Journal of Computer Security 13 (2005) 695
IOS Press

Erratum

Symbolic protocol analysis with an Abelian group operator or Diffie–Hellman exponentiation

Jonathan Millen and Vitaly Shmatikov

[*Journal of Computer Security* **13**(3) (2005), 515–564]

The authors are grateful to Stéphanie Delaune and Ralf Treinen for noticing flaws in our constraint solution procedure. In Section 6.4, if there is a derivation constraint $T \triangleright u$ such that u contains the first occurrence of a variable x, a new variable $\hat{x} = u$ is introduced to eliminate x. This leads to some problems. First, the substitution may create new solutions, making the step unsound. Second, the substitution may lose solutions, making the procedure incomplete.

For example, the system

$$\begin{aligned} a^3 &\triangleright X^2 \\ a^3, X^2 &\triangleright a^3 \end{aligned}$$

does not have a solution, but after setting $\hat{X} = X^2$ so that $X = \hat{X}^{1/2}$, the new system is trivially solvable. However, there is no substitution for X. The fix for this is to require a solution to $u \triangleright \hat{x}$, generating additional Diophantine equations.

Incompleteness is illustrated by the system

$$\begin{aligned} a^2 &\triangleright X^2 \\ a^2, X &\triangleright a \end{aligned}$$

which has the solution $X = a$, but after replacing X^2 with $\hat{X}$ to get

$$\begin{aligned} a^2 &\triangleright \hat{X} \\ a^2, \hat{X}^{1/2} &\triangleright a \end{aligned}$$

the Diophantine equation for the second constraint above is written (incorrectly) as though $\hat{X}^{1/2}$ is expressible as an integer power of a^2, leading to an equation in exponents $2z = 1$ which is not solvable in integers.

The authors are working on a revision of this section to address these problems, which we expect to have ready for the following issue.