Quantitative Cyber-Security Colorado State University Yashwant K Malaiya CS559 L29: Presentations, Overview



CSU Cybersecurity Center Computer Science Dept

Presentations/Final Report

Th Dec 10

- Chen, Sirius. Secure container Technologies
- Shang, Tony. Detection DDOS attack based on deep neural networks

Course Overview

Note: final is comprehensive but most of it will be based on the material covered after the midterm.

• Today is the last day of classes. Please turn the videos on.



Notes

- Q15
- Peer Evaluation of Presentations
 - Due Dec 11
- Final Part 1 Raw: Critical peer review of 2 Reports
 Dec 11-Dec 16 4 Pm
- Final Part 2 S 001 Raw Requires Respondus LockDown Browser + Webcam
 - On-campus/Local: Dec 16, 2-4 PM
 - Non-local/Distance: Dec 16, 2 PM- Dec 17, 4 PM





Advances on virtualization technology of cloud computing

Wei Chen 12/08/2020

1

onten

2 Virtualization technology machine comparison

3 The impact of Docker Container

4

Prospects for the development trend of containers



PART ONE

Virtualization technology

ADD YOUR TITLE HERE



Server virtualization refers to virtualizing a computer into multiple logical computers through virtualization technology.

What is Server Virtualization?

The virtualization of the server is realized by introducing a virtualization layer between the hardware and the operating system to realize the decoupling of the hardware and the operating system.





•Docker is a container platform that can simplify and standardize application deployment in different environments. There are already many ecosystem software related to distributed container management.



The container can provide an isolated operating space for the application, including the complete user environment space; changes in one container will not affect the operating environment of other containers

Multiple containers can share the kernel of the same operating system, so that when the same system library is used by multiple containers, the efficiency of memory usage will be greatly improved

In recent years, with the emergence of Docker, container technology has had a huge impact on the development of cloud computing.

PART TWO

02

Docker container and virtual machine comparison









- 1) Resource isolation problem
- 2) Security issues
- 3) Container management needs to be strengthened

- 4) Compatibility issues
- 5) Windows containers are not yet mature
- 6) The container orchestration engine is not yet mature



03

The impact of Docker Container





Docker container uses cgroups technology to greatly reduce the granularity of control system resources, thereby greatly improving the utilization of system resources.

3

Now public cloud service providers can completely migrate these applications to containers, which can not only reduce resource overhead, but also provide better portability.

Another advantage that the CaaS model brings to enterprises is that CaaS enables enterprises to easily and dynamically migrate services between different public cloud platforms without worrying about platform lock-in issues. PART Four

04

Prospects for the development trend of containers



3

Containers and virtualization technologies will coexist



Running containers in virtual machines will become a trend



The era of container-centric cloud computing is about to begin



The development track of modern cloud computing from the perspec-tive of container and Kubernetes technology [EB/OL]. [2016-10-16]. <u>http://dockone.io/article/140.</u> (The development track of modern cloud computing from container and Kubernetes Technology[EB/OL].[2016-10-16]. <u>http://dockone.io/article/140</u>.)

Wu Zhixue. Introduction to Cloud Computing: Concepts Frameworks and Applications[M]. Beijing: People's Posts and Telecommunications Press, 2016: 43 -52. (WU Z X. Introduction to Cloud Computing: Concepts Frameworks and Applications[M]. Beijing : Posts and Telecom Press, 2016: 43 -52.)

IBM virtualization and cloud computing group. Virtualization and cloud computing[M]. Beijing: Publishing House of Electronics Industry, 2010. (IBM virtualization and cloud computing group. Virtualization and Cloud Computing[M]. Beijing: Publishing House of Electronics Industry, 2010.)

PRATT I, FRASER K, HAND S, et al. Xen 3.0 and the art of virtualization[J]. Proceedings of the Ottawa Linux Symposium, 2005, 36 (5): 164-177.

Ma Bofeng. VMware, Citrix and Microsoft Virtualization Technology Explanation and Application Practice[M]. Beijing: Mechanical Industry Press, 2013. (MA B F. VMware, Citrix and Microsoft Virtualization Technology Explanation and Application Practice[M]. Beijing: China Machine Press, 2013.)

KIVITY A, KAMAY Y, LAOR D, et al. KVM: the Linux virtual machine monitor[EB/OL].[2016-03-10]. https://www.kernel.org/doc/ols/ 2007/ols2007v1-pages-225-230.pdf.

