Improving Security Decision under Uncertainty: A Multidisciplinary Approach

Hashem Dehghanniri[1], Emmanuel Letier[2], Hervé Borrion[1]

[1]Department of Security and Crime Science
University College London
35 Tavistock Square, London WC1H 9EZ
{h.dehghanniri.12, h.borrion}@ucl.ac.uk

[2]Department of Computer Science
University College London
Gower Street, London WC1E 6BT
e.letier@cs.ucl.ac.uk

ABSTRACT

Security decision-making is a critical task in tackling security threats affecting a system or process. It often involves selecting a suitable resolution action to tackle an identified security risk. To support this selection process, decision-makers should be able to evaluate and compare available decision options. This article introduces a modelling language that can be used to represent the effects of resolution actions on the stakeholders' goals, the crime process, and the attacker. In order to reach this aim, we develop a multidisciplinary framework that combines existing knowledge from the fields of software engineering, crime science, risk assessment, and quantitative decision analysis. The framework is illustrated through an application to a case of identity theft.

Keywords*: security; requirements engineering; decision-making; risk; crime script; uncertainty; identity theft*

I. INTRODUCTION

Security decision-making often involves choosing amongst different alternatives to tackle a security problem. This is a complex activity encountered in the production and maintenance of any system comprising valuable assets. It appears at different stages of a system's life cycle, from early requirements analysis to system design, through implementation and maintenance. In all of these stages there may be different alternatives available, each with pros and cons from a security perspective. Although it has been accepted that we could never have a completely secure system [3], the security of a system can generally be improved, with quality improvement resulting from better decisions.

Decision-making is a problem encountered in different fields. Various studies

have been conducted to tackle it, often focusing on representation and management of uncertainty. Saaty introduced the Analytic Hierarchy Process (AHP) for decision-making, which focuses on the important factors that are needed to improve decision-making [4]. Moore, Kazman, Klein, and Asundi introduced a Cost Benefit Analysis Method (CBAM), which involves estimating the value of architectural strategies to support the decision-making process [5]. Letier, Stefan, and Barr argued that modelling uncertainty and mathematically analysing its consequences lead to better decisions than either hiding uncertainty behind point-based estimates or treating uncertainty qualitatively as an inherently uncontrollable aspect of software development [6]. Veerappa and Letier addressed a gap in understanding variations between solutions in the design space to support decision-makers [7]. Mylopoulos, Chung, Liao, Wang, and Yu contributed to the development of concepts, and modelling techniques for the evaluation of alternative system options in the heart of requirements engineering process [8]. Lamsweerde assessed the relation between requirements options and leaves goals in goal graphs to improve decision-making process [9]. Nunes-Vaz, Lord, and Ciuk introduced a framework that can be used to relate the security measures to the desired security performance [10]. Le Sage, Toubaline, and Borrion discussed how security risk scenarios should be formulated [11] to make the relation between offender's actions, offender's goals and the system's anti-goals more explicit. Other studies have focused on techniques for eliciting, analysing and modelling security requirements, and quantitative decision analysis including trade-off analysis among requirements [12], categorising and prioritising security requirements [13], discussing constraints and satisfaction of arguments [14], systematic support for analysing security trade-offs to achieve a good-enough security level [15], formal modelling and analysis of security requirements [16], and emphasising the role of quantitative assessment in risk management [17]. These efforts have provided valuable knowledge to support decision-making. However, evaluating the level of goodness of different security resolution actions (i.e., alternatives) remains a challenging task.

This research aims to introduce a modelling language to represent the effects of resolution actions on the stakeholders' goals, the crime process, and the attacker - the term *attacker* is used to represent a single offender or a group committing the crime. In order to reach this aim, we develop a multidisciplinary security decision-making framework that combines existing knowledge from the fields of software engineering, crime science, risk assessment, and quantitative decision analysis. This framework supports the following activities:

- identifying the stakeholders, and their security goals using security requirements engineering techniques,

- characterising the identified attack using the concept of crime scripts from crime science,
- measuring the identified resolution actions using quantitative decision analysis techniques,
- relating the identified resolution actions to different situations modelled in the crime script. The result of this stage improves the decision-makers' understanding about the effect of each resolution on the crime process,
- defining a modelling language that integrates the results of the above stages to identify the most cost-effective security resolution. This modelling language evaluates the effects of the identified resolution actions on the stakeholders' goals, the crime script, and the attacker.

