Theo Dimitrakos
Fabio Martinelli
Peter Y. A. Ryan
Steve Schneider (Eds.)

LNCS 4691

Formal Aspects in Security and Trust

Fourth International Workshop, FAST 2006
Hamilton, Ontario, Canada, August 2006
Revised Selected Papers

Springer

Theo Dimitrakos Fabio Martinelli
Peter Y. A. Ryan Steve Schneider (Eds.)

Formal Aspects in Security and Trust

Fourth International Workshop, FAST 2006
Hamilton, Ontario, Canada, August 26-27, 2006
Revised Selected Papers

Springer

Volume Editors

Theo Dimitrakos
BT Group Chief Technology Office, Ipswich IP5 3RE, UK
E-mail: Theo.Dimitrakos@bt.com

Fabio Martinelli
National Research Council - C.N.R., Pisa, Italy
E-mail: fabio.martinelli@iit.cnr.it

Peter Y. A. Ryan
University of Newcastle, UK
E-mail: peter.ryan@ncl.ac.uk

Steve Schneider
University of Surrey, UK
E-mail: S.Schneider@surrey.ac.uk

Library of Congress Control Number: Applied for

CR Subject Classification (1998): C.2.0, D.4.6, E.3, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-75226-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-75226-4 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12164677 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4691

Preface

The present volume contains the post-proceedings of the 4th International Workshop on Formal Aspects in Security and Trust (FAST2006), held in Hamilton, Ontario, Canada, August 26–27, 2006. FAST is an event affiliated with the Formal Methods 2006 Congress (FM06). FAST 2006 was held under the auspices of the IFIP WG 1.7 on Foundations of Security Analysis and Design.

FAST2006 aimed at continuing the successful effort of the previous three FAST workshop editions for fostering the cooperation among researchers in the areas of security and trust. The new challenges offered by the so-called ambient intelligence space, as a future paradigm in the information society, demand for a coherent and rigorous framework of concepts, tools and methodologies to provide users with trust and confidence in the underlying communication/interaction infrastructure. It is necessary to address issues relating to both guaranteeing security of the infrastructure and the perception of the infrastructure being secure. In addition, user confidence in what is happening must be enhanced by developing trust models effectively but that are also easily comprehensible and manageable by users.

FAST sought for original papers focusing on formal aspects in: security and trust policy models; security protocol design and analysis; formal models of trust and reputation; logics for security and trust; distributed trust management systems; trust-based reasoning; digital assets protection; data protection; privacy and ID issues; information flow analysis; language-based security; security and trust aspects in ubiquitous computing; validation/analysis tools; Web service security/trust/privacy; GRID security; security risk assessment; and case studies.

The FAST2006 post-proceedings collect the revised versions of 18 papers, selected out of 47 submissions. Each paper was reviewed by at least three members of the Program Committee.

We wish to thank the the Program Committee members for their valuable efforts in properly evaluating the submissions, and the FM06 organizers for accepting FAST as an affiliated event and for providing a perfect environment for running the workshop.

Thanks are also due to the Center for Software Reliability (CSR) of Newcastle University and IIT-CNR for sponsoring FAST2006.

February 2007

Theo Dimitrakos
Fabio Martinelli
Peter Y.A. Ryan
Steve Schneider

Organization

Workshop Organizers

Theo Dimitrakos, BT
Fabio Martinelli, IIT-CNR
Peter Y.A. Ryan,University of Newcastle
Steve Schneider, University of Surrey

Invited Speakers

Joshua D. Guttman, MITRE, USA

Program Committee

Gilles Barthe, INRIA Sophia-Antipolis, France
Stefano Bistarelli, University of Pescara, Italy
Gregor v. Bochmann, University of Ottawa, Canada
John A. Clark, University of York, UK
Frédéric Cuppens, ENST Bretagne, France
Roberto Gorrieri, University of Bologna, Italy
Joshua D. Guttman, MITRE, USA
Masami Hagiya, University of Tokyo, Japan
Chris Hankin, Imperial College (London), UK
Christian Jensen, DTU, Denmark
Audun Jøsang, DSTC, Australia
Jan Jürjens, TU München, Germany
Yuecel Karabulut, SAP, Germany
Igor Kotenko, SPIIRAS, Russia
Heiko Krumm, University of Dortmund, Germany
Ninghui Li, Purdue University, USA
Steve Marsh, Institute for Information Technology, NRC, Canada
Catherine Meadows, Naval Research Lab, USA
Ron van der Meyden, University of New South Wales, Australia
Mogens Nielsen, University of Aarhus, Denmark
Flemming Nielson, Danish Technical University, Denmark
Indrajit Ray, Colorado State University, USA
Babak Sadighi Firozabadi, SICS, Sweden
Pierangela Samarati, University of Milan, Italy
Jean-Marc Seigneur, University of Geneva, Switzerland
Paul Syverson, Naval Research Laboratory, USA
Ketil Stolen, SINTEF, Norway
William H. Winsborough, George Mason University, USA

