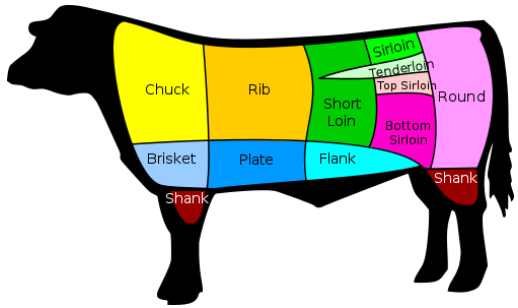
Logika BAN

Piotr Iwaniuk

21 grudnia 2011

Plan



Plan

Przeznaczenie protokołu

Przeznaczenie protokołu

- Prawdopodobnie najprostszy protokół oparty na serwerze uwierzytelniania i kluczu współdzielonym.

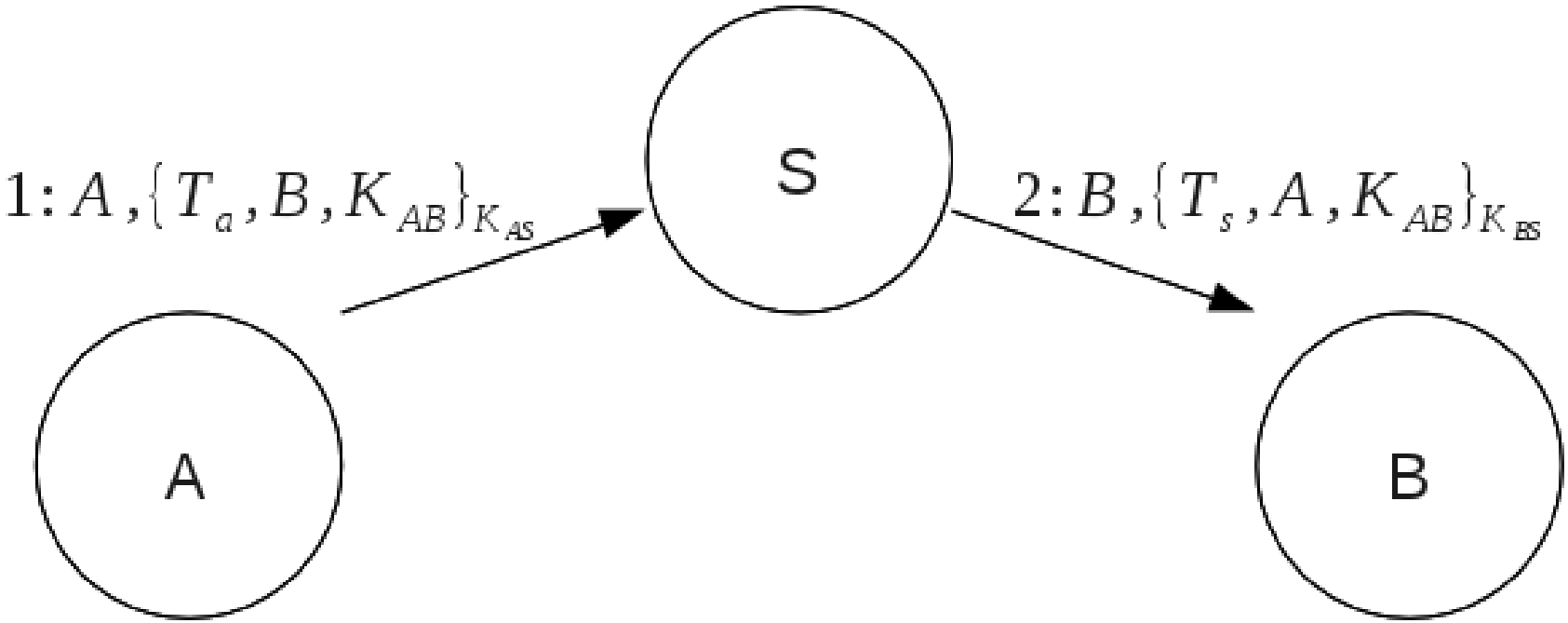
Przeznaczenie protokołu

- Prawdopodobnie najprostszy protokół oparty na serwerze uwierzytelniania i kluczu współdzielonym.
- Opracowany przez Michaela Burrowsa.

