




انجمن رمز ایران  
Iran Society of Cryptology

**هشتادمین**  
**کنفرانس بین‌المللی انجمن رمز ایران**  
دانشگاه فردوس مشهد - ۱۳ و ۱۴ شهریور ۱۳۹۰  
8<sup>th</sup> International ISC Conference on Information Security and Cryptology (ISCISC'11)  
Ferdowsi University of Mashhad-September 14-15, 2011



دانشگاه فردوسی مشهد

**چارچوب شبیه سازی سطح بالای حملات سایبری به منظور ارزیابی  
دسترس پذیری**

**A High Level Cyber Attack Simulation Framework  
for Availability Evaluation**

توسط: مهرداد آشتیانی , دکتر محمد عبدالهی ازگمی

شهریور ماه ۱۳۹۰

**فهرست مطالب**

- مقدمه
- شبیه سازی حملات سایبری به وسیله شبکه های پتر رنگی سلسله مراتبی
- شبیه ساز توزیع شده حملات سایبری
- ارزیابی
- نتیجه گیری و کارهای آینده

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

2

### مقدمه

- دلایل انتخاب رویکرد شبیه سازی
  - جایگزینی مشاهده پذیری بر تئوری سازی محض ( اسکات ماس [1])
  - نبود چالش "انفجار فضای حالت" [2]
  - ایجاد پتانسیل برای مقیاس پذیری
  - کاهش هزینه
  - عدم احتیاج به استخدام تیم های "قرمز" و "آبی"
  - عدم احتیاج به پیکربندی شبکه های واقعی [3]
  - تکرارپذیری سناریوهای تعریف شده

### مقدمه

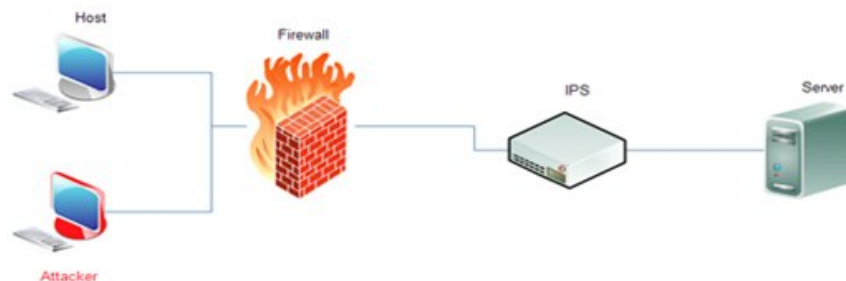
- یکی از انگیزه های استفاده از این روش، ارائه چارچوبی است که به وسیله آن مدیران شبکه قادر باشند عناصر شبکه خود را کنار هم قرار داده و اقدام به شبیه سازی حمله و مشاهده نتایج آن بنمایند.
- به عبارت بهتر به دلیل سلسله مراتبی بودن مدل ایجاد شده، در بالاترین سطح، اجزای شبکه به صورت عناصر قابل استفاده مجددی دیده خواهند شد که می توانند به سادگی کنار هم قرار گرفته و شبکه های مختلفی را مدل سازی کنند.

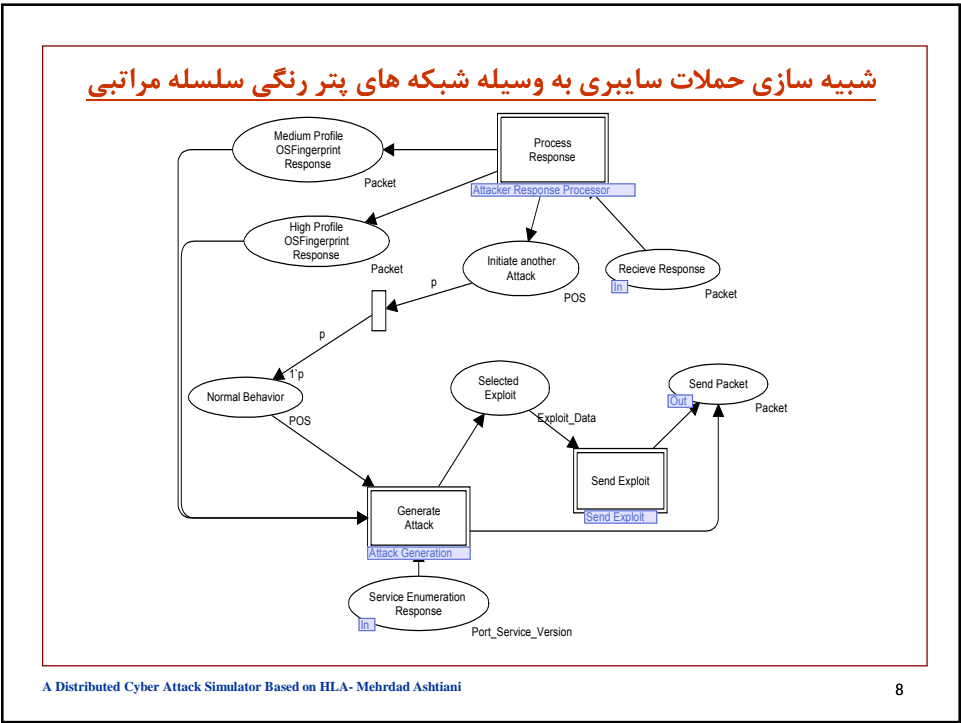
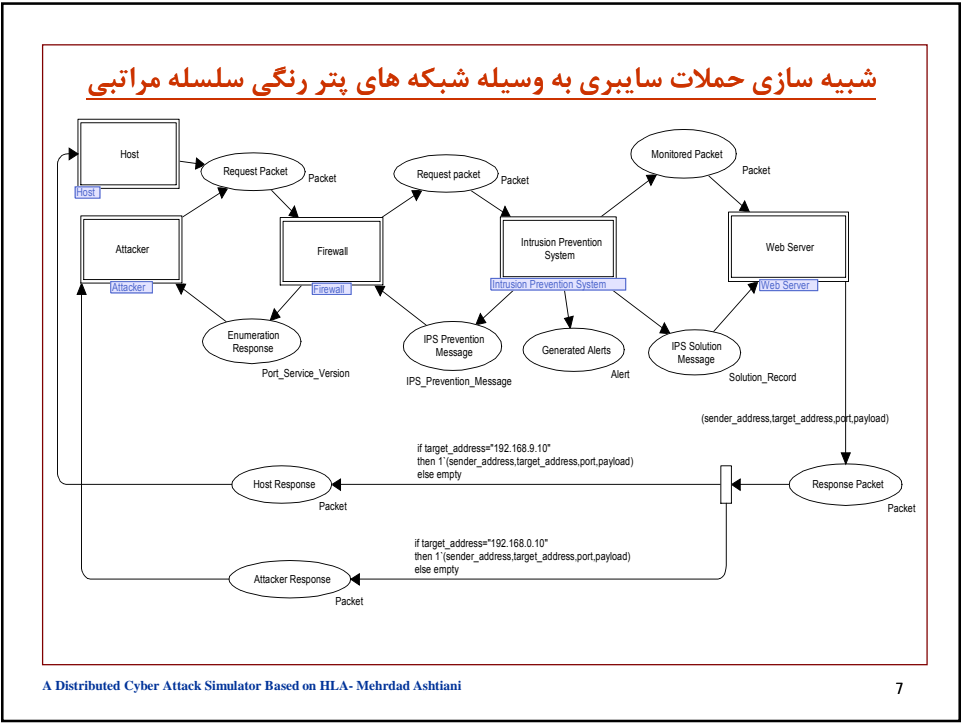
### مقدمه