ROSEN R. Linux Kernel Networking: Implementation and Theory[M]. Berkeley: Apress, 2014: 405 -482. Wang Kai, Zhang Gongxuan, Zhou Xiumin. Research on Virtualization Technology Based on Containers [J]. Computer



Thanks For Listening

Leave Questions on Discussion

Detect DDOS attack based on convolutional neural networks

CS 559 – FINAL PROJECT

Linpeng Shang

Topic

Introduction

- Attack principle of DDoS
- Convolutional neural networks
- SIP flood attack detection model based on convolutional neural networks

Introduction



Motivation

- Distributed Denial of Service (DDoS) attacks can cause serious harm to hosts, servers, and even network infrastructure on a network.
- A peak of 1.35TB/sec traffic hit the developer platform GitHub, the largest recorded DDoS attack to date.
- In most cases, attackers use TCP, UDP, and ICMP protocols to launch DDoS attacks, which disrupt the business of the attacked company and cause huge economic losses.
- Therefore, how to detect and effectively mitigate DDoS attacks in real time has become one of the most important research areas in recent years

Related Works

- In 2005, Jian Yuan. Kevin L. Mills proposes a method to identify DDoS attacks using cross-correlation and weight vectors to analyze backbone network node traffic and detect various types of traffic, such as constant speed traffic and incremental speed traffic [16].
- Gupta et al. propose a neural network detection model to solve the problem of poor stability in identifying low-rate attacks, and Saied et al. improve the detection rate of unknown types of DDoS attacks by constantly updating the learning samples [17].
- Kale et al. propose combining the classifier output with Neyman P In 2009, Chen C L used two statistical t-tests to identify DDoS attacks, the arrival rate of SYN and the number of SYN, ACK groups [16].
- In 2015, Singh.K proposed a DDoS detection method based on the random forest classification model, taking the data stream information as the classification criterion and characterizing the three common DDoS attacks [17].

Background of Neural network

- Neural Network technology originated in the 1950s And 1960s as perceptron, which has an input layer, an output layer, and an implicit layer [7].
- In 2006, Hinton mitigated the local optimal solution problem with a pretraining method that pushed the implicit layers to seven, which is the depth of the NN [3].
- A Convolutional Neural Network (CNN) is a feedforward neural network [4].

Distributed Denial Of Service (DDoS) Attack

Background of DDoS Attack

- Distributed Denial of Service (DDoS) attack is an attack in which multiple attackers in different locations launch attacks against one or more targets simultaneously [4][5].
- Since the attack originates from different locations, this type of attack is called a distributed denial-of-service attack.
- DDoS is the use of more Zombie computers to launch an attack, attacking the victim on a larger scale than before

Structure of DDoS attack

The structure of an attack by an attacker using a zombie computer is shown in right figure.



DDoS attack can be categorized as follows:

► IP Spoofing

LAND attack

ICMP floods

Application

DDoS attack strength





Most attacks per month (peak bandwidth Gbps)

Most attacks per month (peak bandwidth Gbps)

Convolutional Neural Networks (CNNs)



Background of CNNs

- Convolutional neural networks (CNNs) can be traced back to 1986 when Rumelhart proposed the BP algorithm, and then to 1989 when LeCun applied the BP algorithm to multilayer neural networks [5].
- Ten years later, in 1998, LeCun proposed the LeNet-5 model, and the prototype of the neural network was completed [5].
- Convolutional neural networks are introduced to take advantage of the local receptive fields, weight sharing, and pooling features of convolutional neural networks to improve the learning ability, expression ability, and performance of neural networks.



LeNet-5 Convolutional Neural Network Model

Convolutional Neural

el

User Agents			Proxy Se	Servers		Attack Source			SIP Proxy Server		Attack Source			SIP Proxy Server		
	Register 401 Unauthorized												F	Register		
				Register					401 Unauthorized			orized				
	Register					401 Unauthorized						Register				
	←	200 OK											403	Forbidde	en	

Figure 1

Figure 2



Convolutional neural network model

Experimental Environment, Analysis, and Results

BP Algorithm Sampling Time and Results

Sampling time and results of the algorithm for this study

Attack Speed	Early warning rate (%)	Alarm Time (s)	False alarm rate (%)	Attack Speed	Early warning rate (%)		False alarm rate (%)
15	100	4.3	0	15	100	4.3	0
25	100	2.4	0	25	100	2.2	0
45	100	3.2	0	45	100	2.9	0
65	100	2.1	0	65	100	2.0	0
85	100	2.3	0	85	100	2.2	0
100	100	2.1	0	100	100	2.0	0

Figure 1

Figure 2

At the beginning, the alarm time of this method is equal, but as the attack speed increases, the alarm time of this method is faster than the BP algorithm.



