Falcon 9

Protokół NSSK i jego formalizacja

Piotr Iwaniuk

17 października 2012

Plan

Plan

Alice i Bob[3]

- Alice chce ustanowić z Bobem bezpieczny kanał komunikacyjny.
- Używane do tego będzie symetryczne (konwencjonalne) szyfrowanie.
- Obie strony komunikacji muszą ustalić wspólny klucz.

Szczegółowe założenia

- Każdy aktor posiada klucz, który jest znany tylko jemu i zaufanemu serwerowi uwierzytelniana
- Możliwe jest zaszyfrowanie zawartości bez konieczności wysyłania jej
- Sieć jest duża i zdecentralizowana – nie ma kontroli nad tym, kto z niej korzysta i w jakim celu
- Nie ma pojedynczego zegara
- Nie ma kontroli nazw

Zapis protokołu

A, B, S – strony w komunikacji
K – klucze
N – wartości jednorazowe
T – znaczniki czasu

Zapis protokołu

A, B, S – strony w komunikacji
K – klucze
N – wartości jednorazowe
T – znaczniki czasu

$\{X\}_K$ – zawartość zaszyfrowana kluczem K

Zapis protokołu

A, B, S – strony w komunikacji
K – klucze
N – wartości jednorazowe
T – znaczniki czasu

$\{X\}_K$ – zawartość zaszyfrowana kluczem K

X, Y – grupowanie elementów X i Y

Zapis protokołu

A, B, S – strony w komunikacji
K – klucze
N – wartości jednorazowe
T – znaczniki czasu

$\{X\}_K$ – zawartość zaszyfrowana kluczem K

X, Y – grupowanie elementów X i Y

$A \rightarrow B : X$ – wysłanie przez A do B wiadomości X

Protokół NSSK

$$A \rightarrow S \quad : \quad A, B, N_A \tag{1}$$
$$S \rightarrow A \quad : \quad \{N_A, K_{AB}, B, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}} \tag{2}$$

Protokół NSSK

$$A \rightarrow S \quad : \quad A, B, N_A \tag{1}$$
$$S \rightarrow A \quad : \quad \{N_A, K_{AB}, B, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}} \tag{2}$$
$$A \rightarrow B \quad : \quad \{K_{AB}, A\}_{K_{BS}} \tag{3}$$
$$B \rightarrow A \quad : \quad \{N_B\}_{K_{AB}} \tag{4}$$
$$A \rightarrow B \quad : \quad \{N_B + 1\}_{K_{AB}} \tag{5}$$

Atak – Denning i Sacco

Komunikat (3) nie jest zabezpieczany przez wartości jednorazowe. Intruz może przesłać taki komunikat ponownie.[1]

Atak – Denning i Sacco

Komunikat (3) nie jest zabezpieczany przez wartości jednorazowe. Intruz może przesłać taki komunikat ponownie.[1]

$$
\begin{aligned}
C \rightarrow B &: \{K_{AB}, A\}_{K_{BS}} \\
B \rightarrow C &: \{N_B\}_{K_{AB}} \\
C \rightarrow B &: \{N_B + 1\}_{K_{AB}}
\end{aligned}
$$

Poprawka – wartości jedorazowe

$$A \longrightarrow B \quad : \quad A$$
$$B \longrightarrow A \quad : \quad \{A, N'_B\}_{K_{BS}}$$

Poprawka – wartości jedorazowe

$$
\begin{aligned}
A \longrightarrow B &: A \\
B \longrightarrow A &: \{A, N'_B\}_{K_{BS}} \\
A \longrightarrow S &: A, B, N_A, \{A, N'_B\}_{K_{BS}} \\
S \longrightarrow A &: \{N_A, K_A B, B, \{K_{AB}, A, N'_B\}_{K_{BS}}\}_{K_{AS}}
\end{aligned}
$$

Poprawka – wartości jedorazowe

$$
\begin{aligned}
A \rightarrow B &: A \\
B \rightarrow A &: \{A, N'_B\}_{K_{BS}} \\
A \rightarrow S &: A, B, N_A, \{A, N'_B\}_{K_{BS}} \\
S \rightarrow A &: \{N_A, K_A B, B, \{K_{AB}, A, N'_B\}_{K_{BS}}\}_{K_{AS}} \\
A \rightarrow B &: \{K_{AB}, A, N'_B\}_{K_{BS}} \\
B \rightarrow A &: \{N_B\}_{K_{AB}} \\
A \rightarrow B &: \{N_B + 1\}_{K_{AB}}
\end{aligned}
$$