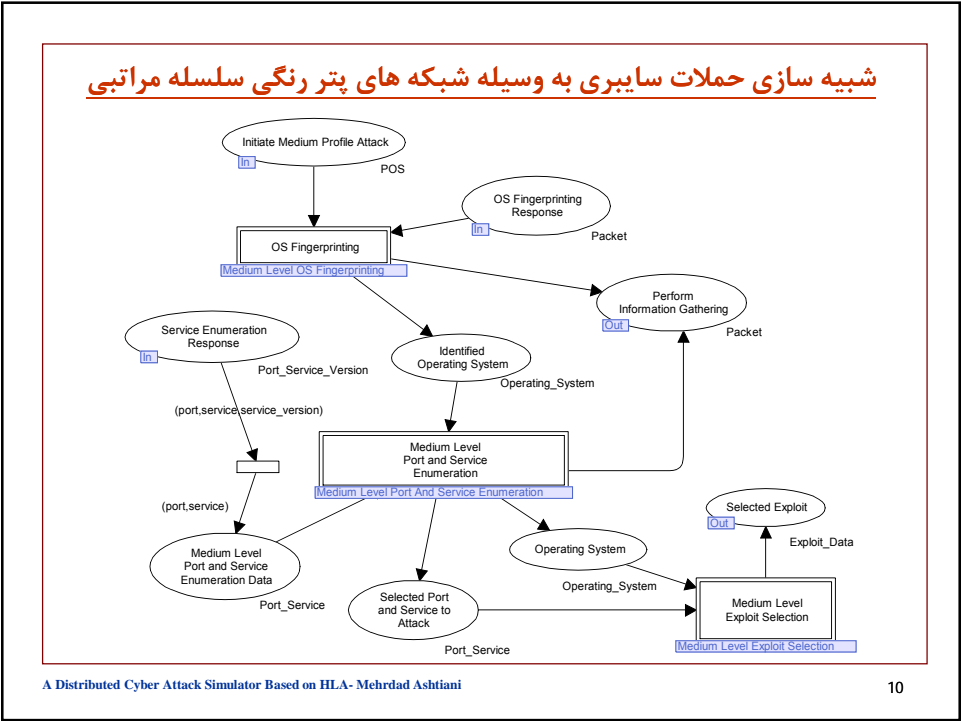
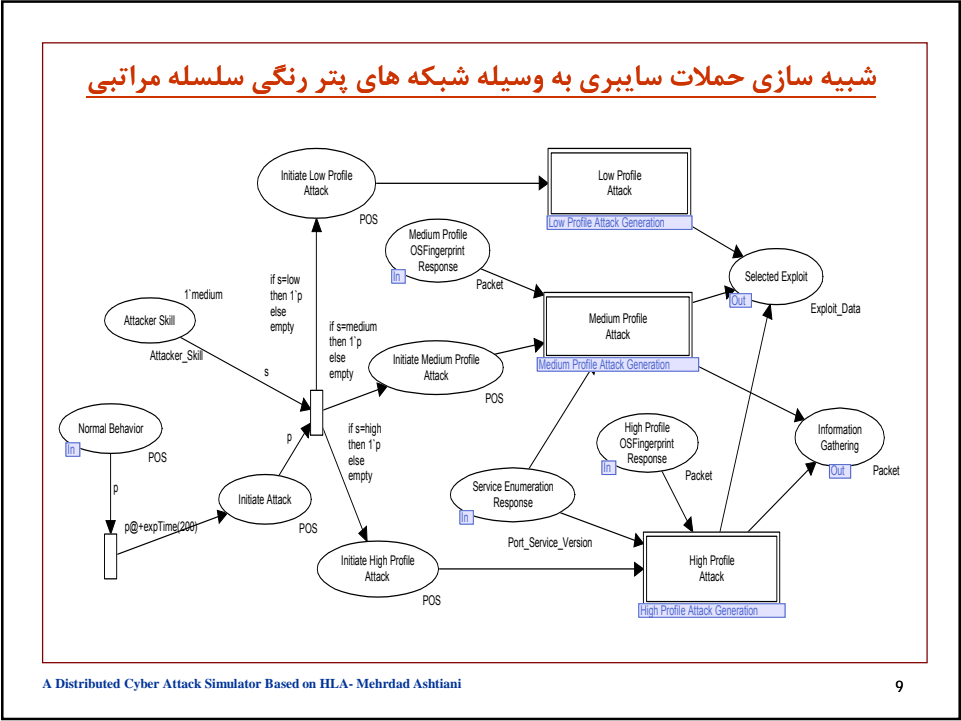
▪ قدم هایی که مهاجمین برای رسیدن به هدف طی می کنند:

- جمع آوری اطلاعات در مورد سیستم هدف
- تعیین آسیب پذیری های سیستم هدف
- ارسال و اجرای کد بهره برداری برای استفاده از آسیب پذیری
- بهره برداری از سیستم

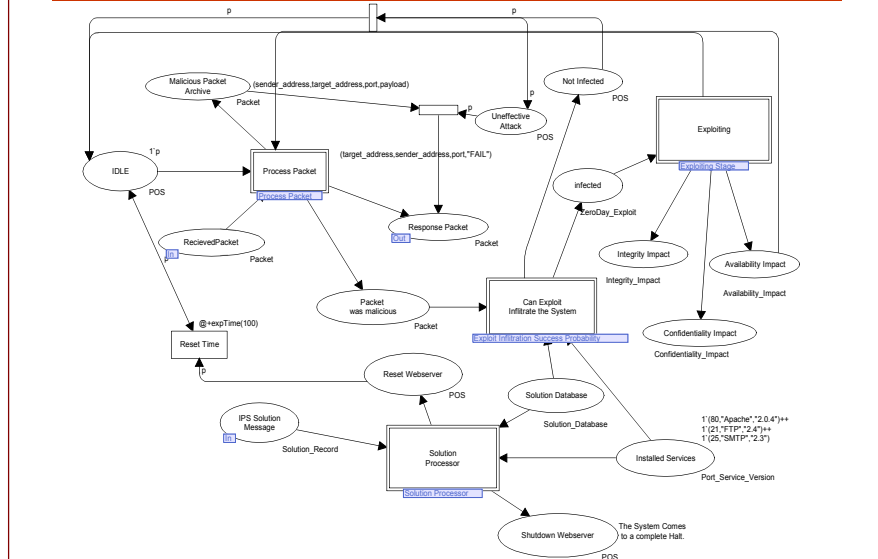
### شبیه سازی حملات سایبری به وسیله شبکه های پترنگی سلسله مراتبی







### شبیه سازی حملات سایبری به وسیله شبکه های پتر رنگی سلسله مراتبی



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

11

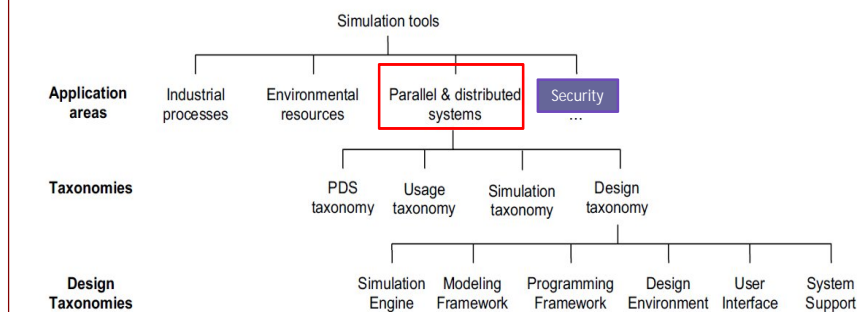
### شبیه ساز توزیع شده حملات سایبری - انگیزه ها و اهداف