Conclusion

- Convolutional neural network-based attack detection method to analyze REGISTER registered message flow in IMS network.
- The experimental results show that the method can detect SIP flooding attacks in IMS networks and has good detection performance.
- In this research, a typical neural network model is chosen and modified as needed. The training of the convolutional neural network model is greatly influenced by the initialization parameters, which has an impact on the experimental results
- This experiment is conducted under CPU only, and later, I will consider using GPU instead of CPU and conduct the experiment again.

Reference

[1] Kei Sakuma, Hiromu Asahina, Shuichiro Haruta, Iwao Sasase, "Traceroute-based target link flooding attack detection scheme by analyzing hop count to the destination", Communications (APCC) 2017 23rd Asia-Pacific Conference on, pp. 1-6, 2017.

[2] Martine Bellaiche, Jean-Charles Gregoire, "SYN Flooding Attack Detection Based on Entropy Computing", Global Telecommunications Conference 2009. GLOBECOM 2009. IEEE, pp. 1-6, 2009.

[3] Xiapu Luo, R.K.C. Chang, "Optimizing the pulsing denial-of-service attacks", Dependable Systems and Networks 2005. DSN 2005. Proceedings. International Conference on, pp. 582-591, 2005.

[4] Obaidat, Mohammed S., and Noureddine A. Boudriga. "Fundamentals of Performance Evaluation of Computer and Telecommunications Systems." (2010).

[5] David, Jisa, and Ciza Thomas. "DDoS attack detection using fast entropy approach on flow-based network traffic." Procedia Computer Science 50 (2015): 30-36. [6] Saied, Alan, Richard E. Overill, and Tomasz Radzik. "Detection of known and unknown DDoS attacks using Artificial Neural Networks." Neurocomputing 172 (2016): 385-393.

[7] Bengio Y. Learning Long-term Dependencies With Gradient Descent is Difficult[J]. IEEE Transactions on Neural Networks, 1994, 5.

[8] Vapnik V. The nature of statistical learning theory[M]. Springer, 1995.

[9] Global DDoS Attack Status and Trend Analysis Report 2018:

https://e.huawei.com/cn/material/networking/networksecurity/dd249481da3e4d0f96c831a7260a0b41

[10] Lecun Y L, Bottou L, Bengio Y, et al. Gradient-Based Learning Applied to Document Recognition[J]. Pro ceedings of the IEEE, 1998, 86(I 1):2278-2324.

Reference

[11] Hinton G E, Salakhutdinov R R. Reducing the dimensionality of data with neural networks[J]. Science, 2006, 313(5786):504.

[12] Mchugh J. Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory [JJ. ACM Transactions on Information and System Security (TISSEC), 2000, 3(4):262-294.

[13] Netzer Y, Wang T, Coates A, et al. Reading Digits in Natural Images with Unsupervised Feature Learning[J]. Nips Workshop on Deep Learning & Unsupervised Feature Learning, 2012.

[14] Krizhevsky A, Sutskever I, Hinton G E. ImageNet classification with deep convolutional neural

networks[C]//International Conference on Neural Information Processing Systems. Curran Associates Inc.2012:1097-1105.

[15] Simonyan K, Zisserman A. Very Deep Convolutional Networks for Large-Scale Image Recognition[J]. Computer Science, 2014.

[16] Yuan J, Mills K L .Monitoring the Macroscopic Effect of DDoS Flooding Attacks[J]. IEEE Transactions on Dependable and Secure Computing, 2005, 2(4):324-335.

[17] CHEN C L. A new detection method for distributed denial-of-service attack traffic based on statistical test[J]. Journal of Computer Science, 2009, 15(2): 488-504.

[18] Bhuyan M H, Bhattacharyya D K, Kalita J K An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection[M]. Elsevier Science Inc. 2015.

[19] Singh K J, De T .An Approach of DDOS Attack Detection Using Classifiers[M]// Emerging Research in Computing, Information, Communication and Applications. Springer India, 2015.

[20] loffe S, Szegedy C .Batch normalization: accelerating deep network training by reducing internal covariate shift[C]// International Conference on International Conference on Machine Learning. JML R.org, 2015.