Poprawka – znaczniki czasu[2]

$$A \rightarrow S \quad : \quad A, B, N_A$$
$$S \rightarrow A \quad : \quad \{N_A, K_A B, B, T, \{K_{AB}, A, T\}_{K_{BS}}\}_{K_{AS}}$$

Poprawka – znaczniki czasu[2]

$$
\begin{aligned}
A \rightarrow S &: A, B, N_A \\
S \rightarrow A &: \{N_A, K_A B, B, T, \{K_{AB}, A, T\}_{K_{BS}}\}_{K_{AS}} \\
A \rightarrow B &: \{K_{AB}, A, T\}_{K_{BS}} \\
B \rightarrow A &: \{N_B\}_{K_{AB}} \\
A \rightarrow B &: \{N_B + 1\}_{K_{AB}}
\end{aligned}
$$

Poprawka – znaczniki czasu[2]

$$
\begin{aligned}
A \rightarrow S &: A, B, N_A \\
S \rightarrow A &: \{N_A, K_A B, B, T, \{K_{AB}, A, T\}_{K_{BS}}\}_{K_{AS}} \\
A \rightarrow B &: \{K_{AB}, A, T\}_{K_{BS}} \\
B \rightarrow A &: \{N_B\}_{K_{AB}} \\
A \rightarrow B &: \{N_B + 1\}_{K_{AB}}
\end{aligned}
$$

$$|czas - T| < \Delta t_1 + \Delta t_2,$$

gdzie *czas* – lokalny czas, Δt_1 – oczekiwana różnica w zegarach, Δt_2 – oczekiwane opóźnienie sieciowe.

Wykorzystanie NSSK

Kerberos jest używanym w praktyce protokołem do uwierzytelniania. Zbudowany został na bazie protokołu NSSK z poprawkami Denning i Saco [4].

Plan

Interpretacja BHK[6]

- Formuły logiki intuicjonistycznej możemy interpretować jako konstrukcje.
- Pochodzi od nazwisk: Brouwer–Heyting–Kołmogorow.

Interpretacja BHK

- Podstawowe spójniki logiczne: koniunkcja, alternatywa, implikacja.
- Żaden z podstawowych spójników nie wyraża się przy pomocy pozostałych.
- Jedna stała $\bot$ oznaczająca fałsz.
- Negacja $\neg\phi$ jest skrótem od $\phi \rightarrow \bot$

Interpretacja BHK

Niech PV oznacza nieskończony zbiór zmiennych zdaniowych.

Definicja

Zbiór Φ formuł to najmniejszy zbiór taki, że:

- $\bot \in \Phi$,
- $p \in \Phi$ dla $p \in PV$,
- $\phi \rightarrow \psi$, $\phi \vee \psi$, $\phi \wedge \psi$ dla $\phi, \psi \in \Phi$.

Interpretacja BHK

Konstrukcje

- Konstrukcja $\phi_1 \wedge \phi_2$ składa się z konstrukcji ϕ_1 oraz konstrukcji ϕ_2.

Interpretacja BHK

Konstrukcje

- Konstrukcja $\phi_1 \wedge \phi_2$ składa się z konstrukcji ϕ_1 oraz konstrukcji ϕ_2.
- Konstrukcja $\phi_1 \vee \phi_2$ składa się ze wskaźnika $i \in \{1, 2\}$ oraz konstrukcji ϕ_i.

Interpretacja BHK

Konstrukcje

- Konstrukcja $\phi_1 \wedge \phi_2$ składa się z konstrukcji ϕ_1 oraz konstrukcji ϕ_2.
- Konstrukcja $\phi_1 \vee \phi_2$ składa się ze wskaźnika $i \in \{1, 2\}$ oraz konstrukcji ϕ_i.
- Konstrukcja $\phi_1 \longrightarrow \phi_2$ to metoda na przekształcenie konstrukcji ϕ_1 w konstrukcję ϕ_2.