Przeznaczenie protokołu

- Prawdopodobnie najprostszy protokół oparty na serwerze uwierzytelniania i kluczu współdzielonym.
- Opracowany przez Michaela Burrowsa.
- 2 komunikaty.

Schemat komunikacji



Rysunek: Schemat protokołu Wide-mouthed-frog

Idealizacja protokołu

Protokół

$$A \rightarrow S \quad : \quad A, \{T_a, B, K_{AB}\}_{K_{AS}}$$
$$S \rightarrow B \quad : \quad B, \{T_s, A, K_{AB}\}_{K_{BS}}$$

Idealizacja protokołu

Protokół

$$\begin{aligned} A \rightarrow S &: A, \{T_a, B, K_{AB}\}_{K_{AS}} \\ S \rightarrow B &: B, \{T_s, A, K_{AB}\}_{K_{BS}} \end{aligned}$$

Protokół wyidealizowany

$$\begin{aligned} A \rightarrow S &: \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}} \\ S \rightarrow B &: \{T_s, A \,\textbf{believes}\, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{BS}} \end{aligned}$$

Założenia

Założenia o A

A **believes** $A \overset{K_{AS}}{\leftrightarrow} S$
S **believes** $A \overset{K_{AS}}{\leftrightarrow} S$
A **believes** $A \overset{K_{AB}}{\leftrightarrow} B$
S **believes fresh**(T_a)

Założenia o B

B **believes** $B \overset{K_{BS}}{\leftrightarrow} S$
S **believes** $B \overset{K_{BS}}{\leftrightarrow} S$
B **believes** A **controls** $A \overset{K}{\leftrightarrow} B$
B **believes** S **controls** A **believes** $A \overset{K}{\leftrightarrow} B$
S **believes fresh**(T_s)

Adnotacje dla pierwszego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

Adnotacje dla pierwszego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

$\{Z\}$

Adnotacje dla pierwszego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

$\{Z\}$

$A \rightarrow S : \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}$

Adnotacje dla pierwszego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

$\{Z\}$

$A \rightarrow S : \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}$

$\{Z, S \textbf{ sees } \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}\}$

Wnioskowanie

Wnioskowanie

$$\frac{S \textbf{ believes fresh}(T_a)}{S \textbf{ believes fresh}(\{T_a, A \overset{K_{AB}}{\leftrightarrow} B\})}$$

Wnioskowanie

$$\frac{S \text{ believes fresh}(T_a)}{S \text{ believes fresh}(\{T_a, A \overset{K_{AB}}{\leftrightarrow} B\})}$$

$$\frac{S \text{ believes } A \overset{K_{AS}}{\leftrightarrow} S, \quad S \text{ sees } \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}}{S \text{ believes } A \text{ said } \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}}$$

Wnioskowanie

$$\frac{S \text{ believes fresh}(T_a)}{S \text{ believes fresh}(\{T_a, A \overset{K_{AB}}{\leftrightarrow} B\})}$$

$$\frac{S \text{ believes } A \overset{K_{AS}}{\leftrightarrow} S, \quad S \text{ sees } \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}}{S \text{ believes } A \text{ said } \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}}$$

$$\frac{S \text{ believes fresh}(\{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}), \quad S \text{ believes } A \text{ said } \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}}{S \text{ believes } A \text{ believes } \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}}$$

Adnotacje dla drugiego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

$\{Z\}$

$A \rightarrow S : \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}$

$Z' := \{Z, S \textbf{ sees } \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}, S \textbf{ believes } A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}$

Adnotacje dla drugiego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

$\{Z\}$

$A \rightarrow S : \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}$

$Z' := \{Z, S \textbf{ sees } \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}, S \textbf{ believes } A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}$

$S \rightarrow B : \{T_s, A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{BS}}$

Adnotacje dla drugiego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

$\{Z\}$

$A \rightarrow S : \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}$

$Z' := \{Z, S \textbf{ sees } \{T_a, A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{AS}}, S \textbf{ believes } A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}$