How to prepare

- You have already been preparing
- Review lectures, slides, quizzes, assignments
- Focus on
 - Terms
 - Ideas and approaches
 - Solving problems
- If interested, locate references cited and read in more detail. This is a research-oriented class.
- Please review <u>Respondus</u> information, <u>video</u>.
 Download and install
- Note: weekend quiz likely



What we have examined L1-16

Before midterm:

- System basics, firewalls, access control
- Risk, its components and evaluation
- Probability, modeling, regression
- Vulnerability Discovery Models
- Metrics: CVSS



Discussed after Midterm (-L24)

- Testing, coverage, tools
- Detectability profile, random and directed testing
- SRGM, Defect density, Coverage based modeling
- Authentication, passwords
- Fuzzing
- Penetration testing
- Attacks
- Security breaches:
 - Probability, Gordon Loeb model
 - Cost models, metrics, examples
- Vulnerability markets



Detectability Profile of a unit under test

- Total M faults, total N possible input combinations. The set of faults can be partitioned into these subsets:
- $H = \{h_1, h_2, \dots h_N\}$
- Where h_k is the number of faults detectable by exactly k inputs. The vector H describes the detectability profile.
 - h₁ is the number of faults that are hardest to find.
 - As testing and debugging continues, harder to find faults will tend to remain.
 Easy to find faults will get eliminated soon.





SRGMs

• **Exponential SRGM**: assumes bug finding rate $\lambda(t)$ is proportional to remaining bugs at time N(t).

$$\lambda(t) = -\frac{dN(t)}{dt} = \beta_1 N(t)$$

Exponential defect finding model is

$$\lambda(t) = \beta_0 \beta_1 e^{-\beta_1 t}$$

- β_0 represents the initial number of bugs.
- If the initial *defect density* is D(0), and the software size (measured in 1000 lines of code, i.e. KLOC) is S, then

$$\beta_0 = D(0) \times S$$

• The initial defect density is a function of the software development process and the degree of prior defect removal.



Eliminating t and rearranging, C⁰ = aⁱ₀ ln[1+aⁱ₁(exp(aⁱ₂Cⁱ)-1)], C⁰ ≤ 1 where C⁰ : defect coverage, Cⁱ : test coverage aⁱ₀, aⁱ₁, aⁱ₂ : parameters; i : branch cov, p - use cov etc.
For "large" Ci, we can approximate

$$C^0 = -A^i + B^i C^i$$





Problem: Password guessing

- If your keyboard has R= 95 unique characters, 12-character password, then L = 12.
- 95¹²= 540,360,087,662,636,962,890,625 passwords

Entropy = $\log_2(R^L)$ = 78.9 bits assuming passwords are created randomly

- Non-randomness makes password guessing easier.
- Measures of password strength proposed and used





Attacking Salted Passwords



Fuzzing PDF Reader

- Download 100s of random PDF files
- Mutate content in the PDF file:
 - flip bits
 - increase size of integers or strings
 - remove data
- Limited by the functionality that the existing files happened to use unlikely to hit less commonly tested code paths



Colorado State University

American Fuzzy Lop (AFL)



Pen Testing Stages



- 1. Planning and reconnaissance
- Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.
- Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.
- 2. Scanning
- Network scanning and topology tracing, id OS and applications, Port scanning to find open ports and services, find net addresses of live hosts, firewalls, routers, etc. vulnerability scans to id potential vulnerabilities.
- 3. Gaining access:
- This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

Colorado State University

Sources: <u>1</u>, <u>2</u>

Pen Testing Stages



4. Maintaining access: See if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access.

• The idea is to imitate advanced persistent threats (APTs), which often remain in a system for months in order to steal an organization's most sensitive data.

5. Analysis and remediation: The results of the penetration test are then compiled into a report with

- Specific vulnerabilities that were exploited, Sensitive data that was accessed
- The amount of time the pen tester was able to remain in the system undetected
- This information is analyzed help configure an enterprise's WAF (web protection firewall) settings and security solutions to patch vulnerabilities and protect against future attacks.

Colorado State University

Sources: <u>1</u>, <u>2</u>

How many pen tests do you do a year?

a. In 2017, cobalt.io collected data from 75 survey respondents in security, management, operations, DevOps, product, and developer roles



PEN TESTS A YEAR



b. WHAT IS MOST CHALLENGING ABOUT PEN TESTING APPLICATIONS?

Source of data



Attack Tree Example 1



aa



Annual Loss Expectancy (ALE)

Note the terminology is from the Risk literature.

