UDC 621.39

EXAMINATION OF MODERN CONCEPTS FOR FIREWALLS AND COLLABORATIVE INTRUSION DETECTION

Andriy Luntovskyy
BA Dresden Univ. of Coop. Education Saxon Academy of Studies Dresden, Germany
Andriy.Luntovskyy@ba-dresden.de
Mikhailo Klimash
Lviv National Technical University "Lviska Polytechnika" Lviv, Ukraine
mklimash@polynet.lviv.ua

Background. Modern firewall systems are compared to classical concepts. The filtering rules are analyzed on the examples of the leading solutions (presented by Gartner Inc.). The collaborative intrusion detection systems and networks as well as the threats based on the insider attacks on CIDN are examined. A common CIDN functionality catalogue is discussed. The aspects of the application of modern systems of network intrusion detection and prevention by the peculiarities of their implementation at different levels are considered in accordance with the model of ISO/OSI. Brief recommendations on the use of known network security solutions in the construction of modern infocommunication networks to overcome various types of threats, in particular DoS type, virus and social engineering, are given.

Objective. The aim of the paper is to study the implementation and application of modern concepts of firewalls and collaborative network intrusion detection systems.

Methods. The research was carried out based on analysis of a large number of literary sources, the theory of building information security systems and avenues of manufacturers of systems for detecting and preventing network intrusion.

Results. The advanced firewalls like SMLIF, IPS, the collaborative intrusion detection systems gain in importance increasingly nowadays. They can be also deployed within the scenarios of NFC and IoT (Internet of Things). The FW and IDS are often combined into individual participating peers (LAN, WLAN, 2G-4G, NFC and Bluetooth) with possibility of collaboration and better prevention of both external and insider attacks.

Conclusions. The conducted research indicates the need to improve the implementation of modern network architecture with the use of integrated systems for detecting and counteracting network attacks. Despite the wide variety of network security solutions, this area of research remains relevant and suggests that the development of new concepts for protecting network architectures meets the current state of the industry, is timely and relevant, given the wide range of capabilities and scenarios for malicious intrusions and network system impacts.

Keywords: firewall; network attacks; intrusion detection systems; intrusion prevention systems; CIDN.

I. MOTIVATION

Since 2012 the development of modern firewalls and the systems based on them (intrusion detection, intrusion prevention) as well as of collaborative systems have been commonly triggered by the trend of "collaborative intrusion detection networks" with increasing of safety and security of the network domains of diverse MAC-layers (including mobile and wireless) and purposes.

The FW and IDS are combined into individual participating peers (LAN, WLAN, 2G-4G, NFC and Bluetooth) with possibility of collaboration and better prevention of both external and insider attacks.

The structure of this paper is as follows:

- Section I represents the motivation to examine the discussed issues;
- Section II deals with the basic Firewall Concepts and their further development like SIF, NGFW, WAF, SMLIF;
- Section III presents IDS, IPS, AEF as well as the collaborative IDS and the network combinations of them called CIDN;
- In Section IV the typical external CIDN Attacks as well as the threats of the Insider Attacks on CIDN are discussed.

The authors are graceful to the BA Dresden Univ. of Coop. Education and Lviv National Technical University "Lviska Polytechnika".

© 2017, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

II. BASIC FIREWALL CONCEPTS

A. Classical Firewalls

Public available services (Web server, FTP server, File Sharing, Web Services etc.) are placed in the DMZ before the actual Firewalls (Table I). Different filtering functionality can be offered (Fig. 1):

- PF (Layer 3);
- CR (Layer 4);
- AG (Layer 5-7).

A FW system with multiple internal services and with DMZ with public offered services is shown in Fig. 2.