- اهداف
- اجرا در محیط توزیع شده
- قابلیت استفاده مجدد از عناصر شبیه سازی توسعه داده شده
- مدلسازی درست ترافیک
- امکان طراحی کامل شبکه
- استفاده از اطلاعات دنیای واقعی در مورد کدهای بهره برداری و امضای سیستم های تشخیص نفوذ
- اندازه گیری معیارهای امنیتی و کارایی

Title and name

12

### شبیه ساز توزیع شده حملات سایبری - مقدمات



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

13

### شبیه ساز توزیع شده حملات سایبری - مقدمات

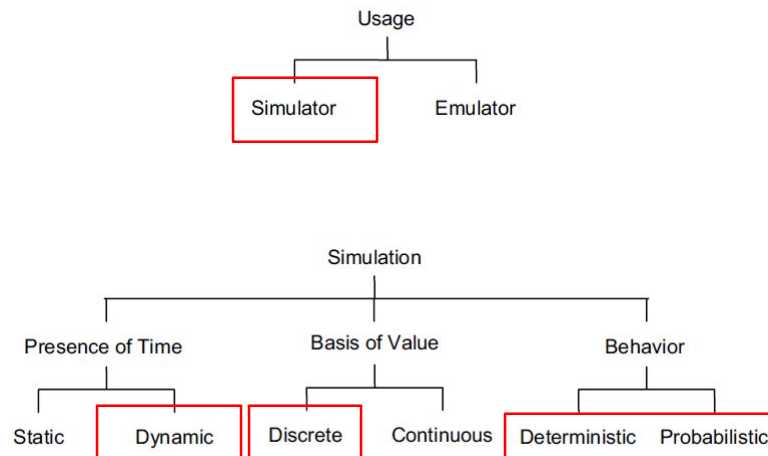
#### ▪ دلایل انتخاب رویکرد توزیع شدگی

- در اختیار گرفتن قدرت پردازشی بیشتر
  - هر چه میزان صداقت در شبیه سازی بیشتر باشد نیاز به قدرت پردازشی نیز بالاتر می‌رود.
- مقیاس پذیری
  - مقیاس پذیری از نظر اندازه
  - مقیاس پذیری از نظر گستردگی جغرافیایی
- ارتباط دهی کاربران متفرق به منابع توزیع شده
- تحمل پذیری

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

14

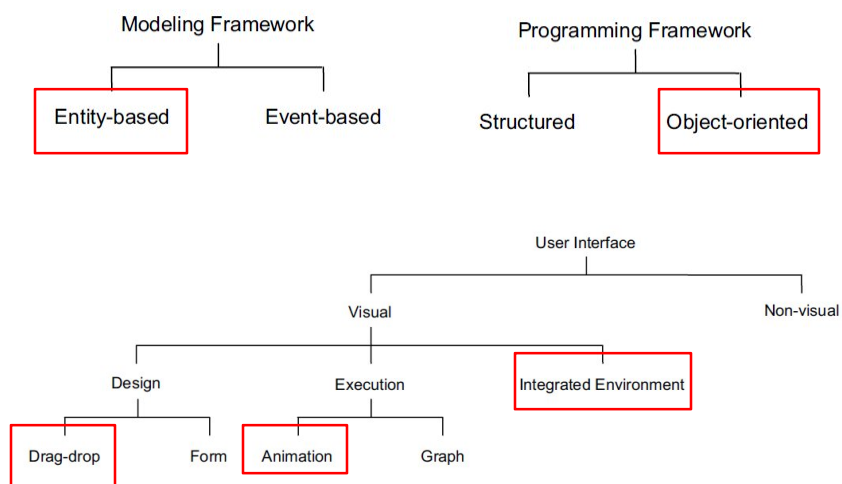
### شبیه ساز توزیع شده حملات سایبری - مقدمات



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

15

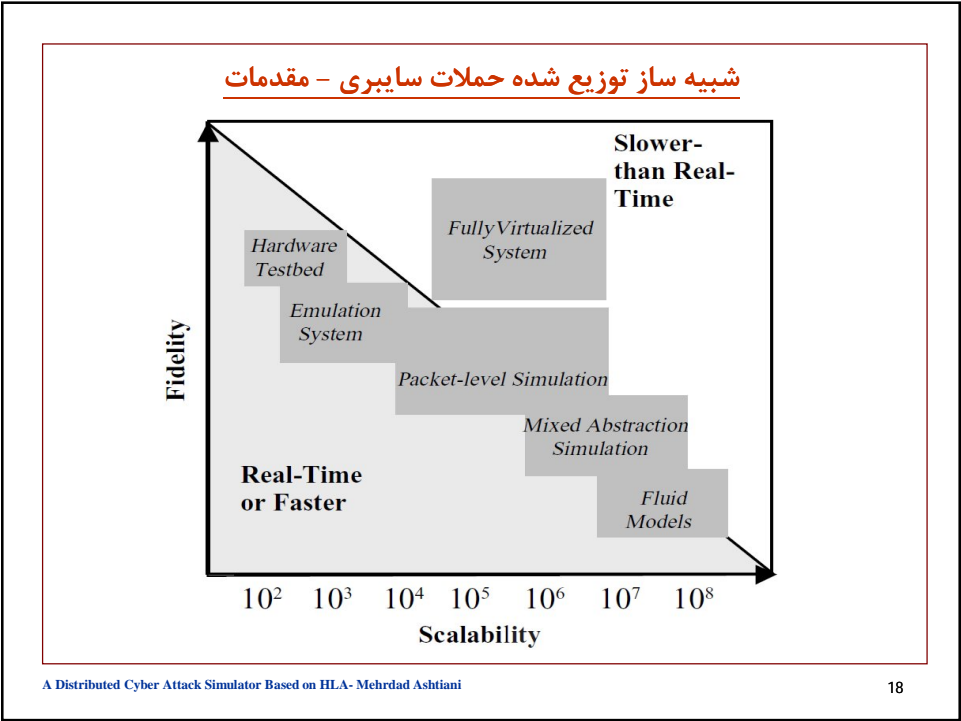
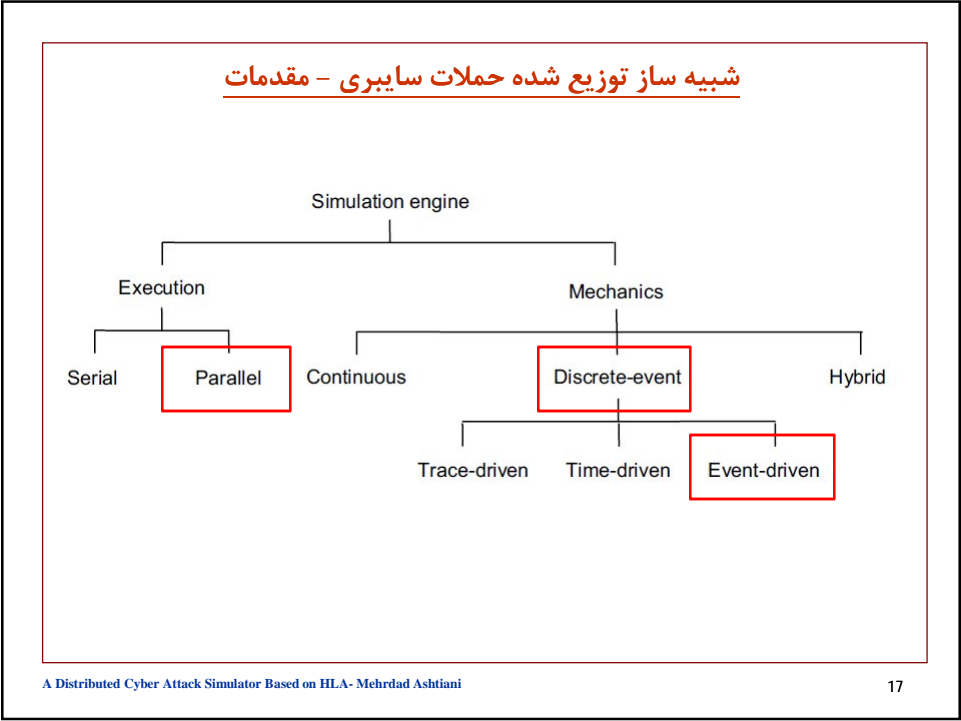
### شبیه ساز توزیع شده حملات سایبری - مقدمات



