2009 International Conference on Multimedia Information Networking and Security

Applying Attack Graphs to Network Security Metric

Anming Xie*, Weiping Wen†, Li Zhang*, Jianbin Hu* and Zhong Chen*
*Institute of Software, School of Electronics Engineering and Computer Science, Peking University, Beijing, China
*Key Laboratory of High Confidence Software Technologies (Peking University), Ministry of Education, Beijing, China
Email: {xieam, zhangli, hjbin, chen}@infosec.pku.edu.cn
†School of Software and Microelectronics, Peking University, Beijing, China
Email: weipingwen@ss.pku.edu.cn

***Abstract*—Since attack graphs provide practical attack context and relationships among vulnerabilities, researchers have been trying to evaluate network security based on attack graphs. However, previous works focus their attention on specific evaluations they concerned, and each does things in his own way. There is no explicit way telling network administrators how to measure network security in a general way. In this paper, we propose a new metric framework, whose main goal is to guide people to perform evaluations based on attack graphs. The main components of proposed metric framework include *Security Index*, *Target of Evaluation*, *Elementary Attribute*, *Composition Algorithm*, and *Arithmetic operators*. Relative definitions and analysis of these five components are also given. The following examples show the applications of our metric framework, and validate it.**

***Index Terms*—network security; attack graphs; metric framework;**

I. Introduction

Over past several years, computer networks play important roles on economy and national infrastructures, including power grids, financial data systems, and communication systems. To protect networks against malicious intrusions, administrators need to understand the security states of their networks, and make efficient plans to harden their networks step by step.

Attack graphs, which describe attack scenarios, are important tools for analyzing network security vulnerabilities. In attack graphs, a single path represents an attack sequence that the attacker may use to intrude the networks. As a result, an attack graph shows all of the possible ways to break into a network, and also reveals the actual effect of each vulnerability. Considering attack context and relationships among vulnerabilities, some models and examples [1][2][3][4][5] have been trying to evaluate network security quantitatively based on attack graphs. Their works have brought about meaningful results, and their examples show how to evaluate networks security. However, there are various kinds of attack graphs and evaluation requests, and those examples evaluate network security based on their own attack graphs. For example, Wang *et al.* [3] show how to compute the probability of compromising a resource successfully, while J. Pamula *et al.* [4] try to measure network security. Previous works focus their attention on specific evaluation, and each does things in his own way. We can not follow those methods to reach our goals simply. In other words, there is no general frameworks telling us how to evaluate a network based on our attack graphs.

In this paper, we proposes a metric framework of network security based on attack graphs, which includes *Security Index*, *Target of Evaluation*, *Elementary attribute*, *Algorithm*, and *Composition operators*. We describe each component in detail, and also give two example showing how to use our framework. Our main goal is to answer the following questions: what could be evaluated by the attack graphs and how should the evaluation start?

The rest of the paper is organized as follows. Section II reviews related works on network security metric. Section III outlines the motivations and principles. Section IV describes the details of security metric framework. Section V gives two application examples. Finally, Section VI concludes the paper.

II. Related work

Various kinds of network security metrics have been talked about in [6][7]. Qualitative security evaluations are mostly based on subjective methods, and reach boolean results, such as whether a network or resource is secure. Security administrators are eager for a general way to evaluate network security quantitatively. Common Vulnerability Scoring System (CVSS) [8] is a public framework designed to assess and quantify the impact of vulnerabilities, which is adopted by many organizations and companies. To get the metric of a target, CVSS evaluates its vulnerabilities one by one, and then calculates the final value after adding time and environmental factors. NESSUS [9] is a computer software which describes network security level by the number of vulnerabilities. M. S. Ahmed *et al.* [10] also propose a security metric framework, whose outstanding feature is considering dynamically changing factors such as emergence of new vulnerabilities and threats, policy structure and network traffics. These traditional methods [8][9][10] evaluate individual vulnerabilities, and then composite the results to a global metric value. They look vulnerabilities' threats as static values, without considering how they could be used by the attackers in different environments. In fact, Network security level is not determined by the number of vulnerabilities, and a network with less vulnerabilities is not necessarily secure [1].