Local Organization

Alessandro Falleni, IIT-CNR

Lecture Notes in Computer Science

Sublibrary 4: Security and Cryptology

Vol. 4734: J. Biskup, J. López (Eds.), Computer Security - ESORICS 2007. XIV, 628 pages. 2007.

Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.

Vol. 4691: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. VIII, 285 pages. 2007.

Vol. 4677: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design. VII, 325 pages. 2007.

Vol. 4657: C. Lambrinoudakis, G. Pernul, A M. Tjoa (Eds.), Trust and Privacy in Digital Business. XIII, 291 pages. 2007.

Vol. 4637: C. Krügel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.

Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.

Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), Information Security and Privacy. XIV, 476 pages. 2007.

Vol. 4582: J. López, P. Samarati, J.L. Ferrer (Eds.), Public Key Infrastructure. XI, 375 pages. 2007.

Vol. 4579: B. M. Hämmerli, R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. X, 251 pages. 2007.

Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), Pairing-Based Cryptography – Pairing 2007. XI, 408 pages. 2007.

Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.

Vol. 4437: J.L. Camenisch, C.S. Collberg, N.F. Johnson, B.A. Hamilton, P. Sallee (Eds.), Information Hiding. VIII, 389 pages. 2007.

Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.

Vol. 4377: M. Abe (Ed.), Topics in Cryptology – CT-RSA 2007. XI, 403 pages. 2006.

Vol. 4341: P.Q. Nguyên (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.

Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4298: J.K. Lee, O. Yi, M. Yung (Eds.), Information Security Applications. XIV, 406 pages. 2007.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S.-i. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4237: H. Leitold, E.P. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4219: D. Zamboni, C. Krügel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.

Vol. 4176: S.K. Katsikas, J. López, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4107: G. Di Crescenzo, A. Rubin (Eds.), Financial Cryptography and Data Security. XI, 327 pages. 2006.

Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4047: M.J.B. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao (Eds.), Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3969: Ø. Ytrehus (Ed.), Coding and Cryptography. XI, 443 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T.G. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.

Vol. 3957: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 325 pages. 2006.

Vol. 3956: G. Barthe, B. Grégoire, M. Huisman, J.-L. Lanet (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 175 pages. 2006.

Vol. 3935: D.H. Won, S. Kim (Eds.), Information Security and Cryptology - ICISC 2005. XIV, 458 pages. 2006.

Vol. 3934: J.A. Clark, R.F. Paige, F.A.C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3919: R. Safavi-Naini, M. Yung (Eds.), Digital Rights Management. XI, 357 pages. 2006.

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3856: G. Danezis, D. Martin (Eds.), Privacy Enhancing Technologies. VIII, 273 pages. 2006.

Vol. 3786: J.-S. Song, T. Kwon, M. Yung (Eds.), Information Security Applications. XI, 378 pages. 2006.

Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.

Vol. 2742: R.N. Wright (Ed.), Financial Cryptography. VIII, 321 pages. 2003.

¥484.00元

Table of Contents

Strategic Games on Defense Trees*

Stefano Bistarelli[1,2], Marco Dall'Aglio[1], and Pamela Peretti[1]

[1] Dipartimento di Scienze, Università degli Studi "G. d'Annunzio", Pescara, Italy
{bista,maglio,peretti}@sci.unich.it
[2] Istituto di Informatica e Telematica, CNR, Pisa, Italy
Stefano.Bistarelli@iit.cnr.it

Abstract. In this paper we use defense trees, an extension of attack trees with countermeasures, to represent attack scenarios and game theory to detect the most promising actions attacker and defender. On one side the attacker wants to break the system (with as little efforts as possible), on the opposite side the defender want to protect it (sustaining the minimum cost).