Section II provides a brief overview of the various components that form the framework including techniques for identifying stakeholders and modelling goals, risk assessment techniques, and crime scripting techniques. Section III describes how these components are integrated together. It comprises the framework that is used to generate the conceptual model representing the relation between the main entities of a security risk problem. Section IV illustrates the application of the framework through a case study concerning identity theft - a significant problem that causes approximately £52 billion per annum to the UK [18]. Finally the article ends with a conclusion and future work in Section V.

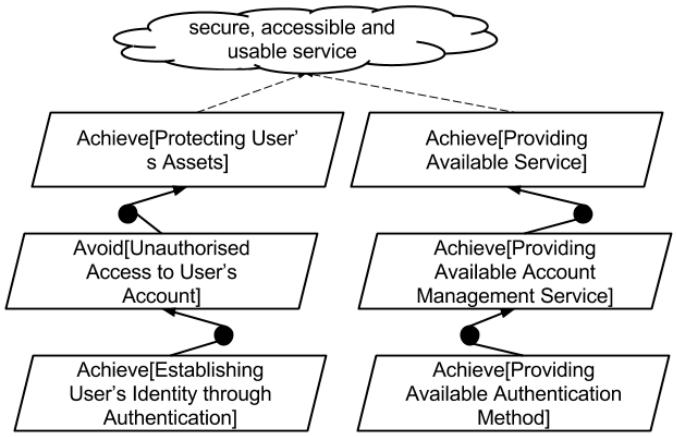

Figure 1: A partial security goal model for a credit card company

II. BACKGROUND

Decision-making under uncertainty is a common problem in different disciplines. The current research aims to address this problem using an integrated approach that involves software engineering, risk assessment, crime scripting, and quantitative decision analysis techniques.

A. Software Engineering

Software engineering (SE) techniques are used to identify stakeholders, their goals, and create a modelling language.

Security Requirements Engineering: in order to evaluate the effects of resolution actions on the security goals of the stakeholders, the goals must first be identified. For this, security requirements engineering techniques can be used.

Table I: *setting up a credit card using a stolen identity* risk's details

Risk	setting up a credit card using a stolen identity
Possible target	the victim's credit
Description	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 [2]

By security goals and requirements, we mean those goals and requirements that relate to the protection of the system's assets against malicious behaviours. A necessary condition for a system to be secure is that all application-specific security requirements should be met by the system [19]. They need to be explicit, precise, adequate, measurable, complete, and non-conflicting with other requirements [14, 16, 20]. Using a credit card company as an example, a security goal for this company can be *avoiding unauthorised access to the user's account*.

Goal Modelling: in our approach, we use GORE (Goal-oriented Requirements Engineering) to elicit and model stakeholders' goals. Leveraging our experience of GORE and SE, we design a modelling language that relates the identified resolution actions to the stakeholders' goals and the attack process.

A goal is an objective the system under consideration should achieve. The benefit of goal modelling is to support heuristic, qualitative, or formal reasoning schemes during requirements elicitation. GORE is based on multi-view model showing how goals, objects, agents, scenarios, operations, and domain properties are inter-related in the system-as-is and the system-to-be. Goals are prescriptive statements of intent whose satisfaction requires the cooperation of agents (or active components), in a software/system and its environment [9, 20-23]. Figure 1 demonstrates a partial

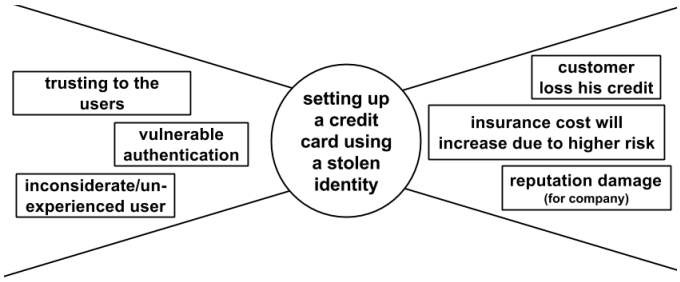

Figure 2: A bow-tie diagram for *setting up a credit card using a stolen identity risk*

security goal model for a credit card company.

