The GATM Computer Assisted Reasoning Framework in a Security Policy Reasoning Context

Johan Garcia
Department of Mathematics and Computer Science
Karlstad University
Karlstad, Sweden
Email: johan.garcia@kau.se

***Abstract*—Humans are often faced with the need to make decisions regarding complex issues where multiple interests need to be balanced, and where there are a number of complex arguments weighing in opposite directions. The ability of humans to understand and internalize the underlying argumentation structure resulting from reasoning about complex issues is limited by the human cognitive ability. The cognitive limit can manifest itself both in relation to an inappropriate level and amount of detail in the presentation of information, as well as in the structuring of the information and the representation of the interrelationships between constituting arguments. The GATM model provides a structured way to represent reasoning, and can be useful both in the decision-making process as well as when communicating a decision. In this work a component-based overview of the GATM model is provided in the context of security policy reasoning, where previous work has shown that decision-making transparency and improved understanding of the reasoning behind a security policy may lead to a beneficial impact on policy compliance.**

Keywords–Security policies; GATM; Reasoning; Argumentation.

I. INTRODUCTION

This paper presents the General Argumentation, Type, and Modifier (GATM) model as a way to structure reasoning of complex issues in scalable way. The objective is to provide a foundation for reasoning representation and visualization in a manner that can make the most of the human cognitive abilities. The GATM model aims to provide a framework for representing, storing, and presenting reasoning involving a complex set of argumentative statements, where the statements in turn can have multiple levels of statements that are either supportive or dismissive. One defining aspect of the GATM model is that it, unlike the well-known Toulmin approach, does not have multiple argument statement classes. Classes such as grounds, warrant, and backing as found in the Toulmin approach means that the exact same statement can belong to different classes, depending on the context in which a statement is used when reasoning about a particular claim. By avoiding the class approach, GATM simplifies the use of statements as well as the construction of joint repositories of reusable statements. Instead of classes, the GATM model uses a statement typology in which type represent an inherent characteristic of an argument statement. The type is invariant regardless of which issue is reasoned about, or where in the hierarchy a statement occurs. Further, the GATM model uses the concept of modifiers to capture the instance-specific aspects of the use of a particular statement in relation to a specific issue.

While the sketched framework can be applied across many domains, in this particular paper, we consider it in the context of security policy creation and effective dissemination. In the context of computer security policies, previous work have identified that information security awareness positively affects both attitude and outcome with regards to policy compliance [5], and concluded that security awareness should be the principal focus of a systematic approach to policy management [13]. It is presumed that an improved ability to communicate the reasoning behind security policy measures can increase security awareness and policy acceptance. This ties in to the well-known tradeoff between the strictness of computer security measures on one side and the willingness and capability of the end-users to successfully follow the measures while providing appropriate effectiveness in their regular activities. Consider, as an example, the case of forced password change. From a strictly security related point of view, it is of benefit to force the users to change passwords frequently, for example once every month, and require long passwords that fulfill criteria such as having characters from multiple groups (a-z, A-Z, 0-9, etc.). Here, there exists a tradeoff between an ideal level of security, and usability and user acceptance.

Furthermore, it is not a straightforward matter to decide what is an appropriate security level and furthermore the appropriate security level might vary between the different domains in one company which potentially leads to further complications. Security policies are typically elaborated and decided upon at the upper management level. Conflicting interests between different areas represented by the individual managers may lead to differences in views on the need for security, the potential criticality of security breaches, the monetary value of security incidents, and other associated factors. Also in this context, a security policy reasoning framework and an associated visualization tool may prove beneficial. Further discussion of the visualization aspects are left for future work, and the focus of this paper is on structural aspects of the GATM model.

The paper is structured as follows. The next section discusses related work, followed by a section that outlines the GATM model. Finally, conclusions are provided.

 ISBN: 978-1-61208-340-7

II. Related work

There are several approaches for reasoning support in the general context and a comprehensive overview and taxonomy is provided by Benathar et al. [3]. The conceptual model of argumentation proposed by Toulmin [15] is one early example of a reasoning model that has been used to guide computer reasoning efforts. An overview of the Toulmin argument structure is provided in Figure 1, where the relationship of the different classes are shown.