As utility function for the attacker and for the defender we consider economic indexes (like the Return on Investment (ROI) and the Return on Attack (ROA)). We show how our approach can be used to evaluate effectiveness and economic profitability of countermeasures as well as their deterrent effect on attackers, thus providing decision makers with a useful tool for performing better evaluation of IT security investments during the risk management process.

Keywords: Security, Risk Analysis, Game Theory.

1 Introduction

Security has become today a fundamental part of the enterprise investment. In fact, more and more cases are reported showing the importance of assuring an adequate level of protection to the enterprise's assets.

In order to focus on the real and concrete threats that could affect the enterprise's assets, a risk management process is needed in order to identify, describe and analyze the possible vulnerabilities that must be eliminated or reduced. The final goal of the process is to make security managers aware of the possible risks, and to guide them toward the adoption of a set of countermeasures which bring the overall risk under an acceptable level.

The determination of the acceptable risk level and the selection of the best countermeasure is unfortunately not an easy task. There are no standard methodologies for the process, and often security managers have to decide among too many alternatives.

To model the attack scenario and the defender possibilities we use *defense trees* [1], an extension of attacks trees with countermeasures. The vulnerabilities are represented as leaf nodes of the tree and are decorated with the countermeasures able to mitigate the damage of threats using such a vulnerability.

* Partially supported by the MIUR PRIN 2005-015491.

T. Dimitrakos et al. (Eds.): FAST 2006, LNCS 4691, pp. 1–15, 2007.

Moreover, economic indexes are used as labels for countermeasures and attacks. The *Return on Investment* (ROI) [18,17] index gives a measure of the efficacy of a specific security investment in a countermeasure w.r.t. a specific attack. The *Return on Attack* (ROA) [3] is instead an index that is aimed at measuring the convenience of attacks, by considering the impact of a security solution on the attacker's behavior.

The computed ROI and ROA function are then considered as utility functions (payoffs) in a two player strategic game. On one side the system administrator wants to protect the system by buying and adopting countermeasures; on the other side the attacker wants to exploit the vulnerabilities and obtain some profit by breaking the system.

We solve the games by looking at their Nash equilibria with both pure and mixed strategies. Our results show that is always worth installing countermeasures for the defender; however, it is not true that increasing the number of countermeasure gives an overall better benefit to the enterprise (as showed in [7] investing in security measure is not profitable beyond a certain level). This is not completely surprising, since more and more sophisticated protection may be accompanied by escalating marginal costs, while the probability that any given type of protection will be needed (that is, its expected benefit) may remain constant. Also interesting is the fact that the strategies of *no-attacks* and *no-countermeasures* is not (unfortunately) a point of equilibrium.

After an introduction to the concepts of security risk management and of defense trees (Section 2) we study the selection of the most promising countermeasures by interpreting the scenario as a game with two players: the defender and the attacker (Section 3). Section 4, instead, shows a realistic example where the attacker wants to steal information about customers maintained in a server. Finally, Section 5 summarizes the paper results and sketches some directions for future work.

2 Security Risk Management and Defense Trees

Defending an IT system is hard because many are the risks that can affect each asset of the system. Organizations need a process that enable to identify, describe and analyze the possible vulnerability that can be exploited by an adverse individual, and identify the security measures necessary to reduce the risks.

In [1] we propose the use of the *defense tree* (extension of *attack trees* [15,16]), an instrument for representing an attack against a system and how it can be mitigated by a set of countermeasures.

The difference between an attack tree and a defense tree is that the first represents only the attack strategies that an attacker can perform, while the second adds the set of countermeasures that can be introduced into the system to mitigate the possible damages produced by an attack.

Integrating countermeasures into threat trees, and more generally into directed acyclic graphs, is not new. In the early 90s researchers used "threat countermeasure diagrams". One may also see examples of countermeasures in DAGs in both Nathalie Foster's thesis [4] and Stuart Schechter's thesis [14], both of which include discussions and histories of the evolution of these structures. Even in the popular Microsoft text by Howard and LeBlanc, "Writing Secure Code", one can find threat trees (another name for attack trees) in which countermeasures are integrated [8].