B. Risk Assessment

In our framework, which is introduced in Section III, we use risk assessment (RA) techniques in *providing input* stage. RA includes three activities: *Risk Identification*, *Risk Analysis*, and *Risk Evaluation* [24]. This paper uses the first two to identify and describe the security risks that a system encounters.

TABLE II the D terms that are used in this paper, the complete list of 11 D techniques can be found in [1]

Defeat	"block access and movement or block/obscure the information that offenders want to collect"
Deter-known	"offenders know what the risk of exposure is, and judge it unacceptable so abandon/ abort HR attempt"
Deter-unknown	offenders are uncertain what control methods they are up against, so judge risk of exposure unacceptable

Risk Identification: risk identification is prerequisite of risk treatment. It provides awareness of possible events that could impact negatively on the objective(s) of a system/process and the goals of the stakeholders [9, 24]. This article focuses on the risks that are identified by the stakeholders. Table I shows an identified risk including its description and the target of the attack.

Risk Analysis: risk analysis aims to identify and characterise the scenarios that include the identified risk events. For this, different techniques can be used to analyse their causes and consequences, also using concepts of threats and vulnerability. More information about risk analysis and the details of different activities and mechanism can be found in [24]. The described framework uses consequence analysis and crime script; the former is described in continue, and the latter is defined in Section II-C.

Consequence Analysis: in this stage, an analysis is carried out that models the possible consequences of the identified risk events [24]. A forward approach is used where the risk analysis begins with the identification of initiating events (the hazard, the event, or the opportunity). Thereafter, the consequences of the various events are analysed to identify relevant events and associated scenarios. Figure 2 shows a consequence analysis for the following risk event: *setting up a credit card using a stolen identity* risk. As explained in [24], this bow-tie diagram represents the initiating event (in the middle), its causes (left), and consequences (right). As it can be seen in Figure 2, the main consequence of the mentioned event is *financial loss*. This includes the compensation of the stolen credit and the overhead costs. This consequence conflicts with one of the security goals of a credit card company, which is *protecting user's asset*.

CRIME SCRIPT

This article uses Cornish's crime script (CS) model to represent the attack process [25] This model is also used to describe the effect of the identified resolution actions, and better understand the mechanisms activated by the resolutions to affect the attacker's activities.

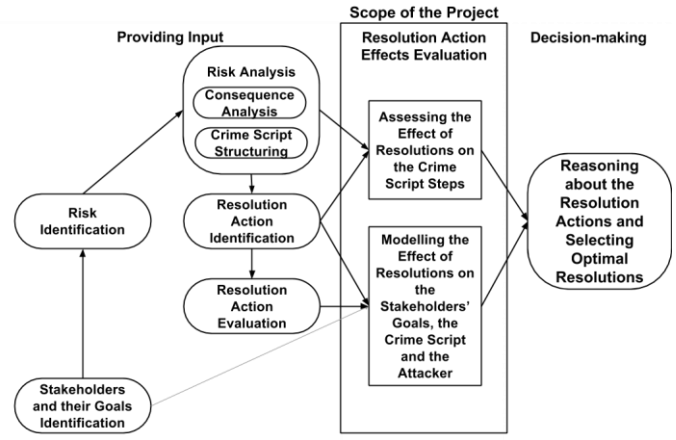

Figure 3: overview of the proposed framework

"Crime scripts hold this innovative capacity of untangling very complex forms of crime by breaking down the crime-commission process into different steps" [26]. A CS represents the complete sequence of actions adopted prior to, during, and following crime commission. The most significant benefit of the crime script concept is that it provides a framework to systematically investigate all of the stages of the crime commission process of a specific crime and in as much details as existing data allow [25-31].

CS is used in crime science to improve the understanding about how certain types of crime occur. It also offers a way to develop Situational Crime Prevention (SCP) techniques, as described in [29, 32].

