Formal Analysis of Insider Threats for Auctions

Florian Kammüller

Middlesex University London & TU Berlin

Université de Rennes, Seminaire SoSySec
10. février 2017
Formal Models for Insider Threat Analysis

- Initial Idea:
  - Model infrastructure, actors, policies
  - Invalidate global policy by complete exploration of state space

  ⇒ Modelchecking

  ⇣ State explosion problem

- Interactive theorem proving in Isabelle [7]
  - Higher Order Logic: expressive
  - Proof of security/violations
  - Simulate “Modelchecking” [14]


Modeling Human Behaviour for Sociological Explanation

- Max Weber’s sociological explanation model
- 3-step logic of explanation (Hempel and Oppenheimer [1])

⇒ Macro-Micro-Macro transition

(a) Macro-Micro: taxonomy of insider as datatypes in HOL based on psychological results, e.g.

\[
\text{datatype } \text{psy\_states} = \text{happy} \mid \text{revenge} \mid \text{stressed}
\]

(b) Micro-Micro: Infrastructure with actors and locations for action theory

(c) Micro-Macro: Analysis of insider attacks: invalidation of global policies
Applications of Isabelle Insider Framework

- Logical Modeling of Insider Threats (Isabelle Insider Framework) [3]
- Attack Tree Analysis for Insider Threats on the IoT using Isabelle. [16]
- Airplane Safety and Security against Insider Threats. [17]
- Formal Analysis of Insider Threats for Auctions. [15]


Formal Analysis of Auctions and Security Protocols

- Interactive theorem proving in Isabelle [7]
  - Analysis of auctions [2]
  - Inductive approach to Security Protocols
  - Insider framework [3]

⇒ Application to Insider Threats on Auctions
- Example Cocaine Auction Protocol
  - Hypothetical auction inspired by eBay
  - Minimizes trust between participants
Several extremely rich and ruthless men are gathered around a table. An auction is about to be held in which one of them will offer his next shipment of cocaine to the highest bidder. The seller describes the merchandise and proposes a starting price. The others then bid increasing amounts until there are no bids for 30 consecutive seconds. At that point the seller declares the auction closed and arranges a secret appointment with the winner to deliver the goods. [1]
Cocaine Auction Protocol: Assumptions/Requirements

• Cocaine auction scenario makes trust issues unambiguous:
  • Nobody trusts anybody else more than strictly necessary
  • Auction participants all know each other (otherwise one might be police agent)
  • No-one who places a bid wants to be identified to the other bidders or to the seller
  • Nobody except buyer and seller should know who won the auction
  • Even the seller should not be able to find out highest bidder before committing to the sale

• But none of the participants should have to trust any other: the protocol cannot rely on a judge or policeman to act as arbitrator and must instead be self-enforcing
Anonymous Cocaine Auction Protocol: Implementation Techniques

- Broadcasting messages to participants without revealing the identity of the sender (anonymity layer)
- Identity of seller is known to buyers
- Buyers’ messages are anonymous, seller’s are not
- Protocol is succession of rounds $i$ of simple bidding
  - Seller announces bid price $b_i$ of round $i$
  - Buyers have up to 30 seconds to say “yes”
  - As soon as buyer says “yes”, he is winner $w_i$
  - New round starts . . .
  - If 30 seconds elapse in round $i$ with no bid, winner is $w_{i-1}$
- Seller needs a mechanism to identify the winner
- At finish of auction, seller prefers to give secret appointment to winner “See you on Tuesday at 06:30 in the car park of Heathrow terminal 5”
Asymmetric Version of Cocaine Auction Protocol

- Public key $K_S$ of seller S and secret $K_S^{-1}$ for decryption
- Public encryption keys $K_{A_i}$ of bidders with corresponding secret decryption keys $K_{A_i}^{-1}$

0. $S \rightarrow D: K_S$
   i. $?A_i \rightarrow D: \{K_{A_i}, b_i\}_{K_S}$
   n. $S \rightarrow D: \{b_{n-1}, MeetingAppointment\}_{K_{A_{n-1}}}$

