Tạp chí Khoa học ĐHQGHN, Khoa học Tự nhiên và Công nghệ 23 (2007) 174-180

Một phương pháp lượng giá an ninh máy tính

Nguyễn Thiện Luận, Trần Hồng Quang*

Khoa Công nghệ Thông tin, Học viện Kỹ thuật Quân sự, 100 Hoàng Quốc Việt, Hà Nội, Việt Nam

Nhận ngày 12 tháng 4 năm 2006

Tóm tắt. Bài báo trình bày phương pháp lượng giá an ninh cho máy tính. Phương pháp lượng giá được xây dựng dựa trên nghiên cứu mô hình quan hệ, sự ràng buộc giữa các yếu tố ảnh hưởng tới an ninh của hệ thống máy tính, từ đó lượng giá mức độ an ninh và rủi ro cho toàn bộ hệ thống máy tính.

1. Đặt vấn đề

Để xác định mức độ an ninh của các hệ thống máy tính đòi hỏi phải có một phương pháp và mô hình cụ thể bao gồm các thực thể, mối liên kết, tham số vào/ra, phương thức xử lý,... Khi đã xác định được giá trị, mức độ an ninh sẽ giúp ích cho công tác xây dựng, củng cố, điều chỉnh hệ thống thông qua việc xử lý các tham số đầu vào. Trong các nghiên cứu [1-3] đã đề cập tới việc chuẩn hóa khái niệm sử dụng trong lượng giá an ninh hệ thống, đồng thời đưa ra phương pháp, mô hình, phương thức xác định giá trị và mức độ an ninh. Tuy nhiên, tham số chính của mô hình an ninh [1,2] minh họa là lưu lượng dữ liệu trong hệ thống, vì vậy kết quả lượng giá an ninh chỉ có thể đánh giá được sự bất thường trong lưu lượng dữ liệu trên mạng. Phương pháp [3] thực hiện lượng giá các thành phần an ninh của hệ thống dựa trên các điều kiện theo tiêu chuẩn cố định (CC, 1999). Nghiên cứu [4,5] tiến hành phân tích một số yếu tố ảnh hưởng tới an ninh hệ thống, và các phương pháp [6-11] chỉ đưa ra được danh sách những rủi ro cần khắc phục. Như vậy, khi đưa mô hình vào hoạt động, các phương pháp đánh giá [1-11] đều xem xét trên những khía cạnh khác nhau trong cùng lĩnh vực an ninh hệ thống, do vậy các yếu tố cấu thành, ảnh hưởng tới vấn đề an ninh hệ thống được nghiên cứu dưới nhiều góc độ và cho ra nhiều kết quả, tiêu chí khác nhau. Phương pháp mà các tác giả nghiên cứu ở đây nhằm tìm ra hai thông số mô tả an ninh hệ thống đó là giá trị an ninh (SE - Security Estimate) và độ rủi ro (Risk Rating). Thông số độ rủi ro được tính toán với mục đích xác định khả năng có thể bị xâm phạm trong điều kiện hệ thống tiếp tục hoạt động. Thông số giá trị an ninh chỉ ra khi bị xâm phạm thì sức mạnh của hệ thống đạt giá trị bao nhiêu. Một hệ thống có độ rủi ro thấp, giá trị an ninh cao chính là mục tiêu đạt tới của các hệ thống máy tính, mạng máy tính hiện nay.

Phần 2 trình bày một số khái niệm, quy ước sử dụng trong bài báo, trong phần 3 nêu ra một mô hình ứng dụng trong việc xác định mức độ

* Tác giả liên hệ. ĐT: 84-4-8360897.
E-mail: uconvert@yahoo.com

và giá trị an ninh máy tính, thiết bị mạng, thiết bị đầu cuối có liên kết mạng. Trong phần này cũng xem xét tới các yếu tố cấu thành an ninh máy tính, mối quan hệ giữa các yếu tố, xây dựng bộ đo và mối quan hệ của bộ đo mức độ an ninh với các yếu tố trên (3.2). Sau khi đã xây dựng những khái niệm cần thiết, phần 4 sẽ trình bày cụ thể kỹ thuật lượng giá an ninh máy tính, bao gồm mô hình, thiết lập hàm số và biến số, giải thuật...

2. Một số khái niệm

Tác nhân xấu: Là những hành động hoặc sự kiện liên quan tới vấn đề an ninh. Sự hoạt động của chúng chính là những yếu tố cấu thành sự mất an ninh cho hệ thống.