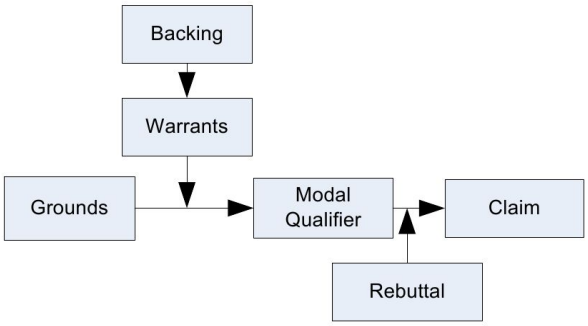

Figure 1. Generic Toulmin-form argument, from [9]

The Toulmin model has also resulted in several extensions such as the one proposed by Bench-Capon [2], which added a presupposition component which adds the ability to add statements which are not under dispute and not core to the claim made, but do represent assumptions that are necessary for the argument. In the GATM model, the same underlying information as in the presupposition component is provided by the recursive statement approach coupled with the statement typology as discussed in the next section. Also related to GATM is the work by Freeman [7], which identifies four central argument structures. The information provided by these argument structures are similar to what is represented in the GATM model, although the GATM model does not consider them in the same explicit manner.

Specifically with regards to security policies, previous research by Bulgurucu et al. [5] has investigated the rationality-based factors that drive an employee to comply with requirements of an Information Security Policy (ISP). The results show that an employee's intention to comply with the ISP is significantly influenced by attitude, normative beliefs, and self-efficacy to comply. A similar result is reported is reported by Knapp and Ferrante [13], where 297 information security professionals were surveyed, and the conclusions stress the importance of awareness. An improved ability to convey the reasoning for particular security policy measures, such as provided the proposed GATM model and associated visualization front-ends, is posited to contribute to improved Information Security Awareness (ISA). An improved ISA is is coupled to positive effects on attitude and outcome of policy compliance [5]. Other aspects of security policy design, such as firewall configuration has been elaborated in the context of reasoning and argumentation by Applebaum et al. [1]. A more formal logic for reasoning about security and security policies is discussed by Glasgow et al. [8]. In other work, Haley et al. [9] aims to to validate security requirements by using propositional logic to construct outer arguments, and informal reasoning is then used to support those with a basis in the Toulmin model of reasoning.

In this paper, password policy is used as an example for GATM. The issue of finding an appropriate tradeoff between security and convenience in a password policy is discussed by Florêncio and Herley [6], where the need for transparency is also highlighted:

> While most of us understand and accept that there is a tradeoff between security and convenience, how and by whom is this tradeoff decided? Few would argue with getting a lot more security for a little inconvenience. But, if the decision-making process is obscure how can we be sure we're not getting lots of inconvenience for little improvement in security?

Along similar lines, Myyry et al. [14], in an empirical study with 163 persons reports findings suggesting that information security policies should be better rationalized, so that the importance of these policies to the organization and the work community is clarified. The GATM model provides one approach to make the decision-making process more transparent and make explicit the consideration that have, or have not, been taken into consideration when arriving at a particular security versus convenience tradeoff.

III. Sketching the GATM model

One novelty of this work is the statement typology approach, which is based on the realization that the Toulmin basic model is cumbersome when considering complex issues with long chains of statements. Whereas the Toulmin classes differentiates between how statements relate to each other using categories such as data, warrant, and backing, the typology approach instead focuses on the basic content of the statement itself and not its relation to the claim. As has been observed by Haley et al. [9], a backing argument can itself be considered a goal which is then supported by additional supportive data, warrants and backing. Given that this recursiveness often occurs when building more elaborate reasoning hierarchies an argumentation model that assigns the argument statements to different classes depending of the vantage point might be problematic. Instead of focusing on the interrelationship between the different arguments the GATM model use an alternative typology abstraction which focuses not on the relative position of the statement to some other claim or statement, but rather on the intrinsic nature of the statement in itself. This intrinsic nature will not change if the statement is viewed as a support for a claim or if it is viewed as a claim for which there are other supporting statements.

