WEIGHTED ATTACK TREES FOR THE CYBERSECURITY ANALYSIS OF SCADA SYSTEMS

Andrea Bobbio[(a)], Lavinia Egidi[(b)], Roberta Terruggia[(c)], Ester Ciancamerla[(d)], Michele Minichino[(e)]

[(a)(b)(c)]DiSIT - Computer Science Institute, Università del Piemonte Orientale, Italy
[(d)(e)]ENEA - CR Casaccia, Italy

[(a)]andrea.bobbio@unipmn.it, [(b)]lavinia.egidi@unipmn.it, [(c)]roberta.terruggia@unipmn.it
[(d)]ciancamerla@casaccia.enea.it, [(e)]minichino@casaccia.enea.it

ABSTRACT

In this paper we address the issue of security of SCADA systems; a topic of paramount importance because of the impact on physical security and very challenging because of the peculiarities that set SCADA systems aside from usual ICT networks. We apply the modeling technique based on structures called weighted Attack and Defense Trees (ADT) to a complex case study based on a typical SCADA architecture, in which the attack tree is enriched with the cost and the impact of the attack. We introduce a new analysis technique for weighted ADT based on the representation of the attack scenario by means of Multi-Terminal Binary Decision Diagrams (MTBDD) that allow the modeler to identify the most probable attack scenarios, in term of probability cost and impact, and gives an indication on how to mitigate the located breaches by means of suitable countermeasures.

1. INTRODUCTION

SCADA systems were developed as closed proprietary systems running in controlled and isolated environments. In the past decades they have gradually opened up to the world to take advantage of the new communication technology that allows remote administration and monitoring. This means that network security problems from the business network and the world at large could be passed onto process and SCADA networks, putting industrial production, environment integrity and human safety at risk (Stamp et al. 2003, Shaw 2012).

Since SCADA systems directly control physical systems, availability and reliability come first, whereas in ICT networks a significant stress is on confidentiality of information. Protection in an industrial control network must be achieved in a resource constrained environment, in which channel bandwidth is very narrow and devices have a limited computational power, whereas in contrast timeliness of response is fundamental. Since resources are bounded and at the same time delays are unacceptable, many security measures that work well in ICT networks cannot be used as is in SCADA networks: cryptography, especially public-key (Fuloria et al. 2010), is often too heavy, both computationally and because of the traffic it creates (American Gas Association 2006), and additional programs like antiviruses risk slowing down systems exceedingly (Kim 2012). Being born as isolated systems, they carry the burden of a legacy of trust in the network and thus they lack the tools for monitoring and self-protection that have long been integrated in ICT networks. For instance, their logging capabilities are geared towards disturbances rather than security attacks (Ahmedi et al. 2012).

Contrary to ICT network devices, SCADA systems are designed to run for years on end (Byres et al. 2006) without a reboot. This complicates the application of software patches and makes even forensics after an attack problematic because the system cannot be taken down and analyzed at wish (Ahmedi et al. 2012). Therefore the security analysis of SCADA systems requires specific tools and specific effort. We stress the need of activating in this field formal qualitative and quantitative evaluation techniques (Ortalo et al. 1999) that can support in the choice and implementation of the most effective protection mechanisms.

1.1 Methodology and related work

Attack trees (ATs) provide a formal, methodological way of describing the security of systems, and have gained acceptance both in industrial and academic environments. The notion of AT is due to Schneier (1999) who introduced them as a visual and systematic methodology for security assessment. An AT is a multi-level hierarchical structure based on logical AND and OR operators (Ten et al. 2007b). The leaves of the tree represent atomic attack exploits. The root node (or top event) is the ultimate goal, whereas internal gates represent intermediate subgoals. There is no standard way to represent ATs (for possible notations, cf. Byres et al. 2003, Ten et al. 2007a, Kordy et al. 2012); we use the notation of Fault Tree

Analysis as in IEC-10125 (1990).

Attack exploits can be considered as Boolean events (present or non-present), whose values propagate up the tree structure to determine which combinations of attack events lead to the final goal. Borrowing the terminology from Fault Tree Analysis, we can identify the list of the minimal combinations of elementary attack exploits that lead to the final goal as the minimal cut sets *(mcs)* of the AT.

Attack exploits can have different probabilities of success, different costs for the attacker, different impacts on the system if successful, thus leading to strategies of attack more or less rewarding for the attacker. These parameters must be then taken into account in a risk assessment, leading to the design of a defense strategy. In order to model these aspect, ATs are enriched by labeling each leaf with the probability of success of the corresponding exploit, the costs for the attacker and the impact of the atomic attack step. AT enriched with cost attributes are called weighted ATs (Bobbio et al. 2013).

