Protocol Verification Techniques - State Enumeration

Design and Verification of Security Protocols and Security Ceremonies

Programa de Pós-Graduacão em Ciências da Computacão
Dr. Jean Everson Martina

March-June 2019

Programa de Pós-Graduação em Ciência da Computação
UFSC

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

Before we start!

Before we start!

To be able to talk about Lowe's attack using FDR and CSP, we need first to get the grips with the theory behind communicating sequential processes (CSP).

Communicating Sequential Processes

- Communicating Sequential Processes (CSP) is a formal language for describing patterns of interaction in concurrent systems;

Communicating Sequential Processes

- Communicating Sequential Processes (CSP) is a formal language for describing patterns of interaction in concurrent systems;
- It is a member of the family of mathematical theories of concurrency known as process algebras;

Communicating Sequential Processes

- Communicating Sequential Processes (CSP) is a formal language for describing patterns of interaction in concurrent systems;
- It is a member of the family of mathematical theories of concurrency known as process algebras;
- CSP was first described in a 1978 paper by Tony Hoare;

Communicating Sequential Processes

- Communicating Sequential Processes (CSP) is a formal language for describing patterns of interaction in concurrent systems;
- It is a member of the family of mathematical theories of concurrency known as process algebras;
- CSP was first described in a 1978 paper by Tony Hoare;
- CSP has been practically applied in industry as a tool for specifying and verifying the concurrent aspects of a variety of different systems.

Communicating Sequential Processes

- The theory of CSP itself is still the subject of active research, including work to increase its range of practical applicability;

Communicating Sequential Processes

- The theory of CSP itself is still the subject of active research, including work to increase its range of practical applicability;
- CSP allows the description of systems in terms of component processes that operate independently, and interact with each other solely through message-passing communication;

Communicating Sequential Processes

- The theory of CSP itself is still the subject of active research, including work to increase its range of practical applicability;
- CSP allows the description of systems in terms of component processes that operate independently, and interact with each other solely through message-passing communication;
- The relationships between different processes, and the way each process communicates with its environment, are described using various process algebraic operators;

Communicating Sequential Processes

- The theory of CSP itself is still the subject of active research, including work to increase its range of practical applicability;
- CSP allows the description of systems in terms of component processes that operate independently, and interact with each other solely through message-passing communication;
- The relationships between different processes, and the way each process communicates with its environment, are described using various process algebraic operators;
- Using this algebraic approach, quite complex process descriptions can be easily constructed from a few primitive elements.

CSP Primitives

- CSP provides two classes of primitives in its process algebra:

CSP Primitives

- CSP provides two classes of primitives in its process algebra:
- Events:

CSP Primitives

- CSP provides two classes of primitives in its process algebra:
- Events:
  - Events represent communications or interactions;

CSP Primitives

- CSP provides two classes of primitives in its process algebra:
- Events:
  - Events represent communications or interactions;
  - Events are assumed to be indivisible and instantaneous;

CSP Primitives

- CSP provides two classes of primitives in its process algebra:
- Events:
  - Events represent communications or interactions;
  - Events are assumed to be indivisible and instantaneous;
  - They may be atomic names, compound names, or input/output events;

CSP Primitives

- CSP provides two classes of primitives in its process algebra:
- Events:
  - Events represent communications or interactions;
  - Events are assumed to be indivisible and instantaneous;
  - They may be atomic names, compound names, or input/output events;
- Primitive processes:

CSP Primitives

- CSP provides two classes of primitives in its process algebra:
- Events:
  - Events represent communications or interactions;
  - Events are assumed to be indivisible and instantaneous;
  - They may be atomic names, compound names, or input/output events;
- Primitive processes:
  - Primitive processes represent fundamental behaviours;

CSP Primitives

- CSP provides two classes of primitives in its process algebra:
- Events:
  - Events represent communications or interactions;
  - Events are assumed to be indivisible and instantaneous;
  - They may be atomic names, compound names, or input/output events;
- Primitive processes:
  - Primitive processes represent fundamental behaviours;
  - STOP (the process that communicates nothing, also called deadlock);

CSP Primitives

- CSP provides two classes of primitives in its process algebra:
- Events:
  - Events represent communications or interactions;
  - Events are assumed to be indivisible and instantaneous;
  - They may be atomic names, compound names, or input/output events;
- Primitive processes:
  - Primitive processes represent fundamental behaviours;
  - STOP (the process that communicates nothing, also called deadlock);
  - SKIP (which represents successful termination).

CSP Algebraic Operators

$$
\begin{array}{lcl}
\mathit{Proc} & ::= & \mathit{STOP} \\
 & | & \mathit{SKIP}
\end{array}
$$

CSP Algebraic Operators

$$
\begin{array}{lcll}
Proc & ::= & STOP & \\
 & | & SKIP & \\
 & | & e \rightarrow Proc & \text{(prefixing)}
\end{array}
$$

CSP Algebraic Operators

$$
\begin{array}{lcll}
Proc & ::= & STOP & \\
 & | & SKIP & \\
 & | & e \rightarrow Proc & \text{(prefixing)} \\
 & | & Proc \mathbin{\Box} Proc & \text{(external choice)}
\end{array}
$$