There exist different SCP techniques. Ekblom and Hirchfield introduced the *11 Ds*, which refer to high level principles that could be adopted to influence an offender's decisions [1]. In our framework, we use the 11 Ds to describe and analyse how (and when) a resolution action affects a particular crime script. Table II lists the principles that are used in this paper,

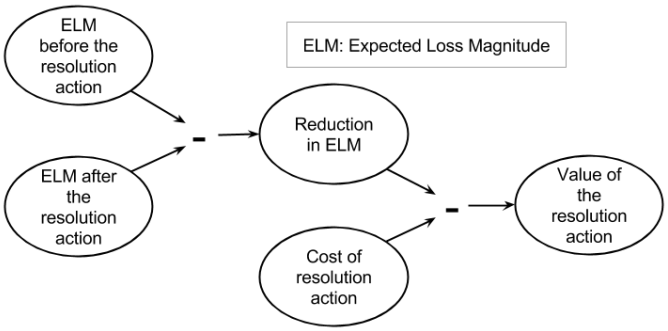

Figure 4: calculation of the value of a resolution action

borrowing from the SCP terminology.

In criminology and crime science, CS is mostly used for crime representation and resolution action identification [26, 27, 33-38]. Here, we assume that the resolution actions have already been identified and we want to assess their effects on the crime process. This is carried out by relating the resolutions to the CS, and investigate in which situations those resolutions would obstruct the CS.

III. INTEGRATED RESOLUTION ACTION EFFECT EVALUATION FRAMEWORK

Figure 3 shows the overall picture of our proposed framework. It comprises three phases, which are *Providing Input*, *Resolution Actions Effect Evaluation*, and *Decision-making*.

A. Providing Input

The data required for our evaluation is provided in this phase, using the techniques introduced in Section II. As it can be seen in Figure 3 this phase includes the following tasks:

Stakeholders and Goals Identification, where the main stakeholders of the system and their goals are identified. The main stakeholders can be the victim, or someone for whom the mitigation actions are designed. Although the main focus is on the security goals, the related goals and requirements from the entire organisation must also be considered, not just system-as-is or system-to-be, as mentioned in [16]. The result of this stage is used in *Risk Identification* and *Resolutions' Effect Evaluation*.

Risk Identification is described in Section II-B.

Risk Analysis is described in Sections II-B and II-C. It has two main stages:

- **Consequence Analysis**, where the main consequences of the risk are identified. The result is used in the next steps to calculate the expected loss magnitude, and assess the value of the resolution actions,
- **Crime Script Structuring**, where the identified risk and corresponding crime script(s) are modelled.

Resolution Action Identification consists of identifying possible resolutions to reduce the identified risk. In this article we assume that resolution actions are identified, for instance, by a security consultant or the victim, and that one of them must be selected by a decision-maker for implementation.

Resolution Action Evaluation is a quantitative estimation of the benefits that would be obtained by implementing the proposed resolution actions. The value of each choice is calculated for a specific period of time. Figure 4 illustrates the principle of this calculation, with:

- the estimated reduction in expected loss magnitude (EML) caused by implementing the action, and
- the estimated cost of executing the action.

This formula is applied using the quantitative analyses found in related studies [5, 6, 24]. In this calculation, we consider the uncertainty about the estimated numbers and use a range of values instead of point estimates, where applicable. The result indicates whether an action is cost-effective and how much reduction the action introduces to the risk magnitude.

B. RESOLUTION ACTIONS EFFECTS' EVALUATION

This phase covers the main evaluation applied to the inputs in order to support the process of decision-making under uncertainty. Two steps are used to assess the effect of the resolution actions on the stakeholders' goals, the crime script, and the attacker:

Assessing the Effect of the Identified Resolution Actions on the Crime Script: in this step we investigate in which situations the crime process is obstructed by the resolution actions. This evaluation provides a picture of how risk is mitigated by the resolution actions. This improves the decision-makers' understanding of the effect(s) of the resolution actions on the crime script and the attacker. We use this result in the conceptual model, which is explained later.

Modelling the effect of the Identified Resolution Actions on the Stakeholders' Goals, the Crime Script, and the Attacker: this step provides an overall picture of the relations between the identified resolution actions