In planning a defense strategy, one must evaluate possible countermeasures in the face of attack exploits. In order to do this, Attack and Defense Trees (Roy et al. 2011, Kordy et al. 2012), to which we refer in the following as ADT, incorporate leaves that represent defense mechanisms or countermeasures (Ten et al. 2007a) that hinder or mitigate with an assigned probability the effect of an attack exploit. The methodology of ADTs has been applied to SCADA systems (Byres et al. 2004, Ten et al. 2007a, Roy et al. 2011) with the aim of quantifying the risk of an attack and the feasibility of a defense strategy. This paper introduces a new representation and analysis technique for weighted ADTs based on an extension of Binary Decision Diagram (BDD), called Multi-Terminal Binary Decision Diagrams (MTBDD). MTBDDs provide a more general and efficient evaluation tool for the weight functions associated to an ADT and allow the modeler to evaluate the probability distribution function of the cost and impact related to any possible attack scenario. A case study of a typical SCADA architecture illustrates the methodology.

2. ATTACK ANALYSIS OF A SCADA CASE STUDY

We assume as a case study a typical SCADA architecture (Shaw 2012) as the one shown in Figure 1. With reference to Figure 1, the characterizing elements are the following. The SCADA control center (SCC) and the Human Machine Interface (HMI) have a complete redundant backup. The primary LAN connects the SCC to different services and facilities like a Web Server and the central Data Base. The SCC is connected to the Remote Terminal Units (RTUs) by means of a Master Terminal Unit (MTU) via a network that in our specific case is composed by a proprietary WAN with a backup connection through a public Telco network as detailed in Ciancamerla et al. (2010).

On the basis of the suggestions and analysis provided in

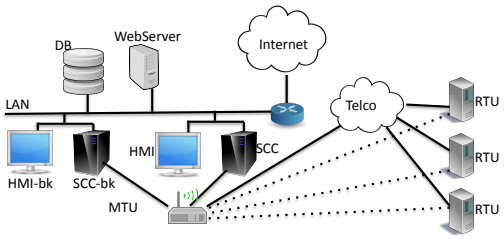

Figure 1: Typical SCADA architecture

Byres et al. (2004), Ten et al. (2007a), Roy et al. (2011), we investigate an attack scenario that assumes the event *SCADA compromised* as final attack goal (the top event of the AT). The attack may penetrate along three main lines:

- The first targets the RTUs (we assume three RTUs in our SCADA system), the MTU and the network that connects the RTUs to the MTU. We assume as basic attack exploits the compromise of an RTU, of the MTU or of one of the two network connections (atomic exploits $E01 - E06$ in Figure 2).
- The second line of attack is through the control center, composed by two blocks: the primary SCC and HMI, and their backups and the switch to commute between primary and backup (atomic exploits $E07 - E11$ in Figure 2).
- The third line of attack targets the central LAN in Figure 1 and the equipment and facilities connected to the LAN, like the hystorian Data Base, and the Web Server to the customers (exploits $E12 - E15$ in Figure 2).

With the above organization, the AT of Figure 2 represents an attack with 15 atomic exploits (leaves $E1 - E15$), 8 intermediate goals (gates $G2 - G9$) and one final goal (the top event, Gate $G1$). Table 1 reports the complete list of the basic attack exploits. If we assume that the time span before an attack exploit is delivered is an exponentially distributed random variable with known rate we can compute the probability vs time of successfully reaching the final goal Gate $G1$ as well as any intermediate gate. The computation can be performed by representing the Boolean structure of the AT by means of a Binary Decision Diagram (BDD) (Rauzy 1993) and computing the probability of reaching any level of the AT on the BDD. A BDD is a binary tree that terminates with two leaves 1 and 0 representing the combination of basic exploits that make the attack successful or non successful, respectively.

Using the attack rates reported in the third column of Table 1, the probability of reaching gate $G1$ vs time is reported in the graph a) of Figure 4.

