Modelování kybernetických útoků
The Modeling of the Cyber Attacks

Josef Požár[1]*,*

Fakulta bezpečnostního managementu, Policejní akademie České republiky v Praze

ABSTRACT

Cyber security methods are continually being developed. To test these methods many organizations utilize both virtual and physical networks which can be costly and time consuming. As an alternative, in this paper, we present a modeling approach to represent computer network and ito efficiently simulate cyber attack scenarios. The outcome of the model is a set of IDS alerts that can be used to test and evaluate cyber security systems. In particular, the methodology is designed to test information vision systems for cyber security that are under development.

ABSTRAKT

Metody kybernetické bezpečnosti se neustále vyvíjí. Testování těchto metod provádějí různé organizace pomocí virtuálních a fyzických sítí, přičemž se jedná o poměrně nákladné a časově náročné postupy a procesy. Jako alternativu se uvádí přístup modelování scénářů kybernetických útoků na počítačové a systémy detekce průniku (IDS) pro účinnou simulaci scénářů. Výsledkem modelu je pak soubor záznamů IDS, které mohou být použity k testování a vyhodnocení systému kybernetické bezpečnosti. Tato metodika je určena k testování informační fúze systémů kybernetické bezpečnosti, která se neustále vyvíjí.

1 ÚVOD

Jak vzrůstá počet a aplikace počítačových sítí, tak také rostou útoky proti těmto sítím a jejím komponentům. Z toho důvodu je nutná efektivní ochrana před kybernetickými útoky. Proto je důležité poznat mechanismus a proces kybernetického útoku. To však není jednoduché, protože v reálném světě existuje obrovská množina variant jednotlivých útoků, která závisí nejen na konfiguraci sítí, ale především na znalostech a zkušenostech útočníků. Proto také administrátoři hledají lepší ochranu sítí a serverů. Nástroje kybernetické bezpečnosti pak automaticky upozorňují na podezřelé síťové aktivity. Většinou se administrátoři musí každý den vypořádat s miliony takových varování (alertů). V současné době se postupně vyvíjejí nástroje pro posuzování rizik kybernetických útoků. Množství údajů a dat potřebných k testování a vyhodnocování jejich relevance se vyhodnocuje podle modelových technik ve většině případů automaticky. Metoda modelování pak umožňuje uživateli vytvořit virtuální počítačovou síť, která generuje počítačové útoky a varuje uživatele, administrátora před narušením systému. Proto je tento rámec flexibilní a umožní modelování a efektivní tvorbu dat testování a hodnocení bezpečnosti jednotlivých objektů.

Existují jisté výsledky modelování počítačové sítě a kybernetických útoků. Například, Lee et al.[2] (2004) a Nicol et al.[3] (2003) uvádějí metody modelování provozu

[1] doc. RNDr. Josef Požár, CSc. Dean, Faculty of Security Management, Police Academy of the Czech Republic in Prague.

počítačové sítě na úrovni paketů. Zde se modeluje tok a zpracování paketů v počítačové síti, přesto je možné (potenciálně několik miliard paketů za den), že i jen malý zlomek paketů způsobí velkou škodu.

Cílem článku je ukázat a trochu osvětlit mechanismus kybernetických útoků a tak pochopit jejich logiku. Proto se dále uvádějí vývojové diagramy a tabulky, které umožňují pochopit procesy kybernetických útoků.

2 Modelování kybernetických útoků

Tato část popisuje podrobně obecné přístupy modelování počítačových sítí a kybernetických útoků při generování odpovídacích dat a informací.

Počítačové sítě jsou modelovány pomocí dvou základních konstrukcí. Jsou to stroje a další objekty - konektory. Třetím objektem jsou podsítě, které představují skupiny počítačů a sítě, které nazýváme moduly. Tyto moduly zastupující stroje, spojovací vodiče a podsítě jsou vizuální reprezentací počítačové sítě. Nicméně, funkčně tyto moduly umožňují uživateli zadávat data do počítačové sítě. To je však pouze mechanistický přístup k problému ochrany pře kybernetickými útoky na daném rozhraní.