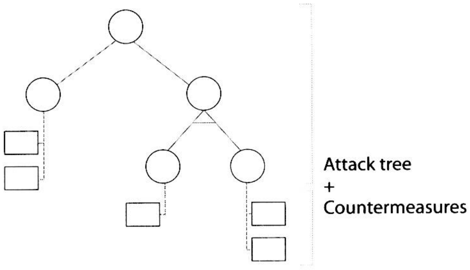


Fig. 1. A defense tree

Figure 1 shows an example of a defense tree: round nodes form the attack tree and square nodes represent the corresponding countermeasures. The root of the tree is associated with an asset of the IT system under consideration and represents the attacker's goal. Leaf nodes in the attack tree represent simple subgoals which lead the attacker to (partially) damage the asset by exploiting a single vulnerability. Non-leaf nodes (including the tree root) can be of two different types: or-nodes and and-nodes. Subgoals associated with or-nodes are completed as soon as any of its child nodes is achieved, while and-nodes represent subgoals which require all of its child nodes to be completed (in Figure 1 we draw an horizontal line between the children of an and-node to distinguish it from the or-node).

We consider defense trees [1] enriched with economic indexes that quantify the cost of attacks and the return on security investments in any branch of the tree. We interpret such indexes as utility functions for the system administrator and for the attacker, by viewing the scenario as a classical game with two player looking for different and usually opposite results (see Section 3).

In particular we label the tree with:

1. the *Return On Investment* (*ROI*) [17] measuring the return that a defender expects from a security investment over the costs he sustains for countermeasures. It is calculated with the formula:

$$ROI = \frac{ALE \times RM - CSI}{CSI}$$

   where:
   - the *Annualized Loss Expectancy* (*ALE*) [9] measures the expected annual financial loss which can be ascribed to a threat to the organization. It is calculated as $ALE = AV \times EF \times ARO$, where:

    - the *Asset Value* (AV) is a measure of the cost of creation, development, support, replacement and ownership values of an asset,
    - the *Exposure Factor* (EF) represents a measure of the magnitude of loss or impact on the value of an asset arising from a threat (expressed as a percentage of the asset value),
    - the *Annualized Rate of Occurrence* (ARO) is a number that represents the estimated number of annual occurrences of a threat.
  - the *Risk Mitigated* by a countermeasure (RM) represents the effectiveness of a countermeasure in mitigating the risk of loss deriving from exploiting a vulnerability (RM is a numeric value in [0,1] that measures the proportion of reduced risk),
  - the *Cost of Security Investment* (CSI) is the cost that an enterprise sustains for implementing a given countermeasure.
2. the *Return On Attack* (ROA) [3] measures the gain that an attacker expects from a successful attack over the losses that he sustains due to the adoption of security measures by his target. It is calculated as:

$$ROA = \frac{GI \times (1 - RM) - (cost_a + cost_{ac})}{cost_a + cost_{ac}}$$

   where:
   - GI is the expected gain from the successful attack on the specified target,
   - $cost_a$ is the cost sustained by the attacker to succeed,
   - $cost_{ac}$ is the additional cost brought by the countermeasure c adopted by the defender to mitigate the attack a.

We will see in Section 3 that other choices for the utility functions are possible. For instance we could consider ROI and ROA without dividing the gain by the costs (CSI and $cost_a + cost_{ac}$ respectively), or by considering the damage of an attack without considering its (often unknown) rate of occurrence (ARO).

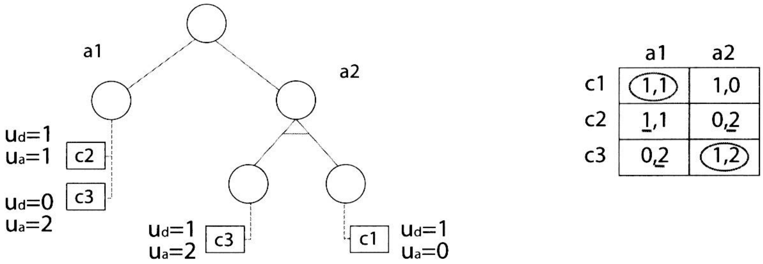
3 Defense Trees as Strategic Games

In this section we will show how game theory can be used to analyze the possible strategies of the system administrator and of the attacker. In our scenario we consider a strategic game [6] that consists of:

- n players (n is usually just 2, but we plan to extend it to the case of 1 defender and k attackers),
- a set of strategies S_i for each player i,
- the utility function (or payoff) u_i for each player i.