Hiểm họa: Bao gồm tập hợp những tác nhân xấu có khả năng ảnh hưởng tới an ninh của hệ thống.

Tiến trình: Được sử dụng mô tả toàn bộ những hoạt động đang diễn trong quá trình xử lý, tương tác của hệ thống.

Điểm yếu: Những lỗ hổng không lường trước phát sinh trong quá trình thiết kế, triển khai, hoạt động của hệ thống.

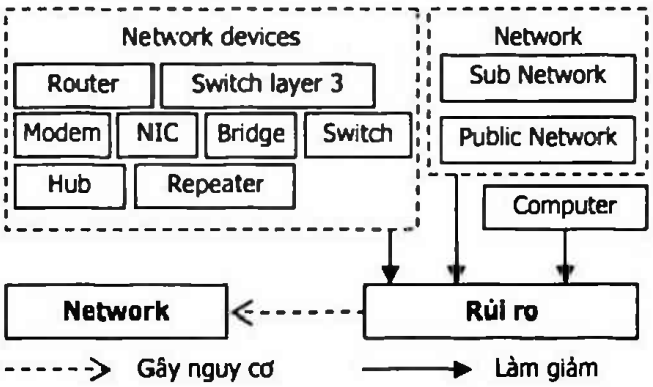
Rủi ro: Tổng hợp của những hiểm họa và những điểm yếu mà hệ thống có thể gặp phải trong quá trình hoạt động.

Khai thác: Phương thức phát hiện, tấn công vào những điểm yếu của hệ thống từ đó xâm phạm tới an ninh của hệ thống đó.

3. Xây dựng mô hình an ninh

3.1. Mối quan hệ giữa các yếu tố trong an ninh mạng

Chúng ta xét mô hình mạng trong trường hợp này là IP based network. An ninh của hệ thống mạng hoàn toàn phụ thuộc vào sự hoạt động của toàn bộ hệ thống bao gồm các thiết bị mạng nằm trên các tầng vật lý, tầng liên kết dữ liệu và tầng mạng, các mạng con thành phần, các kết nối tới mạng công cộng và mạng diện rộng, các hoạt động của máy tính và thiết bị đầu cuối kết nối mạng. Mọi hiểm họa, rủi ro, lỗ hổng, điểm yếu xuất phát từ những thành phần trên đều gây mất an ninh tới hoạt động của hệ thống mạng vì vậy chúng trở thành các yếu tố làm tăng tính rủi ro trong quá trình tương tác, xử lý của mạng máy tính.

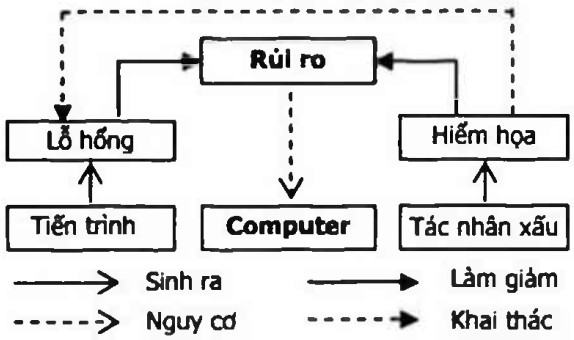


Hình 1. Mối quan hệ giữa các yếu tố ảnh hưởng tới an ninh mạng.

Như vậy, nếu chúng ta xác định được giá trị an ninh và độ rủi ro của các thành phần cấu thành mạng thì chúng ta có thể xác định giá trị an ninh, độ rủi ro cho toàn bộ hệ thống mạng máy tính.

