# مقایسه‌ای بین سیستمهای Linux ، OpenBSD و Windows از نظر امنیت

## ■ مقدمه

وقتی سیستم عاملها را با هم مقایسه می‌کنیم، بعضی از قویترین عقاید بیان می‌شوند ولی هنگامیکه در مورد امنیت بحث می‌کنیم، غلط‌ترین اطلاعات بیان می‌شوند. بخصوص هنگامیکه یک نفر با زمینه ذهنی قوی در ویندوز یا لینوکس، می‌خواهد در مورد سیستم عامل دیگری اظهار نظر کند، اشتباهات فاحشی را مرتکب می‌شود.
این مساله متاسفانه حتی در کتابهایی که بوسیله نویسندگانی آگاه نوشته می‌شوند و توسط معتبرترین ناشران به چاپ می‌رسند نیز ملاحظه می‌شود. از جمله این کتابها کتابی با نام Professional Apache نوشته آقای Peter Wainwright است که توسط انتشارات Wrox به چاپ رسیده است. نویسنده این کتاب چنین می‌گوید: (( سیستمهای ویندوز مفهوم user privilege را پشتیبانی نمی‌کنند. و این یکی دیگر از دلایلی است که باعث شده است Apache سیستم عامل Unix را نسبت به ویندوز ترجیح دهد. )) این نشان می‌دهد که نویسنده کتاب با سیستم ویندوز آشنایی کافی ندارد و تشابه ظاهری Windows NT با خانواده Widows 95 نویسنده را به اشتباه انداخته است.

## ■ نصب Default

در اینجا می‌خواهیم سیستمها را از نظر نصب با گزینه‌های پیش فرض (Default Install) با هم مقایسه کنیم. این مقایسه خیلی راحت است چراکه OpenBSD تنها سیستم عاملی است که بطور default امن است. هیچ رقابتی در این زمینه وجود ندارد. یعنی اگر سیستم عاملهای OpenBSD و لینوکس و ویندوز را با گذاشتن CD هر کدام درون دستگاه نصب کنیم و در حین نصب تمام گزینه‌های پیش فرض را انتخاب کنیم، آنگاه در بین این سیستمها، سیستم عامل OpenBSD کاملا امن است در حالیکه سیستم عاملهای لینوکس و ویندوز هیچ گونه امنیتی ندارند.
مروری بر OpenBSD بعضی از ویژگیهای اصلی این سیستم را نشان می‌دهد و معلوم می‌کند که چگونه این سیستم عامل برای امنیت در نصب default طراحی شده است. در اینجا ما سیستم عاملهای همه منظوره را با هم مقایسه می‌کنیم و منظورمان از سیستم عامل لینوکس در مقایسه‌ها، توزیعهای همه منظوره و پر استفاده آن نظیر Red Hat است. سیستم عامل لینوکس توزیعهای دیگری از جمله Trustix و EnGarde نیز دارد که بطور مشخص لینوکس را برای امنیت تنظیم می‌کنند ولی این توزیعها همه منظوره و پر استفاده نیستند.

## ▪ OpenBSD

### پیدایش OpenBSD

OpenBSD در واقع انشعابی از NetBSD می‌باشد. NetBSD سیستم عاملی است که تمرکز اصلی خود را روی پشتیبانی سکوهای سخت‌افزاری مختلف قرار داده است و از این حیث نسبت به سایر سیستم عاملها برتری دارد. مدتی بعد از پیدایش NetBSD ، FreeBSD از آن منشعب شد چونکه توسعه دهندگان آن قصد داشتند کارایی این سیستم را برای کار روی پردازنده‌های ساخت intel بهینه سازند. در نتیجه امروزه FreeBSD به عنوان سریعترین سیستم عاملی که روی ماشینهای Intel اجرا می‌شود، شناخته شده است. مدتی پس از جدا شدن FreeBSD سیستم عامل OpenBSD با هدف ایجاد یک سیستم عامل ایمن و قابل اطمینان، از NetBSD جدا شد. وقتی یک نفر یا یک سازمان یک هدف واقعی و روشن را بدون هیچ تضادی دنبال کند، بطور معمول می‌تواند به آن هدف دست یابد. بدین ترتیب OpenBSD به هدف از پیش تعیین شده خود دست یافت.