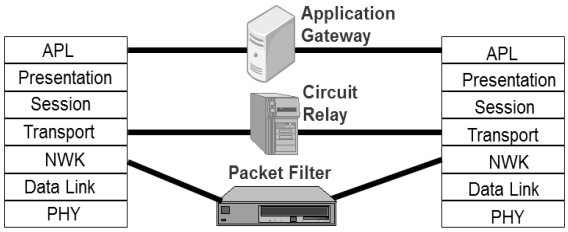

Fig. 1. Classical Firewalls: main concepts ordered to the OSI layers

The main purpose is blocking of the unauthorized access attempts to private networks based on IP-addresses (PF, Packet Filter), TCP/IP-port information (CR, Circuit Relay) or application-related information (AG, Application Gateway):

B. Comparison and Further Development

Table I depicts the filter abilities for basic firewall concepts. The available functions can be separated correspondingly to the following concepts: PF (packet filters), CR (circuit relays) and AG (application gateways). Furthermore the integrated functionality the hybrid FW concept possesses the so called SIF – Stateful Inspection Firewall [1] from Check Point Software Technologies.

The PFs and CRs are very simple and efficient. The AGs, or Application Layer FW, bring tighter the key benefits of the common filtering: they can "understand" certain applications and protocols such as VPN, DNS, FTP, SMTP, POP3/IMAP, HTTP as well as their secured versions, e.g. HTTPS, SSH etc. For use of Cloud Access Monitoring for the virtualized clusters, networks, storages (VLAN, SAN/NAS) and services (VMs, RAICs) as well as SDN there are some special FW solutions.

Since 2012 the new generation of AGs (NGFW) has been deployed. NGFW is nothing more than the "widen" and "deepen" inspection at the application-stack based on the classical SIF solutions (refer Table I). The existing deep packet inspection systems can be extended via:

- Intrusion detection systems (IDS);
- Intrusion prevention systems (IPS);
- User identity integration (by binding user IDs to IP or MAC addresses for "reputation").

The special kind of NGFW is the so called Web Application Firewall (WAF). The defense against the WAF attacks was implemented in the tool "WAF Fingerprinting utilizing timing side channels" (WAFFle) [1-3].

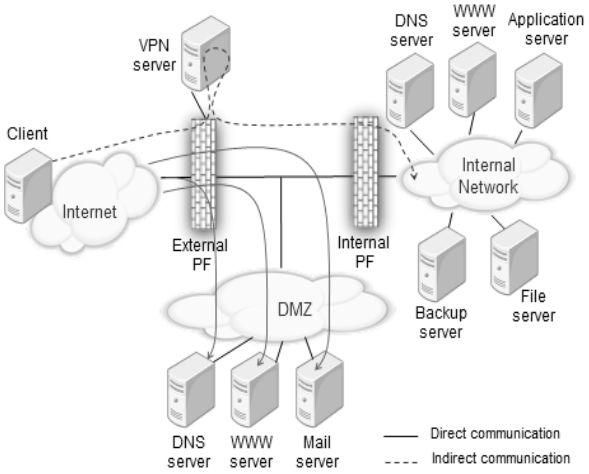

Fig. 2. Example for FW-secured network services including FW systems with DMZ

For better demarcation we should address a firewall, a security system that protects a single computer, the peers or networks against unwanted or illegal access. However, the functionality of a firewall is not directly oriented to detect the external hacker attacks. A classic FW implements only separate filtering rules to protection directly for network (mobile, wireless) communication. The advanced IDS / IPS modules are responsible for the detection of different attack types, which can be also used on the top of the well-known firewall solutions (classical and advanced):

- IDS – describe the detection of attacks that are directed against a computer system or network. IDS serve to increase the security in a network;
- IPS – these systems are the enhanced IDS, which also provide the defense functionality to fend off in the case of the discovered network attacks (external as well as of an insider!).

Therefore, the IDS/ IPS can be a further development of the FW as the advanced firewall modules. The next significant generation of the combined SIF/ NGFW are SMLIF (Stateful Multilayer Inspection Firewalls). By opinion of Gartner Inc. (founded in 1979, reg. NYSE in IT-Branch as the world's leading IT research and advisory company) the following top list of modern SMLIF can be represented [2 - 4]:

- AhnLab
- Barracuda Networks
- Check Point Software Technologies
- Cisco
- Dell SonicWALL
- F5
- Fortinet
- Hillstone Networks
- HP

- Huawei
- Intel Security (McAfee)
- Juniper Networks
- Palo Alto Networks
- Sangfor
- Sophos
- Stormshield
- WatchGuard (by Gartner, Inc.).

