Protocol Verification Techniques - Theorem Provers

Design and Verification of Security Protocols and Security Ceremonies

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

August-November 2016

Programa de Pós-Graduação em Ciência da Computação UFSC

UNIVERSIDADE FEDERAL DE SANTA CATARINA

Attention!

Attention!

This topic will be divided into two lectures. One will deal with automatic theorem provers using FOL and the second will deal with theorem provers using HOL

Higher-Order Logic

- Higher-order logic is a form of predicate logic that is distinguished from first-order logic by additional quantifiers and stronger semantics;

Higher-Order Logic

- Higher-order logic is a form of predicate logic that is distinguished from first-order logic by additional quantifiers and stronger semantics;
- Higher-order logics semantics are more expressive, but their model-theoretic properties are less well-behaved than those of first-order logic;

Higher-Order Logic

- Higher-order logic is a form of predicate logic that is distinguished from first-order logic by additional quantifiers and stronger semantics;
- Higher-order logics semantics are more expressive, but their model-theoretic properties are less well-behaved than those of first-order logic;
- The term "higher-order logic", abbreviated as HOL;

Higher-Order Logic

- Higher-order logic is a form of predicate logic that is distinguished from first-order logic by additional quantifiers and stronger semantics;
- Higher-order logics semantics are more expressive, but their model-theoretic properties are less well-behaved than those of first-order logic;
- The term "higher-order logic", abbreviated as HOL;
- HOL is any predicate logic that has greater order than Second-Order Logic;

Higher-Order Logic

- Second-Order Logic stands for the possibility of quantifying over sets;

Higher-Order Logic

- Second-Order Logic stands for the possibility of quantifying over sets;
- The idea is that you can put a quantifier over other quantifier;

Higher-Order Logic

- Second-Order Logic stands for the possibility of quantifying over sets;
- The idea is that you can put a quantifier over other quantifier;
- For example we can say $\forall x \exists P(x, y) \rightarrow y$

Higher-Order Logic

- Second-Order Logic stands for the possibility of quantifying over sets;
- The idea is that you can put a quantifier over other quantifier;
- For example we can say $\forall x \exists P(x, y) \rightarrow y$
- Third-Order Logic allows for quantification over Second-Order Logic;

Higher-Order Logic

- Second-Order Logic stands for the possibility of quantifying over sets;
- The idea is that you can put a quantifier over other quantifier;
- For example we can say $\forall x \exists P(x, y) \rightarrow y$
- Third-Order Logic allows for quantification over Second-Order Logic;
- Higher-order logic is the union of first-, second-, third-, ..., nth-order logic;

Higher-Order Logic

- Second-Order Logic stands for the possibility of quantifying over sets;
- The idea is that you can put a quantifier over other quantifier;
- For example we can say $\forall x \exists P(x, y) \rightarrow y$
- Third-Order Logic allows for quantification over Second-Order Logic;
- Higher-order logic is the union of first-, second-, third-, ..., nth-order logic;
- Higher-order logic admits quantification over sets that are nested arbitrarily deeply.

HOL Example

- First-order logic quantifies only variables that range over individuals;

HOL Example

- First-order logic quantifies only variables that range over individuals;
- Second-order logic, in addition, quantifies over sets;

HOL Example

- First-order logic quantifies only variables that range over individuals;
- Second-order logic, in addition, quantifies over sets;
- Third-order logic also quantifies over sets of sets, and so on;

HOL Example

- First-order logic quantifies only variables that range over individuals;
- Second-order logic, in addition, quantifies over sets;
- Third-order logic also quantifies over sets of sets, and so on;
- From Second-Order Logic on we are allowed to describe mathematical induction;

HOL Example

- First-order logic quantifies only variables that range over individuals;
- Second-order logic, in addition, quantifies over sets;
- Third-order logic also quantifies over sets of sets, and so on;
- From Second-Order Logic on we are allowed to describe mathematical induction;
- $\forall P((0 \in P \wedge \forall i(i \in P \rightarrow i + 1 \in P)) \rightarrow \forall n(n \in P))$

HOL Example

- First-order logic quantifies only variables that range over individuals;
- Second-order logic, in addition, quantifies over sets;
- Third-order logic also quantifies over sets of sets, and so on;
- From Second-Order Logic on we are allowed to describe mathematical induction;
- $\forall P((0 \in P \wedge \forall i(i \in P \rightarrow i + 1 \in P)) \rightarrow \forall n(n \in P))$
- This is the definition of the set of Natural Numbers.