اگر بخواهیم بطور دقیق‌تر صحبت کنیم، باید بگوییم که یک سیستم عامل نمی‌تواند برای رسیدن به چندین هدف بهینه شود. چراکه بعضی از اهداف با هم در تضاد هستند. مثلا یک سیستم نمی‌تواند هم برای پشتیبانی از بیشترین سکوهای سخت‌افزاری و هم برای اجرای سریع و هم برای امنیت بهینه شود. بنابراین به ترتیب سیستم‌عاملهای NetBSD و FreeBSD و OpenBSD به منظور برآورده سازی این اهداف تولید شدند و توسعه یافتند.

در مورد OpenBSD باید بگوییم که قابلیت اطمینان و امنیت دو مفهوم و دو هدف جدا از هم نیستند. بلکه قابلیت اطمینان پیش‌نیاز امنیت است. و برای ایجاد یک سیستم عامل امن ابتدا باید قابلیت اطمینان سیستم را بالا بریم و باگهای سیستم را برطرف سازیم. چراکه بیشتر مشکلات امنیتی سیستمها بواسطه وجود باگها ایجاد می‌شوند. باگ به این معناست که سیستم کار غیر منتظره‌ای را انجام دهد. یا به خاطر رویدادی غیر منتظره که به ندرت اتفاق می‌افتد، کاری را که از آن درخواست کرده‌ایم به درستی انجام ندهد.

به طور تاریخی، بیشترین و خطرناکترین مشکلات امنیتی سیستمها بر اثر وجود باگهایی که منجر به سرریز شدن بافر می‌گردند، ایجاد می‌شوند. برطرف کردن باگها اولین نیاز یک سیستم عامل امن می‌باشد.

سیستم عاملهای خانواده BSD در مقایسه با سیستم عاملهای دیگر کوچک و ساده هستند. این بدین معناست که این سیستم عامل ها کد کمتری برای وجود باگ دارند. یک ویژگی کلیدی که سیستم عامل OpenBSD را از سایرین جدا می‌کند، بررسی دقیق و دوره‌ای کد این سیستم عامل است. برای این منظور یک تیم شش تا دوازده نفره وجود دارد که کد سورس سیستم عامل را به دقت و فایل به فایل و خط به خط بررسی می‌کنند و به دنبال باگها و حفره‌های امنیتی آن می‌گردند. آنها این کار را از تابستان 1996 آغاز کرده‌اند و در اواخر سال 1996 و اویل سال 1997 هزاران باگ را شناسایی و برطرف کردند.

کار بررسی کد سیستم عامل هر سال بطور منظم انجام می‌شود. و هر شش ماه یکبار نسخه‌های جدید سیستم عامل با قابلیتهای جدید منتشر می‌شوند.

## امنیت با نصب پیش فرض (Secure by default)

چنانچه گفتیم، سیستم عامل OpenBSD چنانچه با انتخاب گزینه‌های پیش فرض نصب شود، کاملا امن است. برای این منظور سیستم عامل OpenBSD در مقایسه با سایر سیستم عامل ها، کمترین تعداد سرویس را بطور پیش فرض فعال می‌سازد. و همه سرویسهای غیر ضروری را غیر فعال می‌سازد.

برای سیستم عاملهایی که می‌خواهند راحت توسط کاربر قابل استفاده باشند، نظیر اکثر سیستم عاملهای تجاری، ایمنی بطور پیش فرض (secure by default) می‌تواند مشکل‌ساز باشد. چون برای رسیدن به secure by default باید اکثر سرویسها را در نصب default غیر فعال کرد و کاربر برای استفاده از این سرویسها مجبور است خود یاد بگیرد که چگونه سرویس را راه اندازی کند و این مساله راحتی استفاده از سیستم عامل را کاهش می‌دهد.