The basic exploits do not have the same effect in determining the success of an attack, but their importance depends both on their probability and their position in the

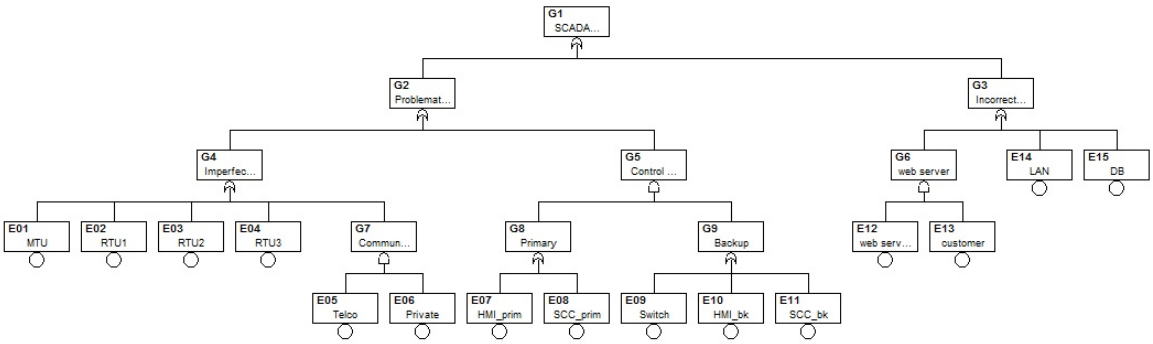

Figure 2: AT of the SCADA architecture

AT. A common indicator utilized to rank the importance of the basic exploits is the Birnbaum importance measure (Birnbaum 1969). It is defined as:

$$I^B_{x_i} = P(G_1(x_i = 1)) - P(G_1(x_i = 0)) \qquad (1)$$

where:

$P(G_1(x_i = 1))$ is the probability of the top event of the tree G_1 when leaf x_i is stuck to 1;

$P(G_1(x_i = 0))$ is the probability of the top event of the tree G_1 when the leaf x_i is stuck to 0.

The Birnbaum importance measure of an attack event represents the change in the probability that the final goal is reached caused by the probability difference when the attack exploit is used $(x_i = 1)$ or not $(x_i = 0)$. Table 1 reports the Birnbaum importance measures in Column 6 (computed at a mission time $T_M = 1800\ h$), and shows that, with the given attack rates, the RTUs turn out to be the most critical elements.

3. WEIGHTED ATS: COST AND IMPACT

A more effective and informative analysis of an attack sequence could be obtained by weighting the AT with specific attributes that have an influence on the attainment of an attack goal and may be therefore relevant to build a defense strategy (Roy et al. 2011). We identify two attributes: the cost of implementing a single atomic attack exploit and the monetary damage related to the implementation of an attack exploit. Propagating these values along the AT up to the final goal, we can evaluate the cost of attaining a successful goal attack, that we call *cost* of the attack, and the monetary damage caused by a successful attack that we call the *impact* of the attack.

Previous work (Roy et al. 2011) was devoted to derive the minimum value of the cost and the maximum value of the impact. Since in a probabilistic AT both the *cost* and the *impact* of the attack are discrete random variables, we propose in this paper to enlarge the view and to evaluate their distribution, i.e. to find which is the probability of reaching a successful attack at a given cost and with a given impact (Bobbio and Terruggia 2009).

A weighted AT is an AT whose basic (or intermediate) events are labeled with a variable representing some specific attribute of the events: in this case cost or impact. A weighted AT can be expressed and analysed by resorting to extensions of BDDs called Multi-Terminal Binary Decision Diagrams (MTBDDs), that, as extensions, inherit properties and algorithms from BDDs for regular ATs. An MTBDD (Clarke et al. 1995) is like an ordinary BDD except that the terminal leaves can be arbitrary real values instead of just 0 and 1 and can be used to represent all the possible values taken by the weight function in any possible attack scenario. To weight the AT of Figure 1, we have assumed for the atomic attack exploits $E1 - E15$ the cost and the impact values reported in the fourth and fifth columns of Table 1, respectively. The value at the terminal leaves of the MTBDD is the value of the total cost (or impact) accumulated in any possible attack scenario, obtained by propagating the cost (or the impact) of the basic attack exploits along the AT up to the top goal, with the following rules (Bobbio and Terruggia 2009, Roy et al. 2011):

1. the *cost* (resp. *impact*) in output to an AND gate is the sum of the costs (resp. impacts) of its inputs elements. The rationale behind this propagation rule is that all the inputs must be true for an AND gate to be true and hence their costs sum up.

2. the *cost* in output to an OR gate is the minimum cost among its inputs while the *impact* in output to an OR gate is, on the contrary, the maximum impact among its inputs. The rationale behind this propagation rule is that in front of a choice represented by an OR gate, the most convenient strategy for the attacker and the worst scenario for the defender is the alternative with the minimum cost and the maximum impact.