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

16





### شبیه ساز توزیع شده حملات سایبری - مقدمات

#### ▪ دلایل انتخاب معماری سطح بالا [4]

- Interoperability
  - فدرال ها و فدراسیون ها در معماری سطح بالا از ۱۰ قاعده باید پیروی کنند.
  - به دلیل وجود این قواعد، فدرال ها در معماری سطح بالا interoperability دارند.
  - یک فدرال میتواند در زبان ++C و دیگری در Java نوشته شود.
- Reuse
- معماری سطح بالا استاندارد تمامی شبیه سازی های انجام شده در ناتو و وزارت دفاع آمریکا است.
- زیرساخت اجرایی (RTI) استفاده شده در پایان نامه Portico نام داشته که منبع باز بوده و تحت پوشش مالی و حمایت وزرات دفاع استرالیا است.

### شبیه ساز توزیع شده حملات سایبری - مقدمات

#### ▪ شبیه سازی توزیع شده حملات سایبری از ۴ منظر اصلی طبقه بندی رویکردهای کمی سازی امنیت [5]

- دیدگاه ( CIA، اقتصادی، اتکاپذیری و غیره)
- هدف ( اقتصادی، سیستمی، آسیب پذیری، تهدید و غیره)
- فرضیات ( اسلاید بعدی!)
- اعتبارسنجی : روش به کار رفته برای اعتبارسنجی و نشان دادن تطابق نتایج با پدیده دنیای واقعی چیست؟

### شبیه ساز توزیع شده حملات سایبری - مقدمات

#### ■ فرضیات

- استقلال: رخدادهای تصادفی با احتمالات مستقل از یکدیگر روی می دهند.
- منطق: چگونگی رفتار عامل ها در محیط شبیه سازی. ( چارچوب رفتاری)
- Stationary: ویژگی های موجود در شبیه سازی ( همانند آسیب پذیری ها و تهدیدها) در طول زمان شبیه سازی ثابت هستند.
- تجماع: ویژگی های سیستم اصلی از تجمیع ویژگی های زیر سیستم ها حاصل خواهد گردید.

### شبیه ساز توزیع شده حملات سایبری - مقدمات

#### ■ تعریف چارچوب منطقی رفتاری مهاجمین در شبیه ساز توزیع شده حملات سایبری

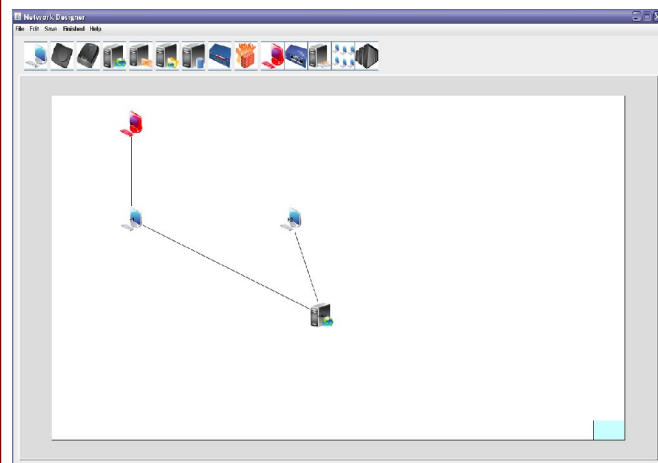
- مهاجمین با سطح توانایی پایین
  - تکیه بر کدهای بهره برداری که به صورت عمومی در دسترس است. ( به دلیل فقدان دانش برنامه نویسی و تشخیص آسیب پذیری و در نتیجه عدم توانایی در تولید کدهای بهره برداری جدید و خصوصی)
  - انتخاب تصادفی در میان کدهای بهره برداری بدون توجه به مشخصات آنها و نیز مشخصات سیستم هدف. [6,7]
- مهاجمین با سطح توانایی متوسط
  - آشنایی کامل با اطلاعات مورد نیاز برای نفوذ موفق به سیستم هدف
  - طی کردن مراحل لازم در فرایند نفوذ برای به دست آوردن اطلاعات مورد نیاز
  - آشنایی و دسترسی به ابزارهای حرفه ای نفوذ و کدهای بهره برداری تجاری
  - عدم آشنایی با برنامه نویسی کدهای بهره برداری جدید و در نتیجه عدم دسترسی به کدهای بهره برداری خصوصی [6,7,8]
- مهاجمین با سطح توانایی بالا
  - آشنایی کامل با اطلاعات مورد نیاز برای نفوذ به سیستم ها
  - آشنایی کامل با مراحل نفوذ به سیستم ها (جمع آوری اطلاعات و غیره)
  - آشنایی کامل با برنامه نویسی کدهای بهره برداری و پیدا کردن آسیب پذیری های جدید و در نتیجه داشتن گنجینه ای از کدهای بهره برداری خصوصی و مخصوص به خود [7,8,9]

### شبیه ساز توزیع شده حملات سایبری - مقدمات

▪ در شبیه ساز توزیع شده حملات سایبری، سه فدرال قرار گرفته اند:

▪ فدرال شبکه

• طراح شبکه



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

23

### شبیه ساز توزیع شده حملات سایبری - مقدمات

▪ در شبیه ساز توزیع شده حملات سایبری، سه فدرال قرار گرفته اند:

▪ فدرال شبکه

• شبیه ساز: در این قسمت، شبکه طراحی شده توسط کاربر شبیه سازی می شود. برای شبیه سازی، از Simjava که یک چارچوب شبیه سازی گسسته رخداد منبع باز است استفاده گردیده است. به عبارت دیگر هرکدام از عناصر قرار گرفته در شبکه به صورت یک موجودیت در Simjava ایجاد می شوند. پس از اتصال این موجودیت ها توسط موتور شبیه سازی به یکدیگر، کار تولید بسته توسط میزبان ها برای سرویس دهنده ها آغاز می شود.

• سیستم های جمع آوری داده و گزارش گیری

▪ به عبارت بهتر شبیه سازی توزیع شده حملات سایبری یک برنامه چندرسمانی است که به صورت فدرالی بر روی یک زیرساخت توزیع شده در حال اجرا است.

• پیچیدگی پیاده سازی!