A. A password policy GATM example

Figure 2 illustrates the structure of the GATM model using a simplified argumentation for a password policy. The figure shows the claim, which regards the mandated use of a password policy that requires users to change passwords every 60 days, as well as selecting passwords with a minimum length and composition requirements. In addition to the claim, the figure also contains a number of statements. Statements that work in support of the claim have arrows pointing right out from them, while statements that work in contradiction to

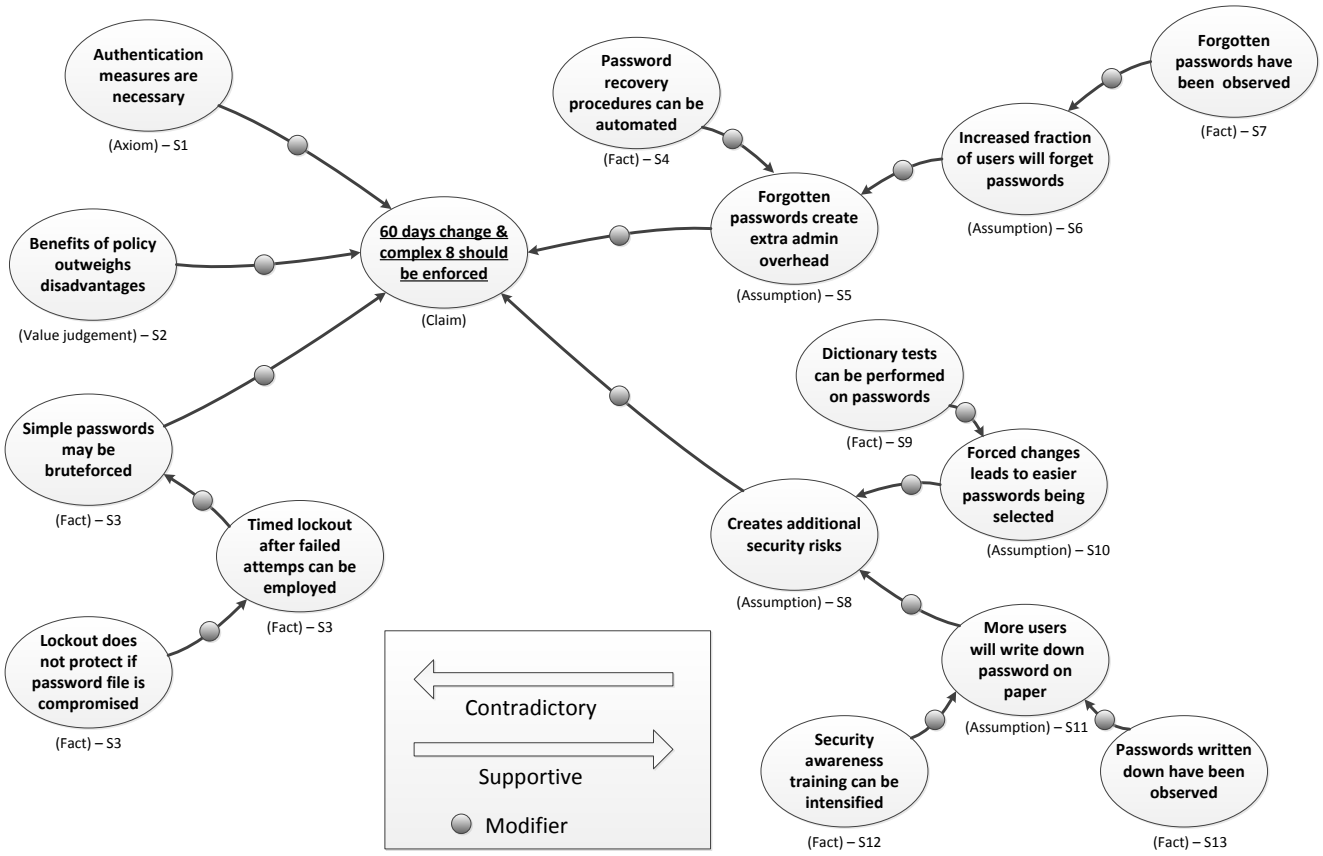

Figure 2. An simplified GATM reasoning graph example for a password policy

the claim have arrows pointing to the left. As an example, statement S5 works in contradiction to the claim, thus having an arrow pointing left. Statement S4 works in contradiction in relation to S5, but in the supportive direction in relation to the claim, and thus have a right pointing arrow. For every statement, the relative effect of the support or contradiction for that statement is captured by a modifier. The modifiers contains attributes such as statement applicability and strength. The properties of the modifier varies between each occurrence of a statement, i.e., the modifier is specific to the instance of a statement that occurs in a particular graph. Statements on the other hand, are in many cases general in the sense that the exact same statements can be used in a several unrelated reasoning graphs. So, while statements often have general applicability also outside a particular reasoning graph, modifiers are coupled to a particular graph. Different reasoning graphs have different claims, thus affecting the contextual aspects of the attributes in the modifier, such as applicability.

Although not discussed here, a feature of the GATM model is that it supports a hierarchical representation and presentation of information. Shown in Figure 2 are only information at the highest abstraction layer, which is the short statement description. In addition to this, there is also a long statement text, and and multi-part slideset that can be used to provide relevant additional information for a particular node. This allows a user to first at a glance get a view of the statements involved with regards to a particular claim. The user can then differentiate between statements which are familiar or new. Statements that are new to the user, or which the user does not agree with, can be examined closer by requesting the additional information contained in the long statement text and/or slide set. This approach lessens the cognitive load, as compared to if all statement information would have been presented at the same level of detail.

As it can be seen in Figure 2, there are several different statement types in the reasoning graph. In the idealized representation used in the figure, the types of the statement is explicitly written below each node. Also provided is a node identifier used in the discussion. In the initial prototype visualization frontend, statement types are instead represented by different geometric shapes of the nodes. A further discussion of the types used in this example are provided in the next subsection.