The results obtained from the analysis of the MTBDD, computed at a mission time $T_M = 1800\ h$ (corresponding to 75 days), are shown in Table 2. Column 1 reports the values that the total cost c can assume in any possible scenario. Column 2 is the probability mass of reaching a successful attack goal with the corresponding cost c; the last row labeled $n.s.$ is the probability that

Table 1: Target of the exploit, attack rate, cost, impact and Birnbaum index for the attack leaves of Figure 2

leaf	*target of the exploit*	*attack rate*	*cost*	*impact*	*Birnbaum index*
$E01$	*MTU*	1.00E-04	275	175	0.1930
$E02$	*RTU*	2.00E-04	300	350	0.2311
$E03$	*RTU*	2.00E-04	300	350	0.2311
$E04$	*RTU*	2.00E-04	300	350	0.2311
$E05$	*TELCO*	5.00E-04	200	30	0.0140
$E06$	*Private WAN*	5.00E-05	20	100	0.0140
$E07$	*HMI Primary*	5.00E-04	100	50	0.0274
$E08$	*SCC Primary*	1.00E-04	150	150	0.0133
$E09$	*Switch to Backup system*	1.00E-03	200	50	0.1084
$E10$	*HMI backup*	5.00E-05	100	50	0.1084
$E11$	*SCC Backup*	1.00E-05	150	150	0.1009
$E12$	*Web Server vulnerabilities*	3.00E-04	50	75	0.0285
$E13$	*Customers*	1.00E-04	175	10	0.0722
$E14$	*LAN*	1.00E-04	175	50	0.1930
$E15$	*DB Data Base*	1.00E-04	250	400	0.1930

Table 2: Probability of successful attacks as a function of cost with mission time $T_M = 1800\,h$

cost	*probability of successful attack*	
c	*of cost* c	*of cost* $\leq c$
200	0.051076	0.051076
225	0.065223	0.116299
250	0.157582	0.273881
275	0.219523	0.493404
300	0.343209	0.836613
350	0.000954	0.837567
375	0.001203	0.838770
n.s.	0.161230	-

Table 3: Probability of successful attacks as a function of impact with mission time $T_M = 1800\,h$

impact	*probability of successful attack of*	
i	*impact* i	*impact* $> i$
n.s.	0.161230	
80	0.001203	0.837567
85	0.011989	0.825578
100	0.015871	0.809707
175	0.082459	0.727248
200	0.010068	0.717180
300	0.123749	0.593431
350	0.428701	0.164730
400	0.164730	0.0

the attack is not successful by time T_M. Column 3 is the cumulative distribution function i.e. the probability that an attack is successful with a cost $\leq c$. Note that the cumulative distribution is defective, since there is a non null probability that the attack is not successful. In Table 3, Column 1 reports the possible impacts i, Column 2 the corresponding probability mass and Column 3 the survivor distribution function i.e. the probability that an attack is successful with an impact $> i$. Note that the survivor distribution is defective at the origin with a mass equal to the probability that the attack is non successful (row *n.s.*).

Additionally, from the MTBDD we can obtain more detailed indications on the most dangerous attack strategy by listing all the possible *mcs* with their probabilities of occurrence, costs and impacts as in the left part of Table 4. The *mcs* are listed according to their occurrence probability, i.e. the first in the list is the most probable. But if we rank the *mcs* according to their cost or impact we get a different order. The attack strategy mcs_4 consisting in compromising the MTU turns out to have a rather high probability coupled with high impact and somewhat low cost.

4. ATTACK AND DEFENSE TREE (ADT) FOR SCADA SYSTEM

The analysis carried on in the previous section gives the rationale to implement effective defense strategies, by activating countermeasures that can hinder an attack exploit: either preventing it altogether or reducing its probability of sucess (Ten et al. 2007a, Roy et al. 2011). Logically, an exploit can be successful only if the countermeasures designed to counter it fail. Therefore countermeasures appear in an AT as *negated* inputs to an AND gate whose other inputs are the events that the countermeasures should inhibit (Roy et al. 2011). In order to avoid cumbersome notation, we let countermeasure leaves denote *negated countermeasures* and omit the explicit negation altogether. Consequently, the probability attached to a countermeasure leaf is the probability of failure of the