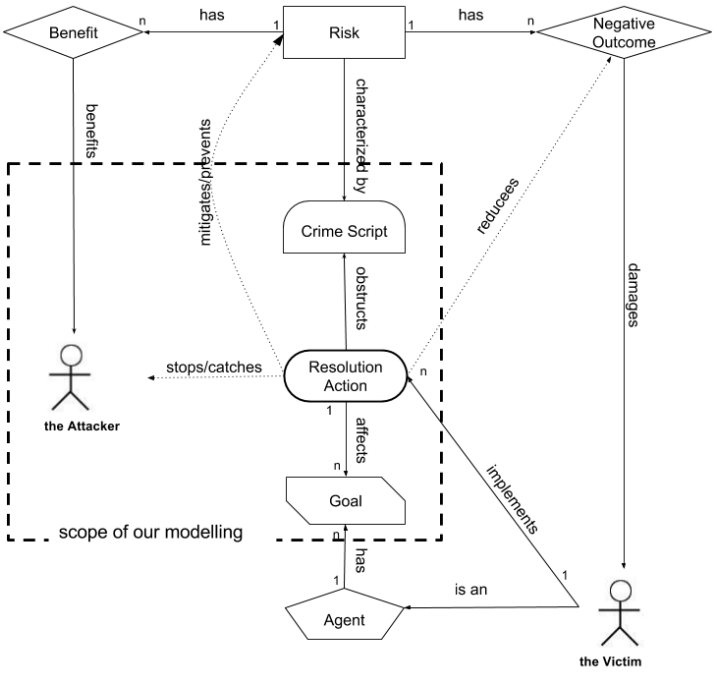

Figure 5: overall picture of the relation between a resolution action and its related entities in our proposed framework

and the entities they affect. These entities include the victim, the victim's goals, the offender, the offender's goals, the attack, and the attack's crime script. Figure 5 illustrates an overall picture of the relationships between the resolution actions and the aforementioned entities. It also shows the scope of our model, which covers the resolution actions, the stakeholders' goals, the crime script, and the attacker.

Figure 5 is designed using the modelling techniques from software engineering. This overall model shows how the main elements of the framework relate to each other. The elements that are located within the scope of our modelling language are:

- the victim's goals, which are the victims security goals. The satisfaction level of these goals has to be improved by implementing the resolution actions,
- the attacker whose actions threaten satisfaction of the victim's security goals,
- the resolution that are identified by the victim to mitigate the current risk or to obstruct the crime script, and
- the crime script that shows the sequence of actions taken by the attacker.

C. Decision-making

In this phase, decision-makers use the gained results to decide which resolution action should be implemented. The outputs of the framework is expected to improve decision-makers' understanding of:

- situations/steps in which each resolution action obstructs the crime script,
- how each resolution action contributes to satisfy the stakeholder's security goals,
- whether all resolution actions introduce the same (negative or positive) effect on different goals,
- the effect of each resolution action is on the attacker.

IV. ILLUSTRATIVE APPLICATION OF THE FRAMEWORK

In this section, we demonstrate the applicability of our framework using a case of *identity theft*[1].

Case Study: ***Setting up a Credit Card using a Stolen Identity***

The selected case study is an identity theft risk against credit card companies and their customers, which was described in Table I. The above framework is applied to a couple of resolutions

TABLE III: the value of the identified resolution actions

	Resolution 1	**Resolution 2**
value	$\sim -3.10^{-2}$	$\sim 6.10^{-2}$

1 The full case study is available at http://www.homepages.ucl.ac.uk/~ucabdeh/BIT.htm

that are considered to tackle this crime. The framework allows the effects of the alternatives to be evaluated on the victim's goals and the crime process.

A. Providing Input

The data needed for the evaluation is provided in this phase, as shown in Figure 3:
The main stakeholder is the credit card company. It identifies and implements the resolution actions,
The stakeholder's related goals are shown in Figure 1. We also consider *Maximising Profit* as an overall goal of the company,
The identified risk is stated in Table I,
The risk's consequences are represented in Figure 2,
The crime script is detailed in Table IV,
Resolution Action Identification generates two alternatives:

- *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.

Resolution Action Evaluation provides information about the gain obtained by implementing the different resolutions. Table III provides a summary of the hypothetical results that could be obtained by applying the formula in Figure 4. In this document, we show the result of the Providing Input phase; the complete case study is available online[1].