Kybernetické útoky jsou inicializovány a spouštěny hackery z prostředí internetu. Mohou se také modelovat akce vnitřního útočníka, ale to není naším primárním cílem. Hacker útočí v závislosti na jeho schopnostech a zranitelnosti počítačové sítě a serverů. Sudit et al. (2005) vypracoval model modelování inicializace a průběhu počítačového útoku prostřednictvím počítačové sítě.

Sudit et al. (2005)[4] sestavil pořadí útočných akcí v dané posloupnosti, kdy hacker používá etapy, stadia, která odpovídají jeho schopnostem a stavu zabezpečení sítě. Tyto fáze jsou označovány jako Stadium 0 až stupeň 9 Stadium, kde 0 představuje obecně průzkum aktivit, vazby na vnější části počítačové sítě. Útočník se pomocí exploitů získává více informací o síti. Externí stroj je přístupný z internetu. Vnitřní stroj, který může být přístupný z externího zařízení přes bránu firewall nebo z jiného vnitřního stroje. Stadia 0 - 4 představují hackerské akce na vnějších strojích. Stadia 5 - 9 představují hackerské akce na vnitřních strojích. Tabulka 1 představuje některé typické hackerské akce, které odpovídají kybernetickému útoku. Hacker může zaútočit na stroj, který je na vnější straně počítačové sítě. Jakmile externí zařízení byla úspěšně kompromitována, pak hacker může využít způsoby této kompromitace k snadnějšímu přístupu k interním strojům. Jakmile se útočník infiltroval do vnitřní sítě, pak jsou zcela jistě ohrožena vnitřní zařízení, když útočník dosáhne svého cíle. Obrázek 2 znázorňuje proces kybernetický útok z internetu cíl na vnitřní stroj.

---

[2] Lee, J.-S. J.- R. Jung, J.-S. Park, and S. D. Chi. 2004. Linux-based system modeling for cyber attack simulation. In *Proceedings of the 13th International Conference on AI, Simulation, and Planning in High Autonomy Systems*, Jeju Island.

[3] Nicol, D.; J. Liu, M. Liljenstam, and G. Yan. 2003. Simulation of large-scale networks using SSF. In *Proceedings of the 2003 Winter Simulation Conference*, ed. S. Chick, P. J. Sánchez, D. Ferrin, and D. J. Morrice, 650-657. Institute of Electrical and Electronics Engineers,Piscataway, NJ.

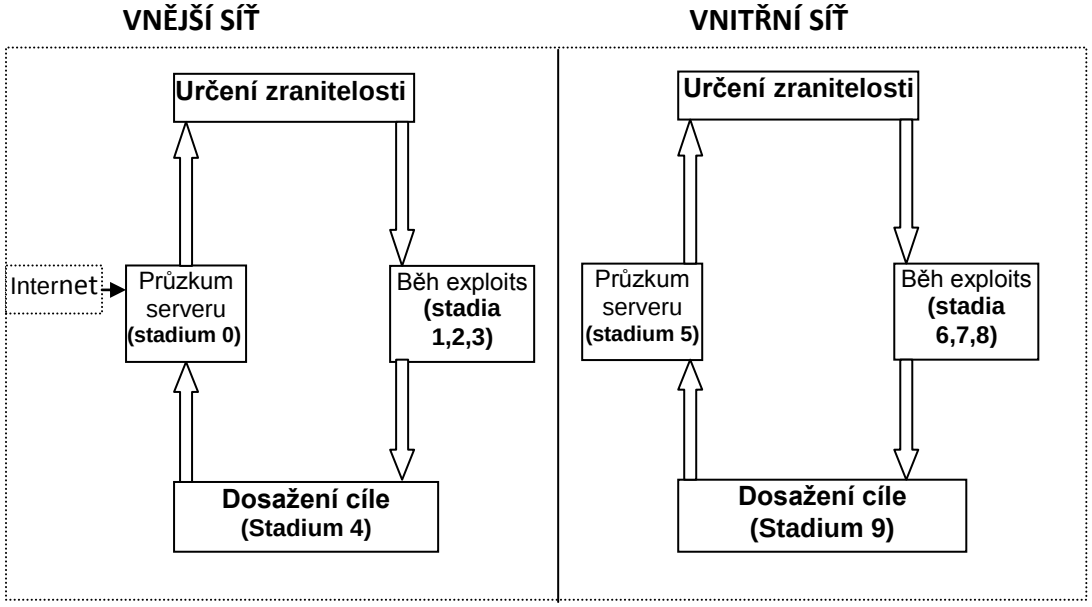
[4] Sudit, M., A. Stotz, and M. Holender. 2005. Situational awareness of coordinated cyber attack. In *Proceedings of the International Society for Optical Engineering Conference*, Orlando, FL.