CSP Algebraic Operators

$$
\begin{array}{rcll}
Proc & ::= & STOP & \\
& | & SKIP & \\
& | & e \rightarrow Proc & \text{(prefixing)} \\
& | & Proc \mathbin{\Box} Proc & \text{(external choice)} \\
& | & Proc \sqcap Proc & \text{(nondeterministic choice)}
\end{array}
$$

CSP Algebraic Operators

$$
\begin{array}{lcll}
\mathit{Proc} & ::= & \mathit{STOP} & \\
 & \mid & \mathit{SKIP} & \\
 & \mid & e \rightarrow \mathit{Proc} & \text{(prefixing)} \\
 & \mid & \mathit{Proc} \mathbin{\Box} \mathit{Proc} & \text{(external choice)} \\
 & \mid & \mathit{Proc} \sqcap \mathit{Proc} & \text{(nondeterministic choice)} \\
 & \mid & \mathit{Proc} \mathbin{|||} \mathit{Proc} & \text{(interleaving)}
\end{array}
$$

CSP Algebraic Operators

$$
\begin{array}{lcll}
Proc & ::= & STOP & \\
 & | & SKIP & \\
 & | & e \rightarrow Proc & \text{(prefixing)} \\
 & | & Proc \,\Box\, Proc & \text{(external choice)} \\
 & | & Proc \sqcap Proc & \text{(nondeterministic choice)} \\
 & | & Proc \,|||\, Proc & \text{(interleaving)} \\
 & | & Proc \,|[\{X\}]|\, Proc & \text{(interface parallel)}
\end{array}
$$

CSP Algebraic Operators

$$
\begin{array}{lcll}
Proc & ::= & STOP & \\
 & \mid & SKIP & \\
 & \mid & e \rightarrow Proc & \text{(prefixing)} \\
 & \mid & Proc \,\Box\, Proc & \text{(external choice)} \\
 & \mid & Proc \;\sqcap\; Proc & \text{(nondeterministic choice)} \\
 & \mid & Proc \,|||\, Proc & \text{(interleaving)} \\
 & \mid & Proc \,|[\{X\}]|\, Proc & \text{(interface parallel)} \\
 & \mid & Proc \setminus X & \text{(hiding)}
\end{array}
$$

CSP Algebraic Operators

$$
\begin{array}{lcll}
Proc & ::= & STOP & \\
 & | & SKIP & \\
 & | & e \rightarrow Proc & \text{(prefixing)} \\
 & | & Proc \,\Box\, Proc & \text{(external choice)} \\
 & | & Proc \,\sqcap\, Proc & \text{(nondeterministic choice)} \\
 & | & Proc \,|||\, Proc & \text{(interleaving)} \\
 & | & Proc \,|[\{X\}]|\, Proc & \text{(interface parallel)} \\
 & | & Proc \setminus X & \text{(hiding)} \\
 & | & Proc; Proc & \text{(sequential composition)}
\end{array}
$$

CSP Algebraic Operators

$$
\begin{array}{lcll}
\mathit{Proc} & ::= & \mathit{STOP} & \\
& | & \mathit{SKIP} & \\
& | & e \rightarrow \mathit{Proc} & \text{(prefixing)} \\
& | & \mathit{Proc} \,\Box\, \mathit{Proc} & \text{(external choice)} \\
& | & \mathit{Proc} \,\sqcap\, \mathit{Proc} & \text{(nondeterministic choice)} \\
& | & \mathit{Proc} \,|||\, \mathit{Proc} & \text{(interleaving)} \\
& | & \mathit{Proc} \,|[\{X\}]|\, \mathit{Proc} & \text{(interface parallel)} \\
& | & \mathit{Proc} \setminus X & \text{(hiding)} \\
& | & \mathit{Proc}; \mathit{Proc} & \text{(sequential composition)} \\
& | & \text{if } b \text{ then } \mathit{Proc} \text{ else } \mathit{Proc} & \text{(boolean conditional)}
\end{array}
$$

CSP Algebraic Operators

$$
\begin{array}{rcll}
\mathit{Proc} & ::= & \mathit{STOP} & \\
& | & \mathit{SKIP} & \\
& | & e \rightarrow \mathit{Proc} & \text{(prefixing)} \\
& | & \mathit{Proc} \,\square\, \mathit{Proc} & \text{(external choice)} \\
& | & \mathit{Proc} \sqcap \mathit{Proc} & \text{(nondeterministic choice)} \\
& | & \mathit{Proc} \,|||\, \mathit{Proc} & \text{(interleaving)} \\
& | & \mathit{Proc} \,|[\{X\}]|\, \mathit{Proc} & \text{(interface parallel)} \\
& | & \mathit{Proc} \setminus X & \text{(hiding)} \\
& | & \mathit{Proc}; \mathit{Proc} & \text{(sequential composition)} \\
& | & \mathrm{if}\ b\ \mathrm{then}\ \mathit{Proc}\ \mathrm{else}\ \mathit{Proc} & \text{(boolean conditional)} \\
& | & \mathit{Proc} \rhd \mathit{Proc} & \text{(timeout)}
\end{array}
$$

