Improving Security Decision under Uncertainty: A Multidisciplinary Approach

Hashem Dehghanniri, Emmanuel Letier, Hervé Borrion
University College London, the UK
Security Decision under Uncertainty

• Which decision to make?
Security Decision under Uncertainty

• Which decision to make?
• Security Decision
  – A critical task at different stages of a system’s life cycle
Security Decision under Uncertainty

• Which decision to make?
• Security Decision
  – A critical task at different stages of a system’s life cycle
• Uncertainty
  – Complicates selection process
Security Decision under Uncertainty

• Which decision to make?

• Security Decision
  – A critical task at different stages of a system’s life cycle

• Uncertainty
  – Complicates selection process

• What is the result of each decision option?
How the previous works dealt with Decision Making

• What are the important factors in decision making?
  – Analytic Hierarchy Process (Saaty - 1990)

• What are the cost and benefit of each decision option?
  – Cost Benefit Analysis Method (Moore, Kazman, Klein, and Asundi - 2003)

• How to deal with uncertainty?
  – Modelling and analysing uncertainty (Letier, Stefan, and Barr - 2013)

• How to model a security risk?
  – How security risk scenarios should be formulated (Le Sage, Toubaline, and Borrion - 2013).

• However, the previous works have not:
  – Focused on security decision making,
  – Evaluated the effects of each decision option on the stakeholders’ goals and the attack process.
Integrated Resolution Action Effect Evaluation Framework

Providing Input

Risk Analysis
- Consequence Analysis
- Crime Script Structuring

Resolution Action Identification

Resolution Action Evaluation

Scope of the Project

Resolution Action Effects Evaluation
- Assessing the Effect of Resolutions on the Crime Script Steps
- Modelling the Effect of Resolutions on the Stakeholders’ Goals, the Crime Script and the Attacker

Decision-making

Reasoning about the Resolution Actions and Selecting Optimal Resolutions

Stakeholders and their Goals Identification
Illustrative Example

• Identity theft
Illustrative Example

• Identity theft
  – Setting up a credit card using a stolen identity

I didn’t buy that!
Providing Input

- Risk Identification
  - Consequence Analysis
  - Crime Script Structuring
  - Resolution Action Identification
  - Resolution Action Evaluation

Stakeholders and their Goals Identification
Providing Input:
Stakeholders and their Goals Identification

A partial security goal model for a credit card company.
Providing Input: Risk Identification

<table>
<thead>
<tr>
<th>Risk</th>
<th>setting up a credit card using a stolen identity risk’s details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible target</td>
<td>the victim’s credit</td>
</tr>
<tr>
<td>Description</td>
<td>One stranger can overtake a person personal details to open a credit card account. Then he collects the credit card, from the delivery point, and spend the victim’s credit, which will be debited from him/her.</td>
</tr>
</tbody>
</table>
Providing Input: Crime Script Structuring

I'll just tell them my legs are tired

So they have to carry me for the rest of the trip
## Providing Input: Crime Script Structuring

<table>
<thead>
<tr>
<th>CRIME SCRIPT</th>
<th>SCRIPT ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SCRIPT SCENE/FUNCTIONS</strong></td>
<td><strong>SCRIPT ACTIONS</strong></td>
</tr>
</tbody>
</table>
| PRE-CONDITION | selecting the victim  
collecting the victim’s personal details  
selecting a credit card company  
placing the order  
waiting for the delivery  
checking the delivery address to collect the card  
collecting the card  
activating the card |
| DOING | using the card’s credit |
| POST-CONDITION | destroying the card  
v vanishing other traces |
Providing Input: Resolution Actions Identification and Evaluation

- **Authenticating the Customers in a Bank Branch**: a new released credit card can only be used after activation in a branch by the credit card holders,
- **Authenticating the Customers using their Online Banking Account**: this resolution requires the credit card holders to activate their credit card using an existing online banking account - with the name of the credit card holder.
Providing Input:
Resolution Actions Identification and Evaluation

- **Authenticating the Customers in a Bank Branch:** a new released credit card can only be used after activation in a branch by the credit card holders,
- **Authenticating the Customers using their Online Banking Account:** this resolution requires the credit card holders to activate their credit card using an existing online banking account - with the name of the credit card holder.