$S \rightarrow B : \{T_s, A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{BS}}$

$\{Z', B \textbf{ sees } \{T_s, A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{BS}}\}$

Wnioskowanie

Wnioskowanie

$$\frac{B \textbf{ believes } B \overset{K_{BS}}{\leftrightarrow} S, \qquad B \textbf{ sees } \{T_s, A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{BS}}}{B \textbf{ believes } S \textbf{ said } \{T_s, A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}}$$

Wnioskowanie

$$\frac{B \text{ believes } B \overset{K_{BS}}{\leftrightarrow} S, \qquad B \text{ sees } \{T_s, A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{BS}}}{B \text{ believes } S \text{ said } \{T_s, A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}}$$

$$\frac{S \text{ believes fresh}(T_s)}{S \text{ believes fresh}(\{T_s, A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B\})}$$

Wnioskowanie

$$\frac{B \text{ believes } B \overset{K_{BS}}{\leftrightarrow} S, \qquad B \text{ sees } \{T_s, A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}_{K_{BS}}}{B \text{ believes } S \text{ said } \{T_s, A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}}$$

$$\frac{S \text{ believes fresh}(T_s)}{S \text{ believes fresh}(\{T_s, A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B\})}$$

$$\frac{\begin{array}{c} S \text{ believes fresh}(\{T_s, A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}), \\ B \text{ believes } S \text{ said } \{T_s, A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B\} \end{array}}{B \text{ believes } S \text{ believes } \{T_s, A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B\}}$$

Wnioskowanie

Wnioskowanie

$$\frac{B \textbf{ believes } S \textbf{ controls } A \textbf{ believes } A \overset{K}{\leftrightarrow} B, \quad B \textbf{ believes } S \textbf{ believes } A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B}{B \textbf{ believes } A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B}$$

Wnioskowanie

$$\frac{B \text{ believes } S \text{ controls } A \text{ believes } A \overset{K}{\leftrightarrow} B, \quad B \text{ believes } S \text{ believes } A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B}{B \text{ believes } A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B}$$

$$\frac{B \text{ believes } A \text{ controls } A \overset{K}{\leftrightarrow} B, \quad B \text{ believes } A \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B}{B \text{ believes } A \overset{K_{AB}}{\leftrightarrow} B}$$

Udowodnione formuły

Udało się pokazać 2 formuły:

$$S \textbf{ believes } A \textbf{ believes } A \overset{K_{AB}}{\longleftrightarrow} B$$
$$B \textbf{ believes } A \overset{K_{AB}}{\longleftrightarrow} B$$

Udowodnione formuły

Udało się pokazać 2 formuły:

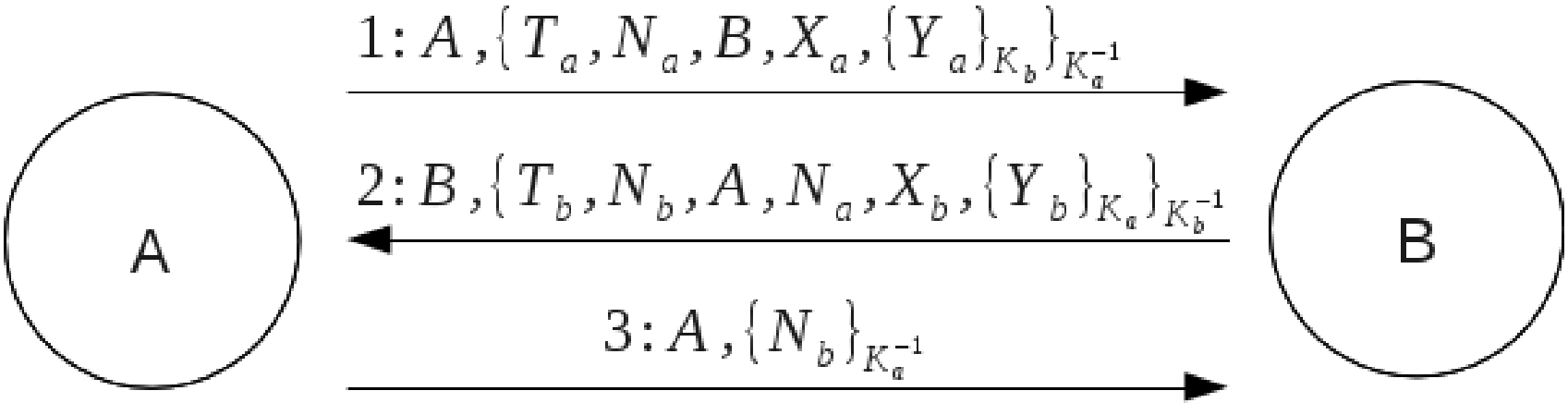
$$S \textbf{ believes } A \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B$$
$$B \textbf{ believes } A \overset{K_{AB}}{\leftrightarrow} B$$