Considering the password policy reasoning in the figure, it can be seen that the representation allows for an overview representation of the considerations that have been taken into account with regards to this particular claim. As have been discussed in Section 2, transparency and rationalization of policy decisions have a positive impact of security policy compliance. Thus, the communicative properties is one potential benefit of using the GATM model. The GATM approach might also be useful during the policy elaboration and decision phase. Representing the advantages and disadvantages in a structured manner can simplify communication and enhance

 ISBN: 978-1-61208-340-7

TABLE I. GATM TYPOLOGY FOR TYPES USED IN THE EXAMPLE

Type	Statement Prefix	Terminal	Temporally Stable
Axiom	"Unless it is accepted that ..."	Yes	Yes
Fact	"There is a (scientific) consensus that ..."	No	Yes, mostly
Current assumption	"The best current (scientific) understanding is that ..."	No	No
Value judgment	"My personal belief is that ..."	Yes	Yes, mostly

understanding during a decision process involving multiple individuals. Although not discussed here, the versioning control integrated in the GATM model supports dialectic evolution of reasoning which might be useful during policy elaboration. While the reasoning graph in Figure 2 works as an illustrative, albeit simplified, example of the GATM model, it can also be extended with further reasoning around additional aspects that influence the design and decision making for password policies.

By allowing the reasoning to become more explicit, GATM can also be helpful in avoiding fallacious reasoning results with regards to policies. The effects of such reasoning fallacies are observed by Florêncio and Herley [6], which based on an examination of 75 websites somewhat surprisingly report that a more stringent password policy is not coupled to a site having greater security concerns. Rather, more stringent policies are found when the site provides functionality which has little sensitivity to the added user inconvenience of a stricter policy, for example when the use of a particular site is mandated by an employer. Other research useful when elaborating the reasoning around password policies include work by Zhang et al. [16] which questions the continued use of password expiration based on the observed predictability of the new passwords chosen after password expiration. The unsuitability of many password policies are also discussed by Inglesant and Sasse [11], which studied password use in two organizations and states that the focus need to be on using Human-Computer Interaction principles to set an appropriately strong password policy, and not strictly focusing on password length and expiration frequency. In fact, they report that for one of the studied organizations the password policy greatly increases the threat from passwords left written down, an observation that is illustrated by the S13-S11-S8 reasoning chain in the example. Herley [10] uses cost-benefit analysis of security advice with regards to passwords and note that much of the current policies do not fully take user costs into account.