Table 4: *MCS*, cost, impact and probability without (left part) and with (right part) countermeasures

	without countermeasures				with countermeasures	
mcs no.	*mcs elements*	*cost*	*impact*	*probability*	*mcs elements*	*probability*
1	E02	300	350	0.302324	E02 C02	0.009070
2	E03	300	300	0.302324	E03 C03	0.009070
3	E04	300	350	0.302324	E04 C04	0.009070
4	E01	250	400	0.164730	E01 C01	0.002471
5	E14	275	175	0.164730	E14 C14	0.003295
6	E15	275	175	0.164730	E15 C15	0.003295
7	E12 E13	225	85	0.068734	E12 C12 E13 C13	0.001031
8	E07 E09	300	100	0.051076	E07 C07.1 C07.2 E09	1.187e-4
9	E07 E10	200	100	0.051076	E07 C07.1 C07.2 E10 C10.1 C10.2	2.043e-3
10	E08 E09	350	200	0.014178	E08 C08 E09	4.942e-5
11	E08 E10	250	200	0.014178	E08 C08 E10 C10.1 C10.2	8.507e-4
12	E07 E11	250	200	0.010586	E07 C07.1 C07.2 E011 C0-11	4.234e-4
13	E05 E06	375	80	0.007408	E05 C05 E06 C06	2.043e-3
14	E08 E11	300	300	0.002939	E08 C08 E11 C11	1.763e-4

countermeasure.

The vulnerabilities of a SCADA system can be evidenced utilizing the methodology and tools offered by the US Department of Homeland Security by means of the Cyber Security Evaluation Tool (CSET 2011), that, additionally, offers the possibility of investigating the effect of various countermeasures. Inspired by CSET (2011) and by (Ten et al. 2007a) we apply to each atomic exploit one or more countermeasures as listed in Table 5, whose probabilities of failure are reported in the last column.

We avoid resorting to cryptographic countermeasures, in view of the delay they impose on the systems, as discussed in the Introduction. On the other hand, we use digital certificates on the Web Server that has no strict timeliness requirements. To enhance reliability and availability of the system, it is very important that only authorized personnel can operate on the system, and that traffic from public networks be accurately monitored. Therefore we focus on secure identification of operators (eliminating guest accounts and default passwords, and implementing biometric authentication and password ageing). Moreover we filter traffic from public newtorks using Intrusion Detection/Prevention Systems (IDS/IPS). In particular we dedicate a more structured protection (that we denote generically "firewall") to RTUs since the analysis on the AT has revealed that they are critical elements (cf. Table 1). Finally, we choose to implement a perimetral network, commonly known as DMZ from Demilitarized Zone, between the corporate network and the control network (following Stouffer et al. 2011, Sect. 5.3.4). On the DMZ we place components that must be accessible from both networks (in our case the Data Base).

To visualize the application of the countermeasures, we have reported in Figure 3 the portion of the total AT of Figure 2, rooted at gate *G*5. By proceeding as in the previous section, from the ADT with all the countermeasures listed in Table 5 we can build the related MTBDD,

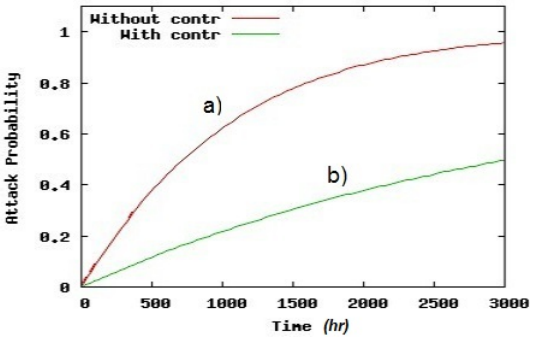

Figure 4: Comparison of attack probability vs time (in *h*) with and without countermeasures

and from the MTBDD we can evaluate the probability of reaching the final goal vs time, and the probability distributions of the cost and the impact in case of a successful attack. Figure 4 compares the probabilities of achieving the ultimate goal computed for the AT (graph a) and for the ADT (graph b) and enlightens the mitigation effect due to the application of the countermeasures. Further, in Tables 6 and 7, we report the mass probabilities, the distribution for the cost and the survivor function for the impact. The difference in the distributions with and without countermeasures taken from Tables 2 and 6 (resp. Tables 3 and 7) is evidenced in Figure 5 (resp. Figure 6), showing how the introduction of the countermeasures reduces the probability that an attacker reaches the final goal investing the same budget. A refinement and a review of the implemented security plan goes through the analysis of the attack strategies that emerge from the examination of the singular *mcs* of the ADT. To this end, we have compared in Table 4 the composition of the 14 *mcs* with and without countermeasures, by reporting the probability of occurrence of each *mcs* in the two cases.