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

24

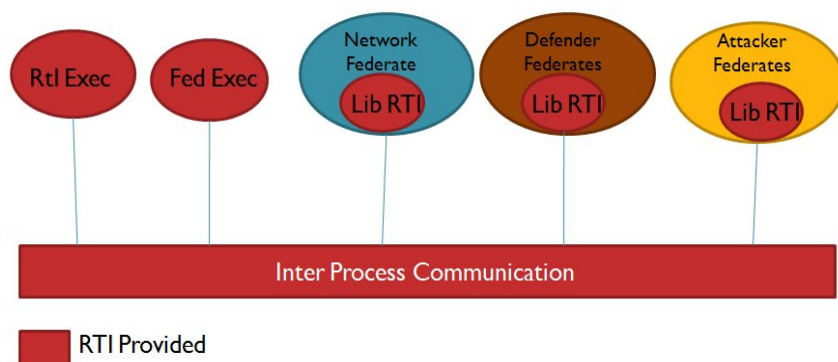
### شبیه ساز توزیع شده حملات سایبری - مقدمات

- فدرال مهاجم: در این فدرال، حمله کننده به وسیله برنامه ای که در اختیارش قرار می گیرد شروع به حمله می کند.
  - مهاجم می تواند از امضای کدهای بهره برداری موجود در پایگاه داده آسیب پذیری OSVDB استفاده کند.
  - همچنین حمله کننده قادر است اعمال لازم برای نفوذ به سیستم ها همانند شمارش سیستم عامل و سرویس ها و پویس درگاه های باز را انجام دهد.
- فدرال مدافع: این فدرال ها به دو دسته کلی سیستم های تشخیص نفوذ و سیستم های پیشگیری کننده از نفوذ تقسیم بندی می شوند.
  - برای شبیه سازی سیستم های تشخیص نفوذ از نحوه کار IDS های مبتنی بر امضا که گونه رایج موجود در شبکه های امروزی هستند الگو برداری شده است. برای این کار نیز از مجموعه قواعد Snort به عنوان یکی از مطرح ترین سیستم های تشخیص نفوذ مبتنی بر امضا استفاده گردیده است.
  - این کار سبب خواهد شد که گذر بسته از سیستم های تشخیص نفوذ به میزان زیادی به واقعیت نزدیکتر باشد.

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

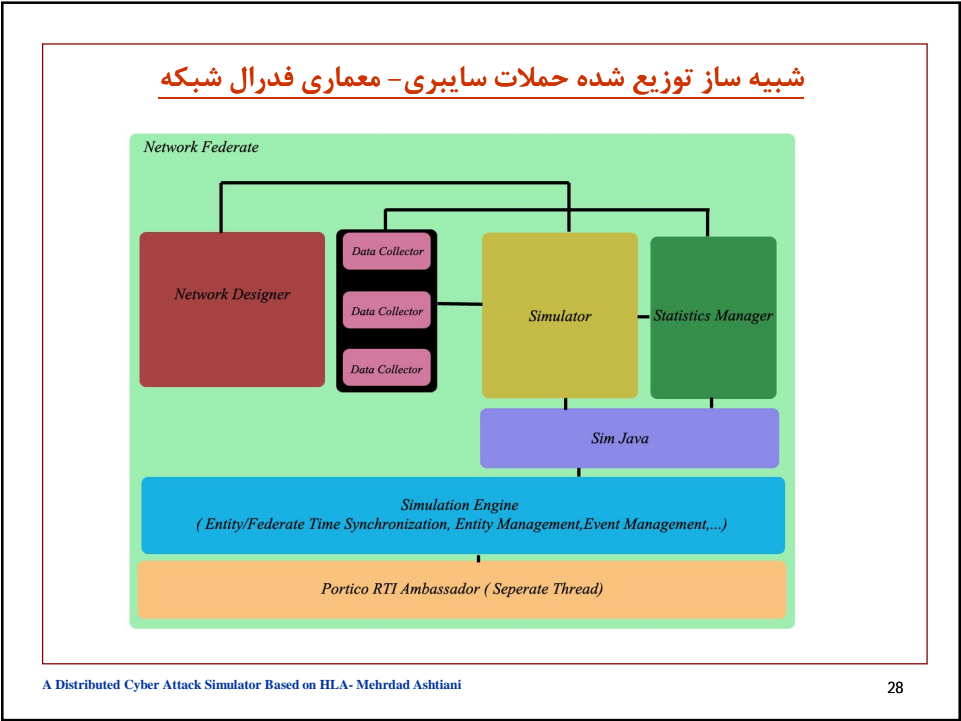
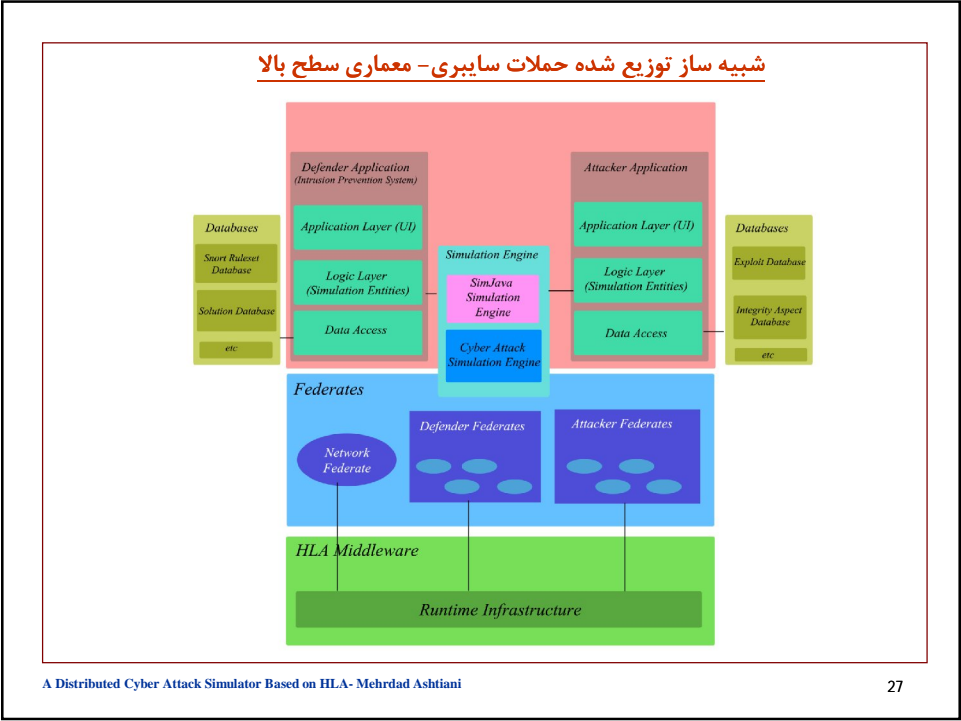
25

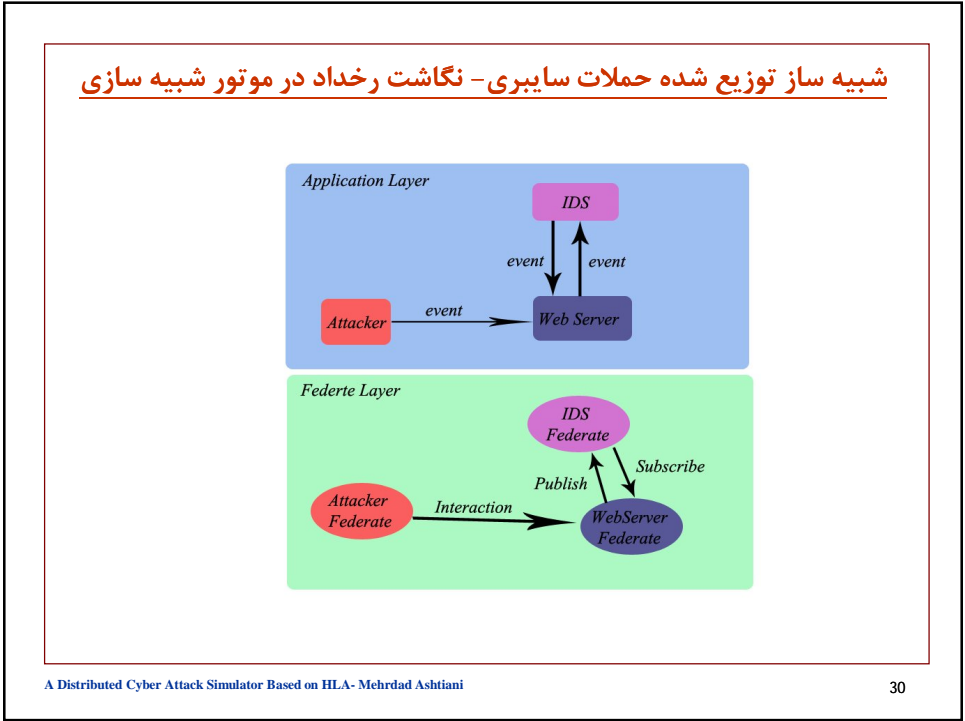
### شبیه ساز توزیع شده حملات سایبری - معماری کلی



