Coq i protokół NSSK

Piotr Iwaniuk

21 marca 2012

Plan

Plan

Protokoły kryptograficzne

- Podstawowe zadanie: przesyłanie danych przez sieć tak, żeby inni nie mogli ich odczytać.
- Wykorzystywana do tego jest kryptografia.
- Standardowe założenia: sieć może być podsłuchana, możliwe jest podrabiania podrabianie wiadomości (włącznie z nadawcą).
- Przykłady protokołów: symetryczny Needhama-Schroedera (NSSK), protokół Otwaya-Reesa.

Weryfikacja protokołów

Atak Denning & Saco na protokół NSSK pojawił się 3 lata po opublikowaniu protokołu.

To pokazało, że konieczna jest dokładna weryfikacja protokołów.

Jeszcze w tym samym roku pojawił się pierwszy model do wyszukiwania luk w bezpieczeństwie (Dolev-Yao).

Metody weryfikacja - oś czasu

- 1981 – Dolev-Yao Model
- 1982 – Dolev-Even-Karp Model
- 1989 – logika Burrows-Abadi-Needham
- 1995 – Użycie model checkera FDR do weryfikacji protokołów (Lowe).
- 1997 – Użycie provera Isabelle do weryfikacji protokołów
- 1999 – Użycie typowania do weryfikacji protokołów
- 2000 – CAPSL: Common Authentication Protocol Specification Language[1]

Dolev-Yao, Dolev-Even-Karp i inne

- Dostępny jest szereg działań takich jak: wysłanie wiadomości, odszyfrowanie.
- Przeszukiwanie dyskretnej przestrzeni stanów.
- Oryginalnie w czasie wielomianowym, ale przy zmianie założeni łatwo wpaść w nierozstrzygalność.

- NRL Protocol Analyzer
- narzędzie do analizy Longley-Rigby

Belief logics

- Wnioskowanie o protokole podobne do logiki Hoare'a.
- Konstrukcje mówiące o statusie elementów i wiedzy stron w protokole.
- Reguły adnotowania komunikatów, oraz reguły wnioskowania.

Model checking dla protokołów

- Najbardziej znane zastosowanie przypisuje się Gavinowi Lowe.
- Odkrycie nowej luki w znanym od długiego czasu protokole Needhama-Schroedera dla kluczy publicznych.
- Zapis protokołu w języku CSP.
- Do weryfikacji użyto komercyjny model checker FDR.

Komputerowo wspomagane dowodzenie

- Narzędzie do dowodzenia Isabelle/HOL.
- Raczej interaktywny pomocnik dowodzenia, ale posiada też możliwość automatyzacji.
- Zarówno program jak i weryfikacja protokołów rozwijane przez Lawrence'a Paulsona.

Inne metody

- Systemy przepisywania.
- Rachunek równościowy.

Plan

Komputerowo wspomagane dowodzenie

- Automatyczne
  - sprawdzanie dowodu
  - dowodzenie
- Interaktywne dowodzenie

Systemy wspomagania dowodzenia

- Dowodzenie odbywa się przez współpracę człowieka z komputerem.
- Interakcja odbywa się najczęściej przez konsolę – wpisywanie komend.
- Zazwyczaj takie programy opierają się na rachunku lambda i odpowiedniości między formułami logiki a typowaniem λ-termów.

Przykłady

Przykłady systemów dowodzenia twierdzeń.

- Coq – INRIA
- Mizar – Uniwersytet w Białymstoku, Uniwersytet Alberty, Uniwersytet Shinshu
- Isabelle - Larry Paulson
- Minlog – Uniwersytet w Monachium

Twierdzenia na sprzedaż

- Uniwersytet w Edynburgu dał możliwość kupienia twierdzenia.
- Nowe twierdzenie nosiłoby nazwę kupującego.
- Cena: £15

Coq

- Oparty na rachunku indukcyjnych konstrukcji.
- Calculus of constructions: polimorfizm, konstruktory typów, typy zależne.
- Calculus of inductive constructions: CoC wzbogacony o definicje indukcyjne.
- Taka jest geneza nazwy.

Coq – interfejs

- Kompilator `coqc` i toplevel `coqtop`.
- Interfejs okienkowy `coqide`.
- Tryb dla Emacsa.

Coq – język programowania

- Do obsługi programu używa się 2 języków: *Gallina* i *The Vernacular*.
- *Gallina* to język termów-definicji.
- *The Vernacular* to język poleceń.
- Możliwe jest rozszerzanie składni.

Coq – działanie

- Dysponujemy zestawem definicji i aksjomatów.
- Można wpisać do programu twierdzenie. Wtedy przechodzi się do trybu edycji dowodu.
- Wykorzystując różne dostępny taktyki pokazujemy cele.
- Kiedy wszystko jest już dowiedzione: `Qed.`
- Dowiedzione twierdzenie jest dołączane do środowiska i można z niego skorzystać w kolejnych.

Literatura


Catherine Meadows.
Formal methods for cryptographic protocol analysis: emerging issues and trends.
IEEE Journal on Selected Areas in Communications, 21(1):44–54, 2003.


Freek Wiedijk.
The Seventeen Provers of the World.
2006.