Table 5: Attack exploits from Table 1 with the implemented countermeasures and the related probability of failure

leaf	*Attack target*	*Counter measure*	*Countermeasure description*	*Failure Probability*
*E*01	*MTU*	*C*01	*IDS/IPS*	0.15
*E*02	*RTU*	*C*02	*Firewall*	0.3
*E*03	*RTU*	*C*03	*Firewall*	0.3
*E*04	*RTU*	*C*04	*Firewall*	0.3
*E*05	*TELCO*	*C*05	*IDS/IPS*	0.2
*E*06	*Private WAN*	*C*06	*IDS/IPS*	0.2
*E*07	*HMI Primary*	*C*07.1	*Eliminate Guest Account*	0.5
		*C*07.2	*Implement Password Age*	0.4
*E*08	*SCC Primary*	*C*08	*Eliminate Factory Default Password*	0.3
*E*09	*Switch Backup system*	-		
*E*10	*HMI backup*	*C*10.1	*Eliminate Guest Account*	0.5
		*C*10.2	*Implement Password Age*	0.4
*E*11	*SCC Backup*	*C*11	*Eliminate Factory Default Password*	0.3
*E*12	*Web Server vulner*	*C*12	*Implement Digital Certificates*	0.5
*E*13	*Customers*	*C*13	*Implement Biometric Authetication*	0.3
*E*14	*LAN*	*C*14	*IDS/IPS*	0.2
*E*15	*DB Data Base*	*C*15	*DMZ (Demilitarized Zone)*	0.2

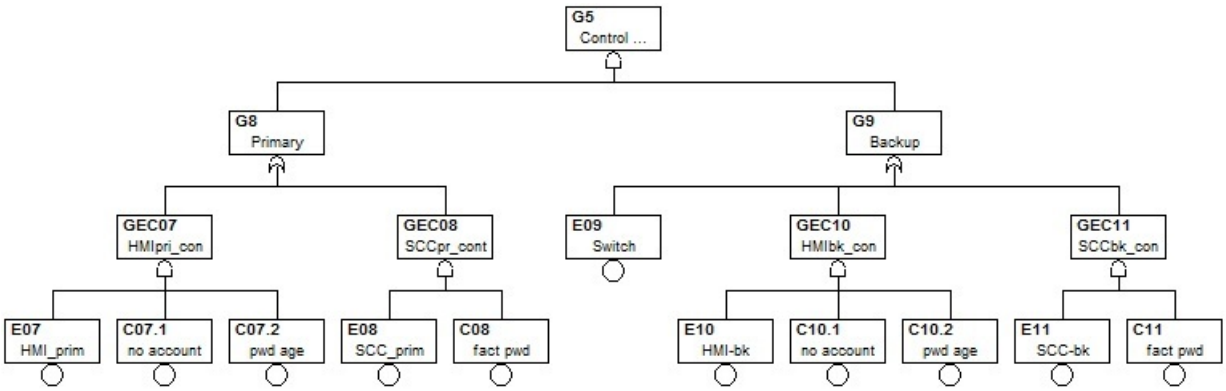

Figure 3: Subtree with countermeasures rooted at Gate *G5*

Observe how the rank of the *mcs* with repsect to their occurrence probability is modified passing from the AT (left part of Table 4) to the ADT (right part of Table 4).

The data of Table 4 are graphically reported in Figure 7 in a logarithmic scale. The most dangerous attack strategies are those in the upper left corner of Figure 7a (low cost and high probability of success), and in the upper right corner of Figure 7b (high impact and high probability of success). The probabilities and costs (resp. impacts) of attack strategies in absence of countermeasures are marked with red crosses, those in presence of countermeasures are marked with green circles. These figures give an evaluation at-a-glance of the security plan implemented: the plan is acceptable if there are no green circles in the upper left corner of Figure 7a and in the upper right corner of Figure 7b. The security plan we implemented turns out to be rather good, but Figure 7a shows that it can be further improved.