CSP Algebraic Operators

$$
\begin{array}{rcll}
Proc & ::= & STOP & \\
& | & SKIP & \\
& | & e \rightarrow Proc & \text{(prefixing)} \\
& | & Proc \,\Box\, Proc & \text{(external choice)} \\
& | & Proc \sqcap Proc & \text{(nondeterministic choice)} \\
& | & Proc \,|||\, Proc & \text{(interleaving)} \\
& | & Proc \,|[\{X\}]|\, Proc & \text{(interface parallel)} \\
& | & Proc \setminus X & \text{(hiding)} \\
& | & Proc ; Proc & \text{(sequential composition)} \\
& | & \text{if } b \text{ then } Proc \text{ else } Proc & \text{(boolean conditional)} \\
& | & Proc \rhd Proc & \text{(timeout)} \\
& | & Proc \bigtriangleup Proc & \text{(interrupt)}
\end{array}
$$

CSP Example - Vending Machine

- One of the archetypal CSP examples is an abstract representation of a chocolate vending machine and its interactions with a person wishing to buy some chocolate;

CSP Example - Vending Machine

- One of the archetypal CSP examples is an abstract representation of a chocolate vending machine and its interactions with a person wishing to buy some chocolate;
- This vending machine might be able to carry out two different events, "coin" and "choc";

CSP Example - Vending Machine

- One of the archetypal CSP examples is an abstract representation of a chocolate vending machine and its interactions with a person wishing to buy some chocolate;
- This vending machine might be able to carry out two different events, “coin” and “choc”;
- They represent the insertion of payment and the delivery of a chocolate respectively.

CSP Example - Vending Machine

- A machine which demands payment before offering a chocolate can be written as:

CSP Example - Vending Machine

- A machine which demands payment before offering a chocolate can be written as:
  - $VendingMachine = coin \to choc \to STOP$

CSP Example - Vending Machine

- A machine which demands payment before offering a chocolate can be written as:
  - $VendingMachine = coin \rightarrow choc \rightarrow STOP$
- A person who might choose to use a coin or card to make payments could be modelled as:

CSP Example - Vending Machine

- A machine which demands payment before offering a chocolate can be written as:
  - $VendingMachine = coin \rightarrow choc \rightarrow STOP$
- A person who might choose to use a coin or card to make payments could be modelled as:
  - $Person = (coin \rightarrow STOP)\Box(card \rightarrow STOP))$

CSP Example - Vending Machine

- A machine which demands payment before offering a chocolate can be written as:
  - $VendingMachine = coin \rightarrow choc \rightarrow STOP$
- A person who might choose to use a coin or card to make payments could be modelled as:
  - $Person = (coin \rightarrow STOP) \Box (card \rightarrow STOP))$
- These two processes can be put in parallel, so that they can interact with each other;

CSP Example - Vending Machine

- A machine which demands payment before offering a chocolate can be written as:
  - $VendingMachine = coin \rightarrow choc \rightarrow STOP$
- A person who might choose to use a coin or card to make payments could be modelled as:
  - $Person = (coin \rightarrow STOP)\Box(card \rightarrow STOP))$
- These two processes can be put in parallel, so that they can interact with each other;
- The behaviour of the composite process depends on the events that the two processes must synchronise on:

CSP Example - Vending Machine

- A machine which demands payment before offering a chocolate can be written as:
  - $VendingMachine = coin \rightarrow choc \rightarrow STOP$
- A person who might choose to use a coin or card to make payments could be modelled as:
  - $Person = (coin \rightarrow STOP) \square (card \rightarrow STOP))$
- These two processes can be put in parallel, so that they can interact with each other;
- The behaviour of the composite process depends on the events that the two processes must synchronise on:
  - $VendingMachine \,|[\{coin, card\}]|\, Person \equiv$
    $coin \rightarrow choc \rightarrow STOP$

CSP Example - Vending Machine

- If synchronization was only required on “coin”, we would obtain:

CSP Example - Vending Machine

- If synchronization was only required on "coin", we would obtain:
  - $\mathit{VendingMachine}\,|[\{\mathit{coin}\}]|\,\mathit{Person} \equiv$ $(\mathit{coin} \rightarrow \mathit{choc} \rightarrow \mathit{STOP})\,\Box\,(\mathit{card} \rightarrow \mathit{STOP})$

CSP Example - Vending Machine

- If synchronization was only required on "coin", we would obtain:
  - $\mathit{VendingMachine} \,|[\{\mathit{coin}\}]|\, \mathit{Person} \equiv$ $(\mathit{coin} \rightarrow \mathit{choc} \rightarrow \mathit{STOP}) \,\Box\, (\mathit{card} \rightarrow \mathit{STOP})$
- If we abstract this latter composite process by hiding the "coin" and "card" events:

CSP Example - Vending Machine

- If synchronization was only required on "coin", we would obtain:
  - $VendingMachine \,|[\{coin\}]|\, Person \equiv$
    $(coin \rightarrow choc \rightarrow STOP) \,\Box\, (card \rightarrow STOP)$
- If we abstract this latter composite process by hiding the "coin" and "card" events:
  - $((coin \rightarrow choc \rightarrow STOP) \,\Box\, (card \rightarrow STOP))$
    $\setminus \{coin, card\}$

CSP Example - Vending Machine

- If synchronization was only required on “coin”, we would obtain:
  - $VendingMachine \,|[\{coin\}]|\, Person \equiv$ $(coin \rightarrow choc \rightarrow STOP) \,\square\, (card \rightarrow STOP)$
- If we abstract this latter composite process by hiding the “coin” and “card” events:
  - $((coin \rightarrow choc \rightarrow STOP) \,\square\, (card \rightarrow STOP))$ $\setminus \{coin, card\}$
- We get the non-deterministic process:

CSP Example - Vending Machine

- If synchronization was only required on "coin", we would obtain:
  - $VendingMachine \,|[\{coin\}]|\, Person \equiv (coin \rightarrow choc \rightarrow STOP) \,\Box\, (card \rightarrow STOP)$
- If we abstract this latter composite process by hiding the "coin" and "card" events:
  - $((coin \rightarrow choc \rightarrow STOP) \,\Box\, (card \rightarrow STOP)) \setminus \{coin, card\}$
- We get the non-deterministic process:
  - $(choc \rightarrow STOP) \sqcap STOP$

CSP Example - Vending Machine

- If synchronization was only required on “coin”, we would obtain:
  - $VendingMachine \mid[\{coin\}]\mid Person \equiv (coin \rightarrow choc \rightarrow STOP) \,\square\, (card \rightarrow STOP)$
- If we abstract this latter composite process by hiding the “coin” and “card” events:
  - $((coin \rightarrow choc \rightarrow STOP) \,\square\, (card \rightarrow STOP)) \setminus \{coin, card\}$
- We get the non-deterministic process:
  - $(choc \rightarrow STOP) \sqcap STOP$
- This process which either offers a “choc” event and then stops, or just stops;

CSP Example - Vending Machine

- If synchronization was only required on "coin", we would obtain:
  - $VendingMachine \,|[\{coin\}]|\, Person \equiv$
    $(coin \rightarrow choc \rightarrow STOP) \,\square\, (card \rightarrow STOP)$
- If we abstract this latter composite process by hiding the "coin" and "card" events:
  - $((coin \rightarrow choc \rightarrow STOP) \,\square\, (card \rightarrow STOP))$
    $\setminus \{coin, card\}$
- We get the non-deterministic process:
  - $(choc \rightarrow STOP) \sqcap STOP$
- This process which either offers a "choc" event and then stops, or just stops;
- Externally non-determinism has been introduced.

Needham-Schroeder Public Key Protocol

1. A $\rightarrow$ B: $\{|N_a, A|\}_{K_b}$

Needham-Schroeder Public Key Protocol

1. A $\rightarrow$ B: $\{|N_a, A|\}_{K_b}$
2. B $\rightarrow$ A: $\{|N_a, N_b|\}_{K_a}$

Needham-Schroeder Public Key Protocol

1. A $\rightarrow$ B: $\{|N_a, A|\}_{K_b}$
2. B $\rightarrow$ A: $\{|N_a, N_b|\}_{K_a}$
3. A $\rightarrow$ B: $\{|N_b|\}_{K_b}$

NSPKP Goals

- The goal of the protocol is to establish mutual authentication between two parties A and B in the presence of adversary;

NSPKP Goals

- The goal of the protocol is to establish mutual authentication between two parties A and B in the presence of adversary;
- A and B obtain a secret shared key though direct communication using public key cryptography;

NSPKP Goals

- The goal of the protocol is to establish mutual authentication between two parties A and B in the presence of adversary;
- A and B obtain a secret shared key though direct communication using public key cryptography;
- This adversary can intercept messages, delay messages, read and copy messages and generate messages;

NSPKP Goals

- The goal of the protocol is to establish mutual authentication between two parties A and B in the presence of adversary;
- A and B obtain a secret shared key though direct communication using public key cryptography;
- This adversary can intercept messages, delay messages, read and copy messages and generate messages;
- This adversary can not learn the privates keys of principals.

Lowe's Specification using CSP

- $MSG1 \equiv \{Msg1.a.b.Encrypt.k.n_a.a' \mid$
  $a \in Initiator, a' \in Initiator, b \in Responder,$
  $k \in Key, n_a \in Nonce\},$

Lowe's Specification using CSP

- $MSG1 \equiv \{Msg1.a.b.Encrypt.k.n_a.a' |$
  $a \in Initiator, a' \in Initiator, b \in Responder,$
  $k \in Key, n_a \in Nonce\},$
- $MSG2 \equiv \{Msg2.b.a.Encrypt.k.n_a.n_b |$
  $a \in Initiator, b \in Responder,$
  $k \in Key, n_a \in Nonce, n_b \in Nonce\},$

Lowe's Specification using CSP

- $MSG1 \equiv \{Msg1.a.b.Encrypt.k.n_a.a' \mid$
  $a \in Initiator, a' \in Initiator, b \in Responder,$
  $k \in Key, n_a \in Nonce\},$
- $MSG2 \equiv \{Msg2.b.a.Encrypt.k.n_a.n_b \mid$
  $a \in Initiator, b \in Responder,$
  $k \in Key, n_a \in Nonce, n_b \in Nonce\},$
- $MSG3 \equiv \{Msg3.a.b.Encrypt.k.n_b \mid$
  $a \in Initiator, b \in Responder, k \in Key, n_b \in Nonce\},$

Lowe's Specification using CSP

- $MSG1 \equiv \{Msg1.a.b.Encrypt.k.n_a.a' \mid$
  $a \in Initiator, a' \in Initiator, b \in Responder,$
  $k \in Key, n_a \in Nonce\},$
- $MSG2 \equiv \{Msg2.b.a.Encrypt.k.n_a.n_b \mid$
  $a \in Initiator, b \in Responder,$
  $k \in Key, n_a \in Nonce, n_b \in Nonce\},$
- $MSG3 \equiv \{Msg3.a.b.Encrypt.k.n_b \mid$
  $a \in Initiator, b \in Responder, k \in Key, n_b \in Nonce\},$
- $MSG \equiv MSG1 \cup MSG2 \cup MSG3.$