Protokół działa poprawnie i jest minimalny. Korzysta jednak z silnych założeń, które są trudne do spełnienia.

Przeznaczenie protokołu

- Protokół bezpieczniej wymiany danych między dwoma stronami.
- Podany w rekomendacji X.509

Schemat komunikacji



Rysunek: Schemat protokołu X.509

Idealizacja protokołu

Protokół

$$
\begin{aligned}
A \rightarrow B &: A, \{T_a, N_a, B, X_a, \{Y_a\}_{K_b}\}_{K_a^{-1}} \\
B \rightarrow A &: B, \{T_b, N_b, A, N_a, X_b, \{Y_b\}_{K_a}\}_{K_b^{-1}} \\
A \rightarrow B &: A, \{N_b\}_{K_a^{-1}}
\end{aligned}
$$

Idealizacja protokołu

Protokół

$$
\begin{aligned}
A \rightarrow B &: A, \{T_a, N_a, B, X_a, \{Y_a\}_{K_b}\}_{K_a^{-1}} \\
B \rightarrow A &: B, \{T_b, N_b, A, N_a, X_b, \{Y_b\}_{K_a}\}_{K_b^{-1}} \\
A \rightarrow B &: A, \{N_b\}_{K_a^{-1}}
\end{aligned}
$$

Protokół wyidealizowany

$$
\begin{aligned}
A \rightarrow B &: \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}_{K_a^{-1}} \\
B \rightarrow A &: \{T_b, N_b, N_a, X_b, \{Y_b\}_{K_a}\}_{K_b^{-1}} \\
A \rightarrow B &: \{N_b\}_{K_a^{-1}}
\end{aligned}
$$

Założenia

Założenia o A

A believes $\overset{K_a}{\mapsto} A$
A believes $\overset{K_b}{\mapsto} B$
A believes fresh(N_a)
A believes fresh(T_b)

Założenia o B

B believes $\overset{K_a}{\mapsto} A$
B believes $\overset{K_b}{\mapsto} B$
B believes fresh(N_b)
B believes fresh(T_a)

Cele

Cele

- Zapewnić, że X_a i X_b zostały nadane odpowiednio przez A i B.

Cele

- Zapewnić, że X_a i X_b zostały nadane odpowiednio przez A i B.
- Zapewnić, że Y_a i Y_b zostaną otrzymane odpowiednio tylko przez B i A.

Adnotacje dla pierwszego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

Adnotacje dla pierwszego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

$\{Z\}$

Adnotacje dla pierwszego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

$\{Z\}$
$A \rightarrow B : \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}_{K_a^{-1}}$

Adnotacje dla pierwszego komunikatu

Niech Z oznacza wszystkie początkowe założenia.

$\{Z\}$
$A \rightarrow B : \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}_{K_a^{-1}}$
$\{Z, B \textbf{ sees } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}_{K_a^{-1}}\}$

Wnioskowanie

Wnioskowanie

$$\frac{B \textbf{ believes } \overset{K_a}{\mapsto} A, \qquad B \textbf{ sees } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}_{K_a^{-1}}}{B \textbf{ believes } A \textbf{ said } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}}$$

Wnioskowanie

$$\frac{B \textbf{ believes } \overset{K_a}{\mapsto} A, \qquad B \textbf{ sees } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}_{K_a^{-1}}}{B \textbf{ believes } A \textbf{ said } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}}$$

$$\frac{B \textbf{ believes } A \textbf{ said } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}}{B \textbf{ believes } A \textbf{ said } \{T_a, X_a\}}$$