We consider here the case with $n = 2$ players: the *defender* (Bob) and the *attacker* (Alice) of a system. The set of defender's strategies is the set of countermeasures that he can introduce into the systems while the set of attacker's strategies is the set of vulnerability that she can exploit. The payoff functions we will consider are the Return on Investment (ROI) for the defender and the

Return on Attack (ROA) for the attacker. Notice that ROI and ROA represent normalized payoffs; in some cases a not normalized utility function could be used instead, that may lead to different equilibrium strategies (because each player is trying to maximize its return rather than its payoff).



	a1	a2
c1	1,1	1,0
c2	1,1	0,2
c3	0,2	1,2

(a) Defence tree

(b) Strategic game

Fig. 2. Defense tree and the corresponding strategic game (with a pure strategy Nash Equilibrium)

As an example consider the defense tree depicted in Figure 2(a). It can be modeled as the strategic game in Figure 2(b), where:

- the players of the game are the defender of the enterprise that can select actions represented in the rows, and the attacker that can choose possible attacks (represented as columns in the table),
- the defender's set of strategies is $S_d = \{c_1, c_2, c_3\}$, that consists of the possible countermeasures that he can enforce to protect the system,
- the attacker's set of action is $S_a = \{a_1, a_2\}$ that represents the two possible attack strategies (the columns in Figure 2(b));
- the goal of each player is to maximize his/her own payoff function (the number in each box of Figure 2(b)). The payoffs associated to a strategy (c_i, a_i) are $u_d(c_i, a_i)$ for the defender, and $u_a(c_i, a_i)$ for the attacker.

Each player chooses the best available action given his belief about the other player's action.

The solution of the game is the (set of) countermeasure that the defender is more likely to adopt, and the (set of) vulnerability that the attacker feels more suitable to exploit. In some special cases the best strategy of the attacker and of the defender converges to a specific action profile s^* with the property that the defender cannot do better by choosing an action different from s^*_d, given that the attacker adopt s^*_a, and viceversa. In this case we say that the game admits a *Nash Equilibrium* [13].

Definition 1 (Nash Equilibrium [6]). *In a strategic game with 2 players, consider the sets S_1, S_2 and the functions u_1, u_2 that are the set of possible* *strategies and the utility functions of players* 1 *and* 2 *respectively. The combination of strategy* (s_1^*, s_2^*) *with* $s_1^* \in S_1$ *and* $s_2^* \in S_2$ *is a Nash Equilibrium if and only if, for each player* i*, the action* s_i^* *is the best response to the other player:*

$$u_1(s_1^*, s_2^*) \geq u_1(s_1, s_2^*) \textit{ for any } s_1 \in S_1$$

$$u_2(s_1^*, s_2^*) \geq u_2(s_1^*, s_2) \textit{ for any } s_2 \in S_2$$

Figure 2(a) shows an example of defense tree where two possible attacks are represented: a_1 and a_2. The first one can be mitigated by two countermeasure c_2 and c_3, the second one can be mitigated by c_1 and c_3. Figure 2(b) shows the corresponding strategic game, where the numbers in the bimatrix are the payoffs associated to each player (associated as label to the tree as we will see in Section 3).

Using Definition 1 we can calculate the possible Nash Equilibria of the game. Notice that if the attacker plays strategy a_1 the best response for the defender is to play the strategies c_1 or c_2 (by looking at the first column on the left we can see that he can gain 1 instead of 0), while if the attacker plays strategy a_2 the best response is to play the strategies c_1 or c_3.

Conversely if the defender plays the strategy c_1 the best response for the attacker is play strategy a_1, if the defender plays the strategy c_2 the best response is to play strategy a_2 and if the defender plays strategy c_3 the best response for the attacker is to play strategies a_1 or a_2. The game admits two different Nash Equilibria (the circled payoffs): the couple of strategies $\{c_1, a_1\}$ and $\{c_3, a_2\}$.

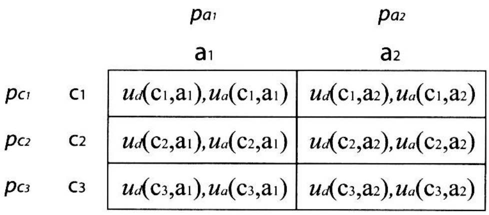
The Nash Equilibrium represents the best strategies for both the attacker and the defender (with the hypothesis that neither the attacker nor the defender have any knowledge of the other). In the case depicted in Figure 2, the defender will select, if possible, both countermeasure *c*1 and *c*3. However if the financial resources available to the system administrator are limited, only countermeasure *c*3 will be selected (because it will cover both strategy of the attacks). In Section 4 a complete more realistic example will be presented where the economic indexes will be used for the selection.