3.2. Mối quan hệ giữa các yếu tố trong an ninh máy tính

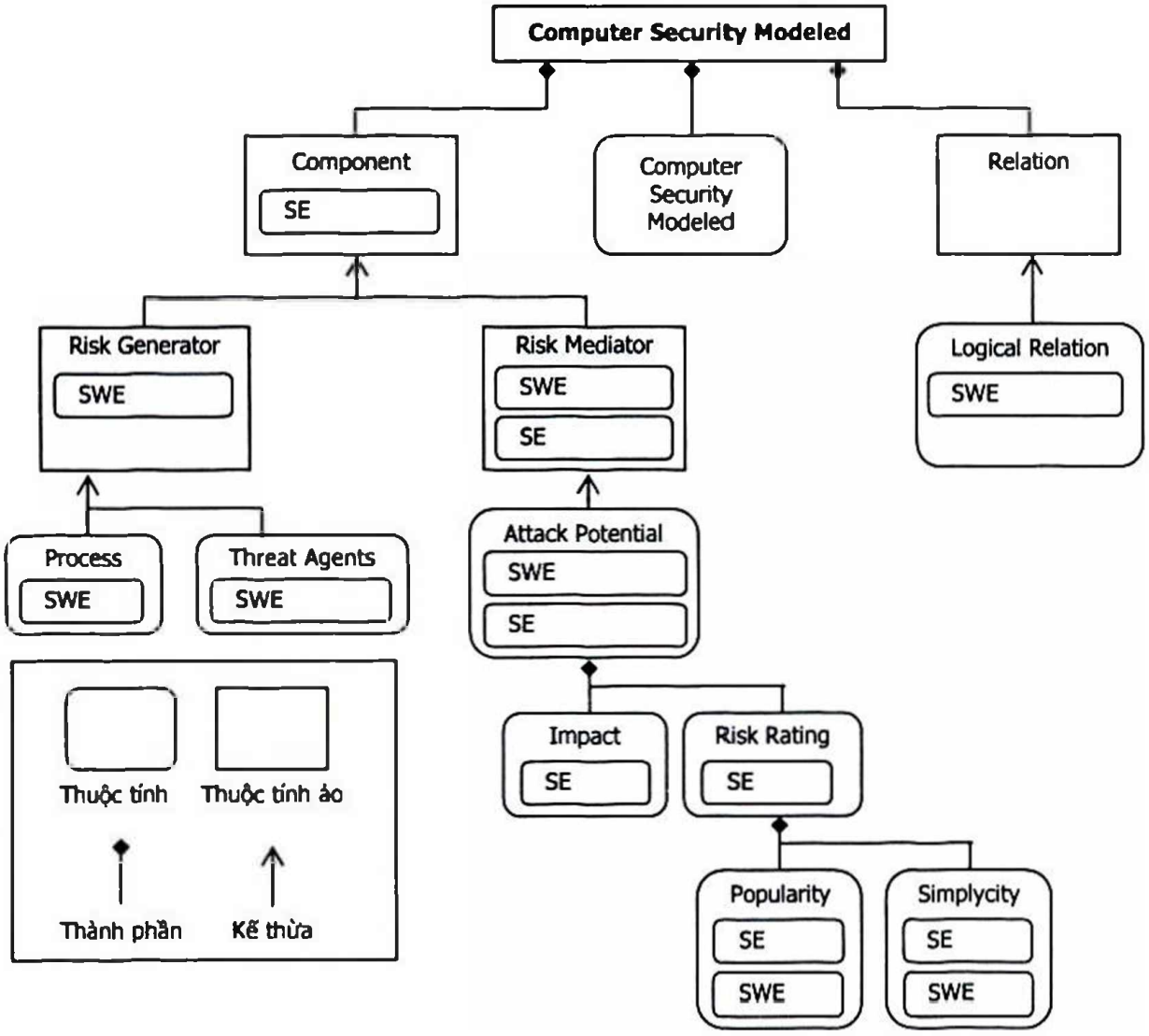
Những tác nhân xấu là yếu tố gây ra những hiểm họa mà hệ thống phải gánh chịu, sự hoạt động của các tiến trình và tiểu tiến trình đang diễn ra trong hệ thống sẽ làm nảy sinh những điểm yếu, lỗ hổng không lường trước ngay trong quá trình thiết kế, phát triển và hoạt động. Điểm yếu, hiểm họa luôn tăng rủi ro mất an ninh của hệ thống, những rủi ro này sẽ gây ra những nguy hiểm tiềm tàng tới hệ thống máy tính.



Hình 2. Mối quan hệ giữa các yếu tố ảnh hưởng tới an ninh máy tính.

3.3. Mô hình quan hệ giữa các thực thể

Khi xem xét các yếu tố và mối quan hệ trên, với quan điểm *"Hệ thống luôn đảm bảo an ninh khi chưa phát hiện ra rủi ro"*, chúng tôi đề cập đến vấn đề lượng giá an ninh của hệ thống dựa trên các yếu tố rủi ro sau quá trình kiểm tra, phát hiện.



Hình 3. Mô hình quan hệ giữa các thành phần lượng giá an ninh máy tính.

Tác động (Impact): Định lượng những thiệt hại gây ra cho hệ thống, được sử dụng để đo mức độ ảnh hưởng của một cuộc tấn công có khả năng thành công.