B. Resolution Actions' Effect Evaluation

The framework is applied to assess the effects of each resolution on the crime script. The results from all the previous stages are then used to draw a conceptual model that shows the effects of every solution on the stakeholder's goals, the attacker, and the attack process.
Assessing the Effect of the Identified Resolution Actions on the Crime Script: Table 4 illustrates how the identified resolution actions can affect the crime script:

- the first resolution action hardens the attack process and obstructs the crime script in two steps:
  - in the *precondition* step, an informed offender would not select a credit card from a company that will request to prove their identity. This obstruction is based on the *Deter-known* principle, as described in Table 2, and would work if offenders are aware of it.
  - in the *doing* step, when the offender wants to activate the credit card, they would be required to prove their identity. This obstruction is based on a *Defeat* principle, and prevent them to activate the credit card.

- the second resolution action hardens the attack process in two steps. In both the steps, the effects are same as the previous resolution. However, the chance of success of this resolution is estimated to be smaller than the previous resolution. This is because providing access to the victim's online bank credentials is more likely than proving the identity in person.

TABLE IV: credit card identity theft's crime script and the effect of the resolution actions on that (X: no effect)

CRIME SCRIPT		**RESOLUTION'S EFFECT**	
SCRIPT SCENE/FUNCTION	**SCRIPT ACTION**	**RESOLUTION ACTION**	
		authentication in a bank branch	**authentication using an online bank account**
PRE-CONDITION	selecting the victim	X	X
	collecting the victim's personal details	X	X
	selecting a credit card company	Deter-known	Deter-known
	placing the order	X	X
	waiting for the delivery	X	X
	checking the delivery address to collect the card	X	X
	collecting the card	X	X
	activating the card	Defeat	Defeat
DOING	using the card's credit	X	X
POST-CONDITION	destroying the card	X	X
	vanishing other traces	X	X

Modelling the Effect of the Identified Resolution Actions on the Stakeholder's Goals and the Attack: Figure 6 shows the effect of the identified resolution actions on the stakeholder's goal, the crime script, and the offender. In the following, we clarify how this model improves the decision-makers' understanding of the effects that the resolutions have on the credit card company's goals, the crime script, and the offender.

C. DECISION-MAKING

The conceptual model in Figure 6 shows that the first resolution:

- does not have same behaviour toward all the goals,

- contributes in satisfying the authentication goal,
- has negative affect against the availability goal,
- has negative affect against the goal *maximising profit* (as its value is a negative number),
- obstructs the crime script in two steps,
- reduces the risk probability and can prevent the attack in 99.9% of the cases.

It also shows the second resolution has almost same effect as the first one but it:

- prevents the attack in only 90% of the cases in this instance,
- contributes in satisfying the goal *maximising profit* (as its value is a positive number).

These results show that while both the identified resolutions have almost same behaviour towards the crime script and the attacker, the second resolution action offers more contributions in the goals' satisfaction. Both the resolutions contribute to the satisfaction of the Goal *authentication*, and both have negative affect on the Goal *availability*. However, the second resolution contributes to satisfy the Goal *maximising profit* while the first one does not. This means the overall positive effects of the second resolution on the stakeholder's goals, crime script, and the attacker overweigh the effects of the first resolution on those entities. So, the second option appears a better decision compared to the first one.

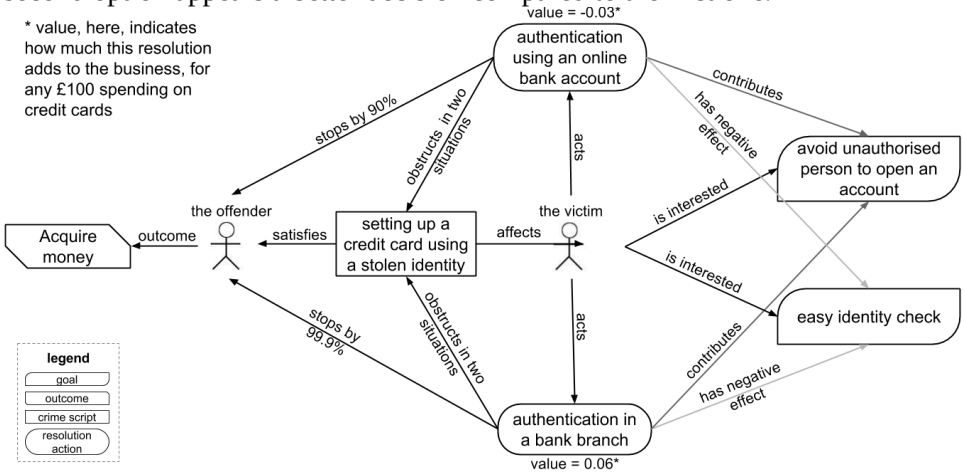

Figure 4: the effect of the resolution actions on the stakeholder's goals, the offender, and the crime script for the credit identity theft

D. RESULTS

We have applied the above framework to a case of identity theft in order to illustrate how it can support security decision-making under uncertainty. In this example, we investigated:

- how the identified resolutions affect the crime script,
- how they affect the stakeholder's goals,
- how they affect the attacker.