They listed that firewall solutions operate the cross-layered multi-defense with combining of multiple filter abilities, like e.g. pos.18-23 (refer Table I as well as the next sections).

C. *Advanced Evasion Technologies*

Advanced Evasion Technologies (AET) work fully anonymously and without any traces so there are new challenges for (virtual) network data security. In contrast to the known evasions/penetrations AET combines and changes the methods to camouflage an attack or malicious code. These combinations allow hackers to infiltrate into network unnoticed in spite of multiple security solutions. According to current estimations, there are more than 2**180 potential combinations of AET. Some combinations include cross-layered functionality and several OSI layer integrated attacks!

Really IPS or AEF (Advanced Evasion Firewalls) represent themselves as effective technologies against AETs. They can combine attack patterns at different OSI layers, e.g. AET-Platform from Stonesoft: http://evader.stonesoft.com. Such kind of the IPS provides a combined protection: IPS, AV, FW, DMZ, Network Zoning (division into protection domains). The deployment makes sense for large companies with multiple branches and structural units.

Some of such patterns and test series are as follows:

- At layers 3, 4: Firstly the opportunities for the attacks on the IP, TCP, UDP are discovered;
- At layers 5-7: The APL-layer protocols such as SMB and RPC are protected. Therefore, the internal threats have to be are assessed;
- Then AET can discover threats for other protocols such as IPv6, HTTP;
- If AET uses HTTP (Port 80), the hackers can also the FW mislead and infiltrate with malware into the network over the web traffic. Therefore is AETs for web services, web applications and cloud computing environments a particularly serious threat.

III. COLLABORATIVE IDS AND NETWORKS. CIDN

The widespread Intrusion Detection Systems (IDS) evaluate and prohibit the potential hacker attacks that aimed at computer systems or network. IDS increase data security significantly in opportune to the classical firewalls which lonely support is not satisfying.

Intrusion Prevention Systems (IPS) are the enhanced IDS which provide the additional functionality aimed to discover and avoid the potential attacks.

Nevertheless, as a rule the classical IDS/IPS are operated autonomously. They can't detect temporary unknown hacker threats which became more sophisticated and complex year by year. Those dangerous threats can serve to disorder the operation of data centers and computing clusters round-the-clock in 24/7-mode. Therefore the cooperation and collaboration of the IDS within a network is of the great meaning. The comparison of the NW-IDS vs. IDS pure is depicted in Fig. 3. The NW-IDS has a lot of new features.

TABLE I. BASIC FIREWALL CONCEPTS AND THEIR FILTER ABILITIES (OWN REPRESENTATION)

Filter abilities	**FW concepts**				
	PF	***CR***	***AG***	***SIF***	***Next genera-tions***
1. IP source/ target addresses	+			+	
2. TCP-Ports and connections		+		+	
3. Denial-of-service attacks (DOS), distributed DOS		+			
4. Enabled or disabled protocols		+	+	+	
5. Proxies for certain services			+	+	
6. HTTP-Proxy, proxy server			+	+	
7. AV-Software (viruses, worms, Trojans)			+	+	
8. Malware blocking			+	+	
9. Anti-Phishing			+	+	
10. APL-specific authentication			+	+	
11. APL-specific encryption			+	+	
12. DMZ	+			+	
13. VPN and IPsec	+			+	
14. Enabled Domain Names (source/ target)	+		+	+	
15. SPAM filtering			+	+	
16. Analysis of content-specific key words			+	+	
17. Blocking of special applications and scripts (Java applets, Active-X, Web Services, further plugins)				+	
18. Web Appl. Firewall					s
19. Cloud Access Monitoring					s
20. Virtualized networks, storages and services					s
21. SDN					s
22. IDS, IPS, NW-IDS (intrusion detection/ prevention/ network collaboration)					s
23. CIDN as the networks of IDS/IPS					s
24. Time window control	+	+	+	+	+
Legend: + – available; s – special solutions available					

TABLE II. THE COMMON CIDN FUNCTIONALITY CATALOGUE (OWN REPRESENTATION BASED ON [4-6])

