Arman Process Journal
(APJ)
Homepage: www.armanprocessjournal.ir

Security Aspects in the Kernel of Distributed Operating Systems

M. Latifi [*,1]
[1] *Electrical and Computer Engineering, Islamic Azad University, Science and Research Branch, Tehran, Iran*

Received: 7 October 2022
Accepted: 26 December 2022

KEYWORDS:
Distributed Operating System,
Security,
Core,
Firmware,
Access Control,

[1] Corresponding author
malatifi1988@gmail.com

ABSTRACT

Nowadays, due to the large amount of information and the need of rapid processing, the need for computers with up-to-date and efficient operating systems with high processing power is felt. During the last decades, progress in the field of information technology has made available fast distribution systems. Distributed systems are one of the best solutions to achieve the above goal. By placing computer systems on the platform of the distribution network, it is possible to create a high processing power, whose complexity and organization are hidden from the eyes of users and in addition, it brings us the availability of resources and scalability. Securing the core of distributed operating systems is a necessity that can help improve the security of information technology in distributed network environments. In order to fundamentally implement this process, it is necessary to create an expert security team. Also, in addition to the technical review and the implementation of protection settings and access controls, there is a need to develop new methods and tools to study the sequence of certain or possible protection operations in the core of distributed operating systems. In this article, we are going to examine the security aspects in the core of distributed operating systems.

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
71	0	1

نشریه تخصصی آرمان پردازش، دوره ۳، شماره ۴، زمستان ۱۴۰۱

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

جنبه های امنیتی در هسته سیستم عامل های توزیعی

مریم لطیفی *[1]،

[1] دانشکده مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران

چکیده

امروزه با توجه به حجم وسیعی از اطلاعات و نیاز به پردازش آن‌ها، نیاز به کامپیوترهایی با سیستم عامل های بروز و کارامد با قدرت پردازشی بالا احساس می‌شود. در طول دهه های اخیر، حصول پیشرفت در حوزه فناوری اطلاعات و تکنولوژی باعث در دسترس قرار گرفتن سیستم های توزیعی سریع شده است. سیستم‌های توزیعی یکی از بهترین راه حل‌ها در جهت رسیدن به هدف فوق است. با قرار دادن سیستم‌های کامپیوتری در بستر شبکه توزیعی می‌توان توان پردازشی بالایی به وجود آورد که پیچیدگی و سازماندهی آن‌ها از دید کاربران مخفی بوده و علاوه بر آن، دسترس‌پذیر بودن منابع و مقیاس‌پذیری را برای ما به ارمغان می‌آورد. ایمن سازی هسته سیستم عامل های توزیعی یک ضرورت است که می تواند به بهبود وضعیت امنیت فناوری اطلاعات محیط های شبکه ای توزیعی کمک شایانی نماید. بمنظور پیاده‌سازی اصولی این فرایند لازم است، یک تیم امنیتی متخصص ایجاد گردد. همچنین علاوه بر بررسی فنی و اجرای تنظیمات حفاظتی، نیاز به ایجاد سطوح دسترسی متفاوت و توسعه روشها و ابزارهای جدید برای مطالعه توالی عملیات حفاظتی معین یا محتمل در هسته سیستم عامل های توزیعی است. در این مقاله قصد داریم جنبه های امنیتی در هسته سیستم عامل های توزیعی را بررسی نمائیم.

واژگان کلیدی:
سیستم عامل توزیعی،
امنیت،
هسته،
میان افزار،
کنترل دسترسی،

تعداد جداول	تعداد شکل ها	تعداد مراجع
۱	۰	۱۷

مقدمه

اصطلاحات سیستم عامل و سیستم عامل توزیع شده امروزه دو اصلاحی هستند که نقش حیاتی در دنیای فناوری اطلاعات و ارتباطات دارند. سیستم‌عامل که به صورت مخفف OS [1] هم نامیده می‌شود، در عمل یک واسط نرم افزاری میان سخت‌افزار و برنامه‌های اجرایی یک سیستم کامپیوتری است. در واقع مجموعه نرم‌افزارهایی که منابع سخت افزاری و نرم افزاری یک سیستم را مدیریت می‌کنند سیستم‌عامل نامیده می‌شوند. در هر سیستم کامپیوتری و شبکه ای، حداقل یک سیستم عامل وجود دارد. بدین ترتیب که با استفاده از سیستم عامل می توان به منابع سخت افزاری سیستم دسترسی داشت و از آن ها بصورت حساب شده استفاده کرد. استفاده از سیستم عامل باعث می شود بتوانیم از قدرت سخت افزارها استفاده کنیم. سیستم‌های عامل در کامپیوترهای شخصی ابتدا برای اهداف دیگری نظیر مدیریت نوارهای مغناطیسی ارائه شد و بعدها با توسعه علم دیجیتال، برای مدیریت فایل‌های دیجیتال در سخت‌افزارها مورد استفاده قرار گرفت [۱]. اساسا سیستم عامل مهمترین برنامه نصب شده در کامپیوتر است که وظایف اصلی ذیل را برعهده دارد [۴-۲]:

- مدیریت و سازماندهی برنامه ها، فایل ها و نرم افزارها
- راه اندازی، مدیریت و بکارگیری سخت افزار
- برقراری ارتباطات بین استفاده کننده کامپیوتر، نرم افزار و سخت افزار
- مدیریت و سازماندهی ارتباط با شبکه
- مدیریت مصرف منابع سیستمی و دستگاههای جانبی سیستم

به تعبیر ساده میتوان گفت سیستم عامل نقش روح را در پیکر سخت افزار و شبکه ایفا میکند. تصمیم درخصوص انتخاب سیستم عامل کلیه ابعاد فنی کامپیوتر و فناوری اطلاعات را تحت الشعاع قرار میدهد و هر سیستم عاملی که انتخاب شود خشت اول و زیربنای توسعه فنی و نرم افزاری فناوری اطلاعات را مشخص میکند. سیستم توزیعی در واقع مجموعه‌ای از کامپیوترهای مستقل است که برای کاربران خود مانند یک سیستم منسجم و منفرد به نظر می‌رسد.

امروزه با توجه به حجم وسیعی از اطلاعات و نیاز به پردازش آن‌ها، نیاز به کامپیوترهایی با سیستم عامل های بروز و کارامد با قدرت پرداز شی بالا احساس می شود. سیستم‌های توزیعی یکی از بهترین راه حل‌ها در جهت رسیدن به هدف فوق است. با قرار دادن سیستم‌های کامپیوتری در بستر شبکه توزیعی می‌توان توان پردازشی بالایی به وجود آورد که پیچیدگی و سازماندهی آن ها از دید کاربران مخفی بوده و علاوه بر آن، دسترس‌پذیر بودن منابع و مقیاس‌پذیری را برای ما به ارمغان می‌آورد. سیستم‌های توزیعی به دلیل گسترش به نسبت آسان آن‌ها، در دسترس بودن همیشگی آن‌ها، قابلیت اطمینان و سرعت بالای اجرای برنامه‌ها به خصوص برنامه‌های چندنخی (موازی)، از اهمیت ویژه‌ای برخوردار هستند. سیستم عامل توزیع شده شامل چندین کامپیوتر مستقل می باشند که به کمک یک واسط یا میان افزار به یکدیگر متصل شده اند. در واقع وظیفه اصلی میان افزار، تخصیص بهینه منابع بین سیستم های توزیع شده می با شد [۵] . تعریف دیگری که از سیستم های توزیع شده وجود دارد بدین گونه است که سیستم های توزیع شده شامل چندین کامپیوتر مستقل هستند که کاربر آن ها را به شکل یک سیستم واحد می بیند که یک لایه نرم افزاری روی این سیستم های توزیع شده به نام Middleware وجود دارد که باعث می شود تا مدل و زیرساخت مورد نظر پیاده سازی شود. سیستم عامل توزیع شده باعث شده است تا سرعت پردازش بسیار بالاتر برود و محدودیت جغرافیایی جهت دسترسی به منابع سخت افزاری نیز تا حد زیادی برداشته شده است. یکی از مهم ترین اهداف این سیستم عامل ها، دسترسی بهینه به منابع می باشد که باعث ایجاد نسل جدیدی از سیستم های مدرن در آینده خواهد شد . امنیت از مهم ترین ضروریات سیستم عامل های توزیعی است. امنیت سیستم عامل شامل تمام تکنیک های کنترل پیشگیرانه است، که در صورت به خطر انداختن امنیت سیستم عامل، از دارایی رایانه ای که قادر به سرقت، ویرایش یا حذف آنها باشد، محافظت می کند. امنیت سیستم عامل بسیاری از تکنیک ها و روش های رایج را تعبیه می نماید که رهائی از تهدیدات و حملات ایمنی را تضمین می نماید [۷-۶] . در این مقاله قصد داریم جنبه های امنیتی در هسته سیستم عامل های توزیعی را بررسی نمائیم.