یکی از فرضها و امیدهای سیستمهای secure by default این است که در مورد سرویسهایی که بطور پیش فرض فعال نیستند، مردم ابتدا باید اطلاعاتی را بیاموزند و سپس از آن سرویس استفاده کنند. حداقل اطلاعاتی که کاربر در رابطه با این سرویس یاد می‌گیرد این است که اولا چنین سرویسی در سیستم وجود دارد. ثانیا علاقه‌مند است که این سرویس را فعال سازد و از آن استفاده کند. و ثالثا اینکه باید یاد بگیرد که چگونه سرویس را راه‌اندازی کند.

در سیستمهایی که secure by default نیستند، بسیاری از سرویسهایی که بطور پیش فرض فعال هستند سرویسهای کم استفاده‌ای هستند که کاربر و یا حتی Administrator ممکن است تا مدتها از وجود چنین سرویسی بر روی سیستم غافل باشد. و لذا هرگز اقدام به بروز رسانی این سرویسها نکند که همین مساله می‌تواند باعث شود که باگی که در یکی از این سرویسها وجود دارد، تا مدتها پنهان باقی بماند و در امنیت سیستم اختلال ایجاد کند.

## بررسی امنیت بطور روزانه در OpenBSD

سیستم عاملهای خانواده BSD و از جمله OpenBSD دارای قابلیتی هستند که کمتر سیستم عامل دیگری چنین قابلیتی را دارا می‌باشد. این قابلیت، بررسی مسائل امنیتی بطور روزانه می‌باشد که بطور پیش فرض در سیستم فعال می‌باشد. این سرویس هر شب بطور خودکار فعال می‌شود و یک email به root می‌فرستد که در آن همه مسائل امنیتی و همه تنظیمات مرتبط با آن در سیستم تحلیل و بررسی می‌شود. اگر یک فایل سیستمی تغییر کرده باشد و یا اجازه دستیابی به یک فایل یا فهرست کلیدی تغییر کرده باشد، یا یک برنامه سیستمی اضافه شده باشد و یا تغییر کرده باشد، و خلاصه اینکه اگر هر مساله‌ای که می‌تواند امنیت سیستم را به خطر بیاندازد بوجود آمده باشد، این email بطور خودکار به root فرستاده می‌شود و تغییرات را گزارش می‌دهد.

این قابلیت بطور پیش فرض فعال است ولی administrator می‌تواند آنرا غیر فعال سازد. که البته غیر فعال کردن این سرویس توصیه نمی‌شود.

## ▪ لینوکس

OpenBSD بـه عنـوان یـک سیسـتم عامـل خیلـی امـن شـناخته شـده اسـت. در حالیکـه Windows NT و Windows 2000 در نصب default از نظر امنیتی در سطح پایینی قرار دارند. در این بین سیستم عامل لینوکس در حد وسط قرار دارد. یعنی نصب default آن به مراتب امن‌تر از Windows NT و Windows 2000 است ولی امنیت آن از OpenBSD کمتر است.

البته لینوکس دارای شکلهای مختلفی است که به هر کدام از آنها یک توزیع می‌گوییم. توزیعهای مختلف لینوکس از نظر امنیت در نصب default ، با یکدیگر بسیار متفاوت هستند و در سطوح مختلفی قرار می‌گیرند.

در یک سو محصولی مانند Corel Linux قرار دارد که مسائل امنیتی در آن کاملا غیر فعـال و مـرده اسـت. ایـن سیستم عامل برای حساب کاربران و حتی برای حساب ریشه، password نمی‌گیرد. و در آن هیچ انتخـابی بـرای اینکه password وارد کنیم و یا هیچ دستو العملی که بواسطه آن بعدا بتوانیم سیستم password را فعال سازیم، وجود ندارد. این سیستم عامل هیچ فایلی برای نگهداری password هـا نـدارد. همچنـین در ایـن سیسـتم هـیچ سرویسی برای اتصال به شبکه پیش بینی نشده است و بنابراین دسـتگاهی کـه ایـن سیسـتم عامـل روی آن نصـب می‌شود، تنها بطور محلی قابل استفاده است.

از سوی دیگر توزیعهای دیگری از لینوکس نظیر Trustix و EnGarde وجود دارند کـه از قبـل بـرای امنیـت سفارشی شده‌اند و همانند OpenBSD و حتی بیش از آن، در نصـب default ، بیشـتر سرویسـها را غیـر فعـال می‌کنند و یا اینکه اصلا آنها را نصب نمی‌کنند. و به همین جهت نصب آنها با گزینه‌های پیش فرض امن است.