Certain CIDN examples	Topology type	Focus	Specialization on the threats	Robustness against attacks A1-A4	Robustness against attacks A5-A9	Privacy awareness	Anonymity awareness
Indra	Distributed	Local	SPAM	R	R	A	A
Domino	Decentralized	Global	Worms	R	R	A	A
Abdias	Centralized	Hybrid	Trojans	R	R	A	A
Crim	Centralized	Hybrid	Social Engineering, WAF	R	R	A	A
Legend: R – Robustness, A – Awareness							

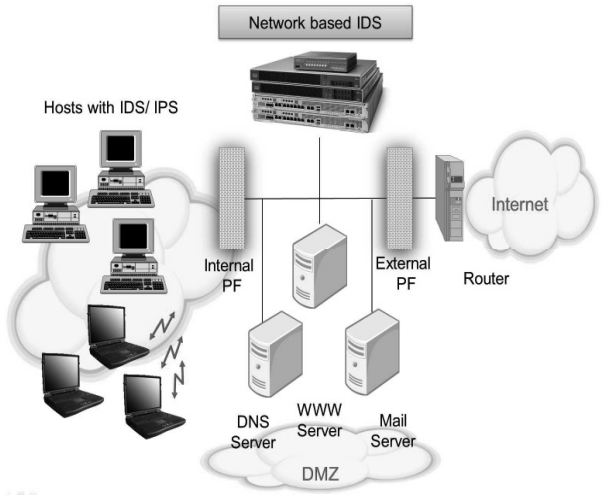

Fig. 3. Comparison of IDS pure vs. NW-IDS

CIDN is a further concept for a collaborative IDS/IPS network intended to bridge over the disadvantage of the standalone defense against the unknown dangerous attacks. The CIDNs allow (Fig. 4) participating IDS as the network peers to share the detected knowledges, experiences and best practices oriented against the hackers' threats [4].

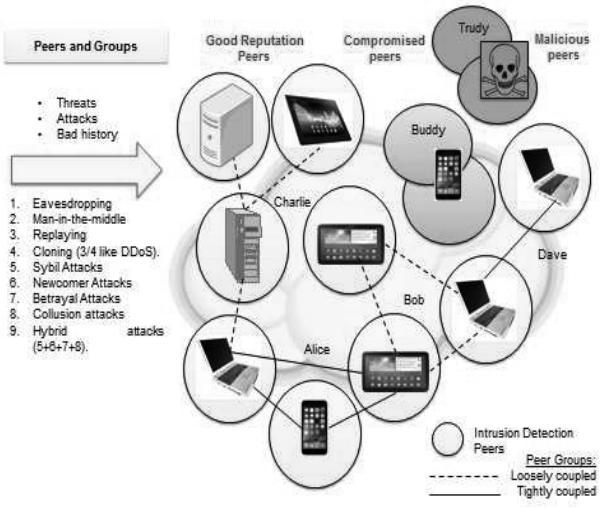

Fig. 4. Example of cooperation within the CIDNs

The main requirements for the construction of a CIDN and the support of such functionality are as follows: efficient communication at short up to middle distance, robustness of the peers (IDS) and links, scalability and mutual compatibility of individual participating peers (IDS). The typical interoperable networks are as follows: LAN, WLAN, 2G-4G as well as nest for NFC and Bluetooth.

Collaborative intrusion detection networks (CIDN) consist of multiple NW-IDS under use of multiple PC, end radio-devices and installed firewalls, the groups of users directed by the users Alice, Bob, Charlie, Dave. The coupling between the groups is loose or tight. However, the insider-attacks to CIDNs are possible (user Eve).

This type of networking improves the overall accuracy on the threat danger grade as well as the intrusion level assessment. The cooperation among the participating single peers (IDS-collaborators) became more efficient within CIDN.

But, unfortunately, the CIDN can become a target of the attacks and malicious software itself. However, some malicious insiders within the CIDN may compromise the inter-operability and efficiency of the intrusion detection networks internally. Therefore a lot of CIDN research problems have to be considered [5, 6], for instance:

- Selection of the peers (collaborators) and trust management;
- Collaborative Intrusion Decision Making;
- Resource Management within CIDNs.