- Annual loss expectancy (ALE). (It is a risk measure)
 ALE = SLE x ARO
 - Where ARO is Annualized rate of occurrence.
- A countermeasure reduces the ALE by reducing one of its factors.

COUNTERMEASURE_VALUE = (ALE PREVIOUS – ALE NOW) – COUNTERMEASURE COST

ALE_PREVIOUS: ALE before implementing the countermeasure. ALE_NOW: ALE after implementing the countermeasure COUTERMEASURE_COST: *annualized* cost of countermeasure



Breach Probability Model

A proposed model for the probability of a breach for the next

P {breach} = Fcountry * FBCM * Findustry * Fbreach_{cause} * Fencryption * Fprivacy * $\alpha exp(-\beta x)$ Where α = 0.4405, β = 4E-05, x the breach size 2015





Data breach probability by country



Data breach probability by country (Ponemon data 2015)

A minimum of 10,000 compromised records



Impact of investment z:

The **expected benefits of an investment in information security**, *EBIS*, are equal to the reduction in the firm's expected loss attributable to the extra security.

EBIS(z) = [v - S(z, v)] L

The **expected net benefits from an investment in information security**, *ENBIS* equal *EBIS* less the cost of the investment, or:

$$ENBIS(z) = [v - S(z, v)] L - z$$

v – Probability of security breach

L - Potential Loss. vL - Expected Loss

z – Level of Investment

S[z, v] - Revised probability of breach



Cost Metrics

Total Cost of a Breach =

Incident investigation cost

- + Customer Notification/crisis management cost
- + Regulatory and industry sanctions cost
- + Class action lawsuit cost

 $\textit{Cost per Record} = \frac{\textit{Total cost of breach}}{\textit{number of affected records}}$



TARGET DATA BREACH ACTUAL REPORTED COSTS

Years	Gross Expenses	Insurance receivable	Net Expenses (before tax deductions)	Net Expenses (after tax deductions)				
2013	\$61m	\$44m	\$17m	\$11m				
2014	\$191m	\$46 m	\$145 m	\$94m				
2015	N/A	N/A	\$39	\$28				
Total	otal \$252m \$90m		\$201m \$133m					
Raw cost per card= \$6.30 (40 million cards affected)								



A consolidated approach for estimation of data security breach costs, AM Algarni, YK Malaiya 2016 2nd International Conference on Information Management (ICIM), 26-39



The breach cost vs. breach size



Our proposed model *Total breach cost* = a * size ^ b

Verizon 2015 data, the claim amount vs. breach size (ranges from single digits to 108 million records)



Average total cost of a data breach by organizational size

• Note economy of scale



Average total cost of a data breach by organizational size



Impact of 25 key factors on the average total cost of a data breach 2020

Change in US\$ from average total cost of \$3.86 million



Colorado State Universit

Cost amplifying factors

Cost Metrics

Total Cost of a Breach =

Direct costs + Indirect costs – Recovered costs

Direct costs: funds spent directly

- = Incident investigation cost
 - + Customer Notification/crisis management cost
 - + Regulatory and industry sanctions cost*
 - + Class action lawsuit cost*

Indirect costs: lost business opportunity

= loss of goodwill, customer churn#

Recovered costs = Insurance recovery + tax break



Chang, Gao, Lee 2020 Hypotheses

- **Hypothesize 1 (H1).** The announcement of a data breach has a negative effect on the short-term market value of the breached company.
- **Hypothesize 2 (H2).** The announcement of data breach has a negative effect on the long-term market value of the breached company.
- **Hypothesize 3.1 (H3.1).** The size of the data breach is positively associated with a higher negative return on the short-term market value of the breached company.
- **Hypothesize 3.2 (H3.2).** The size of the data breach is positively associated with a higher negative return on the long-term market value of the breached company.

The Effect of Data Theft on a Firm's Short-Term and Long-Term Market Value 2020 Colorado State University

Vulnerability flow through markets



Colorado State University

Types of Vulnerability Markets



Presentations

- Ransomware
- Phishing, URL identification
- Cybercrime:
 - motivation/methods
 - prediction
- Smartphones: security models/metrics/vulnerabilities
- Mitre ATT&CK threat modeling for ICS
- Cyber Insurance
- Government security breaches



Topics: Presentations

- Digital payments: protocols
- Penetration testing: effectiveness, tools, OWASP top 10
- Fuzzing
- Security in virtualized/containerized systems
- Cyber security trade-offs