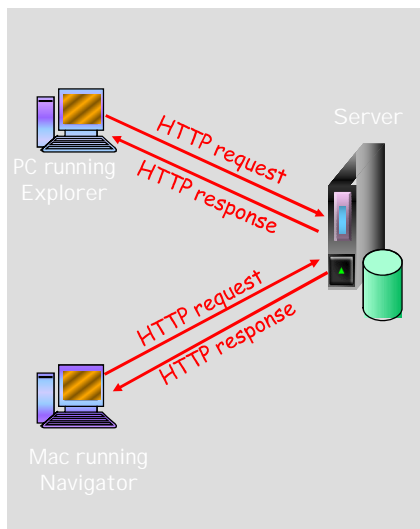
A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

26





### شبیه ساز توزیع شده حملات سایبری - مبانی شبیه سازی



- مکانیزم اصلی انتقال بسته در شبکه شبیه سازی شده مکانیزم Http Request/ Http Response است.
- میزبان بسته درخواست را ارسال کرده و منتظر دریافت پاسخ از سرویس دهنده قرار می گیرد.
- سرویس دهنده پس از دریافت بسته درخواست، بسته پاسخ مناسب را ارسال میکند.

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

31

### شبیه ساز توزیع شده حملات سایبری - مبانی شبیه سازی

- اما در شبیه سازی ترافیک باید به دو نکته توجه کرد:

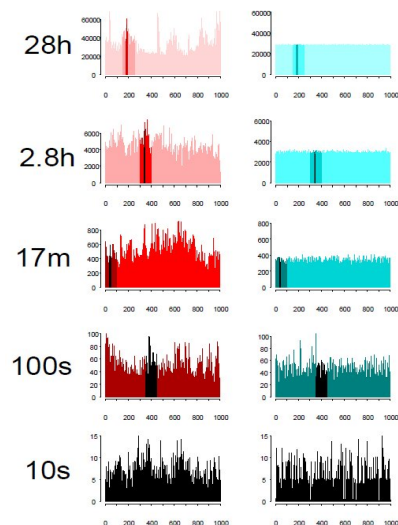
- ترافیک اینترنت Long Tailed است. [10]
  - به این معنی که اغلب زمان های جلسه ( و سائز فایل های رد و بدل شده) کوچک هستند ولی همواره احتمال انتقال فایل هایی با سائز بزرگ نیز وجود دارد.
  - به عبارت بهتر، ترافیک اینترنت دارای خاصیت انفجاری است.
  - این قاعده به تمامی شبکه های LAN و WAN قابل گسترش است.
- ترافیک اینترنت دارای خاصیت خود-شباهت است. [10]
  - بدون توجه به مقیاس، شکل خود را حفظ میکند.

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

32



### شبیه ساز توزیع شده حملات سایبری - مبانی شبیه سازی



■ بنابراین باید توزیع و فرایند مناسب برای شبیه سازی ترافیک در شبیه ساز انتخاب شود.

■ زمان جلسات نمایی نباید باشد. ( بر خلاف بسیاری از کارهای انجام شده در حیطه شبیه سازی حملات)

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

33

### شبیه ساز توزیع شده حملات سایبری - مبانی شبیه سازی

- مدل هایی که میتوانند برای شبیه سازی درست ترافیک شبکه به کار گرفته بشوند
- Collective ON/OFF model
- M/G/Infinity model
- Brownian Model
- Fractional Gaussian Model
- Poisson-Pareto Burst Process

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

34

### شبیه ساز توزیع شده حملات سایبری - مبانی شبیه سازی

- پارامترهای توزیع پارتو برای پروتکل های مختلف متفاوت است.
- این پارامترها از [11] استخراج شده اند.

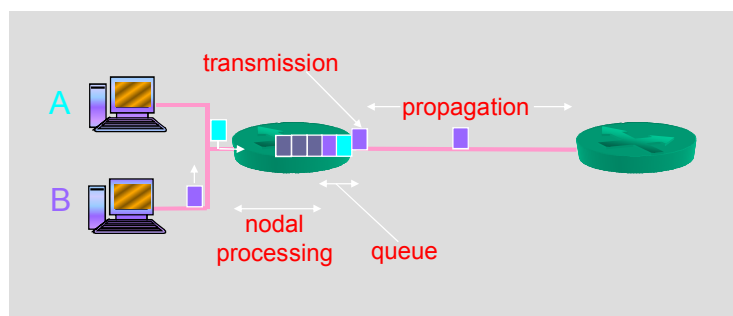
Protocol	Variable Name	Distribution	Parameter
Http	Session Arrival	Poisson	
	Session Duration	Pareto	$\alpha=1.164$ $k=10^{4.25}$
FTP	Session Arrival	Poisson	
	Session Duration	Pareto	$\alpha=1.0595$ , $k=3$
SMTP	Session Arrival	Poisson	
		Pareto	$\alpha=0.8454$ , $k=1250$

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

35

### شبیه ساز توزیع شده حملات سایبری - مبانی شبیه سازی

- تأخیرهای شبکه سازنده برای انتقال بسته ها



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

36

### شبیه ساز توزیع شده حملات سایبری – مبانی شبیه سازی

- کلاس هایی از حملات که شبیه ساز حملات سایبری توزیع شده قادر به شبیه سازی آنها است عبارتند از:
- حملاتی که مبتنی بر تنظیمات نادرست در شبکه هستند ( همانند درگاه های باز اشتباه، نصب سرویس های اضافی آسیب پذیر، تنظیمات اشتباه دیواره آتش)
- حملاتی که در نتیجه تغییر در ترافیک شبکه به وجود می آیند ( DOS و DDOS و DNS Spoofing )
- حملاتی که مبتنی بر استفاده از یک کد بهره برداری برای استفاده از آسیب پذیری های موجود در سیستم هدف به وجود می آید
- حملات زنجیره ای

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

37

### شبیه ساز توزیع شده حملات سایبری – مبانی شبیه سازی

- پارامترهای در نظر گرفته شده برای کدهای بهره برداری

- Access Vector
  - Local
  - Adjacent Network
  - Remote
- Access Complexity
  - Low
  - Medium
  - High
- Authentication
  - None
  - Single Instance
  - Multiple Instance



- Required Operating System to work on
- Required Open Port
- Required Running Service
- Required Appropriate Service Version

