimeofday()
  - Porting Wrappers
  - http://jazz.external.hp.com/src/px_wrappers/index.html

# apache run issues - sockets

- #define USE_FCNTL_SERIALIZED_ACCEPT
  - Apache children must call accept() in a serialized manner to correctly handle multiple sockets (80,443)
  - http://httpd.apache.org/docs/misc/perf-tuning.html
- setsockopt(SO_REUSEADDR) now supported by MPE
  - not supported at time of original apache port
  - enable this code by removing #ifndef MPE
- setsockopt(SO_KEEPALIVE) exists but still errors out on MPE
  - suppress this code with #ifndef MPE
- src/main/rfc1413.c bind() requires INADDR_ANY
  - but what about multiple NICs or IP aliasing???

# apache run issues - processes

- parent and children must be able to use different POSIX uids to ensure server keys and certificates are secure
- children now unconditionally call setuid() instead of requiring MANAGER.SYS as in the original Apache port
- parent must be able to signal children w/different uid
  - patch MPELX51 allows AM parents to do this
- parent and children must be able to manipulate common SVIPC shared memory from different uids
  - on Unix, a superuser (uid 0) parent could do this, but since MPE lacks the concept of uid 0, SHM_R and SHM_W must be redefined to allow group access

# apache run issues - miscellaneous

- third parameter of `int main(int argc, char **argv, char **envp)` not passed by MPE; workaround:

```
extern char **environ;
envp = environ;
```

- proxy_cache.c tries to use link() to create hard links
  - link() exists on MPE, but always returns an error
  - already supported rename() workaround for other OSes
- proxy_util.c filename “@” characters
  - already supported other OSes which lack @
- mpe_dl_stub() workaround to support DSOs before patch MPELX44 was developed

# mod_ssl configure issues

- portable non-GNU way to detect MPE from a script?
  - `if [ -f '/SYS/PUB/MPEXLDIR' -a ".$HPSUSAN" != . ]; then # it's MPE!`
- built-in cat stdin inline redirects are broken (cat >foo <<bar)
  - use /bin/cat instead (alias -x cat=/bin/cat)
- embedded patch program needs -D_POSIX_SOURCE
  - `export CPPFLAGS="-D_POSIX_SOURCE"`
- ld library order is important at link time on MPE
  - move OpenSSL libraries from beginning to end of list

# mod_ssl compile issues

- modify pkg.sslmod/libssl.version to contain WebWise version string
- pkg.sslmod/mod_ssl.h #include <sys/time.h>
  - suppress it with #ifndef MPE

# mod_ssl run issues

- because Apache parent and children run with different POSIX uids, all shared file and SVIPC semaphore permissions had to be modified to permit group access
- pkg.sslsup/mkcert.sh suffers from the built-in cat problem
  - alias -x cat=/bin/cat

# mod_ssl submit-back issues

- not accepting contributions from the U.S. due to our crypto export laws :-(
- CSY will provide these mod_ssl patches upon request to anybody who asks in order to comply with the mod_ssl open-source license

# openssl configure issues

- modify Configure script to include MPE/iX-gcc entry with compile and link options
- modify config script to change machine name (HPCPUNAME) hyphens to underscores
- various modifications so that the OpenSSL RSA, RC2, RC4, and RC5 algorithms are suppressed when configuring with RSA BSAFE Crypto-C patch

# openssl compile issues

- suppress SO_KEEPALIVE code with #ifndef MPE
- modify crypto/des/read_pwd.c to use TERMIOS terminal I/O methods on MPE (tcgetattr()/tcsetattr())
- modify e_os.h to suppress #include of <sys/param.h> and <sys/time.h>
- integrate and extend Gordon Chaffee's and G. Madhusudan's RSA BSAFE Crypto-C patch to include RC2, RC4, and RC5 in addition to the RSA algorithm
  - necessary to be legal before the RSA patent expired
  - ~2800 lines of patch text

# openssl run issues

- crypto/des/read_pwd.c problems reading passwords with echo disabled
  - use stdin instead of opening /dev/tty in order to avoid a console ldev 10 prompt from batch
  - ignore erroneous error code from tcsetattr() when echo is disabled
- reduce socket buffer size from 32769 to the MPE maximum of 30000

# openssl submit-back issues

- RSA BSAFE Crypto-C patch not submitted back to the OpenSSL developers
  - NOTE! The OpenSSL 0.9.5a patch fails to apply to OpenSSL 0.9.6
- http://jazz.external.hp.com/src/openssl/

# mm configure issues

- modify GNU configure script to use callci run testprog;stdin=*bogus method for detecting unresolved externals
  - change each line that sets ac_link

hp e3000

webwise porting

# mm install issues

- modify shtool to remove # and @ from temporary filenames

# mm run issues

- modify SVIPC semget() calls to include group permissions due to Apache parent and children running with different uids

# mm submit-back issues

- not accepting contributions from the U.S. due to our crypto export laws :-(
- CSY will provide these mm patches upon request to anybody who asks in order to comply with the MM open-source license

hp e3000

webwise porting

# RSA BSAFE Crypto-C issues

- censored!
- proprietary code for which HP has a source license
- MPE patches not submitted back to RSA

# summary

- porting was generally fairly easy, with only a couple of items requiring moderate effort that had not been required for previous ports:
  - a minimal MPE implementation of the dlopen() family for dynamically loading code and data from shared libraries
  - modifying permissions to allow differing parent/child uids in MPE's POSIX environment which doesn't support uid 0
- the high effort required to integrate OpenSSL and RSA BSAFE Crypto-C was integration effort, not porting effort

hp e3000

webwise porting

# join the hp3000-l community!

- Available as a mailing list and as the Usenet newsgroup comp.sys.hp.mpe
- In-depth discussions of all things HP e3000
- Talk with other people porting open-source to MPE
  - seek advice, exchange tips & techniques
- Keep up with the latest HP e3000 news
- Interact with CSY
- http://jazz.external.hp.com/papers/hp3000-info.html

hp e3000

webwise porting

# porting is easier than you think!

Any questions?