Interpretacja BHK

Konstrukcje

- Konstrukcja $\phi_1 \wedge \phi_2$ składa się z konstrukcji ϕ_1 oraz konstrukcji ϕ_2.
- Konstrukcja $\phi_1 \vee \phi_2$ składa się ze wskaźnika $i \in \{1, 2\}$ oraz konstrukcji ϕ_i.
- Konstrukcja $\phi_1 \longrightarrow \phi_2$ to metoda na przekształcenie konstrukcji ϕ_1 w konstrukcję ϕ_2.
- Konstrukcja $\bot$ nie istnieje.

Konstrukcja negacji

Konstrukcja $\neg\phi$ to metoda na przekształcenie konstrukcji ϕ w nieistniejący obiekt.

Przykład(y)

- $p \longrightarrow q \longrightarrow p$

Przykład(y)

- $p \longrightarrow q \longrightarrow p$
- $(p \longrightarrow q \longrightarrow r) \longrightarrow (p \longrightarrow q) \longrightarrow p \longrightarrow r$

Przykład(y)

- $p \longrightarrow q \longrightarrow p$
- $(p \longrightarrow q \longrightarrow r) \longrightarrow (p \longrightarrow q) \longrightarrow p \longrightarrow r$
- $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$

Plan

Dedukcja naturalna

- System dowodzenia dla intuicjonistycznej logiki zdaniowej
- Operujemy na osądach $\Gamma \vdash \phi$, gdzie Γ to skończony zbiór formuł, a ϕ to formuła.
- Dowód $\Gamma \vdash \phi$ w dedukcji naturalnej to drzewo, w którym korzeń to $\Gamma \vdash \phi$, liście to aksjomaty, a krawędzie odpowiadają regułom dedukcji.

Dedukcja naturalna

$$(\rightarrow\text{-intro})\ \frac{\Delta, \varphi \vdash \psi}{\Delta \vdash \varphi \rightarrow \psi} \qquad (\rightarrow\text{-elim})\ \frac{\Delta \vdash \varphi \rightarrow \psi \qquad \Delta \vdash \varphi}{\Delta \vdash \psi}$$

$$(\wedge\text{-intro})\ \frac{\Delta \vdash \varphi \qquad \Delta \vdash \psi}{\Delta \vdash \varphi \wedge \psi} \qquad (\wedge\text{-elim})\ \frac{\Delta \vdash \varphi \wedge \psi}{\Delta \vdash \varphi} \qquad (\wedge\text{-elim})\ \frac{\Delta \vdash \varphi \wedge \psi}{\Delta \vdash \psi}$$

$$(\vee\text{-intro})\ \frac{\Delta \vdash \varphi}{\Delta \vdash \varphi \vee \psi} \qquad (\vee\text{-intro})\ \frac{\Delta \vdash \psi}{\Delta \vdash \varphi \vee \psi}$$

$$(\vee\text{-elim})\ \frac{\Delta \vdash \varphi \vee \psi \qquad \Delta, \varphi \vdash \vartheta \qquad \Delta, \psi \vdash \vartheta}{\Delta \vdash \vartheta}$$

Modele Kripkego

Do pokazania semantyki Kripkego dla logiki intuicjonistycznej potrzebna jest definicja modelu Kripkego.

Definicja

Model Kripkego to trójka $M = \langle W, \leq, \Vdash \rangle$, gdzie W jest niepustym zbiorem, $\leq$ jest częściowym porządkiem na W, a $\Vdash$ jest relacją między elementami W a elementami PV spełniającą warunek:

$$\text{Jeśli } w \leq w' \text{ i } w \Vdash p, \text{ to } w' \Vdash p.$$

Sematyka Kripkego

Znaczenie formuł dla modelu Kripkego

- $c \Vdash \phi \vee \psi$ wtw $c \Vdash \phi$ lub $c \Vdash \psi$,

Sematyka Kripkego

Znaczenie formuł dla modelu Kripkego

- $c \Vdash \phi \vee \psi$ wtw $c \Vdash \phi$ lub $c \Vdash \psi$,
- $c \Vdash \phi \wedge \psi$ wtw $c \Vdash \phi$ i $c \Vdash \psi$,