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

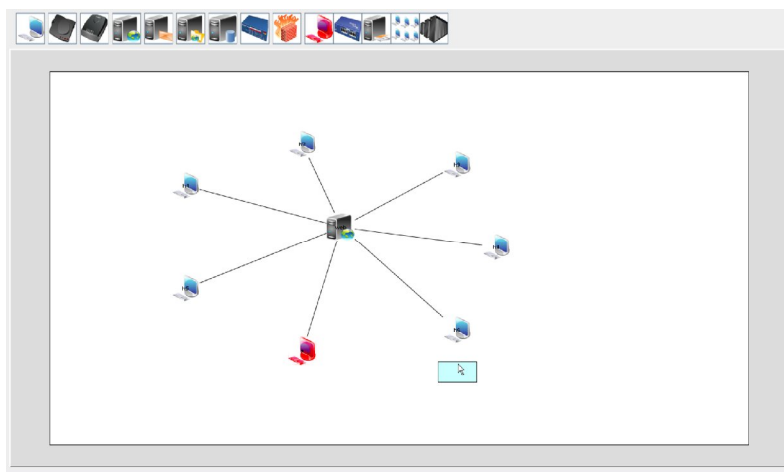
38

### شبیه ساز توزیع شده حملات سایبری – مبانی شبیه سازی

- در ابتدای شبیه سازی، سیستم ها کاملاً وصله نشده هستند. پس از آغاز شبیه سازی، بر روی سیستم هایی که به سیستم های مدافع فعال همانند IPS متصل هستند راه حل های موجود برای آسیب پذیری های مورد حمله قرار گرفته نصب خواهد شد.
- لیست و مشخصات راه حل ها نیز به طور کامل در طول شبیه سازی از OSVDB استخراج خواهد گردید و بر گونه های زیر است:
  - به روز رسانی
  - وصله
  - workaround

### ارزیابی شبیه ساز توزیع شده حملات سایبری

#### ▪ سناریو ۱:



### ارزیابی شبیه ساز توزیع شده حملات سایبری

- سناریو ۱:
- مشخصات سرویس دهنده:
  - سیستم عامل: windows 2000
  - درگاه باز: ۸۰
  - سرویس نصب شده: IIS 6.0
  - آدرس IP: ۱۹۲.۱۷۴.۱۱.۱۰
  - تعداد سوکت های موازی که سرویس دهنده میتواند باز کند: ۴
- آدرس IP مهاجم: ۱۹۲.۱۶۸.۰.۱۰
- هدف: ایجاد تاثیر در دسترس پذیری سرویس دهنده به صورت جزئی

A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

41

### ارزیابی شبیه ساز توزیع شده حملات سایبری

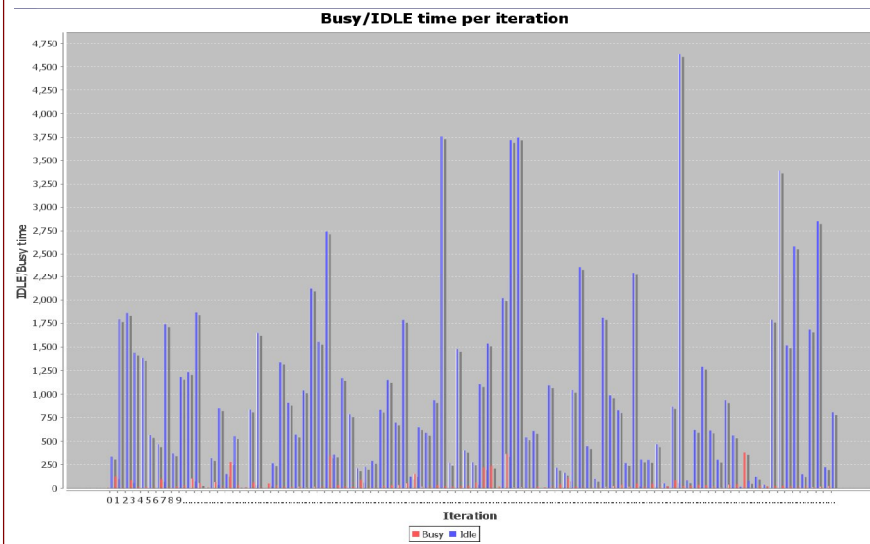
معیارهای  
عملیاتی  
سرویس  
دهنده پیش  
از وقوع حمله



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

42

### ارزیابی شبیه ساز توزیع شده حملات سایبری



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

43

### ارزیابی شبیه ساز توزیع شده حملات سایبری

معیارهای  
عملیاتی  
کامپیوترهای  
میزبان پیش  
از وقوع  
حمله



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

44

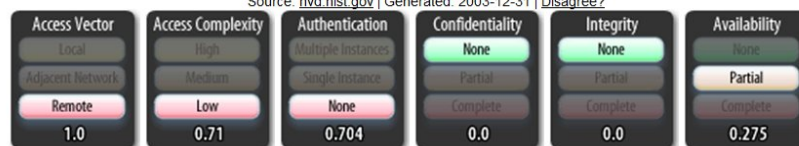
### ارزیابی شبیه ساز توزیع شده حملات سایبری

- اطلاعات مستخرج از OSVDB برای کد بهره برداری انتخاب شده برای سناریوی اول:

Description	Microsoft IIS contains a flaw that may allow a remote attacker to exhaust the available memory and force it to restart. The issue is due to IIS not limiting the memory available for constructing headers to be returned to a web client. If an attacker uploaded a specially crafted ASP page that returned an overly large header to the requesting client, IIS will run out of memory.
Classification	Location: Remote / Network Access Attack Type: Denial of Service Impact: Loss of Availability Exploit: Exploit Public Disclosure: OSVDB Verified

CVSSv2 Base Score = 5.0

Source: [nvd.nist.gov](http://nvd.nist.gov) | Generated: 2003-12-31 | Disagree?

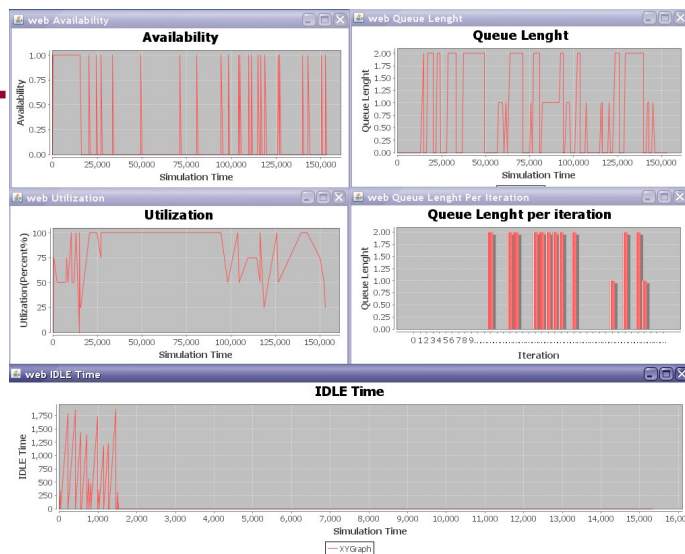


A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

45

### ارزیابی شبیه ساز توزیع شده حملات سایبری

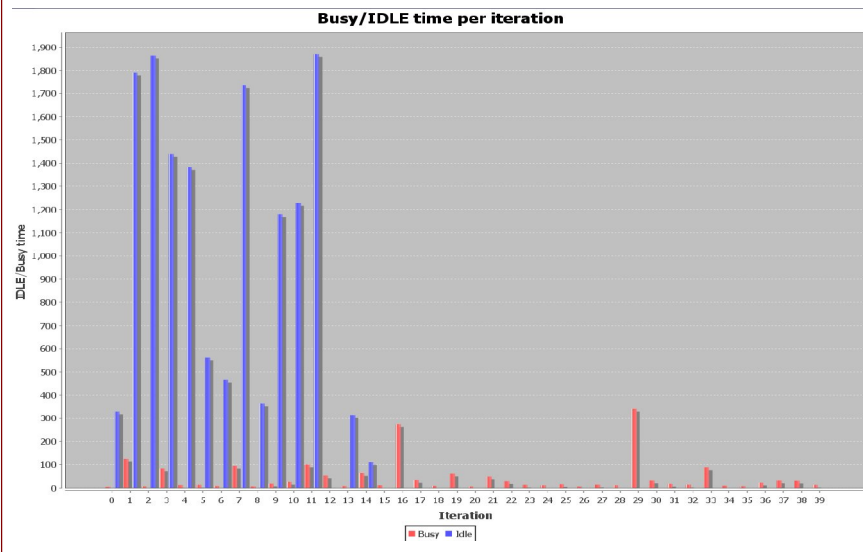
- معیارهای عملیاتی سرویس دهنده پس از وقوع حمله



