Secure Communicating Systems
Design, Analysis, and Implementation[*]

Errata for the **First** Printing

January 16, 2004

Readers of this book are kindly requested to notify Michael Huth (email: `mrh@doc.ic.ac.uk`) of errors they find. These will be included in this file.

- p. 24, the sentence after Definition 2.8: the number 1729 is not a prime since it equals $7 \cdot 13 \cdot 19$;

- ```
  >I believe there may be an error in example 3.22, on page 110. It
  >reads:
  >
  >"xtime(a) = 8A
  > xtime(xtime(a)) = 8A . 02 = 0D
  > xtime(xtime(xtime(a))) = 0D . 02 = 96"
  >
  >I think that 8A . 02 should be 0F[1], which then gives 1E for the third
  >result. Adding 8A to 1E then gives 94, which matches with the result
  >in example 3.19 on the previous page.
  >
  >[1] 8A << 1 = 114; b7 = 1
  > => xtime(8A) = 14 XOR 1B = 0F
  >
  >Regards,
  >Alisdair McDiarmid
  ```

- p. 221, Example 6.18: The first sentence should read "Consider the command `c` given by ... where `c1` and `c2` are arbitrary commands that do not assign to any variables of type `var L`."

Acknowledgments