B. GATM statement types

This subsection provides a first brief sketch of the statement types in the GATM model. Due to space constraints, this presentation focuses on the statement types present in the example in Figure 2, and does not cover all statement types of the GATM model.

"Axiom"

Axiomatic statements are the base on which the reasoning chain in many cases will end if the links of statements and supporting statements are recursively followed until the end. However, it is expected to often be uncalled for to follow the reasoning links all the way to the axioms. The axioms can be universally accepted statements regarding physical entities or statements expected to be universally accepted. When an statement is classified as an axiom it is apparent that if another party is not accepting a statement as an axiom it is not meaningful to have a further discussion in relation to the claim at hand. In relation to security policy, an axiomatic statement could be: "Organizations may deny its employees access to parts of the information within the company". Such axioms work as a basic security policy foundation for most companies, and if a party does not accept that axiom it is not meaningful to reason about security policies.

"Fact"

As the GATM model is a general model, the fact statement type eludes a simple definition. When GATM is applied where scientifically based reasoning is appropriate, fact can be seen as meaning "statements that are verifiable by repeatable experiments". However, in contexts where such a definition is not appropriate fact can be considered as "the state of affairs". This correspond to definitional facts such as "Stockholm is the capital of Sweden", which is a fact resulting from social convention. It is important to not mistakenly consider non-definitional phenomena as definitional as illustrated by the observation that although a large fraction of people 600 years ago believed the earth to be flat, the earth still, in fact, was not flat.

"Current assumption"

Current assumption is something that explicitly signals that there is a degree of uncertainty related to the statement. The uncertainty can be related to different causes. In an engineering context, it may be an effect of imprecise measurements, where the tools used to measure a metric of interest have inherent imprecision. Another case is where the underlying values vary considerably due to random factors that cannot be controlled. With regards to what can be done to reduce uncertainty, there is a difference between uncertainty dependent on inherent variability (also called aleatory uncertainty) and uncertainty due to lack of appropriate information (also called epistemic uncertainty) [12]. Whereas the epistemic uncertainty can be reduced by spending resources to gather more information, aleatory uncertainty is inherent and cannot be readily reduced.

"Value judgment"

In this context, a value judgment is a statement that reflects an individual persons inner beliefs which is considered to be largely outside the realm of rational deliberation, and as such being statements for which there exists no obvious way to objectively ascertain a "true or false" or "better or worse". A trivial example of a value judgment is the favorite color of an individual. It is not possible to say that one individual's choice of color is better than another individuals in any objective sense. Neither is it meaningful to argue about an individual's choice of color. On a higher level, value judgments tend to be individualistic and reflect the belief systems and moral

 ISBN: 978-1-61208-340-7

conditioning of individuals. In regards to computer security policy, value judgments can come into play for example with regards to tradeoffs involving privacy, as discussed by Brey [4].

An overview presentation of the discussed types are shown in Table I. The table contains a statement prefix that can function as a guide in deciding what type a given statement should belong to. It should be noted it is unlikely that there exists a single set of generally applicable guidelines on how to classify statements into types. There is no general and clear-cut boundary between axiom and fact, or between fact and current assumption. Also provided in the table is a column indicating whether the type is terminal or not. Terminal types form a definitive end in the statement chain and will not have any underlying supporting or contradicting statements. The final column in the table relates to temporal stability, which signifies the tendency of statements of a particular type to change in the validity as time passes.

Although not elaborated in this paper, the software framework for storing, representing, and presenting GATM reasoning graphs allows multiple individual representations of the same underlying reasoning graph. This makes it possible for multiple users to change the type of the particular statement in case they consider another type to be more appropriate, while the system still maintains relational links between the two individual representations. The proposed system enhances an individual's ability to represent his or hers individual reasoning which regards to a particular claim, and put his reasoning in relation to other people's reasoning on the same subject matter. From the basic observation that reasonable individuals reach multiple divergent standpoints on a given nontrivial matter, it follows that there also exists a multitude of reasoning chains that have been explicitly or implicitly followed to arrive at each individual's particular standpoint.