The value of the identified resolution actions:

<table>
<thead>
<tr>
<th></th>
<th>Resolution 1</th>
<th>Resolution 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>value</strong></td>
<td>$\sim -3 \times 10^{-2}$</td>
<td>$\sim 6 \times 10^{-2}$</td>
</tr>
</tbody>
</table>
Resolution Action Effects Evaluation

Scope of the Project

Resolution Action Effects Evaluation

Assessing the Effect of Resolutions on the Crime Script Steps

Modelling the Effect of Resolutions on the Stakeholders' Goals, the Crime Script and the Attacker
## Resolution Action Effects Evaluation: Assessing the Effect of Resolutions on the Crime Script Steps

<table>
<thead>
<tr>
<th>CRIME SCRIPT</th>
<th>SCRIPT ACTIONS</th>
<th>RESOLUTION’S EFFECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRE-CONDITION</td>
<td></td>
<td>authentication in a bank branch</td>
</tr>
<tr>
<td></td>
<td>selecting the victim</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>collecting the victim’s personal details</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>selecting a credit card company</td>
<td>Deter-known</td>
</tr>
<tr>
<td></td>
<td>placing the order</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>waiting for the delivery</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>checking the delivery address to collect the card</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>collecting the card</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>activating the card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>using the card’s credit</td>
<td></td>
</tr>
<tr>
<td>DOING</td>
<td>destroying the card</td>
<td></td>
</tr>
<tr>
<td>POST-CONDITION</td>
<td>vanishing other traces</td>
<td></td>
</tr>
</tbody>
</table>
Resolution Action Effects Evaluation: Modelling the Effect of Resolutions on the Stakeholders’ Goals, the Crime Script, and the Attacker

* value, here, indicates how much this resolution adds to the business, for any £100 spending on credit cards

Acquire money

outcome

the offender

satisfies

setting up a credit card using a stolen identity

stops by 99.9%

authenticates in 2 situations

acts

the victim

affects

resolution action

authentication in a bank branch

value = 0.06*

acts

avoid unauthorised person to open an account

is interested

is interested

easy identity check

contributes

has negative effect

contributes

has negative effect

resolution action

goal

outcome

crime script

resolution action

Legend
Decision Making

Reasoning about the Resolution
Actions and Selecting Optimal Resolutions
Decision Making:
Reasoning about the Resolution Actions and Selecting Optimal Resolutions

* value, here, indicates how much this resolution adds to the business, for any £100 spending on credit cards.
Decision Making: Reasoning about the Resolution Actions and Selecting Optimal Resolutions

* value, here, indicates how much this resolution adds to the business, for any £100 spending on credit cards.
Decision Making: Reasoning about the Resolution Actions and Selecting Optimal Resolutions

* value, here, indicates how much this resolution adds to the business, for any £100 spending on credit cards.

- Acquire money
- outcome
- the offender
- satisfies
- setting up a credit card using a stolen identity
- affects
- the victim
- acts
- authentication using an online bank account
  - stops by 90%
  - obstructs in 2 situations
  - acts
  - avoidance of unauthorised person to open an account
  - is interested
  - is interested
- easy identity check
- acts
- authentication in a bank branch
  - stops by 99.9%
  - obstructs in 2 situations
  - acts
  - contributes
  - has negative effect
- value = 0.06*
- value = -0.03*
Conclusion

• Novelty
  – A multidisciplinary framework
    • software engineering, crime script, risk assessment
  – for security decision making process
  – that assesses decision options’ affects on
    • the stakeholders’ goals,
    • the crime process, and
    • the attacker.

• Using the result of the framework
  – Decision makers would expect to have a clearer understanding about the outcome of each resolution action, and make decision more confidently.
Future Work

• Examine the framework using more complex industrial case studies

• Investigating the factor that influence the decision making process

• Providing validation techniques to assess the quality of Crime Scripts
Future Work

• Examine the framework using more complex industrial case studies
• Investigating the factor that influence the decision making process
• Providing validation techniques to assess the quality of Crime Scripts
References


Improving Security Decision under Uncertainty: A Multidisciplinary Approach

Hashem Dehghanniri, Emmanuel Letier, Hervé Borrion
University College London, the UK