Lowe's Specification using CSP

- Standard communications in the system will be modelled by the channel comm;

Lowe's Specification using CSP

- Standard communications in the system will be modelled by the channel comm;
- We also want to model the fact that the intruder can fake or intercept messages, and so we introduce extra channels fake and intercept;

Lowe's Specification using CSP

- Standard communications in the system will be modelled by the channel comm;
- We also want to model the fact that the intruder can fake or intercept messages, and so we introduce extra channels fake and intercept;
- $\mathit{channel} \quad \mathit{comm}, \mathit{fake}, \mathit{intercept} : \mathit{MSG}.$

Lowe's Specification using CSP

- Standard communications in the system will be modelled by the channel comm;
- We also want to model the fact that the intruder can fake or intercept messages, and so we introduce extra channels fake and intercept;
- $channel \quad comm, fake, intercept : MSG.$
- This will ensure that the receiver of a faked message is not aware that it is a fake, and that the sender of an intercepted message is not aware that it is intercepted.

Lowe's Specification using CSP

- We introduce two extra channels, defining the external interface of the protocol;

Lowe's Specification using CSP

- We introduce two extra channels, defining the external interface of the protocol;
- We represent a request from a user for initiator "a" to connect with responder "b" by the event *user.a.b*;

Lowe's Specification using CSP

- We introduce two extra channels, defining the external interface of the protocol;
- We represent a request from a user for initiator "a" to connect with responder "b" by the event *user.a.b*;
- We represent the resulting session by the event *session.a.b*;

Lowe's Specification using CSP

- We also add channels to represent the state of the agents:

Lowe's Specification using CSP

- We also add channels to represent the state of the agents:
  - We represent the initiator "a" thinking it is taking part in a run of the protocol with "b" by the event *I_running.a.b*;

Lowe's Specification using CSP

- We also add channels to represent the state of the agents:
  - We represent the initiator "a" thinking it is taking part in a run of the protocol with "b" by the event *I_running.a.b*;
  - We represent the responder "b" thinking it is taking part in a run of the protocol with "a" by the event *R_running.a.b*;

Lowe's Specification using CSP

- We also add channels to represent the state of the agents:
  - We represent the initiator "a" thinking it is taking part in a run of the protocol with "b" by the event *I_running.a.b*;
  - We represent the responder "b" thinking it is taking part in a run of the protocol with "a" by the event *R_running.a.b*;
  - We represent the initiator committing to the session by the *I_commit.a.b*;

Lowe's Specification using CSP

- We also add channels to represent the state of the agents:
    - We represent the initiator "a" thinking it is taking part in a run of the protocol with "b" by the event *I_running.a.b*;
    - We represent the responder "b" thinking it is taking part in a run of the protocol with "a" by the event *R_running.a.b*;
    - We represent the initiator committing to the session by the *I_commit.a.b*;
    - We represent the responder committing to the session by *R_commit.a.b*;

Lowe's Specification using CSP

- We also add channels to represent the state of the agents:
  - We represent the initiator "a" thinking it is taking part in a run of the protocol with "b" by the event *I_running.a.b*;
  - We represent the responder "b" thinking it is taking part in a run of the protocol with "a" by the event *R_running.a.b*;
  - We represent the initiator committing to the session by the *I_commit.a.b*;
  - We represent the responder committing to the session by *R_commit.a.b*;
- We declare these channels by:
- *channel* *user*, *session*, *I_running*, *B_running*, *I_commit*, *B_.commit* : *Initiator.Responder.*

Lowe's Specification using CSP

- We will represent a responder with identity "a", who has a single nonce n_a, by the CSP process $INITIATOR(a, na)$.;

Lowe's Specification using CSP

- We will represent a responder with identity "a", who has a single nonce n_a, by the CSP process $INITIATOR(a, na)$.;
- If we want to consider a responder with more than one nonce, then we can compose several such processes, either sequentially or interleaved;

Lowe's Specification using CSP

- We will represent a responder with identity "a", who has a single nonce n_a, by the CSP process $INITIATOR(a, na)$.;
- If we want to consider a responder with more than one nonce, then we can compose several such processes, either sequentially or interleaved;
- Ignoring, for the moment, the possibility of intruder action, the process can be defined by:
  - $INITIATOR(a, n_a) \equiv user.a?b \rightarrow I\_.running.a.b \rightarrow$
    $comm!Msg1.a.b.Encrypt.key(b).n_a, a \rightarrow$
    $comm.Msg2.b.a.Encrypt.key(a)?n'_a.n_b \rightarrow$
    $if \quad n_a = n'_a$
    $\quad then \quad comm!Msg3.a.b.Encrypt.key(b).n_b \rightarrow$
    $\quad I\_commit.a.b \rightarrow session.a.b \rightarrow SKIP$
    $else \quad STOP.$

Lowe's Specification using CSP

- We now introduce the possibility of enemy action by applying a renaming to the above process;

Lowe's Specification using CSP

- We now introduce the possibility of enemy action by applying a renaming to the above process;
- Our renaming specification should ensure that message 1s and message 3s sent by the initiator can be intercepted;