Since attack graphs have much information about the attack sequences, which describe how the vulnerabilities could be used, they are also suitable for network security analysis. O. Sheyner *et, al.* [11], Tsz-Yeung Wong *et, al.* [12], and D. Man *et, al.* [13] apply the probability of success to the relevant

978-0-7695-3843-3/09 $26.00 © 2009 IEEE
DOI 10.1109/MINES.2009.136

IEEE computer society

Authorized licensed use limited to: Peking University. Downloaded on March 14,2021 at 05:15:36 UTC from IEEE Xplore. Restrictions apply.

vulnerabilities and attack rules, then compose these individual values into a global probability value through attack graphs' structures. R. Lippmann, K. Ingols *et al.* [14][15] point that the network security would not be simply computed by the number of vulnerabilities, and then analysis the network security with their attack graphs.

Based on attack graphs, Chen Feng and Su Jin-Shu [16] propose a new approach to measure network security, which could get accurate results with incomplete input data. Noel *et al.* [2] represent their exploit-dependency graphs into symbolic equation, and compute the least cost change to be done in order to guarantee the safety of critical network resources. J. Pamula *et al.* [4] describe another method to measure network security. Their method expresses the targets as the minimal sets of required initial attributes, and the security metric is the strength of the weakest adversary who can successfully penetrate the network.

Wang *et al.* [1] make a further analysis on network metric with attack graphs, and they propose a simple security metric framework, which mainly describes the basic principles and the basic requirements of operators. Then, Wang *et al.* [3] give a metric example with probability of success, discussing the processing methods on cycles in attack graphs. M. Frigault *et al.* [5] interpret attack graphs as special Dynamic Bayesian networks, and their outstanding contribution is considering the effect between the vulnerabilities in a dynamic environment, for example, exploiting one vulnerability may change the difficulty of exploiting another vulnerability.

All in all, researchers pay much attention to network security, and attempt to evaluate network security metric based on attack graphs. Related papers talk about generation and evaluation methods, and ignore the importance of a metric framework. This paper aims at establishing a security metric framework based on attack graphs, describing the evaluation targets and models.

III. Motivations and Principles

A. Motivations

In practice, attack graphs are produced manually by Red Teams. However, their works were tedious, error-prone, and impractical for large networks. The following research turns to generate attack graphs automatically by computer. Over the past ten years, various kinds of attack graphs [17][11][18][2][14][19][20][21][15] have been proposed for network security analysis. Based on attack graphs, the generic evaluation process is to apply some security attributes, such as probability of success and cost, to attack graphs, and then evaluate network security through the graphs structures.

Interestingly, the following conclusions could be reached from these papers.

1) A variety of potential targets. [11] looks obtaining access right at one specific host as its target, and generates attack graphs for just one target. [3] aims at obtaining the success probability of destroying a database host. Attack graphs in [17] are generated to the total network, showing all potential scenarios after exploiting all the vulnerabilities by the attackers.
2) A variety of metric indices. [3] shows the probability of success to final target. [19] looks attack cost as the metric index. [4] expresses the metric index as strength of the required initial security attributes set.
3) A variety of elementary security attributes. [11] uses the transition probability. [19] considers the attack cost. [20] focus its attention in access right.
4) A variety of methods to generate attack graphs. [17] describes all potential resources may be attacked. [11] mainly cares about one resources. [21] pays attention to the access right transitions among the hosts.
5) A variety of iteration algorithms. [3] traverss from the root of attack graphs to the final target. [4] uses the reverse searching algorithm, expressing the final target as the minimal sets of initial conditions. [11] interpret the graph as a Markov Decision Process.

Obviously, network analysis technique is followed the structures of relevant attack graphs. Currently, there are many kinds of generation methods of attack graphs, and resulting in many kinds of representation forms. When analyzing network security, each researcher gets its unique result based on his own representation, and using his own method. So, network administrators could not use these methods simply, they need to know their targets, metric indices before then start their evaluations. And unfortunately, there is no explicit way telling them how to measure network security based on their own kind of attack graphs. To address these problems, a general framework on evaluating network security based on attack graphs is largely needed.

