Submitter: Robert C. Seacord
Submission Date: 2016-04-14
Source: WG14
Reference Document: N2043
Subject: definition of out-of-bounds store

Summary

The definition of out-of-bounds store in Annex L is problematic in that it refers to a fetch of a volatile object although the definition is for out-of-bounds store. Out-of-bounds store is inadequate for security purposes as it may help prevent arbitrary code execution vulnerabilities but will fail to prevent information leakage that might result in the leakage of sensitive information such as key information (e.g., heartbleed), passwords, personally identifiable information (PII), etc. Consequently, the definition is expanded to include all out-of-bounds access.

Suggested Technical Corrigendum

Change §L.2.1, p1:

> out-of-bounds store
> an (attempted) access (3.1) that, at run time, for a given computational state, would modify (or, for an object declared volatile, fetch) one or more bytes that lie outside the bounds permitted by this Standard.

To:

> out-of-bounds access
> an (attempted) access (3.1) that, at run time, for a given computational state, would access one or more bytes that lie outside the bounds permitted by this Standard.

Change §L.2.2, p1:

> bounded undefined behavior
> undefined behavior (3) that does not perform an out-of-bounds store

To :

> bounded undefined behavior
> undefined behavior (3) that does not perform an out-of-bounds access

Change §L.2.3, p2:

NOTE The behavior might perform an out-of-bounds store or perform a trap.

To:

NOTE The behavior might perform an out-of-bounds access or perform a trap.