Lowe's Specification using CSP

- We now introduce the possibility of enemy action by applying a renaming to the above process;
- Our renaming specification should ensure that message 1s and message 3s sent by the initiator can be intercepted;
- And message 2s can be faked;

Lowe's Specification using CSP

- We now introduce the possibility of enemy action by applying a renaming to the above process;
- Our renaming specification should ensure that message 1s and message 3s sent by the initiator can be intercepted;
- And message 2s can be faked;
- We define an initiator with identity A and nonce Na by:
$INITIATOR1 \equiv INITIATOR(A, N_a)$
$[[comm.Msg1 \leftarrow comm.Msg1, comm.Msg1 \leftarrow intercept.Msg1,$
$comm.Msg2 \leftarrow comm.Msg2, comm.Msg2 \leftarrow fake.Msg2,$
$comm.Msg3 \leftarrow comm.Msg3, comm.Msg3 \leftarrow intercept.Msg3]].$

Lowe's Intruder

- The intruder should be able to:

Lowe's Intruder

- The intruder should be able to:
    - Overhear and/or intercept any messages being passed in the system;

Lowe's Intruder

- The intruder should be able to:
    - Overhear and/or intercept any messages being passed in the system;
    - Decrypt messages that are encrypted with his own public key, so as to learn new nonces;

Lowe's Intruder

- The intruder should be able to:
    - Overhear and/or intercept any messages being passed in the system;
    - Decrypt messages that are encrypted with his own public key, so as to learn new nonces;
    - Introduce new messages into the system, using nonces he knows;

Lowe's Intruder

- The intruder should be able to:
  - Overhear and/or intercept any messages being passed in the system;
  - Decrypt messages that are encrypted with his own public key, so as to learn new nonces;
  - Introduce new messages into the system, using nonces he knows;
  - Replay any message he has seen (possibly changing plain-text parts), even if he does not understand the contents of the encrypted part;

Lowe's Intruder

- The intruder should be able to:
  - Overhear and/or intercept any messages being passed in the system;
  - Decrypt messages that are encrypted with his own public key, so as to learn new nonces;
  - Introduce new messages into the system, using nonces he knows;
  - Replay any message he has seen (possibly changing plain-text parts), even if he does not understand the contents of the encrypted part;

Lowe's Intruder

- Replay any message he has seen (possibly changing plain-text parts), even if he does not understand the contents of the encrypted part;

Lowe's Intruder

- Replay any message he has seen (possibly changing plain-text parts), even if he does not understand the contents of the encrypted part;
- We assume that the intruder is a user of the computer network;

Lowe's Intruder

- Replay any message he has seen (possibly changing plain-text parts), even if he does not understand the contents of the encrypted part;
- We assume that the intruder is a user of the computer network;
- We will define the most general (i.e. the most non-deterministic) intruder who can act as above;

Lowe's Intruder

- Replay any message he has seen (possibly changing plain-text parts), even if he does not understand the contents of the encrypted part;
- We assume that the intruder is a user of the computer network;
- We will define the most general (i.e. the most non-deterministic) intruder who can act as above;
- We consider an intruder with identity I, with public key K_i, who initially knows a nonce N_i.

Lowe's Intruder Definition in CSP

$I(m1s, m2s, m3s, ns)$

Lowe's Intruder Definition in CSP

$$
\begin{aligned}
&I(m1s, m2s, m3s, ns) \\
&\quad comm.Msg1?a.b.Encrypt.k.n.a' \rightarrow \\
&\quad \textit{if} \quad k = K_i \quad \textit{then} \quad I(m1s, m2s, m3s, ns \cup \{n\}) \\
&\quad \textit{else} \quad I(m1s \cup \{Encrypt.k.n.a'\}, m2s, m3s, ns)
\end{aligned}
$$

Lowe's Intruder Definition in CSP

$$
\begin{array}{l}
I(m1s, m2s, m3s, ns) \\
\quad comm.Msg1?a.b.Encrypt.k.n.a' \rightarrow \\
\quad \text{if} \quad k = K_i \quad \text{then} \quad I(m1s, m2s, m3s, ns \cup \{n\}) \\
\quad \text{else} \quad I(m1s \cup \{Encrypt.k.n.a'\}, m2s, m3s, ns) \\
\quad \Box intercept.Msg1?a.b.Encrypt.k.n.a' \rightarrow \\
\quad \text{if} \quad k = K_i \quad \text{then} \quad I(m1s, m2s, m3s, ns \cup \{n\}) \\
\quad \text{else} \quad I(m1s \cup \{Encrypt.k.n.a'\}, m2s, m3s, ns)
\end{array}
$$

Lowe's Intruder Definition in CSP

$$
\begin{array}{l}
I(m1s, m2s, m3s, ns) \\
\quad comm.Msg1?a.b.Encrypt.k.n.a' \rightarrow \\
\quad if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n\}) \\
\quad else \quad I(m1s \cup \{Encrypt.k.n.a'\}, m2s, m3s, ns) \\
\quad \Box intercept.Msg1?a.b.Encrypt.k.n.a' \rightarrow \\
\quad if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n\}) \\
\quad else \quad I(m1s \cup \{Encrypt.k.n.a'\}, m2s, m3s, ns) \\
\quad \Box comm.Msg2?b.a.Encrypt.k.n.n' \rightarrow \\
\quad if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n, n'\}) \\
\quad else \quad I(m1s, m2s \cup Encrypt.k, n.n', m3s, ns)
\end{array}
$$