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

46

### ارزیابی شبیه ساز توزیع شده حملات سایبری

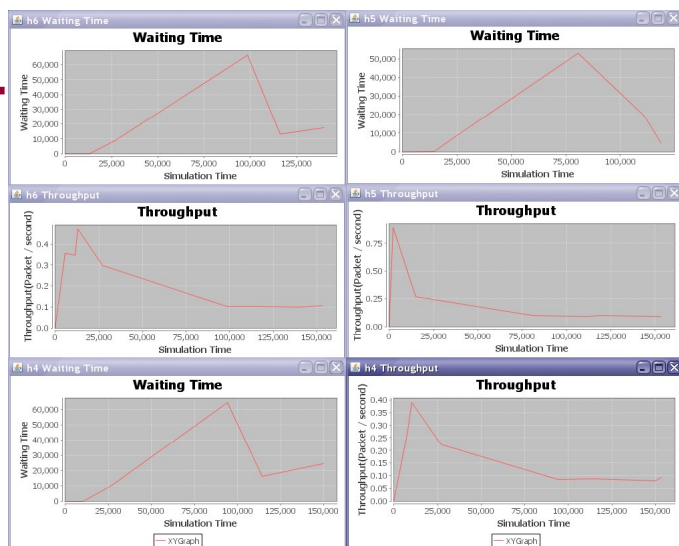


A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

47

### ارزیابی شبیه ساز توزیع شده حملات سایبری

معیارهای  
عملیاتی  
کامپیوترهای  
میزبان پس از  
وقوع حمله



A Distributed Cyber Attack Simulator Based on HLA- Mehrdad Ashtiani

48



### نتیجه گیری

- شبیه سازی حملات سایبری این امکان را به مدیران شبکه می دهد که به درک درستی از میزان امنیت شبکه های طراحی شده خود دست یابند.
- از آنجایی که شبیه سازی عناصر مختلف شبکه به صورت واقعی، به محاسبات فراوانی نیاز دارد، استفاده از رویکرد توزیع شدگی در این شبیه سازی ها در حال افزایش است. توزیع شده بودن شبیه سازی این امکان را می دهد که افراد و برنامه ها در مکان های متفرق جغرافیایی قرار گرفته و از طریق متصل شدن به شبیه سازی، با یکدیگر در تعامل قرار گیرند.
- شبیه ساز حملات سایبری توزیع شده امکان طراحی، شبیه سازی دقیق اجزای مختلف شبکه و ارائه چگونگی تغییر معیارهای عملیاتی مهم در اجزای شبکه را به کاربران خود می دهد.
- این شبیه ساز در دو حالت تحلیلی و تعاملی قابل اجرا است.
- در این شبیه ساز از نگاشت معماری مبتنی بر موجودیت بر روی معماری مبتنی بر فدرال استفاده شده است. استفاده از معماری سطح بالا به عنوان زیربنای شبیه ساز، دو ویژگی اصلی قابلیت استفاده مجدد از عناصر شبیه سازی و نیز سازگاری میان عناصر را به ارمغان می آورد.
- همچنین برای شبیه سازی ترافیک از فرایند انفجاری پواسن - پارتو برای دست یافتن به نتایج واقعی تر بهره گرفته شده است.
- در نهایت نیز شبیه ساز، با به دست آوردن معیارهای عملیاتی مختلف کمک فراوانی به مدیران شبکه برای شناخت ضعف های شبکه خود می نماید.

### کارهای آینده

- تعریف یک زبان تعریف رفتاری عناصر برای شبیه ساز توزیع شده حملات سایبری
- افزودن IDS ها مبتنی بر میزبان و شبیه سازی تکنیک های Information Fusion
- افزودن Honey Pot به شبیه ساز
- تعریف نویز در رفتار عناصر دفاعی
- افزودن پارامترهای متنوع تر به فرایند حمله

## مراجع

1. G.K.Troitzsch, "Validating simulation models," Proc. of the 18th European Simulation Multi Conference on Networked Simulation and Simulation Networks, Graham Horton SCS Europe, Koblenz-Germany, pp.265-270, July-2004.
2. G.Elahi, E.Yu, and N.Zannone, "A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities," Requirements Engineering Journal, Vol.15, 2010, pp. 41-62.
3. S.Sträßburger, "Distributed simulation based on the high level architecture in civilian application domains," Proc. of the 14th European Simulation And Modeling Conference, vol.14, Lisbon, Portugal, 17-February, pp. 119-131, 2001.
4. J.Dahmann, R.Fujimoto, and R.Weatherly, "The department of defense high level architecture," Proc. of the 29th Workshop on Distributed and Parallel Simulation, Atlanta, USA, vol.12, 10-October pp. 142-149, 1997.
5. V.Vilhelm, "Quantified security is a weak hypothesis: a critical survey of results and assumptions," Proc. of the 2009 Workshop on New Security Paradigms, NY, USA, April 01 -06, 2009.
6. E.J.Canavan, Fundamentals of network security, Library of Congress Cataloging-in-Publication Data, 2000, ISBN= 1-58053-176-8.
7. S.Bosworth, M.E.Kabay, Computer security handbook fourth edition, JOHN WILEY & SONS, INC., 2002, ISBN= 0-471-41258-9
8. E.Skoudis, T.Liston, Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses, Prentice Hall, 2005, ISBN= 978-0-13-148104-6.
9. M.Tulloch, Microsoft Encyclopedia of Security, Microsoft Press, 2003, ISBN= 0-7356-1877-1.
10. T.Niame, Characterization and modeling of internet traffic streams. Thesis for the degree of Doctor of Philosophy, University of Melbourne, Feb 2003.
11. Internet Traffic Modelling Project, Feb 2010, [www.cs.ucf.edu/~sluo/internet\\_traffic\\_modeling.htm](http://www.cs.ucf.edu/~sluo/internet_traffic_modeling.htm).
12. F.Stevens, T.Courtney, S.Singh, A.Aqbaria, J.F.Meyer, W.H.Sanders, and P.Pal, "Model based validation of an intrusion-tolerant information system," Proc. of the 23rd Symposium on Reliable Distributed Systems (SRDS 2004), Florianopolis, Brazil, October 2004.
13. V.Venkataraghavan, S.Nair, and P.M.Seidel, "Simulation-based validation of security protocols", Proc. of OPNETWORKS conference, August 2002.
14. M.Kuhl, J.Kistner, K.Costantini, and M.Sudit, "Cyber attack modeling and simulation for network security analysis," Proc. of the 39th Winter Conference on Parallel and Distributed Simulation, vol.78, Atlanta, USA, 16-December, pp. 1180-1188, 2007.
15. L.Flagg, G.Streeter, K.Costantini and A.Potter, "Bringing knowledge to network defense," Proc. of the 2007 Spring Simulation Multi Conference, vol.3, San Diego, USA, 25-March, pp. 370-377, 2007.
16. L.Flagg, G.Streeter, K.Costantini and A.Potter, "Bringing knowledge to network defense," Proc. of the 2007 Spring Simulation Multi Conference, vol.3, San Diego, USA, 25-March, pp. 370-377, 2007.

## با تشکر از توجه شما

؟