B. Principles

Principles are fundamental rules as guides to establish the metric framework. Referencing [6][7][1], we set up the required principles as follows.

1) Significance. The metric results should be meaningful in practice, and be not abstract or meaningless.
2) Normativeness. The input and output of framework should be normative and quantitative, and be not qualitative.
3) Objectiveness. The metric processes and results are not influenced by the measurers and the outer conditions.
4) Repeatability. The framework should return the same metric result when repeated in the same context and with same conditions.
5) Simplicity. The metric process is simple to be performed.

The first principle describes the significance of measurement. Metrics should be useful for tracking performance and directing resources. A useful metric result could help the system administrators to harden networks, while a meaningless metric result would only lead to discussions, or even guide people to take wrong actions. The second and third principles jointly show the practicability of the framework. People

Authorized licensed use limited to: Peking University. Downloaded on March 14,2021 at 05:15:36 UTC from IEEE Xplore. Restrictions apply.

always want to know how security their networks are, and the qualitative answers would be insufficient. So, if the input and metric process are both normativeness and objectiveness, the output is close to an actual existence value. As a typical example of quantitative value, when comparing the security level between two similar networks, the quantitative results show the difference in numerical value. The fourth principle requires the metric framework to set up certainty algorithms, and metric process should be repeatable. This principle increases the usefulness of metric framework in practice. The last principle says that the metric framework is easy to realize. A framework which is difficult to be performed would not be generalized or liked by system administrators.

IV. The Metric Framework

A. The General Framework

As the basis of metric framework, here is the definition about attack graphs.

Definition 1: Supposing V is the set of vulnerabilities in a network, an attacker breaks into the network through a chain of exploiting vulnerabilities, $CP = \{v_1 v_2 \cdots v_n \mid v_i \in V,\ i = 1, 2, \cdots, n\}$, where each exploit in the chain helps to execute subsequent exploits. Such a chain, CP, is called an attack path.

Definition 2: Attack graphs are used to describe network security. To a network, the set of all possible attack paths from an attack graph, that is $AG = \{CP_i \mid CP_i \ is\ an\ attack\ path,\ i = 1, 2, \cdots, m\}$.

To help apply attack graphs to network metric in practical, this paper propose a metric framework, whose main goal is to tell researchers what could be evaluated with attack graphs and how evaluation process should be organized.

The metric framework is shown as Figure 1, whose main components are *Security Index*, *Target of Evaluation*, *Elementary attribute*, *Composition Algorithm*, and *Arithmetic operator*. The next subsection gives comments to these components in detail.

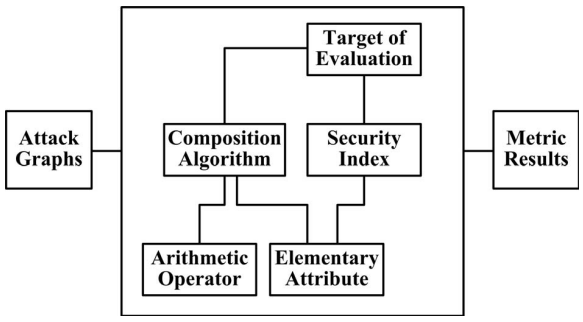

Fig. 1. The General Framework

B. Details of the Metric Framework

- *Security Index*

Security Index shows the objective security meanings based on attack graphs. Here is the definition of *Security Index*.

Definition 3: Security Index is the set of evaluable security attributes, which indicating the network security level. The values of *Security Index* are the output of the framework, and provide users the quantitative results of interested targets.

The above definition shows that, *Security Index* is relevant to the user's security requirements, and whose values tell users how safe the targets are. The important categories of *Security Index* are shown as Table I.

TABLE I
Categories of *Security Index*

Categories	Description	Examples
Integral security	Network's security level as a whole	- Security scores to the whole network - Risk evaluation scores of a network
Probability of success	Likelihood of reaching some targets	- Probability of successfully destroying a database server - Probability of gaining "root" right on some internal hosts
Attack cost	Cost used to reach some targets	- Time cost to successfully break into networks - Minimal technique cost to reach targets
Loss	Losses of relevant resources or cost needed to take	- Pecuniary losses after a attack - Time needed to recovery a system - Cost needed to harden a network for prevent suffering attacks

- *Target of Evaluation*

In general, *Target of Evaluation* is the target in attack graphs, and its definition is as follows.

