دانشگاه الزهرا، دانشکده فنی و مهندسی

تشخیص نفوذ مبتنی بر ناظر بر اساس رویکرد سیستم های ایمنی مصنوعی

نویسندگان

رضا عزمی، بشری پیشگو و حامد نعمتی

رئوس مطالب

- مقدمه و مفاهیم ابتدایی
- معماری و پیاده سازی مدل پیشنهادی
- ارزیابی مدل پیشنهادی
- نتیجه گیری

مقدمه و مفاهیم ابتدایی

- نفوذ
- سیستم های تشخیص نفوذ
- سیستم های تشخیص نفوذ مبتنی بر میزبان
- مکانیزم های هوشمند طراحی
- سیستم های ایمنی مصنوعی

نفوذ

هرگونه فعالیتی که

- جامعیت
- محرمانگی
- در دسترس بودن

و در یک کلمه *امنیت* سیستم را به خطر اندازد

5 / 25

سیستم های تشخیص نفوذ

- متدهای تشخیصی

تشخیص آنومالی و تشخیص سوء استفاده

- نحوه مقابله با نفوذ

آنلاین و آفلاین

- محل قرارگیری

سمت میزبان و سمت شبکه

6 / 25

سیستم های تشخیص نفوذ سمت میزبان

- اطلاعات وبی
- اطلاعات سیستمی
- قرارگیری سیستم در سطح کاربر
- قرارگیری سیستم در سطح هسته
- قرارگیری سیستم در سطح ناظر
- ایمن سازی فرایند رویدادنگاری فراخوان های سیستمی

مکانیزم های هوشمند طراحی

- تشخیص آنومالی مبتنی بر مدلسازی رفتار یا یادگیری ماشین
  - مدل پنهان مارکو
  - شبکه های عصبی
  - ماشین بردار پشتیبان
  - k نزدیک ترین همسایه
  - شبکه های بیزین
  - .... و
- سیستم های ایمنی مصنوعی

سیستم های ایمنی مصنوعی

- شبکه های ایمنی مصنوعی
- انتخاب غیر خودی
- تشخیص دهنده با شعاع ثابت
- تشخیص دهنده با شعاع متغیر
- تئوری خطر

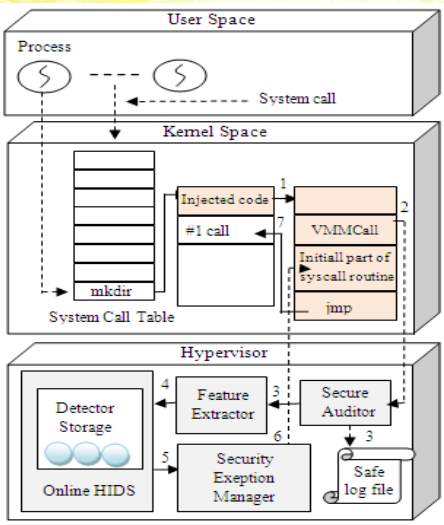
رئوس مطالب

- مقدمه و مفاهیم ابتدایی
- معماری و پیاده سازی مدل پیشنهادی
- ارزیابی مدل پیشنهادی
- نتیجه گیری

معماری و پیاده سازی مدل

- معماری مفهومی
- رویدادنگار امن
- استخراج کننده ویژگی
- سیستم تشخیص نفوذ آنلاین
- مدیر استثنائات امنیتی

معماری مفهومی



رویدادنگار امن

- پیاده سازی رویدادنگاری از طریق تکنیک تزریق کد در زمان اجرا و به وسیله ناظر که به تمام نواحی حافظه دسترسی دارد، انجام می گیرد.
- اختصاص فضا برای کد تزریقی از طریق kmalloc() و ارسال آدرس این فضا به ناظر از طریق vmmcall()
- کشف آدرس اولین دستور call در روتین مربوط به فراخوان سیستمی و تزریق کد، پیش از این آدرس
- وظایف کد تزریق شده :
- ذخیره مقادیر ثبات ها و فراخوانی getuid() ،getgid() و getpid() برای یافتن uid و gid و pid
- فراخوانی رویدادنگار امن از طریق vmmcall() در کد تزریق شده برای رویدادنگاری مقادیر
- پرش به اولین دستور call در روال فراخوان سیستمی برای اجرای این سیستم کال

13 / 25

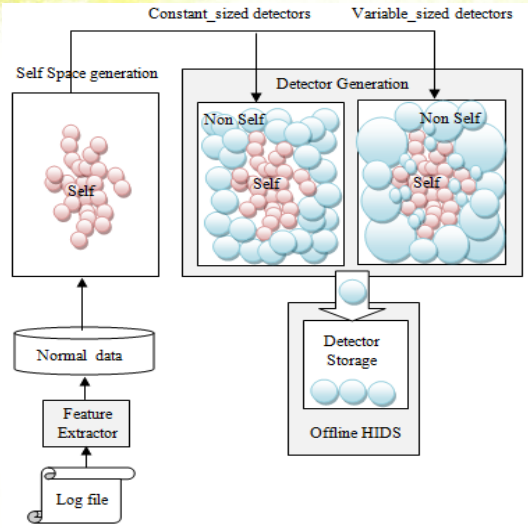
استخراج کننده ویژگی

- این واحد از میان اطلاعات ثبت شده برای هر فراخوان سیستمی، ۶ ویژگی مناسب را که قادر به تفکیک میان رفتارهای هنجار و ناهنجار هستند، استخراج می کند

