FDR2 jako narzędzie do weryfikacji protokołów kryptograficznych.

autor: Mateusz Chrzęst

Seminarium Protokoły Komunikacyjne

Plan

Model-checking

CSP

FDR2

Protokół Needhama-Schroedera

Model-checking

Polega na skonstruowaniu matematycznego modelu badanego programu i pokazaniu w sposób formalny, najlepiej automatycznie, że wszystkie możliwe wykonania programu i ich przeploty nie mają niepożądanych własności.

Model danych

Komunikacja synchroniczna

Atomowość zdarzeń

Składnia CSP

P = ... - definicja procesu

a -> P – operator prefiksu

P[|A|]Q - synchronizacja

P ||| Q przeplot

P |~| Q – wybór wewnętrzny

P []Q – wybór zewnętrzny

Składnia CSP

SKIP - Poprawne zatrzymanie

STOP – Zakleszczenie

C !v -> P - Wyjście w kanale *C*

c?x -> P(x) - Wejście w kanale *c*

Semantyka śladów

Przyporządkowuje procesom zbiory śladów zdarzeń (*traces()*) generowanych przez te procesy.

P [T= Q <=> *traces(Q)* jest podzbiorem *traces(P)*

Semantyka uszkodzeń

Przyporządkowuje procesom zbiór par (*s*,X), gdzie:

s – ślad procesu

X – zbiór akcji, których proces może odmówić po śladzie *s*

P [F= Q <=> failures(Q) jest podzbiorem failures (P)

Semantyka uszkodzeń i rozbieżności

Semantyka uszkodzeń rozszerzona o zbiór "rozbieżności" [ang. *divergence*] – zbiór śladów po których może nastąpić livelock

P [FD= Q <=> *failures(Q)* jest podzbiorem *failures(P)*

oraz

divergences(Q) jest podzbiorem *divergences(P)*

Deadlock

Zakleszczenie – proces nie jest w stanie wykonać żadnych operacji.

Livelock (divergence)

Proces wykonuje nieskończony ciąg akcji wewnętrznych, bez występowania akcji zewnętrznych.

Deterministic

Proces nie jest deterministyczny jeśli:

- ślad nie wyznacza jednoznacznie zbioru kolejnych akcji,
- może nastąpić livelock,
- dla danego śladu istnieje akcja, która jest możliwa i może zostać odmówiona.

Protokół Needhama-Schroedera

(A)licja: SK(A), PK(S)

(B)ob: SK(B), PK(S)

(S)erver: PK(A), PK(B), SK(S)

Protokół Needhama-Schroedera krok 1

1. A -> S: A, B

- Alicja wysyła pytanie o klucz publiczny Boba

Protokół Needhama-Schroedera krok 2

1. A -> S: A, B
2. S -> A: {B,PK(B)}SK(S)

- Serwer odsyła Alicji klucz publiczny Boba zaszyfrowany swoim kluczem prywatnym

Protokół Needhama-Schroedera krok 3

1. A -> S: A, B
2. S -> A: {B,PK(B)}SK(S)
3. A -> B: {A,Na}PK(B)

- Alicja wysyła Bobowi zaszyfrowany (kluczem publicznym Boba) znacznik Na oraz swój identyfikator

Protokół Needhama-Schroedera krok 4

1. A -> S: A, B
2. S -> A: {B,PK(B)}SK(S)
3. A -> B: {A,Na}PK(B)
4. B-> S : B, A

- Bob prosi Server o klucz publiczny Alicji

Protokół Needhama-Schroedera krok 5

1. A -> S: A, B
2. S -> A: {B,PK(B)}SK(S)
3. A -> B: {A,Na}PK(B)
4. B-> S : B, A
5. S -> B: {A,PK(A)}SK(S)

- Server odsyła Bobowi klucz Alicji zaszyfrowany swoim kluczem prywatnym

Protokół Needhama-Schroedera krok 6

1. A -> S: A, B
2. S -> A: {B,PK(B)}SK(S)
3. A -> B: {A,Na}PK(B)
4. B-> S : B, A
5. S -> B: {A,PK(A)}SK(S)
6. B -> A: {Na,Nb}PK(A)

- Bob losuje nowy znacznik Nb i odsyła go razem z Na Alicji, wiadomość szyfruje jej kluczem publicznym

Protokół Needhama-Schroedera krok 7

1. A -> S: A, B
2. S -> A: {B,PK(B)}SK(S)
3. A -> B: {A,Na}PK(B)
4. B-> S : B, A
5. S -> B: {A,PK(A)}SK(S)
6. B -> A: {Na,Nb}PK(A)
7. A -> B: {Nb} PK(B)

- Alicja odsyła Bobowi jego znacznik zaszyfrowany jego kluczem publicznym

Protokół Needhama-Schroedera

1. A -> B: {A,Na}PK(B)
2. B -> A: {Na,Nb}PK(A)
3. A -> B: {Nb} PK(B)

Atak na protokół Needhama-Schroedera

1. A -> I: {A,Na}PK(I)
2. I -> B: {A,Na}PK(B)
3. B -> I: {Na, Nb}PK(A)
4. I -> A: {Na, Nb}PK(A)
5. A -> I: {Nb}PK(I)
6. I -> B: {Nb}PK(B)

Instalacja FDR2

- Ściągnąć z http://www.fsel.com/fdr2_download.html
- Ustawić FDRHOME na katalog z FDR2
- Uruchomić $FDRHOME/bin/fdr2

Linki

FDR - http://www.fsel.com/

http://www.fsel.com/documentation/fdr2/fdr2manual.pdf

http://web.comlab.ox.ac.uk/oucl/work/gavin.lowe/Security/Casper/

http://www.anta13.neostrada.pl/csp_fdr.html

Pytania ?