Lowe's Intruder Definition in CSP

$$
\begin{array}{l}
I(m1s, m2s, m3s, ns) \\
\quad comm.Msg1?a.b.Encrypt.k.n.a' \rightarrow \\
\quad if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n\}) \\
\quad else \quad I(m1s \cup \{Encrypt.k.n.a'\}, m2s, m3s, ns) \\
\quad \Box intercept.Msg1?a.b.Encrypt.k.n.a' \rightarrow \\
\quad if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n\}) \\
\quad else \quad I(m1s \cup \{Encrypt.k.n.a'\}, m2s, m3s, ns) \\
\quad \Box comm.Msg2?b.a.Encrypt.k.n.n' \rightarrow \\
\quad if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n, n'\}) \\
\quad else \quad I(m1s, m2s \cup Encrypt.k, n.n', m3s, ns) \\
\quad \Box intercept.Msg2?b.a.Encrypt.k.n.n' \rightarrow \\
\quad if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n, n'\}) \\
\quad elseI(m1s, m2s \cup Encrypt.k.n.n', m3s, ns)
\end{array}
$$

Lowe's Intruder Definition in CSP

$\Box \mathit{comm}.\mathit{Msg}3?a.b.\mathit{Encrypt}.k.n \rightarrow$
$\mathit{if} \quad k = K_i \quad \mathit{then} \quad I(m1s, m2s, m3s, ns \cup \{n\})$
$\mathit{elseI}(mls, m2s, rn3s \cup \mathit{Encrypt}.k.n, ns)$

Lowe's Intruder Definition in CSP

$\Box comm.Msg3?a.b.Encrypt.k.n \rightarrow$
$if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n\})$
$elseI(mls, m2s, rn3s \cup Encrypt.k.n, ns)$
$\Box intercept.Msg3?a.b.Encrypt.k.n \rightarrow$
$if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n\})$
$elseI(m1s, m2s, m3s \cup Encrypt.k.n, ns)$

Lowe's Intruder Definition in CSP

$\Box comm.Msg3?a.b.Encrypt.k.n \rightarrow$
$if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n\})$
$else I(mls, m2s, rn3s \cup Encrypt.k.n, ns)$
$\Box intercept.Msg3?a.b.Encrypt.k.n \rightarrow$
$if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n\})$
$else I(m1s, m2s, m3s \cup Encrypt.k.n, ns)$
$\Box fake.Msg1?a.b?m : m1s \rightarrow I(m1s, m2s, m3s, ns)$
$\Box fake.Msg2?a.b?m : m2s \rightarrow I(m1s, m2s, m3s, ns)$
$\Box fake.Msg3?a.b?m : m3s \rightarrow I(m1s, m2s, m3s, ns)$

Lowe's Intruder Definition in CSP

$$\Box comm.Msg3?a.b.Encrypt.k.n \rightarrow$$
$$if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n\})$$
$$elseI(mls, m2s, rn3s \cup Encrypt.k.n, ns)$$
$$\Box intercept.Msg3?a.b.Encrypt.k.n \rightarrow$$
$$if \quad k = K_i \quad then \quad I(m1s, m2s, m3s, ns \cup \{n\})$$
$$elseI(m1s, m2s, m3s \cup Encrypt.k.n, ns)$$
$$\Box fake.Msg1?a.b?m : m1s \rightarrow I(m1s, m2s, m3s, ns)$$
$$\Box fake.Msg2?a.b?m : m2s \rightarrow I(m1s, m2s, m3s, ns)$$
$$\Box fake.Msg3?a.b?m : m3s \rightarrow I(m1s, m2s, m3s, ns)$$
$$\Box fake.Msg1?a.blEncrypt?k?n : ns?a' \rightarrow I(m1s, m2s, m3s, ns)$$
$$\Box fake.Msg2?b.a!Encrypt?k?n : ns?n' : ns \rightarrow I(m1s, m2s, m3s, ns)$$
$$\Box fake.Msg3?a.b!Encrypt?k?n : ns \rightarrow I(m1s, m2s, m3s, ns).$$

Lowe's Intruder Definition in CSP

- We consider an intruder who initially knows the nonce N_i:
    - $INTRUDER \equiv I(\{\}, \{\}, \{\}, \{N_i\})$.

Lowe's Intruder Definition in CSP

- We consider an intruder who initially knows the nonce N_i:
  - $INTRUDER \equiv I(\{\}, \{\}, \{\}, \{N_i\})$.
- We may now define a system with an intruder:
  - $AGENTS \equiv$
    $INITIATOR1|[\{|comm, session.A.B|\}]|RESPONDER1$,
    $SYSTEM \equiv AGENTS|[\{|fake, comm, intercept|\}]|INTRUDER$.