Syscall_No	mode	flags	pid	gid	uid

14 / 25

سیستم تشخیص نفوذ آنلاین



15 / 25

رئوس مطالب

- مقدمه و مفاهیم ابتدایی
- معماری و پیاده سازی مدل پیشنهادی
- ارزیابی مدل پیشنهادی
- نتیجه گیری

16 / 25

ارزیابی مدل پیشنهادی

- زمان اجرا
- میزان حافظه مصرفی
- قدرت تشخیص

زمان اجرا

- افزودن مکانیزم های امنیتی سرباره زمانی دارد
- رویدادنگاری فراخوان های سیستمی
- سیستم تشخیص نفوذ
- فاز آموزش
- فاز تشخیص
- وابسته به تعداد تشخیص دهنده

فراخوان سیستمی	عدم وجود رویدادنگاری	وجود رویدادنگاری
Getpid	۸	۱۶
Getuid	۹	۱۸
Getgid	۸	۱۹
Open	۱۷	۴۵
Read	۱۵	۳۴
Write	۴۱	۱۰۵
Close	۱۴	۲۲
Mkdir	۳۱	۷۵
Rmdir	۲۴	۴۷

میزان حافظه مصرفی

- تخصیص مقداری حافظه از فضای آدرس هسته در مرحله تزریق کد
- 30 syscall x 3kbyte = 90 kbyte
- تشخص فضایی برای تشخیص دهنده ها در ناظر
- وابسته به تعداد تشخیص دهنده ها
- مرکز تشخیص دهنده + شعاع

19 / 25

قدرت تشخیص

- جمع آوری داده
- رویدادنگاری رفتار نرمال و غیرنرمال توسط مدل پیشنهادی
- برچسب گذاری الگوها از طریق chkrootkit
- امضای بدافزارهای مخرب را جستجو و PID آن را برمیگرداند
- پیش پردازش
- نرمال سازی
- حذف رکوردهای تکراری

20 / 25

قدرت تشخیص (ادامه)

- تست کارایی
- معیارهای ارزیابی
  - Accuracy (Acc) ➢ $Acc = \frac{TP + TN}{TP + TN + FP + FN}$
  - False Alarm (FA) ➢ $FA = \frac{FP}{TN + FP}$
- متد ارزیابی
  - k-cross fold (k=3) ➢

قدرت تشخیص (ادامه)

روش‌های تشخیص نفوذ		طبقه‌بند بیزین		سیستم‌های ایمنی مصنوعی (روش‌های انتخاب غیرخودی)			
				تشخیص‌دهنده‌ها با طول ثابت		تشخیص‌دهنده‌ها با طول متغیر	
شرایط آزمایش	فاز آموزش	داده‌های نرمال و غیرنرمال		تنها داده‌های نرمال			
	فاز تست	داده‌های نرمال و غیرنرمال		داده‌های نرمال و غیرنرمال			
معیارهای ارزیابی		دقت (٪)	نرخ خطا (٪)	دقت (٪)	نرخ خطا (٪)	دقت (٪)	نرخ خطا (٪)
نتایج آزمایشات	اجرای ۱	۶۸.۸۳	۳۰.۷۳	۸۸.۵۳	۱.۵۰	۸۰.۹۲	۱۲.۸۴
	اجرای ۲	۶۹.۵۳	۲۹.۷۹	۸۵.۲۷	۴.۲۳	۸۶.۵۹	۶.۸۳
	اجرای ۳	۶۹.۰۷	۳۱.۱۷	۸۸.۵۳	۱.۹۱	۸۴.۴۲	۱۰.۱۱
	اجرای ۴	۷۰.۲۵	۳۰.۷۱	۸۸.۱۶	۱.۵۰	۸۴.۳۰	۹.۱۵
	اجرای ۵	۶۹.۰۷	۳۰.۶۳	۸۷.۵۶	۱.۰۹	۸۵.۸۷	۷.۵۱
	میانگین	۶۹.۳۵±۰.۵۷	۳۰.۶۱±۰.۵	۸۷.۶۱±۱.۳۷	۲.۰۵±۱.۲۶	۸۴.۴۲±۲.۱۹	۹.۲۹±۲.۳۷

رئوس مطالب

- مقدمه و مفاهیم ابتدایی
- معماری و پیاده سازی مدل پیشنهادی
- ارزیابی مدل پیشنهادی
- نتیجه گیری

23 / 25

نتیجه گیری

- تضمین سلامت رویدادنگاری سیستم کال ها
- با استفاده از معماری مبتنی بر ناظر
- بهره گیری از سیستم کال ها به عنوان الگوهای رفتار
- مدل سازی رفتار
- بر اساس سیستم های ایمنی مصنوعی

24 / 25


دانشگاه الزهراء
تشخیص نفوذ مبتنی بر ناظر
بر اساس رویکرد سیستم های ایمنی مصنوعی
نویسندگان
رضا عزمی، بشری پیشگو و حامد نعمتی