Ti lệ rủi ro (Risk rating): Định lượng khả năng hệ thống có thể bị xâm phạm bằng một phương pháp cụ thể tới các rủi ro đang tồn tại trên hệ thống.

Tính phổ biến (Popularity): Định lượng khả năng có thể áp dụng phương pháp phá hoại cụ thể trong khai thác rủi ro của hệ thống.

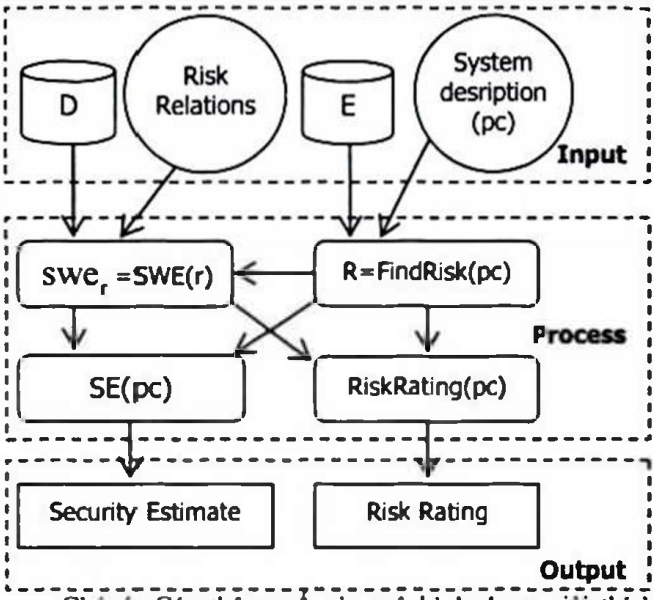
Tính đơn giản (Simplycity): Định lượng độ dễ dàng khi áp dụng phương pháp phá hoại cụ thể trong khai thác rủi ro của hệ thống.

Trong mô hình quan hệ giữa các thực thể ảnh hưởng tới an ninh máy tính, yếu tố đơn giản và tính phổ biến của một phương pháp xâm phạm tới an ninh hệ thống sẽ cấu thành yếu tố tỉ lệ rủi ro phải gánh chịu cuộc tấn công bằng chính phương pháp này. Có nhiều máy tính tồn tại nhiều điểm yếu nhưng vẫn hoạt động, một trong những lý do chính là những lỗ hổng tồn tại trên hệ thống đó có tính phổ biến thấp và yếu tố phức tạp cao vì vậy tỉ lệ rủi ro hệ thống đó phải gánh chịu sự xâm nhập qua lỗ hổng tồn tại là thấp, mặc dù nếu thực hiện thành công sự xâm nhập có thể những tác động gây hại tới hệ thống là rất lớn. Những yếu tố kế thừa từ Risk Generator như Process, Threat Agents đều có những mối quan hệ logic trong quá trình hoạt động, chúng tương tác và giúp hệ thống hoạt động tốt hơn, nhưng ngược lại cũng có thể quá trình tương tác đó gây ra những hiểm họa tiềm tàng.

Để lượng giá và đo các thuộc tính trong mô hình trên chúng tôi sử dụng hai tham số là SE ($0 \le SE \le 1$, Security Estimate - Giá trị an ninh) và SWE ($0 \le SWE \le 1$, Security Weight Estimate - Giá trị trọng số an ninh). Các giá trị SE, SWE sử dụng lượng giá cho tính đơn giản, tính phổ biến, tỉ lệ rủi ro, tác động sẽ được xác định thông qua tri thức chuyên gia [12].

4. Kỹ thuật lượng giá an ninh máy tính

4.1. Mô hình lượng giá



Chú ý: Các thông số của mô hình được giải thích trong phần 4.2, 4.3, 4.4.

4.2. Hàm tìm kiếm rủi ro

Thiết lập hàm số, biến số

- FindRisk(pc): Hàm tìm kiếm những rủi ro trên mục tiêu pc cần lượng giá.
- E: Cơ sở dữ liệu chuẩn về những rủi ro được phát hiện và công bố.

R: Cơ sở dữ liệu những rủi ro được phát hiện trên mục tiêu lượng giá ($R \subset E$), đây chính là tập kết quả trả về cho hàm FindRisk(pc).

e: rủi ro được lấy ra từ E ($e \in E$)

- check(e): mục tiêu có thể được khai thác qua điểm yếu e.
- attack(e): tấn công thử nghiệm mục tiêu qua điểm yếu e.