Definition 4: In metric framework, *Target of Evaluation* is the object which would be evaluated, and is the entity to which *Security Index* should be applied.

Target of Evaluation exists in network or attack graphs, and maybe a host, a resource, or an attack path. Table II shows the categories of *Target of Evaluation*.

TABLE II
Categories of *Target of Evaluation*

Categories	Description	Examples with *Security Index*
Integral network	Network's security level as a whole	- Security scores of the whole network - Risk evaluation scores of the whole network
Resource	Anything useable in the network	- Probability of successfully compromising a database server - Pecuniary losses of the internal network has been broken into by attackers
Security target	Some specific security requirements	- Probability of gaining "user" right by remote attackers - Probability of gaining "root" right on a host
Attack paths	Attack chains composed by exploits	- Probability of successful executing an attack path - Cost needed to harden a network for prevent an shortest attack path

- *Elementary Attribute*

Definition 5: In metric framework, *Elementary Attribute* is the basic evaluable security attribute, which is associated with atomic attacks and vulnerabilities, such as probability, time, and right.

Authorized licensed use limited to: Peking University. Downloaded on March 14,2021 at 05:15:36 UTC from IEEE Xplore. Restrictions apply.

Since atomic attacks and network vulnerabilities are represented by nodes and edges in attack graphs, *Elementary Attribute* is the information associated with nodes and edges actually.

Elementary Attribute and *Security Index* are closed, because the value of *Security Index* is composed from the values of *Elementary Attribute*. There are two different points between them. First, *Elementary Attribute* is applied to atomic attacks and network vulnerabilities, while *Security Index* is the attribute of *Target of Evaluation*. Second, in a general way, the value of *Elementary Attribute* is original value through measurements or from expert database, while *Composition Algorithm* composes multi-*Elementary Attribute's* value into the result of *Security Index*. For example, the general risk evaluation scores of a network could be obtained through probability of success of atomic attack and the losses of compromised resources. The examples of *Elementary Attribute* are shown as Table III.

TABLE III
EXAMPLES OF *Elementary Attribute*

Categories	Examples
Probability	- Probability of executing an atomic attack successfully - Probability of identifying a vulnerability successfully - Detected Probability of an atomic attack
Money	- Losses when some resource have been compromised - Cost to patch a vulnerability
Time	- Average time needed to execute an atomic attack successfully - Minimal time needed to recovery a compromised host
Right	- Access right gained by an atomic attack
Capability	- Attack difficulty of an atomic attack, which is the requirement to an attacker

- *Composition Algorithm*

Algorithm is a set of well-defined rules for solving a problem in a finite number of steps, so the definition of *Composition Algorithm* is as follows.

Definition 6: In metric framework, *Composition Algorithm* is a set of well-defined rules to calculate the result security metric of specific *Target of Evaluations* in a finite number of steps, and these rules are based on attack graphs.

The input of *Composition Algorithm* includes the attack graphs and the value of relative *Elementary Attribute*, and the output is the metric value of *Security Index*. Under the principles in section III-B, *Composition Algorithm* could setup different rules, for example, [3] uses a forward iteration algorithm, while [4] uses the reverse searching algorithm.

- *Arithmetic Operators*

Operator represents mathematical operations, and the definition of *Composition Algorithm* is shown as follows.

Definition 7: Arithmetic Operators is a symbol or function applied to *Composition Algorithm*. In metric framework, the operands of *Arithmetic Operators* are the values of security attributes.

The examples of *Elementary Attribute* are shown as Table IV.

TABLE IV
CATEGORIES OF *Arithmetic Operators*

Categories	Description	Examples
"or" operator	Disjunctive relation between multi network components, any of these components would reach the target	- Parallel operator in parallel circuit, - $\wedge$ (max operator), - $\vee$ (min operator)
"and" operator	Conjunctive relation between two network components. To reach the target, all of these components should be satisfied	- simple addition, - simple multiplication, - boolean operations
"conditional" operator	One component may affect anointer component's state. e.g., exploiting one vulnerability may change the difficulty of exploiting another vulnerability	- conditional operators in Bayesian network

[19] give a simple example of the "or" operator and "and" operator, in which, "or" operator is the parallel operator in parallel circuit, and "and" operator is the simple addition operator.

