Chapter 1d

Examples on Using Proposition and Predicate Logic

Discrete Mathematics II

(Materials drawn from **Chapter 2** in:
"Michael Huth and Mark Ryan. *Logic in Computer Science: Modelling and Reasoning about Systems*, 2nd Ed., Cambridge University Press, 2006.")

Nguyen An Khuong, Huynh Tuong Nguyen
Faculty of Computer Science and Engineering
University of Technology, VNU-HCM

Contents

Electing Puzzle

- Four men and four women are nominated for two positions.
- Exactly one man and one woman are elected.
- The men are A, B, C, D and the women are E, F, G, H. We know:
  - if neither A nor E won, then G won
  - if neither A nor F won, then B won
  - if neither B nor G won, then C won
  - if neither C nor F won, then E won.
- Who were the two people elected?

Nguyen An Khuong, Huynh Tuong Nguyen

Huth and Ryan [2], Exercises 2.1.5: Protocol Requirements

- The following sentences are taken from the **RFC3157 Internet Task-force Document 'Securely Available Credentials – Requirements.'**
- Specify it in predicate logic, defining predicate symbols as appropriate:
  a. An attacker can persuade a server that a successful login has occurred, even if it hasn't.
  b. An attacker can overwrite someone else's credentials on the server.
  c. All users enter passwords instead of names.
  d. Credential transfer both to and from a device MUST be supported.
  e. Credentials MUST NOT be forced by the protocol to be present in cleartext at any device other than the end user's.
  f. The protocol MUST support a range of cryptographic algorithms, including symmetric and asymmetric algorithms, hash algorithms, and MAC algorithms.
  g. Credentials MUST only be downloadable following user authentication or else only downloadable in a format that requires completion of user authentication for deciphering.
  h. Different end user devices MAY be used to download, upload, or manage the same set of credentials.

Nguyen An Khuong, Huynh Tuong Nguyen

Huth and Ryan [2], Exercises 2.1.5: Solutions

a. An attacker can persuade a server that a successful login has occurred, even if it hasn't:
$\phi := \exists a \exists s((\neg loggedIn(a, s)) \longrightarrow (canPersuade(a, s)))$.

b. An attacker can overwrite someone else's credentials on the server: $\phi := \exists u \exists c \exists s \exists d((\neg ownsCredentials(u, c)) \longrightarrow canWrite(u, c, s, d))$.

Nguyen An Khuong, Huynh Tuong Nguyen