Security TR Session

• N1055.pdf	Working draft of TR
• N1059.htm	Editor’s Report
• N1063	These slides (next mailing)
• N1049	Comments from Bill

N1063

Late Issues with n1055

(From email and n1049)

Got versus Have

- Should `__GOT_SECURE_LIB__` be `__HAVE_SECURE_LIB__` ?
- “HAVE” is consistent with widespread Open Source software practice
- “GOT” implies acquisition of a dynamic resource/ “Have” implies static capability
- From Nelson Beebe, off-reflector email

Consensus

- `__STDC_WANT_SECURE_LIB__` replaces `__USE_SECURE_LIB__`

- `__STDC_SECURE_LIB__` replaces `__GOT_SECURE_LIB__`

N1049 Second Batch

- Suggestion: Borrow concept of “precision” from `printf` for `scanf`/`scanf_s` format specifiers `c`, `s`, `[`

```
char a[100];
scanf(“%.100s”, a);
scanf(“%.*s”, (size_t)100, a);
```

scanf, cont.

- Default precision for `scanf_s` is 0, requiring use of precision
- Disadvantage: Decreased possibility for compile-time checking that secure practice is being followed. Contrast with Footnote 4, page 7.
- Note `“%*.*s”` would be an assignment suppressed scan with indirect precision.

getenv_s (via reflector)

- The `needed` parameter should be used to store the length+1 of the environment string found, since that is how much space needs to be allocated for the string.
- Note that `snprint` returns the length, not length+1. Inconsistent?
- Behavior of other existing functions?

asctime_s (via reflector)

- Sample code will store a null char even if size of output array is zero. Add red line:

```
 if (n < 1 || n >= maxsize) {
    if (maxsize > 0)
       s[0] = '\0';
    return ERANGE;
  }
```

n1049 Fourth Batch

- Secure library functions should have defined, and safe, semantics for null pointer arguments.

<string.h>

- `gets_s` should return a null pointer for a null pointer argument.
- `strncpy_s` and `strncat_s` should return `ERANGE` for null pointer arguments.
- `strnlen_s` should return zero for a null pointer argument.

<wchar.h>

- `wcsncpy_s` and `wcsncat_s` should return `ERANGE` for null pointer arguments.
- `wcsnlen_s` should return zero for a null pointer argument.

All headers and functions should be checked!

N1049 Second Batch

- `tmpnam_s` should compare the length of the filename to `maxsize-1`, not `maxsize`
- Not needed: TR uses “size” for number elements of an array and “len” for length of string.

```
strlen(“abc”) < sizeof “abc”
```

New functions coming

- mbsrtowcs_s
- wcsrtombs_s
- wcrtomb_s

Details not available. Goals: always null terminate, add size parameter for dst, remove optional static state.