جنبه های امنیتی در هسته سیستم عامل های توزیعی

گسترش شبکه های رایانه ای در سطح دنیا و امکان ارتباط همه کامپیوترها به یکدیگر، خلاء های امنیتی و پتانسیل نفوذ به هر سیستم کامپیوتری از هر جای دنیا را فراهم نموده است. وجود نقطه ضعف یا آسیب پذیری در سیستم عامل، راه نفوذ رایج تر و در دسترس تری را در اختیار مهاجمین قرار می دهد. بر این اساس، جنبه های امنیتی در هسته سیستم عامل به منزله مهمترین مولفههای امنیت اطلاعات و شبکه های توزیعی رایانه ای محسوب میشود. وجود ارتباطات و اتصالهای رایانه ای گسترده، مسئله جدی امکان جاسوسی الکترونیکی به نفع سازندگان سیستم عامل و قدرتهای سیاسی حاکم بر آنها را

[1] Operating System

مطرح میسازد. از نظر فنی، فناوری فعلی به شکل ساده ای امکان اجرای برنامه در محیط طرف مقابل در یک اتصال الکترونیکی را فراهم آورده است. یک سیستم عامل مثل یک مرکز فرماندهی به شما اجازه افزایش یا کاهش امنیت و سطوح دسترسی سیستم را می دهد . سیستم عامل های توزیعی به داشتن نقاط آسیب پذیر فراوان مشهور است، اما در صورت عدم نیاز به نصب سیستم عامل دیگر، باید یک آگاهی اولیه در مورد روش های بالا بردن امنیت کامپیوتر داشت . فرآیندهای سیستم عامل و هسته، وظایف تعیین شده را طبق دستورالعمل انجام می دهند . اگر یک برنامه کاربر باعث شده است که این فرآیند وظایف مخرب را انجام دهد، امنیت سیستم عامل پس از آن به عنوان برنامه تهدید شناخته می شود. یکی از نمونه های متداول تهدیدات برنامه ، برنامه های نصب شده در سیستم است که می تواند اعتبار کاربر را از طریق شبکه به برخی از هکرها ذخیره و ارسال کند . در زیر لیستی از تهدیدهای رایج در این حوزه ذکر گردیده است [۱۰-۸] :

- Trojan Horse: چنین برنامه ای اعتبار نامه ورود کاربر را به دام می اندازد و آنها را ذخیره می کند تا به کاربر مشکوکی ارسال کند که بعداً می تواند وارد رایانه شود و به منابع سیستم دسترسی پیدا کند.

- Trap Door: اگر برنامه ای که به گونه ای طراحی شده است که مطابق نیاز کار کند، دارای سوراخ امنیتی در کد آن بوده و بدون اطلاع کاربر ، اقدامات غیرقانونی را انجام می دهد، پس از آن گفته می شود که یک درب تله دارد.

- Bomb: بمب منطقی شرایطی است که یک برنامه فقط وقتی شرایط خاصی را برآورده می کند، دچار اشتباه می شود و در غیر این صورت به عنوان یک برنامه واقعی کار می کند.

- Virus: همانطور که از نام آن مشخص است، ویروس می تواند خود را در سیستم رایانه ای تکرار کند. آنها بسیار خطرناک هستند و می توانند پرونده های کاربر، امنیت سیستم عامل سیستم های خرابی را تغییر داده و حذف کنند . ویروس به طور کلی یک کد کوچک است که در یک برنامه تعبیه شده اس. عموما با دسترسی کاربر به برنامه ویروس شروع به جاسازی در سایر پرونده ها یا برنامه های سیستمی می کند و می تواند سیستم عامل را برای کاربر غیرقابل استفاده کند. برای بالا بردن امنیت کامپیوتر روش های زیادی وجود دارد، که در اینجا به مهم ترین این روش ها را می پردازیم:

- عدم نصب اتصالات شبکه ای جانبی وکاربردها و نرم افزار های اضافی
- کاربران باید این نکته را در نظر داشته باشند که نیازی به نصب هر نرم افزاری در کامپیوتر نمی باشد و یا اگر یک نرم افزار در حال انجام کار است نیازی به نصب نرم افزار های مشابه دیگر نمی باشد . اضافه کردن نرم افزار های اضافی نه تنها باعث انجام بهتر کار شما نمی شوند بلکه باعث کند شدن و نا امن شدن هسته سیستم عامل می شوند.
- سعی در استفاده از سیستم عامل های اصل و به روز
- با بروزرسانی سیستم عامل بسیاری از درگاه های باز بسته می شوند امنیت ارتقا می یابد.
- عدم استفاده شخصی از سرویس ها، واسط ها و سیستم های عمومی ناشناخته
- استفاده از ماژول ها، واسط ها و نرم افزار های امنیتی معتبر و به روز
- اجتناب از در اختیار گذاشتن پسوردها
- دانلود واسط ها و نرم افزارها از مراجع معتبر
- باز نکردن لینک های مشکوک
- لینک های مشکوک و ناشناس معمولا لینک های مخربی هستند که اکثراً برای دزدی اطلاعات و هک کردن استفاده می شوند.
- دقت در اتصال به فلش مموری ها

از جنبه دیگر، امنیت نرم افزاری یک سیستم عامل توزیعی یک مفهوم انتزاعی است که به پارامترهای فکری هر شخص وابسته است، چون درجه آسیب پذیری امنیتی، از خط به خط کدهای برنامه نویسی به وجود می آید . هر حوزه امنیتی از درجه حساسیت خاصی برخوردار است . در نتیجه تعابیر بسیار زیادی برای امنیت وجود دارد. پارامترهای متعددی برای درجه بندی امنیت وجود دارد که میتوان از آن طریق باگهای برطرف شده یک مجموعه نرم افزاری خاص را محاسبه کرد . همچنین بر اساس معیار ارزیابی سیستم‌های مورد اعتماد رایانه‌ای که از سوی وزارت دفاع ایالات متحده تدوین شده است، چهار طبقه‌بندی امنیتی عمومی وجود دارد که با حروف A ، B، C و Dنشان داده می‌شوند. این معیار به طور گسترده‌ای برای تعیین مدل امنیت سیستم‌ها و راه‌حل‌های امنیتی مورد استفاده قرار می‌گیرد. در ادامه توصیف فشرده‌ای از هر یک از طبقه‌بندی‌های امنیتی ارائه شده است [۱۳-۱۱] :

جدول۱. توصیف طبقه بندی های امنیتی

نوع طبقه‌بندی امنیتی	توصیف
نوع A	بالاترین سطح طبقه‌بندی امنیتی است. در این سطح از خصوصیات طراحی و فناوری‌های اعتبار سنجی استفاده می‌شود. در این سطح میزان بالایی از امنیت پردازش تضمین می‌شود.
نوع B	در این سطح از طبقه‌بندی امنیتی حفاظت اجباری سیستم ارائه شده است و سیستم همه مشخصات سطح C2 طبقه‌بندی امنیتی را دارد در این سطح به هر شیء یک برچسب حساسیت داده می‌شود که بر سه نوع است: • B1 – حداقل برچسب امنیتی هر شیء در سیستم است. این برچسب برای تصمیم‌گیری در مورد کنترل دسترسی مورد استفاده قرار می‌گیرد. • B2 – برچسب‌های امنیتی را به منابع سیستم مانند شیء‌های ذخیره‌سازی گسترش می‌دهد و از کانال‌های covert و حسابرسی رویدادها پشتیبانی می‌کند. • B3 – امکان ایجاد فهرست‌ها یا گروه‌های کاربری برای کنترل دسترسی، اعطای دسترسی یا بازپس‌گیری دسترسی برای شیء‌های واجد نام را فراهم می‌سازد.
نوع C	این سطح از طبقه‌بندی امنیتی حفاظت و حسابرسی کاربر را با استفاده از ظرفیت‌های حسابرسی ارائه می‌کند. این سطح دارای دو نوع است: • C1 – از کنترل‌هایی استفاده می‌کند که با استفاده از آن‌ها کاربران می‌توانند از اطلاعات خود حفاظت کرده و کاربران دیگر را از خواندن/حذف تصادفی داده‌هایشان باز دارند. نسخه‌های یونیکس غالباً دارای سطح C1 هستند. • C2 – یک سیستم کنترل دسترسی چندگانه برای ظرفیت‌های یک سیستم سطح C1 ارائه می‌کند.
نوع D	پایین‌ترین سطح طبقه‌بندی امنیتی است که کمترین حفاظت را ارائه می‌کند. سیستم‌های عامل MS-DOS و ویندوز ۳,۱ چنین سطح امنیتی را ارائه می‌کنند.