Stadium	Typická akce
0	Průzkum PC (Serveru)
1	Narušení
2	Escalation service, útok
3	Vniknutí
4	Dosažení cíle
5	Průzkum PC (Serveru)
6	Narušení
7	Escalation service, útok
8	Narušení
9	Dosažení cíle

Tabulka 1. Typické hackerské akce při kybernetickém útoku

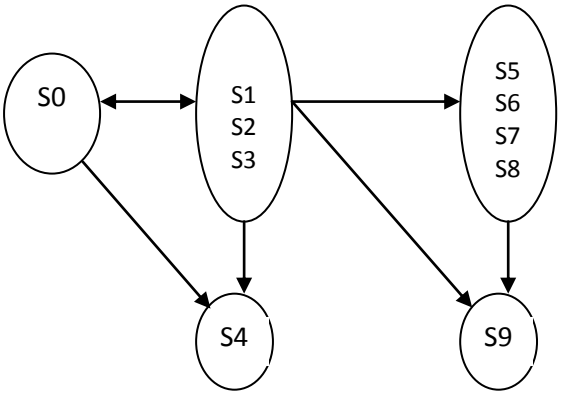
Tento model obsahuje automatizovaný systém a uživatelem specifikované kybernetické útoky. Automatizované metody využívají síťové konektivity a specifikace v kombinaci se šablonami v závislosti na schopnostech útočníka a zranitelnosti sítě a vytvářejí vhodný postup jednotlivých kroků kybernetického útoku.

Na obrázku 1 je znázorněný postup a mechanismus kybernetického útoku z Internetu.



Obrázek 1. Postup, vývoj kybernetického útoku na počítačovou síť z Internetu

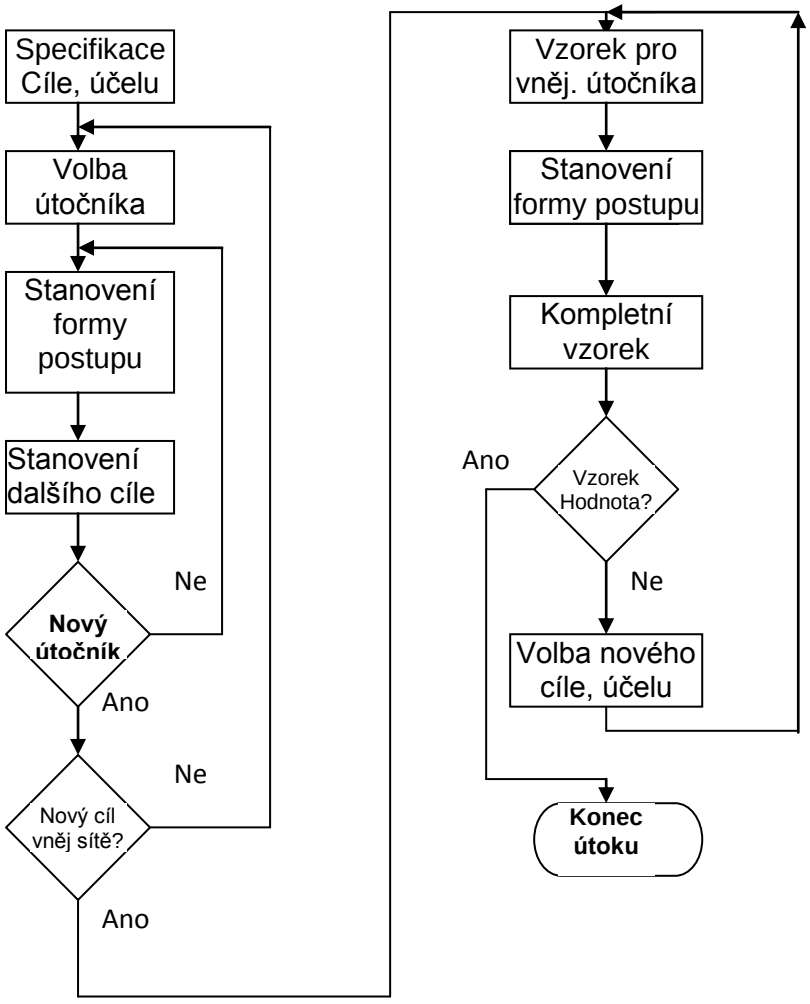
V další části je možné uvést graf, který znázorňuje postup modelování kybernetického útoku. Ten vychází z obrázku 1. Tento model řídí je zobrazen na obrázku 2 (stadia S0, S1, ..., S9).