The conceptual model represented in Figure 4 provides an overall picture of the effects that each resolution action is expected to have on the CS, stakeholder's goals, and the attacker. This helps decision-makers to gain a better understanding of the consequences of the different decision choices, and adopt a cost-benefit perspective to address a security problem.

V. CONCLUSION AND FUTURE WORK

The focus of this article was on facilitating assessment of decision options in security problems. The output of the proposed framework is a conceptual model that aims to clearly represent the effects of each resolution action on the stakeholders' goals, the crime script, and the attacker. By using this conceptual model, decision makers are expected to gain a better understanding about the outcome(s) of their decision(s) and make decisions that result in quality improvement. We have demonstrated the framework by applying it on cases of *identity theft* discussed in Section IV.

In the future, application on more complex industrial case studies would be required to better evaluate the applicability of this framework, and refine it. The decision-making phase, which is shown in Figure 3, is another area of improvement. Investigating factors influencing the decision-making process would help improve the framework. In addition, we consider providing a validation technique that assesses the quality of crime scripts.

ACKNOWLEDGMENT

This work was conducted under EPSRC Grant No: EP/G037264/1 as part of UCL's Security Science Doctoral Training Centre.

REFERENCES

[1] P. Ekblom and A. Hirschfield, "Developing an alternative formulation of SCP principles--the Ds (11 and counting)," *Crime Science*, vol. 3, pp. 1--11, 2014.

[2] (2014). Available: http://www.bankaccountadvice.co.uk/identity-theft-case-study.html

[3] D. Falessi, G. Cantone, R. Kazman, and P. Kruchten, "Decision-making techniques for software architecture design: A comparative survey," *ACM Computing Surveys (CSUR)*, vol. 43, p. 33, 2011.

[4] T. L. Saaty, "How to make a decision: the analytic hierarchy process," *European journal of operational research*, vol. 48, pp. 9--26, 1990.

[5] M. Moore, R. Kazman, M. Klein, and J. Asundi, "Quantifying the value of architecture design decisions: lessons from the field," presented at the Proceedings of the 25th International Conference on Software Engineering, 2003.

[6] E. Letier, D. Stefan, and E. T. Barr, "Uncertainty, risk, and information value in software requirements and architecture.," presented at the ICSE, 2014.

[7] V. Veerappa and E. Letier, "Understanding clusters of optimal solutions in multi-objective decision problems," presented at the Requirements Engineering Conference (RE), 2011 19th IEEE International, 2011.

[8] J. Mylopoulos, L. Chung, S. Liao, H. Wang, and E. Yu, "Exploring alternatives during requirements analysis," *Software, IEEE*, vol. 18, pp. 92--96, 2001.

[9] A. van Lamsweerde, "Reasoning about alternative requirements options," in *Conceptual Modeling: Foundations and Applications*, ed: Springer, 2009, pp. 380--397.

[10] R. Nunes-Vaz, S. Lord, and J. Ciuk, "A more rigorous framework for security-in-depth," *Journal of Applied Security Research*, vol. 6, pp. 372--393, 2011.

[11] T. Le Sage, S. Toubaline, and H. Borrion, "An Object-Oriented Approach for Modelling Security Scenarios," presented at the Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on, 2013.

[12] N. R. Mead, "Experiences in eliciting security requirements," DTIC Document2006.

[13] N. R. Mead and T. Stehney, *Security quality requirements engineering (SQUARE) methodology* vol. 30: ACM, 2005.

[14] C. B. Haley, R. Laney, J. D. Moffett, and B. Nuseibeh, "Security requirements engineering: A framework for representation and analysis," *Software Engineering, IEEE Transactions on*, vol. 34, pp. 133--153, 2008.