لازم به ذکر است، عموما فعالیت های لازم در فرآیند امن سازی سیستم عامل های توزیعی، به صورت زیر در قالب چهار مرحله طرح ریزی(Plan)، اجرا (Do)، بررسی و ارزیابی (Check)و اصلاح وارتقاء (Act) دسته بندی می شوند [۱۵-۱۴]:

• طرح ریزی

- تعیین حوزه عملکرد
- تهیه طرح کلان امنیتی فضای تبادل اطلاعات
- تدوین معماری امنیتی و یکپارچه سازی عناصر (طرح کلان،خط مشی،معماری و استانداردهای امنیتی) و تعیین خط مشی امنیت
- ارزیابی و مدیریت مخاطرات
- انتخاب کنترل های امنیتی مورد نیاز

• اجرا

- تدوین و اجرای شیوه های کنترل مدیریتی و عملیاتی

• بررسی و ارزیابی

- نظارت برحسن پیاده سازی طرح های امنیتی
- بررسی و نظارت برمیزان انطباق دسترسی ها و خروجی های کارکرد منابع سیستم عامل با استانداردهای امنیتی

از سوی دیگر ایجاد امنیت و استفاده از شبکه های توزیعی، نیازمند استفاده از برنامه های متعدد و متنوع است. این امکان وجود دارد که در برخی از سیستم های توزیعی، برخی از برنامه ها قابلیت اجرا نداشته باشند. این موضوع نیز می تواند نقص باشد. به این واسطه مشکلات دیگری نیز به وجود خواهد آمد. در نتیجه حتی اگر شرایط برنامه ریزی شده برای ایجاد امنیت نیز با بالاترین امکانات آن شکل گیرد، سوء استفاده برخی از اعضاء و ارسال اطلاعات به خارج از شبکه می تواند به عنوان نقص بزرگ این سیستم تلقی شود [۱۶]. سیستم تشخیص نفوذ شبکه، قادر به ردیابی هکرها و تشخیص نقض های

امنیتی و استفاده های غیرمجاز و حمله به سیستم عامل، شبکه یا سیستم ارتباطی نیز می باشد . این سیستم سرورهای مجازی و نرم افزارها را نظارت کرده و هر زمان که فعالیت مخربی پیدا کند، اعلان می دهد . سیستم تشخیص نفوذ زمانی کارایی لازم را پیدا می کند که بتواند اعلان ها را اولویت بندی و یک پیام ارسال کند. از آنجا که فایل لاگ شامل مراحل مختلف همه حملات است، ارسال یک اعلان اولویت بندی شده بهتر از ارسال کل فایل است . در نتیجه سیستم تشخیص نفوذ باید با یک سیستم ممانعت از نفوذ شبکه ترکیب شود تا ترافیکهای غیرنرمال را شناسایی، متوقف و گزارش دهد. راهکار امنیتی دیگر در هسته سیستم عامل های توزیعی مجازی سازی است [۱۷] . مجازی سازی یکی از مکانیزم های اصلی است که در مقابل تلاش های کاربران برای حمله به یکدیگر و متعاقباً حمله به زیرساخت سیستم عامل توزیعی، دفاع قدرتمندی را از خود نشان می دهد. با به کارگیری تکنولوژی مجازی سازی سیستم قادر خواهد بود به صورت مجزا هر سرویس و برنامه را روی یک ماشین مجازی نصب و راه اندازی کرد تا علاوه بر حل مشکلات ناسازگاری برنامه ها و سرویس ها بتوان به راحتی سرور را عیب یابی کرد. به علاوه در صورت نیاز می توان به ماشین مجازی حافظه، رم و ... اختصاص داد و از هدر رفت منابع سخت‌افزاری جلوگیری کرد. نکته نهایی این بخش نیز اشاره به این موضوع دارد که ایجاد امنیت نیز به راحتی امکان پذیر نیست. باید برنامه نویسان متبحری در این زمینه فعالیت نمایند. زیرا سیستم های توزیعی، عموما به حالت رمزنگاری شده طراحی می شوند. به این منظور علاوه بر بررسی فنی و نحوه اجرای تنظیمات حفاظتی، نیاز به توسعه روشها و ابزارهای جدید برای مطالعه توالی عملیات حفاظتی معین یا محتمل در هسته سیستم عامل های توزیعی است.