Sematyka Kripkego

Znaczenie formuł dla modelu Kripkego

- $c \Vdash \phi \vee \psi$ wtw $c \Vdash \phi$ lub $c \Vdash \psi$,
- $c \Vdash \phi \wedge \psi$ wtw $c \Vdash \phi$ i $c \Vdash \psi$,
- $c \Vdash \phi \rightarrow \psi$ wtw

Sematyka Kripkego

Znaczenie formuł dla modelu Kripkego

- $c \Vdash \phi \vee \psi$ wtw $c \Vdash \phi$ lub $c \Vdash \psi$,
- $c \Vdash \phi \wedge \psi$ wtw $c \Vdash \phi$ i $c \Vdash \psi$,
- $c \Vdash \phi \rightarrow \psi$ wtw $c' \Vdash \psi$ dla każdego $c' \geq c$ takiego, że $c' \Vdash \phi$,

Sematyka Kripkego

Znaczenie formuł dla modelu Kripkego

- $c \Vdash \phi \vee \psi$ wtw $c \Vdash \phi$ lub $c \Vdash \psi$,
- $c \Vdash \phi \wedge \psi$ wtw $c \Vdash \phi$ i $c \Vdash \psi$,
- $c \Vdash \phi \rightarrow \psi$ wtw $c' \Vdash \psi$ dla każdego $c' \geq c$ takiego, że $c' \Vdash \phi$,
- $c \Vdash \bot$ nigdy nie zachodzi.

Sematyka Kripkego

Znaczenie formuł dla modelu Kripkego

- $c \Vdash \phi \vee \psi$ wtw $c \Vdash \phi$ lub $c \Vdash \psi$,
- $c \Vdash \phi \wedge \psi$ wtw $c \Vdash \phi$ i $c \Vdash \psi$,
- $c \Vdash \phi \rightarrow \psi$ wtw $c' \Vdash \psi$ dla każdego $c' \geq c$ takiego, że $c' \Vdash \phi$,
- $c \Vdash \bot$ nigdy nie zachodzi.

Znaczenie negacji

$c \Vdash \neg\phi$ wtw dla żadnego $c' \geq c$ nie zachodzi $c' \Vdash \phi$.

Wielorodzajowa logika predykatów

Definicja[5]

Wielorodzajowa sygnatura składa się z krotki $\langle S, \Sigma^f, \Sigma^r, ar^f, ar^r \rangle$, gdzie:

- S to zbiór nazw rodzajów,
- Σ^f to zbiór symboli funkcyjnych,
- Σ^r to zbiór symboli relacyjnych,
- $ar^f : \Sigma^f \longrightarrow S^* \times S$,
- $ar^r : \Sigma^r \longrightarrow S^*$.

Wielorodzajowa logika predykatów

Przykład

$$
\begin{aligned}
S &= \{Int, List\} \\
\Sigma^r &= \{head, tail\} \\
ar^r(head) &= \langle List, Int \rangle \\
ar^r(tail) &= \langle List, List \rangle
\end{aligned}
$$

Semantyka Kripkego dla logiki predykatów

Definicja

Model Kripkego dla logiki predykatów to trójka $M = \langle W, \leq, \{\mathcal{A}_w | w \in W\}\rangle$, gdzie W jest niepustym zbiorem, $\leq$ jest częściowym porządkiem na W, a $\mathcal{A}_w$ są klasycznymi strukturami pierwszego rzędu między spełniającymi warunek:

$$\text{Jeśli } w \leq w', \text{ to } \mathcal{A}_w \subseteq \mathcal{A}_{w'}.$$

Semantyka Kripkego dla logiki predykatów

Definicja

Mając formułę ϕ i wartościowanie ρ w $\mathcal{A}_w$. Definiuję relację $w, \rho \Vdash \phi$ indukcyjnie:

- $w, \rho \Vdash \exists_a \phi(a)$, jeśli $w, \rho[a \mapsto \mathbf{a}] \Vdash \phi$, dla pewnego $\mathbf{a} \in \mathcal{A}_w$,

Semantyka Kripkego dla logiki predykatów

Definicja

Mając formułę ϕ i wartościowanie ρ w $\mathcal{A}_w$. Definiuję relację $w, \rho \Vdash \phi$ indukcyjnie:

- $w, \rho \Vdash \exists_a \phi(a)$, jeśli $w, \rho[a \mapsto \mathbf{a}] \Vdash \phi$, dla pewnego $\mathbf{a} \in \mathcal{A}_w$,
- $w, \rho \Vdash \forall_a \phi(a)$, jeśli $w', \rho[a \mapsto \mathbf{a}] \Vdash \phi$, dla każdego $w \leq w'$ i $\mathbf{a} \in \mathcal{A}_{w'}$,
- dla pozostałych przypadków analogicznie jak w logice zdaniowej.