V. EXAMPLES

Since the security metric framework is established, it helps people to make sure of the evaluation targets and execute the metric process easily. This section gives two examples showing how the metric framework works.

The first example is to calculate the probability of successfully intruding a network.

Description: Suppose a company provides public news and announcements services via internet, so a few servers connect with internet directly and also connect with inside network of this company. Now, network administers care about the security of the web systems and wants to know the likelihood of the webpages may be tampered by malicious attacker from internet.

Solution: In the example, the *Targets of Evaluation* are the web systems which providing news and announcements services, so all states related to the security of web systems in attack graphs are key states, and should be paid attention to. After analyzing the descriptions, it is easy to know the *Security Index* is probability of gaining write right to the web systems, and so the *Elementary Attribute* is probability of executing an atomic attack successfully. After applying the probability of success to related nodes and edges in attack graphs, the *Composition Algorithm* could use the forward iteration algorithm, which accumulates the probability of success in attack paths. The *Arithmetic Operators* include "or" operator and "and" operator simply. The "or" operator would be set as max operator, while "and" operator would be set as the simple multiplication.

The second example is to get the risk evaluation scores.

Description: Suppose a company's network is divided into three parts, which are outer part, office part, and database part. The outer part is the area where WEB systems are, which provides web services for the users from internet. The

Authorized licensed use limited to: Peking University. Downloaded on March 14,2021 at 05:15:36 UTC from IEEE Xplore. Restrictions apply.

database part is the area where database systems are, and may store important business information there. Although there are firewalls and access rules between these parts, the security officer wants to know the risk evaluation scores of database servers, especially the risk of malicious users stealing and destroying the business information from internet.

Solution: In this example, the *Targets of Evaluation* are the database servers which storing business information, so all states relating to the security of database servers in attack graphs are key states. The *Security Index* is the risk evaluation scores. The *Elementary Attributes* should include probability of executing an atomic attack successfully, the losses of data be stolen or destroyed, and the difficulty of executing an atomic attack. Then, a set tuple $(S, E, T, I, R, Lost, Succ, Dfct)$ is set up, where S is the set of nodes in attack graphs, E is the set of edges in attack graphs, T is the set of *Targets of Evaluation*, I is the set of *Security Index*, R is the atomic attack rules set, $Lost$ is the set of losses of data, $Succ$ is the set of probability of executing atomic attacks successfully, and *Dfct* is the set of difficulty of executing atomic attacks. In this tuple, $S \times E \rightarrow S$ and $T \subseteq S$ could be gotten from the attack graphs. Furthermore, the *Composition Algorithm* is to find a realistic mapping relation: $(T \times Lost) \times (R \times Succ) \times (R \times$ *Dfct*$) \rightarrow I$. To calculate the *Security Index*, "or" and "and" operators could be set as parallel operator in parallel circuit, and simple multiplication respectively.

VI. Conclusions

As to network security, there is not a widely-accepted network security metrics [1]. Since attack graphs are important tools for analyzing network security vulnerabilities, and could provide the practical attack context and relationships among vulnerabilities, researchers start to use them to evaluate network security. However, they construct many kinds of attack graphs, and describe different methods to compute different security metrics. There is no explicit way telling network administrators how to measure network security based on attack graphs. In other words, they do not know which metrics attack graphs could evaluate and how evaluation processes start when set up a target.

To address these problems, we proposes a security metric framework based on attack graphs, which includes *Security Index*, *Target of Evaluation*, *Elementary attribute*, *Algorithm*, and *Composition operators*. We give the definitions for these components, and describe them in detail. As a comment, two examples are also given, which helps us to understand how to use this framework. In fact, if we know our evaluation targets, our framework could also help us to generate some special types of attack graphs which are useful in calculating some special *Security Indices*.

However, this metric framework is still in conceptual phase. It will be enriched in our future work, including classifications of components and formalization of metric framework. More discussions on *Composition Algorithms* are also helpful in practice.