Obrázek 2. Orientovaný graf reprezentující strukturu útoku

Tento graf je orientovaný graf, což znamená, že hrana (oblouk) uvádí pouze reálný přechod jistým směrem. Uzly v rámci stejné skupiny tvoří kompletní graf, v němž každý uzel je připojen na každém uzlu. Tento graf je reprezentován jako přilehlosti (incidence) matice 1 a 0. Struktura útoku je pak reprezentovaná orientovaným grafem.

Struktura útoku (v podobě návodů a šablon) a konfigurace sítě je tak specifikována, že uživatel může specifikovat cílový stroj, cíl Obrázek 3 znázorňuje algoritmus zautomatizované metody, která slouží ke generování specifických stadií útoku.



Obrázek 3. Metoda generování automatického útoku

Při generování jednotlivých kroků je možné přesněji specifikovat postupy a algoritmy pro kybernetickou bezpečnost sítí a serverů. Je to důležité pro další vývoj metodiky pochopení topologie sítí a serverů s cílem omezit kybernetické útoky.

3. Závěr

Uvedený model pouze stručně naznačuje postupy a procesy, které je nutné zvažovat při ochraně systému před kybernetickými útoky. Mezi významné funkce náleží zejména:

- Konstrukce scénářů jednotlivých kybernetických útoků.
- Separace generování automatizovaných útoků a událostí.
- Definování seznamu služeb běžících na počítači.
- Definice seznamu portů a protokolů, jež jsou povoleny či zakázány.
- Současné výzkumy uvádějí další validace a funkce pro zvýšení účinnosti modelů kybernetických útoků.

Současné výzkumy uvádějí další validace a funkce pro zvýšení účinnosti modelů kybernetických útoků.

Literatura

LEE, J.- S., J.-R. JUNG, J.-S. PARK, and S. D. CHI. 2004. Linux-based system modeling for cyber attack simulation. In *Proceedings of the 13th International Conference on AI, Simulation, and Planning in HighAutonomy Systems*, Jeju Island.

LINUS, J. 2001. An Introduction to Data and Information Fusion. (Presentation) Available Online via <http://www.infofusion.buffalo.edu/t utorialPage.php> [Accessed July 15, 2007].

KELTON, W. D., R. P. SADOWSKI, and D. T. STURROCK. 2004. *Simulation with ARENA*, Third Edition, McGraw-Hill, Boston, MA.

NICOL, D., LIU J., LILJENSTAM M., and YAN, G. 2003. Simulation of large-scale networks using SSF. In *Proceedings of the 2003 Winter Simulation Conference*, ed. S. CHICK, P. J. SÁNCHEZ, D. FERRIN, and D. J. MORRICE, 650-657. Institute of Electrical and Electronics Engineers, Piscataway, NJ.

SUDIT, M., A. STOTZ, and M. HOLENDER. 2005. Situational awareness of coordinated cyber attack. In *Proceedings of the International Society for Optical Engineering Conference*, Orlando, FL.