نتیجه گیری

ایمن سازی هسته سیستم عامل های توزیعی می تواند به بهبود وضعیت امنیت فناوری اطلاعات محیط های شبکه ای کمک کند. با این حال، ایمن سازی سیستم یک فرآیند پیچیده است. بمنظور پیاده‌سازی اصولی این فرایند لازم است، یک تیم امنیتی متخصص ایجاد گردد. متخصصان باید به طور پیوسته لاگ‌های سیستمی را تحت نظر داشته باشند تا بتوانند هرگونه فعالیت مشکوکی را در نطفه خفه کنند. همچنین، ارتقاء دسترسی، ایجاد دسترسی برای کاربران و احراز هویت کاربران باید کاملا تحت نظارت باشد. گذشته از این موارد تیم متخصص باید به طور پیوسته اسکن‌هایی را برای شناسایی بدافزارها و آسیب‌پذیری‌های احتمالی در سیستم توزیعی انجام دهند. در این حیطه انجام تست‌های نفوذ دوره‌ای نیز توصیه می‌شود. همچنین از دیگر اصول امنیت سایبری و امن سازی سیستم عامل های توزیعی، پشتیبان‌گیری منظم از داده‌های حساس است. آنچه واضح است این است که سطح حمله هیچ‌وقت صفر نمی‌شود و احتمال حملات به زیرساخت‌های توزیعی همواره وجود دارد. با پشتیبان‌گیری منظم از داده‌های حساس می‌توان خسارت‌های خرابی ها و حملات احتمالی را به حداقل رساند.

منابع

[1] Na SH, Park JY, Huh EN. Personal cloud computing security framework. In2010 IEEE Asia-Pacific Services Computing Conference 2010 Dec 6 (pp. 671-675). IEEE.

[2] Abdelmoumin G, Hazzazi N. Distributed Operating System Security and Protection: A Short Survey. In17th International Conference on Information Technology–New Generations (ITNG 2020) 2020 (pp. 145-151). Springer International Publishing.

[3] Wang M, Goscinski A. The development and testing of the identity-based conference key distribution system for the RHODOS distributed system. InComputer Security—ESORICS 92: Second European Symposium on Research in Computer Security Toulouse, France, November 23–25, 1992 Proceedings 2 1992 (pp. 209-228). Springer Berlin Heidelberg.

[4] Priyadarshini SB, Bagjadab AB, Mishra BK. Security in distributed operating system: A comprehensive study. Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies. 2019 Mar 25:221-30.

[5] Dhamdhere D. Operating systems. McGraw-Hill, Inc.; 2008 Jan 9.

[6] Schwarzkopf M, Grosvenor MP, Hand S. New wine in old skins: the case for distributed operating systems in the data center. InProceedings of the 4th Asia-Pacific Workshop on Systems 2013 Jul 29 (pp. 1-7).

[7] Vinter ST, Casey TA, Huber KA. The Secure Distributed Operating System

Design Project. BBN LABS INC CAMBRIDGE MA; 1988 Jun 1.

[8] Zhang C, Shaw R, Heckman MR, Benson GD, Archer M, Levitt K, Olsson RA. Towards a Formal Verification of a Secure and Distributed System and Its Applications. CALIFORNIA UNIV DAVIS DEPT OF COMPUTER SCIENCE; 1994 Jan 1.

[9] Caelli WJ. Security in open and distributed systems. Information Management & Computer Security. 1994 Mar 1;2(1):18-24.

[10] Tanenbaum AS, Van Renesse R. Distributed operating systems. ACM Computing Surveys (CSUR). 1985 Dec 10;17(4):419-70.

[11] Arenas AE, Aziz B, Maj S, Matthews B. An autonomic security monitor for distributed operating systems. InTowards a Service-Based Internet: 4th European Conference, ServiceWave 2011, Poznan, Poland, October 26-28, 2011. Proceedings 4 2011 (pp. 112-121). Springer Berlin Heidelberg.

[12] Nessett DM. Identifier protection in a distributed operating system. ACM SIGOPS Operating Systems Review. 1982 Jan 1;16(1):26-31.

[13] Xiao Y, Pan Y, editors. Security in distributed and networking systems. World Scientific; 2007.

[14] Mullender SJ, Van Rossum G, Tananbaum AS, Van Renesse R, Van Staveren H. Amoeba: A distributed operating system for the 1990s. Computer. 1990 May;23(5):44-53.

[15] Chapin PC. Distributed Operating Systems.

[16] Khan S, Waqas SM, Ahmed A. A Survey of Security Threats in Distributed Operating System. i-Manager's Journal on Computer Science. 2020 Sep 1;8(3):44.

[17] Sinha PK. Distributed operating systems: concepts and design. PHI Learning Pvt. Ltd.; 1998.