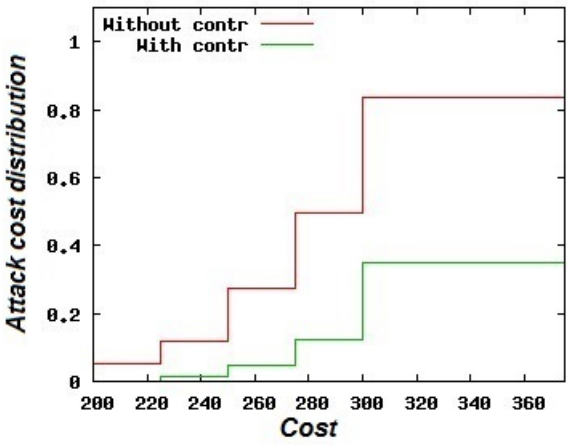

Figure 5: Distribution of cost with and without countermeasures

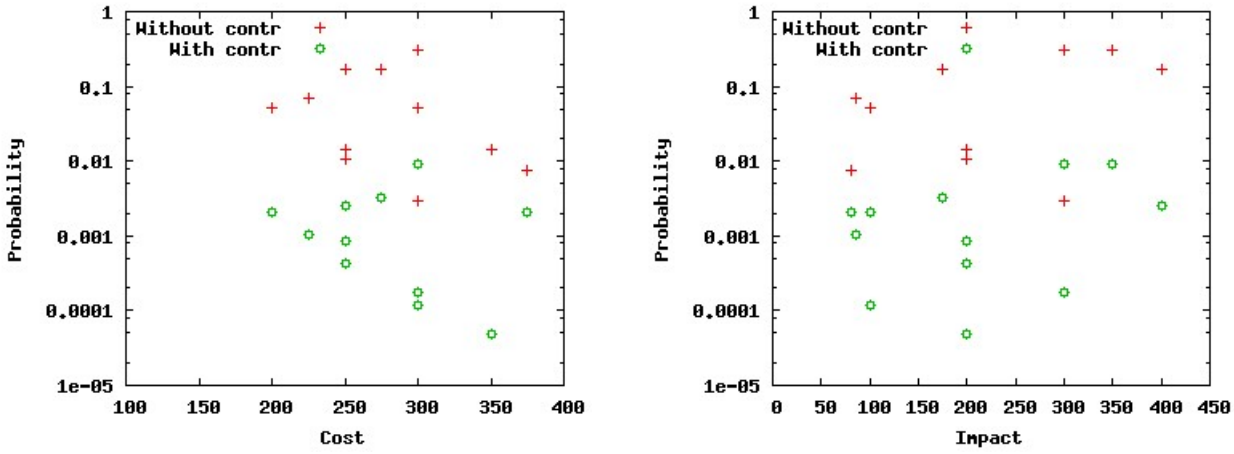

Figure 7: Comparison of *mcs* probability for AT and ADT vs cost a) and impact b)

Table 6: Probability of successful attacks as function of cost for the ADT for the SCADA system with mission time $T_M = 1800\,h$

cost c	*probability of successful attack* *of cost* c	*of cost* $\leq c$
n.s.	0.649845	-
200	0.002043	0.002043
225	0.010289	0.012332
250	0.033855	0.046187
275	0.077008	0.123195
300	0.224344	0.347539
350	0.002424	0.349963
375	0.000193	0.350155

Table 7: Probability of successful attacks as functions of impact for the ADT for the SCADA system with mission time $T_M = 1800\,h$

impact i	*probability of successful attack of* *impact* i	*impact* $> i$
80	0.000193	0.349962
85	0.006772	0.343191
100	0.007635	0.335555
175	0.058357	0.277199
200	0.004077	0.273121
300	0.072713	0.200409
350	0.167463	0.032946
400	0.032946	0.0
n.s.	0.649845	-

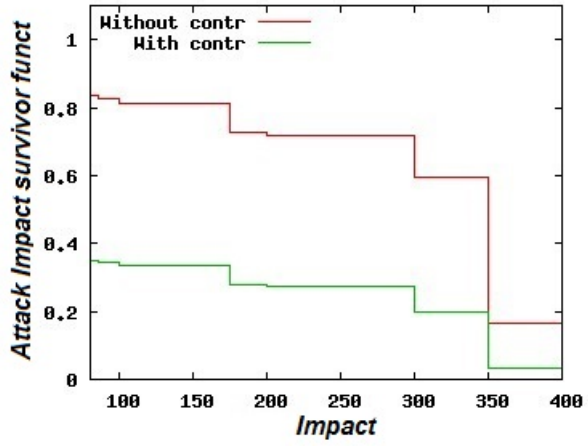

Figure 6: Distribution of impact with and without countermeasures

5. CONCLUSIONS

SCADA systems are highly critical systems and their cyber-security has its own peculiarities with respect to standard ICT systems, so that the study of the possible attacks to SCADA systems requires specific formal modeling and analysis tools able to provide qualitative and quantitative evaluations. We have investigated, in details, the modeling tool based on Attack and Defense Trees (ADTs). Standard ADTs are based on Boolean logic, and their qualitative and probabilistic properties can be analyzed by resorting to BDDs. However, if the analysis is enriched with a parametrization of the cost and the impact of the attack, the binary representation is not sufficient and we should resort to a more effective analysis technique. We have shown in this paper that the extension of the BDD called MTBDD provides an effective technique to represent and solve weighted ADT. Future work is oriented to include in the analysis the cost of implementing the countermeasures and to investigate how the budget of an attacker must be incremented in presence of countermeasures.