IV. CIDN ATTACKS. INSIDER ATTACKS ON CIDN

The traditional network attacks can significantly compromise the security inside a CIDN. The simple attacks are as follows (A1-A4 list positions):

1. Eavesdropping.
2. Man-in-the-middle.
3. Replaying.
4. Cloning (3/4 like DDoS).

The advanced insider-attacks to CIDNs (list positions A5-A9) which can suddenly occur from the peers-insiders within a not-compromised CIDN are as follows [5, 6]:

5. Sybil attacks: distribution of a large amount of pseudonyms (fake identities) via a malicious peer.
6. Newcomer attacks: a malicious peer tries to erase its "bad history" with other peers in the network.

7. Betrayal attacks: the trust mechanism robust to betrayal attacks shall satisfy the social norm: “It takes a long-time interaction and consistent good behavior to build up a high trust, while only a few bad actions to ruin it.” When a trustworthy peer acts dishonestly, its trust value should drop down quickly, hence making it difficult for this peer to deceive others or gain its previous trust within a short time back.
8. Collusion attacks: Collusion attacks occur when a group of compromised/malicious peers cooperate together in order to compromise the network.
9. Hybrid attacks (5+6+7+8).

A typical CIDN must provide the following common functionalities against these kinds of attacks (s. Table II). They can be represented by a catalogue (own matrix representation is based on [5, 6]).

V. Conclusions

The advanced firewalls like SMLIF, IPS, the collaborative intrusion detection systems are becoming more and more important nowadays. They can be also deployed within the scenarios of NFC and IoT (Internet of Things).

The FW and IDS are often combined into individual participating peers (LAN, WLAN, 2G-4G, NFC and Bluetooth) with possibility of collaboration and better prevention of both external and insider attacks.

The paper compares the modern firewall systems with their classical concepts. The extended filtering rules are analyzed and compared with the basic rules under use of practical examples for certain leading solutions presented by Gartner Inc.

The collaborative intrusion detection systems and networks as well as the threats based on the insider attacks on CIDN are examined. A common CIDN functionality catalogue is offered.

References

[1] Firewalls: in excITingIP.com (Online): http://www.excitingip.com.
[2] Greg Young. Hype Cycle for Infrastructure Protection, in Gartner Inc., 11 August 2015, Reg.-Nr. G00277614, P. 45.
[3] Adam Hils, Greg Young, Jeremy D'Hoinne. Magic Quadrant for Enterprise Network Firewalls, in Gartner Inc., 22 April 2015, Reg.-Nr. G00263955, P. 30.
[4] Andriy Luntovskyy, Josef Spillner. Architectural Transformations in Network Services and Distributed Systems: Service Vision. Case Studies, XXIV, 344p., 238 pict., Springer Nature Verlag, April 2017 (ISBN: 9-783-6581-484-09).
[5] Carol Fung, Raouf Boutaba. Intrusion Detection Networks: A Key to Collaborative Security (ISBN-13: 978-1466564121), 2013, 261p.
[6] Carol Fung. Collaborative Intrusion Detection Networks and Insider Attacks, Univ. of Waterloo, ON, Canada, 2012.

Лунтовський А.О., Климаш М.М.

Дослідження сучасних концепцій брандмауерів та спільного виявлення мережних вторгнень

Проблематика. У цій роботі проаналізовано сучасні підходи до організування мережних брандмауерів, які порівнюються з класичними концептуальними рішеннями в галузі мережної безпеки. Правила фільтрації мережного трафіку аналізуються на основі розгляду прикладів у рамках обраних рішень (які представлені компанією Gartner Inc.). Розглядаються спільні системи і мережі виявлення вторгнень (CIDN), а також загрози, засновані на основі розгляду випадків інсайдерських нападів на CIDN. Коротко проаналізовано загальний перелік функціональних можливостей CIDN систем. Розглянуто аспекти застосування сучасних систем виявлення та запобігання мережним вторгненням за особливостями їх реалізації на різних рівнях згідно моделі EMBBC. Надано стислі рекомендації щодо застосування відомих рішень мережної безпеки при побудові сучасних інфокомунікаційних мереж для подолання загроз різного типу, зокрема DoS типу, вірусних та соціальної інженерії.