Refining CSP with FDR

- FDR takes as two inputs, a specification and an implementation, and test whether the implementation refines the specification;

Refining CSP with FDR

- FDR takes as two inputs, a specification and an implementation, and test whether the implementation refines the specification;
- We are working in the traces model of CSP, so checking for refinement amounts to testing whether each trace of the implementation is also a trace of the specification;

Testing NSPKP with FDR

- To test whether the protocol correctly authenticates the responder, we need to find a specification that allows only those traces where the initiator A commits to a session with B only if B has indeed taken part in the protocol run;

Testing NSPKP with FDR

- To test whether the protocol correctly authenticates the responder, we need to find a specification that allows only those traces where the initiator A commits to a session with B only if B has indeed taken part in the protocol run;
- The initiator committing to a session is represented by an I_commit.A.B event; the responder taking part in a run of the protocol with A is represented by R_running.A.B;

Testing NSPKP with FDR

- To test whether the protocol correctly authenticates the responder, we need to find a specification that allows only those traces where the initiator A commits to a session with B only if B has indeed taken part in the protocol run;
- The initiator committing to a session is represented by an I_commit.A.B event; the responder taking part in a run of the protocol with A is represented by R_running.A.B;
- Thus the authenticity of the responder can be tested using the specification AR:
  - $AR_0 \equiv R\_running.A.B \rightarrow I\_commit.A.B \rightarrow AR_0$,
    $A1 \equiv \{|R\_running.A.B, I\_commit.A.B|\}$,
    $AR \equiv AR_0 ||| RUN(\sum A1)$.

Testing NSPKP with FDR

- We now consider authentication of the initiator. The protocol should ensure that the responder B commits to a session with initiator A only if A took part in the protocol run;

Testing NSPKP with FDR

- We now consider authentication of the initiator. The protocol should ensure that the responder B commits to a session with initiator A only if A took part in the protocol run;
- Formally, an R_commit.A.B event should occur only if there has been a corresponding I_running.A.B event;

Testing NSPKP with FDR

- We now consider authentication of the initiator. The protocol should ensure that the responder B commits to a session with initiator A only if A took part in the protocol run;
- Formally, an R_commit.A.B event should occur only if there has been a corresponding I_running.A.B event;
- This requirement is captured by the specification AI:
  - $AI_0 \equiv I\_running.A.B \rightarrow R_commit.A.B \rightarrow AI_0$,
    $A_2 \equiv \{|I\_running.A.B, R\_commit.A.B|\}$,
    $AI \equiv AI_0|||RUN(\sum \; A2)$.

Testing NSPKP with FDR - the Flaw

- FDR can be used to discover that SYSTEM does not refine AI;

Testing NSPKP with FDR - the Flaw

- FDR can be used to discover that SYSTEM does not refine AI;
- It finds that after the trace:
  - $(user.A.I, I\_running.A.I,$
    $intercept.Msg1.A.I.Encrypt.K_i.N_a.A,$
    $fake.Msgl.A.B.Encrypt.K_b.N_a.A,$
    $intercept.Msg2.B.A.Encrypt.K_a.N_a.N_b,$
    $fake.Msg2.I.A.Encrypt.K_a.N_a.N_b,$
    $intercept.Msg3.A.I.Encrypt.K_i.N_b,$
    $fake.Msg3.A.B.Encrypt.K_b.N_b)$

Lowe's Attack - Translated

1. A $\rightarrow$ C: $\{|N_a, A|\}_{K_c}$

1'. C(A) $\rightarrow$ B: $\{|N_a, A|\}_{K_b}$

2'. B $\rightarrow$ C(A): $\{|N_a, N_b|\}_{K_a}$

2. C $\rightarrow$ A: $\{|N_a, N_b|\}_{K_a}$

3. A $\rightarrow$ C: $\{|N_b|\}_{K_c}$

3'. C $\rightarrow$ B: $\{|N_b|\}_{K_b}$

- Bob believes to be talking to Alice , while he is talking to Charlie;

Lowe's Attack - Translated

1. A $\rightarrow$ C: $\{|N_a, A|\}_{K_c}$
1'. C(A) $\rightarrow$ B: $\{|N_a, A|\}_{K_b}$
2'. B $\rightarrow$ C(A): $\{|N_a, N_b|\}_{K_a}$
2. C $\rightarrow$ A: $\{|N_a, N_b|\}_{K_a}$
3. A $\rightarrow$ C: $\{|N_b|\}_{K_c}$
3'. C $\rightarrow$ B: $\{|N_b|\}_{K_b}$

- Bob believes to be talking to Alice , while he is talking to Charlie;
- Charlie uses Alice as an oracle to answers Bob's challenges;

Lowe's Attack - Translated

1. A $\rightarrow$ C: $\{|N_a, A|\}_{K_c}$
1'. C(A) $\rightarrow$ B: $\{|N_a, A|\}_{K_b}$
2'. B $\rightarrow$ C(A): $\{|N_a, N_b|\}_{K_a}$
2. C $\rightarrow$ A: $\{|N_a, N_b|\}_{K_a}$
3. A $\rightarrow$ C: $\{|N_b|\}_{K_c}$
3'. C $\rightarrow$ B: $\{|N_b|\}_{K_b}$

- Bob believes to be talking to Alice , while he is talking to Charlie;
- Charlie uses Alice as an oracle to answers Bob's challenges;
- Charlie can use Nb to prove to Bob he is Alice.

Discussion

- Would Lowe be able to find this attack by hand?

Discussion

- Would Lowe be able to find this attack by hand?
- What else could be testes using this strategy?

Discussion

- Would Lowe be able to find this attack by hand?
- What else could be testes using this strategy?
- Was it the methodology or the Threat Model?

Questions????

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

UNIVERSIDADE FEDERAL
DE SANTA CATARINA