Wnioskowanie

$$\frac{B \textbf{ believes } \overset{K_a}{\mapsto} A, \qquad B \textbf{ sees } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}_{K_a^{-1}}}{B \textbf{ believes } A \textbf{ said } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}}$$

$$\frac{B \textbf{ believes } A \textbf{ said } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}}{B \textbf{ believes } A \textbf{ said } \{T_a, X_a\}}$$

$$\frac{B \textbf{ believes fresh}(T_a)}{B \textbf{ believes fresh}(\{T_a, X_a\})}$$

Wnioskowanie

$$\frac{B \textbf{ believes } \overset{K_a}{\mapsto} A, \qquad B \textbf{ sees } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}_{K_a^{-1}}}{B \textbf{ believes } A \textbf{ said } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}}$$

$$\frac{B \textbf{ believes } A \textbf{ said } \{T_a, N_a, X_a, \{Y_a\}_{K_b}\}}{B \textbf{ believes } A \textbf{ said } \{T_a, X_a\}}$$

$$\frac{B \textbf{ believes fresh}(T_a)}{B \textbf{ believes fresh}(\{T_a, X_a\})}$$

$$\frac{B \textbf{ believes fresh}(\{T_a, X_a\}), \qquad B \textbf{ believes } A \textbf{ said } \{T_a, X_a\}}{B \textbf{ believes } A \textbf{ believes } \{T_a, X_a\}}$$

Udowodnione formuły

W podobny sposób można przeprowadzić wnioskowanie dla drugiego komunikatu.

Udowodnione formuły

W podobny sposób można przeprowadzić wnioskowanie dla drugiego komunikatu.

Uzyskaliśmy zatem pierwszy cel:

$$B \textbf{ believes } A \textbf{ believes } X_a$$
$$A \textbf{ believes } B \textbf{ believes } X_b$$

Podatność na atak

Nie możemy wywnioskować podobnych stwierdzeń o Y_a i Y_b.
Mamy tylko:

$$B \text{ sees } Y_a$$

$$A \text{ sees } Y_b$$

Podatność na atak

Nie możemy wywnioskować podobnych stwierdzeń o Y_a i Y_b.
Mamy tylko:

$$B \text{ sees } Y_a$$
$$A \text{ sees } Y_b$$

Oznacza to, że wysyłający nie musi być pewien przesyłanej zaszyfrowanej treści.

Niepotrzebne elementy

Analiza pokazuje też, że element T_b nie jest potrzebny do zweryfikowania aktualności drugiego komunikatu. Można go było usunąć z protokołu.

Niepotrzebne elementy

Analiza pokazuje też, że element T_b nie jest potrzebny do zweryfikowania aktualności drugiego komunikatu. Można go było usunąć z protokołu.

Rekomendacja X.509 mówi za to, że nie trzeba sprawdzać aktualności elementu T_a. Jest to błędem, ponieważ z perspektywy B jest to jedyny element potwierdzający aktualność pierwszego komunikatu.

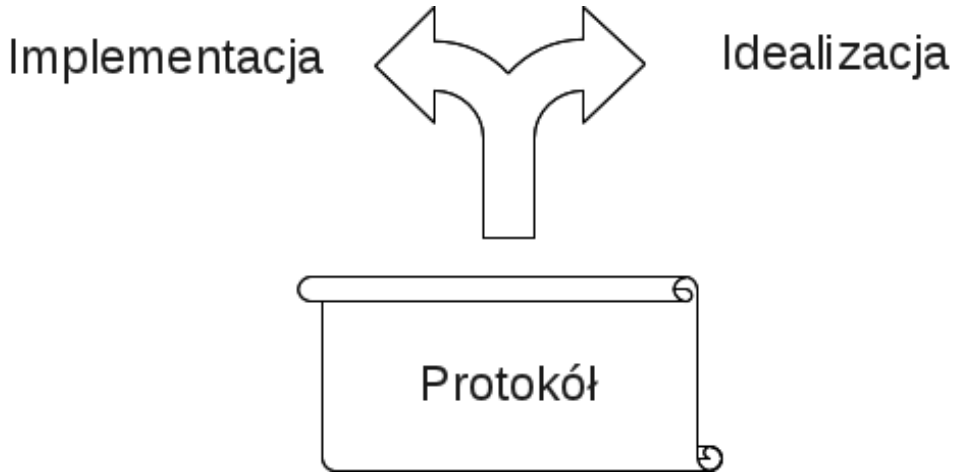
Plan

Semantyka

- Semantyka konstruktów nie jest jasno określona.
- Niejasne zachowanie krotek pod konstruktami.