Мета досліджень. Дослідження особливостей реалізації та застосування сучасних концепцій брандмауерів та спільного виявлення мережних вторгнень.

Методика реалізації. Дослідження виконано на основі аналізу великої кількості літературних джерел, теорії побудови систем захисту інформації та проспектів виробників систем виявлення та запобігання мережним вторгненням.

Результати досліджень. Процеси удосконалення брандмауерів, таких як SMLIF, IPS, спільних систем виявлення вторгнення набувають все більшого значення в наші дні. Вони також можуть бути розгорнуті в рамках сценаріїв NFC та IoT (Інтернет речей). Брандмауери та системи виявлення мережних втручань часто об'єднуються в індивідуальних пірингових конфігураціях (LAN, WLAN, 2G-4G, NFC та Bluetooth) з можливістю співпраці та кращої профілактики зовнішніх та внутрішніх атак.

Висновки. Проведене дослідження вказує на необхідність удосконалення реалізацій сучасної мережної архітектури із застосуванням комплексних систем виявлення та протидії мережним атакам. Незважаючи на велике розмаїття рішень щодо мережної безпеки, цей напрямок досліджень залишається актуальним та дає підстави стверджувати, що розроблення нових концепцій захисту мережних архітектур відповідає сучасному стану галузі, є своєчасним та актуальним, враховуючи велику множину можливостей і сценаріїв для зловмисних вторгнень і впливів на мережні системи.

Ключові слова: брандмауер; мережні атаки; системи виявлення вторгнень; системи запобігання вторгненням; CIDN.

Лунтовский А.О., Клымаш М.М.

Исследование современных концепций брандмауэров и совместного выявления сетевых вторжений

Проблематика. В этой работе проанализированы современные подходы к организации сетевых брандмауэров, которые сравниваются с классическими концептуальными решениями в области сетевой безопасности. Правила фильтрации сетевого трафика анализируются на основе рассмотрения примеров в рамках избранных решений (которые представлены компанией Gartner Inc.). Рассматриваются совместные системы и сети обнаружения вторжений (CIDN), а также угрозы, основанные на основе рассмотрения случаев инсайдерских нападений на CIDN. Коротко проанализирован общий перечень функциональных возможностей CIDN систем. Рассмотрены аспекты применения современных систем обнаружения и предотвращения сетевых вторжений по особенностям их реализации на различных уровнях согласно модели ЭМВВС. Предоставлены краткие рекомендации по применению известных решений сетевой безопасности при построении современных инфокоммуникационных сетей для преодоления угроз различного типа, в том числе DoS типа, вирусных и социальной инженерии.

Цель исследований. Исследование особенностей реализации и применения современных концепций брандмауэров и совместного выявления сетевых вторжений.

Методика реализации. Исследование выполнено на основе анализа большого количества литературных источников, теории построения систем защиты информации и проспектов производителей систем обнаружения и предотвращения сетевых вторжений.

Результаты исследований. Процессы совершенствования брандмауэров, таких как SMLIF, IPS, совместных систем обнаружения вторжений приобретают все большее значение в наши дни. Они также могут быть развернуты в рамках сценариев NFC и IoT (Интернет вещей). Брандмауэры и системы обнаружения сетевых вмешательств часто объединяются в индивидуальных пиринговых конфигурациях (LAN, WLAN, 2G-4G, NFC и Bluetooth) с возможностью сотрудничества и лучшей профилактики внешних и внутренних атак.

Выводы. Проведенное исследование указывает на необходимость совершенствования реализаций современной сетевой архитектуры с применением комплексных систем обнаружения и противодействия сетевым атакам. Несмотря на большое разнообразие решений по сетевой безопасности, это направление исследований остается актуальным и дает основания утверждать, что разработка новых концепций защиты сетевых архитектур соответствует современному состоянию отрасли, является своевременным и актуальным, учитывая широкое множество возможностей и сценариев для злонамеренных вторжений и воздействий на сетевые системы.

Ключевые слова: брандмауэр; сетевые атаки; системы обнаружения вторжений; системы предотвращения вторжений; CIDN.