Lawrence Charles Paulson - Larry

- Lawrence Charles Paulson (Larry) is a professor at the University of Cambridge;

Lawrence Charles Paulson - Larry

- Lawrence Charles Paulson (Larry) is a professor at the University of Cambridge;
- His research is based around the interactive theorem prover Isabelle, which he introduced in 1986;

Lawrence Charles Paulson - Larry

- Lawrence Charles Paulson (Larry) is a professor at the University of Cambridge;
- His research is based around the interactive theorem prover Isabelle, which he introduced in 1986;
- He has worked on the verification of cryptographic protocols using inductive definitions;

Lawrence Charles Paulson - Larry

- Lawrence Charles Paulson (Larry) is a professor at the University of Cambridge;
- His research is based around the interactive theorem prover Isabelle, which he introduced in 1986;
- He has worked on the verification of cryptographic protocols using inductive definitions;
- He has also formalized the constructible universe of Kurt Gödel;

Lawrence Charles Paulson - Larry

- Lawrence Charles Paulson (Larry) is a professor at the University of Cambridge;
- His research is based around the interactive theorem prover Isabelle, which he introduced in 1986;
- He has worked on the verification of cryptographic protocols using inductive definitions;
- He has also formalized the constructible universe of Kurt Gödel;

Curiosities about Larry

- He was one of the most cited researchers on a paper that demonstrated the existence of God by a machine on Gödel's world;

Curiosities about Larry

- He was one of the most cited researchers on a paper that demonstrated the existence of God by a machine on Gödel's world;
- He is a deep minded atheist;

Curiosities about Larry

- He was one of the most cited researchers on a paper that demonstrated the existence of God by a machine on Gödel's world;
- He is a deep minded atheist;
- He has a page called: "Larry Paulson - Portrait of a God";

Curiosities about Larry

- He was one of the most cited researchers on a paper that demonstrated the existence of God by a machine on Gödel's world;
- He is a deep minded atheist;
- He has a page called: "Larry Paulson - Portrait of a God";
- http://www.geocities.ws/robrich18/Larry.html

Larry's Protocol Verification Time-line

- Isabelle theorem prover;

Larry's Protocol Verification Time-line

- Isabelle theorem prover;
    - General tool;

Larry's Protocol Verification Time-line

- Isabelle theorem prover;
    - General tool;
    - Works with protocols since 1997;

Larry's Protocol Verification Time-line

- Isabelle theorem prover;
  - General tool;
  - Works with protocols since 1997;
- Many papers describing the Inductive Method he created;

Larry's Protocol Verification Time-line

- Isabelle theorem prover;
  - General tool;
  - Works with protocols since 1997;
- Many papers describing the Inductive Method he created;
- Many case studies, including:

Larry's Protocol Verification Time-line

- Isabelle theorem prover;
  - General tool;
  - Works with protocols since 1997;
- Many papers describing the Inductive Method he created;
- Many case studies, including:
  - Verification of SET protocol (6 papers)

Larry's Protocol Verification Time-line

- Isabelle theorem prover;
  - General tool;
  - Works with protocols since 1997;
- Many papers describing the Inductive Method he created;
- Many case studies, including:
  - Verification of SET protocol (6 papers)
  - Kerberos (3 papers)

Larry's Protocol Verification Time-line

- Isabelle theorem prover;
  - General tool;
  - Works with protocols since 1997;
- Many papers describing the Inductive Method he created;
- Many case studies, including:
  - Verification of SET protocol (6 papers)
  - Kerberos (3 papers)
  - TLS protocol

Larry's Protocol Verification Time-line

- Isabelle theorem prover;
  - General tool;
  - Works with protocols since 1997;
- Many papers describing the Inductive Method he created;
- Many case studies, including:
  - Verification of SET protocol (6 papers)
  - Kerberos (3 papers)
  - TLS protocol
  - Yahalom protocol, smart cards, etc

Larry's Protocol Verification Time-line

- Isabelle theorem prover;
  - General tool;
  - Works with protocols since 1997;
- Many papers describing the Inductive Method he created;
- Many case studies, including:
  - Verification of SET protocol (6 papers)
  - Kerberos (3 papers)
  - TLS protocol
  - Yahalom protocol, smart cards, etc
- Last work published in 2015: "Verifying multicast-based security protocols using the inductive method. Martina, J.E., Paulson, L.C."