Protocol works as follows

0. **Step 0**: seller S sends to all bidders in $D$ a public key $K_S$ enabling them to send secret message to S.
   i. **Round $i$ for $i = 1, \ldots, n − 1$**: bidder uses anonymous sender address $?A_i$ to send his public key for round $K_{A_i}$ and prearranged bid $b_i$ encrypted with $K_S$ to S.
   n. **Final round (after timeout)**: S broadcasts to all bidders in $D$ the highest bid $b_{n−1}$ and the secret message with the $MeetingAppointment$. This broadcast message is encrypted with the public key $K_{A_{n−1}}$ of the winner of round $n − 1$ that S got from winning round $n − 1$. 
Sweetheart Deal and Collusion

• **Sweetheart deal**: seller S and a bidder (his “sweetheart”) agree before the auction that S sells the good to sweetheart.

• **Collusion**: bidders collude against S.

⇒ it looks as if there were many but colluding bidders count only as one.

• Both attacks involve Insiders

• Insider threat guide CMU-CERT [10]: Ambitious leader pattern is a collusion

⇒ Isabelle Insider framework application example
The Inductive Approach

- Model communication scenario including attacker (Dolev-Yao) in Isabelle
- Proof properties like authentication and key knowledge of agents
- Principals as datatypes
  \[
  \text{datatype agent} = \text{Server} \mid \text{Friend nat} \mid \text{Spy}
  \]
- Recursive datatype \texttt{msg} of messages
  \[
  \text{datatype msg} = \text{Agent agent} \mid \text{Number nat} \mid \text{Nonce nat} \mid \text{Key key} \mid \text{MPair msg msg} \mid \text{Crypt key msg}
  \]
Formalising CAP with Inductive Approach

- **Inductive set**
  
  \[\text{inductive\_set\ cocaine\_auction} :: \text{event list set}\]

  with base case
  
  \[\text{Nil:} \; [] \in \text{cocaine\_auction}\]

- **Step 0:**
  
  \[\text{CA0:} \; [\text{Says Server (Friend } i) \; (\text{Key(pubK Server))}. \; i \leftarrow [0..<\text{friends}]] \in \text{cocaine\_auction}\]

- **Final round CAn**
  
  \[\text{CAn:} \; \text{evs} \in \text{cocaine\_auction} \implies \]
  
  \[\text{evs} = \text{Says (Friend friends) Server} \; \text{Crypt (pubK Server) \{Key(pubK(Friend } j)), Number(bid } i)\}}\]
  
  \[# \; [\text{Says (Friend friends)(Friend } k) \; \text{Key(pubK(Friend } j)), Number(bid } i)\}].\]

  \[k \leftarrow [0..<\text{friends}]] @ \text{evsf}\]

  \[\implies [\text{Says Server (Friend } k) \; \text{Crypt (pubK(Friend } j)) \; \{\text{Number(bid } i), \text{Number mtng}\}].\]

  \[k \leftarrow [0..<\text{friends}]]\]

  \[@ \; \text{evs} \in \; \text{cocaine\_auction}\]
No Sweetheart Deal

Theorem (No sweetheart deal)

*If a cocaine auction ends with a broadcast by the Server that the bidder Friend j is the winner, then the trace evs prior to this must have been a broadcast of Friend j.*

\[
0 < \text{friends} \implies [\text{Says Server (Friend k)} (\text{Crypt (pubK (Friend j))} \{\text{Number(bid i)}, \text{Number mtng}\})].
\]

\[
k \leftarrow [0.. < \text{friends}]
\]

\[
@ \text{evs} \in \text{cocaine_auction} \implies \exists \text{evsf. evs} = \text{Says (Friend friends) Server (Crypt (pubK Server) \{Key(pubK(Friend j)), \text{Number(bid i)}\})}
\]

# [\text{Says Server (Friend k)} (\text{Crypt (pubK Server) \{Key(pubK(Friend j)), \text{Number(bid i)}\})].

\[
k \leftarrow [0.. < \text{friends}]
\]

\[
@ \text{evsf}
\]
Rational Insider: Homo Oeconomicus

- **Homo oeconomicus**: agent $a$ will not spend more than necessary to get an asset, i.e., if $a$ can get the asset for price $X$, he will not pay price $Y > X$ to get it.
- Additional use of Isabelle Insider framework allows assuming impersonation

$\Rightarrow$ Insider can impersonate other bidders.