Giải thuật

```
function FindRisk(pc)
R = ∅
   for each e in E  do
     if check(e) then
```

```
        if attack(e) then
              R = R∪e
        endif
        endif
endfor
return R
end function.
```

4.3. Hàm tính tỉ lệ rủi ro

Thiết lập hàm số, biến số

SWE(r): hàm tính tỉ lệ rủi ro bị đối phương tấn công khi điểm yếu r tồn tại trên mục tiêu cần lượng giá, đồng thời là trọng số của giá trị Attack potential.

D: Cơ sở dữ liệu tri thức chuyên gia cho các thông số Impact, Popularity, Simplycity.

r: rủi ro được lấy ra từ R ($r \in R$)

LookupI(r,D),LookupP(r,D),LookupS(r,D: hàm lấy ra thông số Impact, Popularity, Simplycity của rủi ro r trong cơ sở dữ liệu D.

Giải thuật

```
function SWE(r)
   p=LookupP(r,D)
   s=LookupS(r,D)
   return p*swe_p +s*swe_s
end function
```

4.4. Hàm lượng giá an ninh, rủi ro máy tính

Thiết lập hàm số, biến số

SE(pc): Hàm lượng giá giá trị an ninh cho mục tiêu pc.

RiskRating(pc): hàm tính tỉ lệ rủi ro bị đối phương tấn công mục tiêu cần lượng giá.

Giải thuật

```
function SE(pc)
      R = FindRisk(pc)
      for each r in R do
            swe_i =SWE(r)
            se_i =LookupI(r)
      endfor
return (1 - Σ(se_i * swe_i) / Σswe_i)
end function
function RiskRating(pc)
      R = FindRisk(pc)
      for each r in R do
            swe_i =SWE(r)
            se_i =LookupI(r)
      endfor
return Σ(se_i * swe_i) / Σswe_i
end function
```

5. Triển khai phương pháp lượng giá

5.1. Tiếp cận hệ thống

Có một số phương pháp tiếp cận hệ thống [6,7,11,13] tuy nhiên cần tách biệt giữa tiếp cận an ninh máy tính và an ninh mạng máy tính. Trong phương pháp lượng giá mà chúng tôi xây dựng, để tiếp cận hệ thống kiểm tra an ninh cho máy tính, chúng ta sử dụng cách tiếp cận kiểu insider (white box), associate (gray box), không nên sử dụng phương pháp tiếp cận outsides (black box) do mức độ hạn chế của chúng sẽ không xác định được toàn bộ những rủi ro trên hệ thống lượng giá. Chúng ta xem xét bảng so sánh một số tiêu chí giữa ba cách tiếp cận trên.

Phương pháp tiếp cận	Phá hoại qua mạng	Phá hoại mức vật lý	Đã biết hệ thống	Đã biết tài khoản
• Outsiders • Black box	Có	Không	Không	Không
• Associates • Gray box	Có	Có	Có	Không
• Insiders • White box	Có	Có	Có	Có

5.2. Kỹ thuật kiểm tra

Phổ biến hiện nay có ba phương pháp kỹ thuật kiểm tra rủi ro về an ninh của máy tính và mạng là Flaw hypothesis testing (Richard R. Linde-1975), Penetration testing (Weissman-1995, Polk-1992) và Attack trees testing (Bruce Schneier-1999). Dựa trên các biện pháp kỹ thuật của ba phương pháp này, người ta đưa ra một số quy trình kiểm tra an ninh hệ thống máy tính như NSA IEM [6,7], OSSTMM (Peter Vincent Herzog[9]),... Để xác định các tham số SE và SWE bài báo sử dụng tri thức chuyên gia được mô tả trong [12] qua đó ta xây dựng được cơ sở dữ liệu lượng giá các giá trị an ninh và trọng số an ninh của các tham số đầu vào như Impact, Risk Rating, Popularity, Simplycity, Attack Potential.