Idealizacja

- Proces idealizacji protokołu nie jest jednoznaczny.
- Być może odrzucanie niezaszyfrowanych danych ma znaczenie.



Model intruza

- Logika zakłada, że nadawca i odbiorca wiadomości nie mogą zostać podmienieni.
- Przez to nie wykrywa luki w asymetrycznym protokole Needhama-Schroedera.

Asymetryczny protokół Needhama-Schroedera

Asymetryczny protokół N-S

Zapis protokołu:

$$
\begin{aligned}
A \rightarrow S &: A, B \\
S \rightarrow A &: \{K_{PB}, B\}_{K_{SS}} \\
A \rightarrow B &: \{N_A, A\}_{K_{PB}} \\
B \rightarrow S &: B, A \\
S \rightarrow B &: \{K_{PA}, B\}_{K_{SS}} \\
B \rightarrow A &: \{N_A, N_B\}_{K_{PA}} \\
A \rightarrow B &: \{N_B\}_{K_{PB}}
\end{aligned}
$$

Asymetryczny protokół Needhama-Schroedera

Asymetryczny protokół N-S

Zapis protokołu:

$$
\begin{aligned}
A \rightarrow S &: A, B \\
S \rightarrow A &: \{K_{PB}, B\}_{K_{SS}} \\
A \rightarrow B &: \{N_A, A\}_{K_{PB}} \\
B \rightarrow S &: B, A \\
S \rightarrow B &: \{K_{PA}, B\}_{K_{SS}} \\
B \rightarrow A &: \{N_A, N_B\}_{K_{PA}} \\
A \rightarrow B &: \{N_B\}_{K_{PB}}
\end{aligned}
$$

Protokół zaproponowany w 1978 roku.

Luka w protokole

Luka w protokole

- Znaleziona w 1995 przez Gavina Lowe.

Luka w protokole

- Znaleziona w 1995 przez Gavina Lowe.
- Model Doleva-Yao: 1983.

Luka w protokole

- Znaleziona w 1995 przez Gavina Lowe.
- Model Doleva-Yao: 1983.
- Logika BAN: 1989.

Luka w protokole

- Znaleziona w 1995 przez Gavina Lowe.
- Model Doleva-Yao: 1983.
- Logika BAN: 1989.
- Opis protokołu był konwertowany do CSP przy pomocy kompilatora Casper.

Luka w protokole

- Znaleziona w 1995 przez Gavina Lowe.
- Model Doleva-Yao: 1983.
- Logika BAN: 1989.
- Opis protokołu był konwertowany do CSP przy pomocy kompilatora Casper.
- Następnie model w CSP był weryfikowany przy pomocy model checkera FDR.

Poprawiony protokół

Protokół Needhama-Schroedera-Lowe'a

Zapis protokołu:

$$
\begin{aligned}
A \rightarrow S &: A, B \\
S \rightarrow A &: \{K_{PB}, B\}_{K_{SS}} \\
A \rightarrow B &: \{N_A, A\}_{K_{PB}} \\
B \rightarrow S &: B, A \\
S \rightarrow B &: \{K_{PA}, B\}_{K_{SS}} \\
B \rightarrow A &: \{N_A, N_B, B\}_{K_{PA}} \\
A \rightarrow B &: \{N_B\}_{K_{PB}}
\end{aligned}
$$

Literatura


Michael Burrows, Martín Abadi, and Roger Needham.
A logic of authentication.
Technical report, Digital Equipment Corporation, Systems Research Centre, 1989.


Martijn Warnier.
The rise and fall of BAN logic, 2004.