[15] G. Elahi and E. Yu, "A goal oriented approach for modeling and analyzing security trade-offs," in *Conceptual Modeling-ER 2007*, ed: Springer, 2007, pp. 375--390.

[16] P. Giorgini, F. Massacci, J. Mylopoulos, and N. Zannone, "Modeling security requirements through ownership, permission and delegation," presented at the Requirements Engineering, 2005. Proceedings. 13th IEEE International Conference on, 2005.

[17] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," *Risk analysis*, vol. 1, pp. 11--27, 1981.

[18] N. F. Authority, "Annual Fraud Indicator, 2013," ed.

[19] A. van Lamsweerde, "Elaborating security requirements by construction of intentional anti-models," presented at the Proceedings of the 26th International Conference on Software Engineering, 2004.

[20] A. van Lamsweerde, "Goal-oriented requirements engineering: A guided tour," presented at the Requirements Engineering, 2001. Proceedings. Fifth IEEE International Symposium on, 2001.

[21] A. van Lamsweerde, "Goal-oriented requirements enginering: a roundtrip from research to practice [enginering read engineering]," presented at the Requirements Engineering Conference, 2004. Proceedings. 12th IEEE International, 2004.

[22] E. Letier and A. Van Lamsweerde, "Reasoning about partial goal satisfaction for requirements and design engineering," *ACM SIGSOFT Software Engineering Notes*, vol. 29, pp. 53--62, 2004.

[23] A. van Lamsweerde, *Requirements Engineering: From System Goals to UML Models to Software Specifications*: Wiley, 2009.

[24] T. Aven, *Risk analysis: assessing uncertainties beyond expected values and probabilities*: John Wiley \& Sons, 2008.

[25] D. B. Cornish, "The procedural analysis of offending and its relevance for situational prevention," *Crime prevention studies*, vol. 3, pp. 151--196, 1994.

[26] Y.-N. Chiu, B. Leclerc, and M. Townsley, "Crime Script Analysis of Drug Manufacturing In Clandestine Laboratories Implications for Prevention," *British journal of criminology*, vol. 51, pp. 355--374, 2011.

[27] D. B. Cornish, "Crimes as scripts," presented at the Proceedings of the international seminar on environmental criminology and crime analysis, 1994.

[28] H. Borrion, "Quality assurance in crime scripting," *Crime Science*, vol. 2, p. 6, 2013.

[29] R. V. G. Clarke, *Situational crime prevention*: Criminal Justice Press, 1997.

[30] P. Ekblom, "Talking to offenders: Practical lessons for local crime prevention," presented at the Urban crime Statistical approaches and analyses. International seminar held under the auspices of Ajuntament de Barcelona Forum des Collectives Territoriales Europeenes pour la Securit6 Urbaine. Barcelona: Institut d□Estudis Metropolitans de Barcelona, 1991.

[31] B. Leclerc, R. Wortley, and S. Smallbone, "Getting into the script of adult child sex offenders and mapping out situational prevention measures," *Journal of research in crime and delinquency*, p. 0022427810391540, 2011.

[32] R. V. Clarke, "Situational crime prevention: Theoretical background and current practice," in *Handbook on crime and deviance*, ed: Springer, 2009, pp. 259--276.

[33] E. Beauregard, J. Proulx, K. Rossmo, B. Leclerc, and J.-F. Allaire, "Script analysis of the hunting process of serial sex offenders," *Criminal Justice and Behavior*, vol. 34, pp. 1069--1084, 2007.

[34] R. V. G. Clarke and G. R. Newman, *Outsmarting the terrorists*: Greenwood Publishing Group, 2006.

[35] J. Lacoste and P. Tremblay, "Crime and innovation: A script analysis of patterns in check forgery," *Crime Prevention Studies*, vol. 16, pp. 169--196, 2003.

[36] C. Morselli and J. Roy, "BROKERAGE QUALIFICATIONS IN RINGING OPERATIONS*," *Criminology*, vol. 46, pp. 71--98, 2008.

[37] M. J. Smith and D. B. Cornish, *Secure and tranquil travel: Preventing crime and disorder on public transport*: Routledge, 2006.

[38] D. A. Bright and J. J. Delaney, "Evolution of a drug trafficking network: Mapping changes in network structure and function across time," *Global Crime,* vol. 14, pp. 238--260, 2013.