References

[1] L. Wang, A. Singhal, and S. Jajodia, "Toward measuring network security using attack graphs," in *QoP*, G. Karjoth and K. Stølen, Eds. ACM, 2007, pp. 49–54.

[2] S. Noel, S. Jajodia, B. O'Berry, and M. Jacobs, "Efficient minimum-cost network hardening via exploit dependency graphs," in *ACSAC*. IEEE Computer Society, 2003, pp. 86–95.

[3] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, "An attack graph-based probabilistic security metric," in *DBSec*, ser. Lecture Notes in Computer Science, V. Atluri, Ed., vol. 5094. Springer, 2008, pp. 283–296.

[4] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup, "A weakest-adversary security metric for network configuration security analysis," in *QoP*, G. Karjoth and F. Massacci, Eds. ACM, 2006, pp. 31–38.

[5] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, "Measuring network security using dynamic bayesian network," in *QoP*, A. Ozment and K. Stølen, Eds. ACM, 2008, pp. 23–30.

[6] A. Hecker, "On system security metrics and the definition approaches," in *SECURWARE*, 2008, pp. 412–419.

[7] A. Atzeni and A. Lioy, "Why to adopt a security metric? a brief survey," in *QoP2005, First Int. Workshop on Quality of Protection*, 2005, pp. 1–12.

[8] P. Mell, K. Scarfone, and S. Romanosky. Cvss. A Complete Guide to the Common Vulnerability Scoring System Version 2.0. [Online]. Available: http://www.first.org/cvs s/cvss-guide.html,

[9] Nessus. Open source vulnerability scanner project. [Online]. Available: http://www.nessus.org/nessus/

[10] M. S. Ahmed, E. Al-Shaer, and L. Khan, "A novel quantitative approach for measuring network security," in *The 27th Conference on Computer Communicationsm, INFOCOM*, 2008, pp. 1957–1065.

[11] O. Sheyner, J. W. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in *IEEE Symposium on Security and Privacy*, 2002, pp. 273–284.

[12] T. Y. Wong, M. H. Wong, and J. C. S. Lui, "A precise termination condition of the probabilistic packet marking algorithm," *IEEE Trans. Dependable Sec. Comput.*, vol. 5, no. 1, pp. 6–21, 2008.

[13] D. Man, W. Yang, Y. Yang, W. Wang, and L. Zhang, "A quantitative evaluation model for network security," in *CIS '07: Proceedings of the 2007 International Conference on Computational Intelligence and Security*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 773–777.

[14] K. Ingols, R. Lippmann, and K. Piwowarski, "Practical attack graph generation for network defense," in *ACSAC*. IEEE Computer Society, 2006, pp. 121–130.

[15] R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz, and R. Cunningham, "Validating and restoring defense in depth using attack graphs," in *Proceedings of MILCOM2006*, Washington, DC, 2006.

[16] C. Feng and S. Jin-Shu, "A flexible approach to measuring network security using attack graphs," in *ISECS*, F. Yu, Q. Luo, Y. Chen, and Z. Chen, Eds. IEEE Computer Society, 2008, pp. 426–431.

[17] C. A. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Workshop on New Security Paradigms*, 1998, pp. 71–79.

[18] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," in *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2002, pp. 217–224.

[19] L. Wang, A. Singhal, and S. Jajodia, "Measuring the overall security of network configurations using attack graphs," in *DBSec*, ser. Lecture Notes in Computer Science, S. Barker and G.-J. Ahn, Eds., vol. 4602. Springer, 2007, pp. 98–112.

[20] R. Dewri, N. Poolsappasit, I. Ray, and D. Whitley, "Optimal security hardening using multi-objective optimization on attack tree models of networks," in *ACM Conference on Computer and Communications Security*, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 204–213.

[21] P. Ammann, J. Pamula, J. A. Street, and R. W. Ritchey, "A host-based approach to network attack chaining analysis," in *ACSAC*, 2005, pp. 72–84.

Authorized licensed use limited to: Peking University. Downloaded on March 14,2021 at 05:15:36 UTC from IEEE Xplore. Restrictions apply.