امروزه پر استفاده ترین توزیع سیستم عامل لینوکس ، توزیع Red Hat می‌باشد. و در این مقایسه منظور اصلی مـا از سیستم عامل لینوکس در واقع همین توزیع Red Hat می‌باشد. در نصب این سیستم عامل با انتخاب گزینه‌های پیش فرض، سرویسهای امنیتی نسبتا کمی نصب می‌شود و البته علاوه بر آن برای حسـاب کـاربر و حسـاب ریشـه password انتخاب می‌شود. و چنانچه گفتیم این نسخه از لینوکس به لحاظ امنیتی مابین OpenBSD و خـانواده ویندوز قرار می‌گیرد.

اجازه دستیابی به سیستم فایلها و فهرستها در لینوکس مانند اکثر سیستم عاملهای معاصر مبتنی بر UNIX است. که البته این سیستم منطقی و قابل قبول است ولی کافی نیست. مثلا اینکه اجازه خواندن از سیستم فایلها بـه همـه داده می‌شود. هر چند بعضی از برنامه‌ها برای کارکرد صحیح احتیاج به وجود چنین اجازه‌ای از سوی سیستم دارند، ولی در هر صورت وجود چنین سطح اجازه‌ای در سیستم الزامی و ضروری نیست. وجود این مطلب به حمله کننـدگان به سیستم، این اجازه را می‌دهد که کمی میزان دستیابیشان به سیستم افزایش یابـد. و بخصـوص کسـانیکه دسـتیابی محدودتری به سیستم دارند می‌توانند تا حدی سطح دستیابی خود را بالاتر ببرند. بنابراین لازم است کـه بعضـی از فایلها تنها توسط ریشه قابل خواندن باشند، تا شخص حمله کننده برای خواندن آنها و کشف محتویات آن مجبـور باشد که ابتدا به حساب ریشه دستیابی پیدا کند.

یک گام برای افزایش ایمنی سیستم عامل لینوکس آن است که سرویسهای اضافی آن که بدون استفاده هستند و با به وجود آنها فعلا نیازی نداریم را غیر فعال سازیم. با این کار علاوه بر اینکه شـانس وجـود بـاگ در سیسـتم را کـم کرده‌ایم، می‌توانیم تعداد پورتهای باز را کاهش دهیم و بنابراین خطر حمله از طریق این پورتها کاهش می‌یابـد. در سیستم عاملهای مبتنی بر UNIX غیر فعال کردن یک سرویس به راحتی امکان پذیر است چراکه بطور معمول یک فایل اجرایی به ازای یک سرویس در سیستم وجود دارد و معمولا هر سرویس تنها به یک پورت گوش می‌دهد.

در نقطه مقابل در سیستم ویندوز حذف یک سرویس به راحتی امکان پذیر نیست. مثلا سرویسهایی مانند NetBIOS بیشتر شبیه به یک مجموعه سرویسهای مرتبط با هم هستند. بخشی از یک سرویس ممکن است در چندین فایل اجرایی نوشته شده باشد و یا اینکه یک فایل شامل اجزایی از چندین سرویس باشد. توابع مختلفی که در ارتباط با سرویس NetBIOS کار می‌کنند، از پورتهای 135 تا 139 و همچنین از UDP و TCP استفاده می‌کنند.

نتیجه اینکه در همه سیستم عاملهای مبتنی بر UNIX به راحتی می‌توان سرویس NFS را غیر فعال کرد، بدون آنکه اثری روی سایر توابع سیستم بگذارد. ولی در سیستم عامل Windows NT و Windows 2000 اگرچه می‌توان سرویس مربوط به اشتراک دیسک در سیستم را غیر فعال کرد، ولی هیچ راهی وجود ندارد که سیستم به اشتراک گذاری دیسک را غیر فعال کنیم، بدون آنکه سیستم به اشتراک گذاری پرینتر و یا سایر سرویسهای مرتبط با NetBIOS در سیستم غیر فعال شود.

