Overview of Analysis Methods for Re-Trust

Amitabh Saxena

University of Trento

Italy

Why Analysis?

- Evaluate effectiveness of proposed solutions.
- Evaluate overhead of proposed solutions
  - Is it really worthwhile to use technique X?
- Discover any weaknesses in our Trust model.
- To write Deliverables 4.1, 4.2, 4.3

Layout of Talk

- Expected outcome
- Trust Model
- Attack Model
- Attack Goals
- Summary of current work
  - Discussion of attack methods
  - Empirical studies
- Directions for future work
- Questions/discussion

Expected Outcome

- A rigorous methodology to evaluate solutions of Re-Trust
  - At high level, obtain some metrics
    - *"Approach X is 80% reliable for problem Y"*
    - *"Approach X satisfies goal Y"*
    - *"Approach X fails under attack Y"*
    - *"Approach X fails after time Y"*
    - *"Approach X guarantees security for time Y"*
- Need clear(er) understanding of "goals" and what it means to "guarantee security"

Trust Model (D2.1/3.1)

- What can and cannot be trusted.
  - "Should we trust the OS?"
- Up to what level can it be trusted?
  - "Alice will not disclose her (symmetric) key but might provide access to decryption oracle."
- Attacker is not trusted at all.
  - Cannot make any assumptions on its behavior

Attack Model

- What the attacker can and cannot do
- Who is the attacker ?
  - NSA may be difficult to protect from
  - Next-door neighbor might not pose much threat
- Formulate notion of “reasonable” attacker
  - Computing resources
  - Human resources
- Formulate value of assets to be protected
  - What can be gained by a successful attack?

Attack Goals

- Need reasonable formalization of goals such that analysis can be carried out
- At present attack goals not very clear
  - Likely to depend on entrusting agent
  - May depend on type of application
  - May depend on the design philosophy of application
  - May depend on business model

Attack Goals (contd.)

- Attack goals could possibly be defined based on business goals
  - Typical business goals:
    - "Cannot make free calls using Skype"
    - "Cannot play media more than 3 times"
  - Attack goal is to defeat business goal(s)
- Business goals very application specific
  - Difficult to do generic analysis
  - Need a formal method (language) to describe

Attack Goals (contd.)

- Attack goals must be defined so as to capture the strongest level of security.
- Consider, for instance, WB crypto.
  - G1: “*Attacker cannot extract embedded key*”
    - Is it strong enough? Maybe not!
      Attacker might be able to decrypt without the key
  - G2: “*Attacker cannot obtain any information about the plaintext, given the ciphertext*”
- G2 is a more reasonable goal.

Attack Methods

- Although attack goals not very clear, we have a reasonable notion of the attack methods to achieve these goals (whatever they may be).
- Attack methods classified at a high level:
  - **Reverse engineering and direct code modification**
  - **Modification of execution environment**
  - **Dynamic state-change attack**
  - **Memory-copy attack**
  - **Network attack** (intercept, delete, insert messages)
  - *Application specific attacks*

Attack Methods (contd.)

- At this stage, instead of focusing on attack goals, we are focusing on attack methods
  - Solutions designed to disable certain attacks
    - Analogous to modern medicine – Most doctors prescribe medicines to alleviate symptoms rather than the actual ailment
    - However, it is still good enough for a start.
  - Solutions evaluated w.r.t. attack methods.
    - Currently no efficient solution to bypass all attacks.

Empirical Studies

- Many of the proposed solutions are based on some sort of obfuscation
- One of the tasks is to analyze the complexity of "reverse engineering" obfuscated programs
- Empirical study underway
  - Based on specific application, attack model and limited attack resources
  - Nevertheless, may help in extrapolating results
  - Might be useful in developing some metrics

Lessons Learned

- Attack goals are likely to be app specific, so a "generic solution" for Re-Trust seems difficult.
  - May be easier to instead focus on attack methods
- Take environment into account for certain apps
  - TCP window size depends on network traffic
    - Need to monitor network traffic in addition to protocol stack
  - Interface between program-environment exploitable
    - Obfuscation will not help here
- Composition of solutions may not be possible
  - Eg. barrier slicing is incompatible with obfuscation

Current/Future Research

- Define high-level generic attack goals:
  - Tamper-resistance of programs (important but tricky)
  - Confidentiality of programs
  - Correct input/Correct output
  - Privacy of program inputs
  - Undebuggability
- Develop techniques for modeling business requirements of Re-Trust applications.
  - Using "game-based" techniques (Eg. IND-CCA2 encryption)
- Composition of different solutions
  - Are they still secure (or work) when combined?
- Clearly defined criteria to decide if an application or goal is "outside the scope" of Re-Trust

Summary

- Need to formalize key concepts
  - Business requirements
  - What does it mean for a program to be “tamper resistant”?
- Existing solutions for Re-Trust do not enjoy the same benefits as conventional crypto:
  - Crypto:
    - Security independent of attacker (all or nothing security)
    - Concrete metrics (provable under reasonable assumptions)
  - Re-Trust
    - Security depends on attacker resources (something or nothing)
    - Fuzzy security, with metrics based on empirical data
- Depending on value of assets protected and the incurred overhead, some solutions may not be worthwhile
  - Eg., Barrier slicing may be too expensive for some apps
- DRM-type apps may need H/W-based solutions
  - If stakes are very high