Bộ đo Risk Mediator sẽ hoạt động dựa trên hai kỹ thuật là Penetration testing và Attack trees testing với cơ sở dữ liệu lỗ hổng, rủi ro được lấy từ cơ sở dữ liệu chuẩn, được công bố tại SANS, BugTraq. Đồng thời sử dụng các kỹ thuật [6-10,12-14] Footprinting, Scanning, Enumeration, Sniffers, Denial of Service, Session hijacking,... để xác định toàn bộ những hiểm họa có thể xảy ra với mục tiêu

6. Kết luận

Phương pháp lượng giá an ninh hệ thống trong bài báo đã xác lập được các yếu tố cấu thành an ninh trong từng trường hợp cụ thể. Tư tưởng chính của phương pháp là giả định hệ thống cần lượng giá là mục tiêu cần tấn công, bộ đo mức độ an ninh trở thành đối phương muốn xâm phạm tới hệ thống.

Các yếu tố ảnh hưởng tới an ninh hệ thống máy tính (khái niệm máy tính được hiểu ở đây bao gồm máy tính, thiết bị mạng, thiết bị đầu cuối kết nối mạng) có mối quan hệ logic với nhau đã được phối hợp trong nội dung của phương pháp. Tuy nhiên, đây chưa phải là mô hình đầy đủ về các thành phần cấu thành an ninh hệ thống, đồng thời các thông số, trọng số cũng chưa thể hiện hết được những yếu tố có tính định tính. Trong nghiên cứu tiếp theo, phương pháp sẽ được phát triển tiến tới lượng giá an ninh cho hệ thống mạng, đồng thời triển khai thử nghiệm trên các bộ dữ liệu chuẩn, số lượng lớn, qua đó sẽ có những đánh giá và hiệu chỉnh phù hợp hơn với điều kiện thực tiễn.

Tài liệu tham khảo

[1] Jonas Hallberg, Amund Hunstad and Mikael Peterson, A Framework for System Security Assessment, *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security*, United States Military Academy, New York, (2005) 224.

[2] Hallberg, J. Hunstand, A. Bond, A. Peterson, M. Humtad, A. Pahlsson, *Scientific report - System IT Securlfy Assessment*, Linkdping university, Sweden, 11/2004.

[3] Amund Hunstad, Jonas Hallberg, Richard Andersso, Measuring IT security - a method based on common criteria's security functional requirements, *Proceedings of the 5th IEEE Workshop on Information Assurance*, United States Military Academy, New York, (2004) 226.

[4] Jac Seung Lee, Sang Choon Kim, and Seung Won Sohn, A Design of the Security Evaluation System for Decision Support in the Enterprise Network Security Management, *Springer-Verlag*, Berlin Heidelberg, 2015 (2001) 246.

[5] Tai-hoon Kim and Seung-youn Lee, Security Evaluation Targets for Enhancement of IT Systems Assurance, *Springer-Verlag*, Berlin Heidelberg, 3481 (2005) 491.

[6] Russ Rogers, *Network Security Evaluation Using the NSA IEM*, Syngress Publishing, USA, 2005.

[7] Brad C. Johnson, *INFOSEC Assessment Methodology (IAM), INFOSEC Evaluation Methodology (IEM)*, National Security Agency (NSA), Washington, 2004.

[8] John Wack, Miles Tracy, Murugiah Souppaya, *Guideline On Network Security Testing, Recommendations of National Institute of Standards and Technology*, NIST Special Publication 800-42, USA, 10/2003.

[9] Peter Vincent Herzog, *Open-Source Security Testing Methodology Manual*, The Institute for Security and Open Methodologies, USA, 08/2003.

[10] Chris McNab, *Network Security Assessment*, O'Reilly Media Publishing, USA, 03/2004.

[11] Igor Kotenko, Active Vulnerability Assessment of Computer Network by Simulation of Complex Remote Attacks, *Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing (ICCNMC'03)*, Shanghai, China, (2003) 40.

[12] Joel Scambray, Stuart Mcclure, George Kurtz, *Hacking Exposed: Network Security Secrets and Solutions 2nd Edition*, McGraw-Hil Publishing, California, 2001.

[13] Nguyen Thien Luan, Tran Hong Quang, Finding target in the Distributed systems for Attack, *Journal of Science and Technique*, Vietnam Military Technical Academy 112 (2005) 19.

[14] Thomas Mathew, *Ethical Hacking: Student Courseware*, OSB Publisher, New York , 2004.

A new method for computer security assessment

Nguyen Thien Luan, Tran Hong Quang

Faculty of Information Technology, Vietnam Military Technical Academy,

100 Hoang Quoc Viet, Hanoi, Vietnam

This paper presents a new methodology for computer and network security assessment. The methodology is built on the base of researching the model of computer and network security relations and their elements. Also, the author introduces the model and framework, which in turn assest the overall computer security.