سیستم طراحی گیج کننده‌ای که در ویندوز پیاده شده است، در بخشهای دیگر سیستم مانند طراحی ساختار فهرستها و در طراحی registry نیز به چشم می‌خورد. و این مساله باعث شده است که ویندوز یک سیستم عامل نا امن به حساب بیاید. و سیستم عامل ویندوز را نمی‌توان با کم کردن تعداد سرویسهای فعال امن کرد. چون هر سرویسی را که بخواهیم حذف کنیم، این خطر وجود دارد که توابع دیگری در سیستم موجود باشند که به آن سرویسها نیاز داشته باشند و با حذف آنها، در کارشان اختلال ایجاد شود.

## نتیجه‌گیری از نصب default

سیستم عامل OpenBSD پس از نصب با انتخاب گزینه‌های پیش فرض به مراتب امن تر از نصب default سیستم عامل ویندوز است. و البته به همین میزان کارایی آن کمتر است. چون بسیاری از توابع و سرویسهای آن غیر فعال هستند و یا اساسا نصب نشده‌اند. در این مقایسه سیستم عامل لینوکس هم از نظر امنیت و هم از نظر کارایی (که نقطه مقابل آن است) در حد وسط OpenBSD و ویندوز قرار می‌گیرد.

البته اگر نصب firewall را نیز به حساب بیاوریم، باید بگوییم که چنانچه در هنگام نصب سیستم عامل لینوکس (Red Hat 7.1) گزینه پیش فرض را در مورد نصب firewall انتخاب نکنیم و در عوض بیشترین میزان امنیت را در لایه firewall انتخاب کنیم، آنگاه سیستم بدست آمده به لحاظ امنیت حتی از جهاتی بهتر از OpenBSD (در حالت نصب default) می‌باشد.

در مجموع سیستم عامل OpenBSD از توزیعهای استاندارد لینوکس امن‌تر است. پس از نصب default هر دوی این سیستم عاملها می‌توان با انجام یکسری اقدامات امنیتی روشن و مشخص، با گامهای مشابه و نسبتا استانداردی، این سیستمها را به سطح امنیتی بسیار بالایی رساند.

اما برای آنکه سیستم عامل ویندوز را بتوانیم به سطح امنیتی بالایی برسانیم کار چندان ساده نیست. باید کارهای نسبتا زیادی انجام دهیم تا بتوانیم آنرا به اندازه نصب default سیستم عامل لینوکس امن سازیم و چنانچه بخواهیم آنرا به اندازه نصب default سیستم عامل OpenBSD امن سازیم، باز هم باید تنظیمات امنیتی بیشتری را روی آن اعمال کنیم.

بزرگترین تفاوت سیستمهای OpenBSD و لینوکس در تعداد باگهای آنهاست. سیستم لینوکس به مراتب باگهای بیشتری نسبت به OpenBSD دارد و بنابراین از نظر امنیتی در سطح پایین‌تری قرار دارد. سیستم عامل ویندوز

نسبت به هر دو سیستم عامل لینوکس و OpenBSD باگهای بیشتر و امنیت کمتری دارد. و به نظر نمی‌رسد که سیستم عامل ویندوز هرگز بتواند به لحاظ امنیتی با OpenBSD قابل قیاس گردد.

## ▪ مقایسه امنیت ذاتی

سوالی که گاهی اوقات پرسیده می‌شود این است که تفاوت سیستم عاملها از نظر امنیت ذاتی به چه صورت است. ما قبلا اشاره کردیم که سیستم اجازه دستیابی به فایلها و فهرستها در ویندوز بسیار پیچیده است. که البته این سیستم پس از نصب default خاموش است و به ندرت ممکن است که استفاده از آن مفید واقع شود.

یعضی علما سعی کرده‌اند که سیستم عاملهای ویندوز و لینوکس را ارزیابی کنند و آنها را از نظر امکانات ذاتی با هم مقایسه کنند. نتیجه این مقایسات و بررسیها این بوده است که این سیستم عاملها تفاوتهای زیادی با هم دارند و در زمینه‌های مختلف هر یک مزایا و معایبی نسبت به دیگری دارند. اما در حالت کلی نمی‌توان یکی از این سیستم عاملها را بطور کلی نسبت به دیگری برتری داد.