REFERENCES

Ahmedi, I., Obermeieri, S., Naedelei, M., and Richard III, G., 2012. Scada systems: Challenges for

forensic investigators. *Computer*, 45(12):44–51. ISSN 0018-9162.

American Gas Association, 2006. Cryptographic protection of SCADA communications part 1: Background, policies and test plan. In *AGA Report no.12, Part. 1*. http://scadahacker.com/library/Documents/Standards/AGA - Cryptographic Protection of SCADA Communications - 12 Part1.pdf.

Birnbaum, Z., 1969. On the importance of different components in a multicomponent systems. In Krishnaiah, P., editor, *Multivariate Analysis - II*, pages 581–592. Academic Press.

Bobbio, A. and Terruggia, R., 2009. Reliability and quality of service in weighted probabilistic networks using algebraic decision diagrams. In *Proceedings IEEE Annual Reliability and Maintainability Symposium*, pages 19–24, Fort Worth, TX.

Bobbio, A., Egidi, L., and Terruggia, R., 2013. A methodology for qualitative/quantitative analysis of weighted attack trees. In *4th IFAC Workshop on Dependable Control of Discrete Systems*.

Byres, E., Lissimore, D., and N., K., 2006. Who turned out the lights? - security testing for scada and control systems. In *CanSecWestri*. Slides available at http://cansecwest.com/slides06/csw06-byres.pdf.

Byres, J., Carter, J., Elramly, A., and Hoffman, D., 2003. Worlds in collision-ethernet and the factory floor. In *ISA 2002 Emerging Technologies Conference*, Chicago.

Byres, J., Franz, M., and Miller, D., 2004. The use of attack trees in assessing vulnerabilities in SCADA systems. In *IISW'04*, Lisbon.

Ciancamerla, E., Blasi, S. D., Foglietta, C., Lefevre, D., Minichino, M., Lev, L., and Shneck, Y., 2010. Qos of a scada system versus qos of a power distribution grid. In *Procs. PSAM 10*, Seattle, WA.

Clarke, E., Fujita, M., and Zhao, X., 1995. Applications of multi-terminal binary decision diagrams. Tech.Rep. CMU-CS-95-160.

CSET, 2011. Cyber security evaluation tool. http://www.us-cert.gov/control_systems/satool.html. National Cyber Security Division of the US DHS.

Fuloria, S., Anderson, R., McGrath, K., Hansen, K., and Alvarez, F., 2010. The protection of substation communications. In *S4 2010*. http://www.cl.cam.ac.uk/~sf392/publications/S4-2010.pdf.

IEC-10125, 1990. *Fault Tree Analysis*. IEC-Standard-No. 10125.

Kim, H., 2012. Review article: Security and vulnerability of scada systems over ip-based wireless sensor networks. *IJDSN*. Article ID 268478.

Kordy, B., Pouly, M., and Schweitzer, P., 2012. Computational aspects of attack & defense trees. In *Security and Intelligent Information Systems*, volume 7053 of *LNCS*, pages 103–116. Springer. ISBN 978-3-642-25260-0.

Ortalo, R., Deswarte, Y., and Kaaniche, M., 1999. Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Trans Software Engineering*, 25(5):633 –650. ISSN 0098-5589.

Rauzy, A., 1993. New algorithms for fault tree analysis. *Reliability Engineering and System Safety*, 40: 203–211.

Roy, A., Kim, D. S., and Trivedi, S., 2011. Act : Towards unifying the constructs of attack and defense trees. *Security and Communication Networks*, 3:1–15.

Schneier, B., 1999. Attack trees. *Dr. Dobb Journal of Software Tools*, 24(12):21–29.

Shaw, W., 2012. SCADA system vulnerabilities to cyber attack. In *Electric Energy online.com*. available at http://www.electricenergyonline.com/?page=show_article&mag=23&article=181.

Stamp, J., Dillinger, J., Young, W., and Depoy, J., 2003. Common vulnerabilities in critical infrastructure control systems. Technical report, Sandia National Laboratories, SAND2003-1772C.

Stouffer, K., Falco, J., and Scarfone, K., 2011. Guide to Industrial Control System (ICS) security. Technical report, NIST Special Publication 800-82.

Ten, C.-W., Liu, C.-C., and Manimaran, G., 2007a. Vulnerability assessment of cybersecurity for scada systems using attack trees. In *Procs. IEEE Power Engineering Society General Meeting*, pages 1–8.

Ten, C.-W., Manimaran, G., and Liu, C.-C., 2007b. Cybersecurity for electric power control and automation systems. In *IEEE ICSMC, 2007. ISIC.*, pages 29–34.