**Theorem (Collusion Inevitable)**

*Let one bidder, Friend 0, be an insider and at the tipping point, then the insider can impersonate any bidder, i.e., they can act as one and the seller only gets the reserve price bid 1.*

$homo_{oeconomicus} \Rightarrow tipping\_point(astate \ 0) \\
\Rightarrow Insider \ 0 \ \{i. \ i < friends\} \Rightarrow \forall \ t \in cocaine\_auction. \ \\
t = [Says \ Server \ (Friend \ k) \ (Crypt \ (pubK(Friend \ j)) \ \{Number(bid \ i), \ Number \ msg\}). \ k \leftarrow [0..<friends]] \ \\
@ evs \\
\rightarrow i = 1$
Results

- Formal model of the Cocaine Auction Protocol in Isabelle
  - Proof of absence of sweetheart deals
  - Proof of impossibility to exclude collusion.
- Conceptual improvements
  - Inductive approach to security protocols: formalisation of arbitrary numbers of rounds, broadcast, and anonymous message sending
  - Integrating the Isabelle insider framework with the inductive approach enables reasoning about collusion of insiders for auctions.
  - The collusion exhibits that the assumption *homo oeconomicus* suffices to prove that rational insiders may use collusion to force the reserve price.

**New** Extended Paper for special issue: *Generating executable Scala code for identifying secure Cocaine Auction Protocol traces*
Current Projects for Practical Application

CHIST-ERA (EU) project SUCCESS: SecUre aCCESSibility for the internet of things (IoT)

- Formal design of privacy-critical IoT scenarios
- Risk visualisation by attack trees
- Certified implementation for IoT component architectures
- IoT Pilot scenario: sensor based monitoring for dementia patients
• Using Isabelle Higher Order Logic allows expression of
  • Infrastructure
  • Policies and protocols
  • Human aspects

• Downside: proofs are interactive
  \[\Rightarrow\] Enables expression of rich models and machine-supported proof of properties (safety, security, etc)
  \[\Rightarrow\] Enables code generation

• Project SUCCESS for Security and Privacy of IoT


References II


Model Checking

- Turing Award for Model Checking (2007)
- Fully automated technique for mathematical verification of state based systems
- Specify Model as a finite state transition system
- Natural specification of system properties with so-called “temporal logics”

\[ \text{AG send} \implies (X \text{ receive}) : \text{send is always followed by receive}\]

\[ \implies \text{Other modalities possible: e.g. probabilities or epistemic logic, i.e. “beliefs”}\]
Interactive Theorem Proving (ITP)

Higher Order Logic (B. Russell): expressive but undecidable ⇒ ITP

Applications in CS:
- Certified C-compiler in Coq (CompCert, INRIA)
- Java in Isabelle/HOL (TU München)
- L4-kernel in Isabelle/HOL (NICTA, Sidney)

Applications in Mathematics:
- Mechanized proof of 4-colour theorem in Coq (G. Gonthier, INRIA/MSR)
- Keppler’s conjecture in Isabelle (T. Nipkow, TU München)
Verification of Security

Security problems automated verification can deal with:

- **Application: Security Protocols**
  - **Authentication**: proof of identity
  - **Key agreement**: negotiate session keys
  - Automated verification finds bugs in established protocols
    - *Man-in-the-Middle* attacks (CSP/FDR/Isabelle inductive approach)
    - DNSsec in Isabelle/HOL [4]
    - Quantum Cryptography in Coq [8]
    - Social networks [5]

- **Application: Information Flow Security**
  - Discover implicit flows (covert channels) in program code
    - \[ \text{if } x_H = 1 \text{ then } y_L := 1 \text{ else } y_L := 0 \text{ end} \]
  - Security Type System for ASPfun [6]
  - Static analysis of Noninterference [12]

- **Application Insider Attacks** (necessitates modeling human behaviour)[4,10]