The Inductive Method

- Starts with an informal protocol description;

The Inductive Method

- Starts with an informal protocol description;
- Out of that we extract:

The Inductive Method

- Starts with an informal protocol description;
- Out of that we extract:
  - An inductive abstract trace model;

The Inductive Method

- Starts with an informal protocol description;
- Out of that we extract:
  - An inductive abstract trace model;
  - Correctness theorem about the traces;

The Inductive Method

- Starts with an informal protocol description;
- Out of that we extract:
  - An inductive abstract trace model;
  - Correctness theorem about the traces;
- We then add the attacker inference rules;

The Inductive Method

- Starts with an informal protocol description;
- Out of that we extract:
  - An inductive abstract trace model;
  - Correctness theorem about the traces;
- We then add the attacker inference rules;
- We stated the goals ad theorems and lemmas;

The Inductive Method

- Starts with an informal protocol description;
- Out of that we extract:
  - An inductive abstract trace model;
  - Correctness theorem about the traces;
- We then add the attacker inference rules;
- We stated the goals ad theorems and lemmas;
- We prove the theorems inductively to demonstrate correctness.

The Inductive Method Mechanics

- Larry Paulson advocates a simple approach:

The Inductive Method Mechanics

- Larry Paulson advocates a simple approach:
  - A protocol in a context describes a set of traces;

The Inductive Method Mechanics

- Larry Paulson advocates a simple approach:
  - A protocol in a context describes a set of traces;
  - These traces are defined inductively;

The Inductive Method Mechanics

- Larry Paulson advocates a simple approach:
  - A protocol in a context describes a set of traces;
  - These traces are defined inductively;
  - A specification is again a property of traces;

The Inductive Method Mechanics

- Larry Paulson advocates a simple approach:
  - A protocol in a context describes a set of traces;
  - These traces are defined inductively;
  - A specification is again a property of traces;
  - Checking requires proving that all the traces satisfy the property, by induction on the construction of the traces;

The Inductive Method Mechanics

- Larry Paulson advocates a simple approach:
  - A protocol in a context describes a set of traces;
  - These traces are defined inductively;
  - A specification is again a property of traces;
  - Checking requires proving that all the traces satisfy the property, by induction on the construction of the traces;
  - Main point: these proofs are big, uninteresting, and better left to machines;

The Inductive Method Mechanics

- Larry Paulson advocates a simple approach:
  - A protocol in a context describes a set of traces;
  - These traces are defined inductively;
  - A specification is again a property of traces;
  - Checking requires proving that all the traces satisfy the property, by induction on the construction of the traces;
  - Main point: these proofs are big, uninteresting, and better left to machines;
  - Use a theorem prover (Isabelle)to write the proofs.

Isabelle

- Automated support for proof development, which supports:

Isabelle

- Automated support for proof development, which supports:
  - Higher-order logic;

Isabelle

- Automated support for proof development, which supports:
  - Higher-order logic;
  - Serves as a logical framework;

Isabelle

- Automated support for proof development, which supports:
    - Higher-order logic;
    - Serves as a logical framework;
    - Supports ZF set theory and HOL;

Isabelle

- Automated support for proof development, which supports:
  - Higher-order logic;
  - Serves as a logical framework;
  - Supports ZF set theory and HOL;
  - Generic treatment of inference rules;

Isabelle

- Automated support for proof development, which supports:
  - Higher-order logic;
  - Serves as a logical framework;
  - Supports ZF set theory and HOL;
  - Generic treatment of inference rules;
- Powerful simplifier, classical reasoner and connected tools;

Isabelle

- Automated support for proof development, which supports:
  - Higher-order logic;
  - Serves as a logical framework;
  - Supports ZF set theory and HOL;
  - Generic treatment of inference rules;
- Powerful simplifier, classical reasoner and connected tools;
- Strong support for inductive definitions.

Inductive Method Support in Isabelle

Due to my lack of time we will jump to my Ph.D Thesis to get the explanation from there. I promise next time it will be everything on the slides..

Discussion

- What else can you foresee modelled using this strategy?

Discussion

- What else can you foresee modelled using this strategy?
- Can this be extended?

Discussion

- What else can you foresee modelled using this strategy?
- Can this be extended?
- What this strategy can not do?

Questions????

UNIVERSIDADE FEDERAL
DE SANTA CATARINA