Semantyka Kripkego dla logiki predykatów

Definicja

Mając formułę ϕ i wartościowanie ρ w $\mathcal{A}_w$. Definiuję relację $w, \rho \Vdash \phi$ indukcyjnie:

- $w, \rho \Vdash \exists_a \phi(a)$, jeśli $w, \rho[a \mapsto \mathbf{a}] \Vdash \phi$, dla pewnego $\mathbf{a} \in \mathcal{A}_w$,
- $w, \rho \Vdash \forall_a \phi(a)$, jeśli $w', \rho[a \mapsto \mathbf{a}] \Vdash \phi$, dla każdego $w \leq w'$ i $\mathbf{a} \in \mathcal{A}_{w'}$,
- dla pozostałych przypadków analogicznie jak w logice zdaniowej.

$\Gamma \Vdash \phi$ oznacza, że dla każdego modelu $\mathcal{W}$ i każdego $w \in \mathcal{W}$ warunek $w, \rho \Vdash \Gamma$ implikuje $w, \rho \Vdash \phi$.

Przykłady

- $\forall_a \phi \rightarrow \exists_a \phi$
- $\forall_a (\phi \rightarrow \psi) \rightarrow (\forall_a \phi \rightarrow \forall_a \psi)$

Plan

Formalizacja

- Rodzaje
- Relacje
- Definicje
- Aksjomaty
- Własności

Rodzaje

- *Actor*
- *Session*
- *Message*
- *Key*
- *Content*
- *Nonce*

Relacje

Właściwości wiadomości

$$\begin{aligned} in\_session &: Message \times Session \\ sender &: Message \times Actor \\ recipient &: Message \times Actor \end{aligned}$$

Relacje

Właściwości wiadomości

$$
\begin{aligned}
content &: Message \times Content \\
content_c &: Content \times Content \\
content_k &: Content \times Key \\
content_a &: Content \times Actor \\
content_b &: Content \times Actor \\
content_n &: Content \times Nonce \\
encrypted &: Content \\
encrypted_k &: Content \times Key
\end{aligned}
$$

Relacje

Wiedza

$$known_m : Actor \times Message$$
$$known_a : Actor \times Actor$$
$$known_c : Actor \times Content$$
$$known_k : Actor \times Key$$
$$known_n : Actor \times Nonce$$

Relacje

Pozostałe

$$\begin{aligned} reverse\_key &: Key \times Key \\ successor &: Nonce \times Nonce \end{aligned}$$

Definicje

→ `NSSK_definitions.v`

Modele Kripkego w formalizacji

- Aby pokazać że formuła jest prawdziwa, musi zachodzić we wszystkich modelach w których zachodzą aksjomaty
- Łatwiej używać modeli Kripkego do budowania kontrprzykładów
- Uniwersalny model?

Literatura I


Dorothy E. Denning and Giovanni Maria Sacco.
Timestamps in key distribution protocols.
Commun. ACM, 24(8):533–536, August 1981.


R M Needham and M D Schroeder.
Authentication revisited.
SIGOPS Oper. Syst. Rev., 21(1):7–7, January 1987.


Roger M. Needham and Michael D. Schroeder.
Using encryption for authentication in large networks of computers.
Commun. ACM, 21(12):993–999, December 1978.

Literatura II


C. Neuman, T. Yu, S. Hartman, and K. Raeburn.
The Kerberos Network Authentication Service (V5).
RFC 4120 (Proposed Standard), July 2005.
Updated by RFCs 4537, 5021, 5896, 6111, 6112, 6113, 6649.


D. Sanella and A. Tarlecki.
Foundations of Algebraic Specification and Formal Software Development.
Springer, 2010.


M. H. Sørensen and P. Urzyczyn.
Lectures on the Curry-Howard isomorphism.
Elsevier, 2006.