Sometimes in a strategic game it is impossible to find a Nash Equilibrium. Moreover we often need to take into account the uncertainty of the player's behavior. In this case a player may consider a *mixed strategy.*

Definition 2 (Mixed strategy [6]). *Consider a strategic game with* 2 *players,* $G = \{S_1, S_2; u_1, u_2\}$ *where* $S_i = \{s_{i1}, \ldots, s_{ik}\}$ *the strategies of player* i*. A* mixed strategy *for player* $1 \leq i \leq 2$ *is a probability distribution* $p_i = (p_{i1}, \ldots, p_{ik})$*, where* $0 \leq p_{ik}$*.*

In our context the use of mixed strategies finds a justification in the fact that a player, especially the defender, deals with a single attacker, whose behavior is not known. He may assume, however, that this players is drawn from a population of attackers whose actions can be estimated as frequencies from previous attacks (leading to the notion of *repeated games* where the players can randomize their strategies).

What we obtain is shown in Figure 3. The Attacker A can play the strategy a_1 with probability p_{a_1}, and the strategy a_2 with probability p_{a_2}, whilst the Defender D plays the strategy c_i with probability p_{c_i}, with $1 \leq i \leq 3$.



		p_{a_1}	p_{a_2}
		a_1	a_2
p_{c_1}	c_1	$u_d(c_1,a_1), u_a(c_1,a_1)$	$u_d(c_1,a_2), u_a(c_1,a_2)$
p_{c_2}	c_2	$u_d(c_2,a_1), u_a(c_2,a_1)$	$u_d(c_2,a_2), u_a(c_2,a_2)$
p_{c_3}	c_3	$u_d(c_3,a_1), u_a(c_3,a_1)$	$u_d(c_3,a_2), u_a(c_3,a_2)$

Fig. 3. Mixed strategies

We can compute payoffs in presence of mixed strategies by taking into account probability distributions and computing expectations. If the defender uses a pure strategy[1] in response to a mixed strategy of the attacker, the resulting payoffs for each possible countermeasure c_i is:

$$u_d(c_i) = u_d(c_i, a_1) \times p_{a_1} + u_d(c_i, a_2) \times p_{a_2}$$

If the attacker uses a pure strategy in response of a mixed strategy of the defender the resulting payoffs for each attack a_i is:

$$u_a(a_i) = u_a(c_1, a_i) \times p_{c_1} + u_a(c_2, a_i) \times p_{c_2} + u_a(c_3, a_i) \times p_{c_3}$$

Definition 3. *Given a game with 2 players, and 2 sets of strategies $S_1 = \{s_{11}, \ldots, s_{1K_1}\}$ and $S_2 = \{s_{21}, \ldots, s_{2K_2}\}$, if player i believes that player j will play the strategies $(s_{j1}, \ldots, s_{jK_j})$ with probability $(p_{j1}, \ldots, p_{jK_j})$, the expected payoff for player i obtained with the pure strategy s_{ij} is:*

$$\sum_{k=1}^{K_j} p_{jk} u_i(s_{ij}, s_{jk})$$

We can use Definition 3 to solve the game in Figure 2 by using the mixed strategies. In particular suppose that the defender uses a pure strategy and the attacker plays a mixed strategy $\{a_1, a_2\}$ with probability (p_{a_1}, p_{a_2}) (as shown in Figure 4). The expected payoff for the defender, if the attacker plays a mixed strategy are:

$$\begin{array}{ll} 1 \cdot p_{a_1} + 1 \cdot p_{a_2} = p_{a_1} + p_{a_2} & \text{for countermeasure } c_1 \\ 1 \cdot p_{a_1} + 0 \cdot p_{a_2} = p_{a_1} & \text{for countermeasure } c_2 \\ 0 \cdot p_{a_1} + 1 \cdot p_{a_2} = p_{a_2} & \text{for countermeasure } c_3 \end{array}$$

[1] A pure strategy is a strategy that a player plays with probability 1.