C. Modifiers

There are two types of modifiers in the GATM model, unipolar modifiers and multipolar modifiers. Unipolar modifiers are related to a single statement and can convey attributes relating to a particular instantiation of an statement, i.e., the use of an statement in reasoning about a specific claim. Similarly, a multipolar modifier conveys attributes but also ties together statements which are functionally dependent. For example, a statement S23 might only work as a support for a statement S18 if a statement S22 is also valid. Such dependencies are captured by the multipolar modifier.

IV. Conclusion

In this paper, we have provided an alternative model to the classical Toulmin model which can be challenging to use with hierarchical reasoning given the relative relations of data, warrant, and backing. The GATM model considers a typology of statements where the type of statement is inherent to the statement itself and not relative to its position in a reasoning hierarchy. We have used the domain of security policies to provide an example for the new model, noting that the model is primarily intended for computer supported human reasoning. While illustrating the GATM concepts with a password policy reasoning graph, the possibility to provide more transparent decision-making is also discussed. In the particular domain of security policy reasoning, it is hypothesized that the use of the GATM framework along with a visualization front-end will be beneficial to information security awareness and security policy compliance. Greater decision-making transparency and improved understanding of the underlying rationale can be important factors in influencing attitudes and normative beliefs of the users so that they strive for increased security awareness and policy compliance.

Although the focus of the GATM model is to provide support for human-centered reasoning, since the data used to represented the reasoning graph is formally structured with typology classes, statement links, etc., GATM data can also be useful for building up more formalized knowledge management systems as well as agent-based reasoning approaches.

References

[1] A. Applebaum, K. N. Levitt, J. Rowe, and S. Parsons, "Arguing about firewall policy." in *COMMA*, 2012, pp. 91–102.

[2] T. J. M. Bench-Capon, "Deep models, normative reasoning and legal expert systems," in *Proceedings of the 2nd International Conference on Artificial Intelligence and Law*, ser. ICAIL '89, 1989, pp. 37–45.

[3] J. Bentahar, B. Moulin, and M. Bélanger, "A taxonomy of argumentation models used for knowledge representation," *Artificial Intelligence Review*, vol. 33, no. 3, pp. 211–259, 2010.

[4] P. Brey, "Ethical aspects of information security and privacy," in *Security, Privacy, and Trust in Modern Data Management*, ser. Data-Centric Systems and Applications, M. Petković and W. Jonker, Eds., 2007, pp. 21–36.

[5] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *Management Information Systems Quarterly*, vol. 34, no. 3, pp. 523–548, Sep. 2010.

[6] D. Florêncio and C. Herley, "Where do security policies come from?" in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 2010, pp. 10:1–10:14.

[7] J. B. Freeman, *Dialectics and the macrostructure of arguments: A theory of argument structure*. Walter de Gruyter, 1991, vol. 10.

[8] J. Glasgow, G. MacEwen, and P. Panangaden, "A logic for reasoning about security," *ACM Transactions on Computer Systems (TOCS)*, vol. 10, no. 3, pp. 226–264, 1992.

[9] C. B. Haley, J. D. Moffett, R. Laney, and B. Nuseibeh, "Arguing security: Validating security requirements using structured argumentation," in *in Proceedings of the Third Symposium on Requirements Engineering for Information Security (SREIS'05)*, 2005.

[10] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *Proceedings of the 2009 workshop on New security paradigms workshop*. ACM, 2009, pp. 133–144.

[11] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010, pp. 383–392.

[12] A. D. Kiureghian and O. Ditlevsen, "Aleatory or epistemic? does it matter?" *Structural Safety*, vol. 31, no. 2, pp. 105–112, 2009.

[13] K. J. Knapp and C. J. Ferrante, "Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations." *Journal of Management Policy & Practice*, vol. 13, no. 5, pp. 66–80, 2012.

[14] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, and A. Vance, "What levels of moral reasoning and values explain adherence to information security rules? An empirical study," *European Journal of Information Systems*, vol. 18, no. 2, pp. 126–139, 2009.

[15] S. E. Toulmin, *The uses of argument*. Cambridge University Press, 1958.

[16] Y. Zhang, F. Monrose, and M. K. Reiter, "The security of modern password expiration: an algorithmic framework and empirical analysis," in *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010, pp. 176–186.

 ISBN: 978-1-61208-340-7