به نظر من در مقایسه امنیت ذاتی این دو سیستم عامل یک ایراد بزرگ وجود دارد. سوال کردن در مورد امنیت ذاتی ویندوز و لینوکس، مثل این است که بخواهیم سیستم عاملها را در یک دنیای فرضی با هم مقایسه کنیم که در آن همه administrator ها به خوبی آموزش دیده‌اند و همگی وقت کافی برای انجام کارهای لازم را دارند. اما در دنیای واقعی، این طور نیست و چنین شرایطی وجود ندارد. بنابراین این پرسش نمی‌تواند جواب روشن و مشخصی داشته باشد و اگر هم جوابی داشته باشد، آن جواب ارزش عملی نخواهد داشت. چراکه عملا اکثر administrator ها سواد و اطلاعات کافی در مورد کارشان ندارند و علاوه بر آن administrator های سیستمهای ویندوز معمولا کم سوادتر و نا آگاه تر از administrator های سیستم عاملهای لینوکس هستند. همچنین تقریبا همه administrator ها وقت کافی برای انجام کارهای خود ندارند و از بابت زمان همگی شدیدا در محدودیت هستند.

## ویندوز یک سیستم عامل امن نیست

یکی از ویژگیهای اصلی مایکروسافت این است که آنها محصولاتشان را در قالب محیط های مجتمع پیچیده‌ای که قابلیتهای زیادی دارند و شدیدا به هم وابسته هستند، تولید می‌کنند. برای آنکه این محصولات خوب کار کنند و حداکثر توانمندیهای خود را در اختیار کاربر قرار دهند، باید روی ماشینی که نصب شده‌اند، یک مجموعه سرویسهایی از قبل اجرا شده باشد. در واقع این مجموعه سرویسها بستر مناسبی را فراهم می‌کند که به محصولات مختلف اجازه فعالیت می‌دهد.

اگر بخواهیم مراحلی را برای ایمنی بخشیدن به سیستم عامل ویندوز دنبال کنیم، یکی از این مراحل حذف امکان به اشتراک گذاری فایلها و غیر فعال کردن سرویس NetBIOS است. این کار باعث می‌شود که سیستم بسیاری از قابلیتهای خود را (بخصوص از دیدگاه کاربر) از دست بدهد. چون در این صورت هیچ راهی برای به اشتراک گذاشتن دیسک در شبکه وجود ندارد. در واقع همه مشکل در سیستم های ویندوز این است که کارها شدیدا به هم گره خورده‌اند و نمی‌توان یک سرویس را بدون لطمه زدن به سرویسهای دیگر حذف کرد. علاوه بر حذف یک سرویس از سیستم ویندوز که با مشکلاتی همراه است، حتی اضافه کردن سرویس جدید به سیستم ویندوز نیز

خالی از دردسر نیست. زیرا ممکن است بخاطر آن مجبور شوید که سرویسها و توابع دیگری را نیز بر روی سیستم خود نصب کنید.

یک عامل مهم که می‌تواند در تصمیم گیری بین ویندوز و یک سیستم عامل مبتنی بر یونیکس، نقش تعیین کننده‌ای داشته باشد، انتخاب بین کارکرد بالاتر و امنیت بیشتر است. اگر شما می‌خواهید امنیت بیشتری داشته باشید باید به سراغ یک سیستم عامل مبتنی بر یونیکس بروید ولی اگر می‌خواهید سیستمتان کارکرد بالاتری داشته باشد، بهتر است که ویندوز را انتخاب کنید.

دقت کنید که نمی‌توان هر دو نیاز کارکرد بالا و امنیت زیاد را به کمک ویندوز برآورده کرد. این تصور که ابتدا سیستم عامل ویندوز را انتخاب کنیم و سپس به روشهای مختلف آنرا ایمن سازیم تا هر دو هدف ما را تامین کند، صحیح نیست. چون هر چند که می‌توان سیستم عامل ویندوز را به کمک firewall ها ایمن کرد، اما امنیت بخشیدن به ویندوز به قیمت پایین آوردن قابلیتها و تواناییهای آن تمام می‌شود. و در چنین حالتی که ویندوز کارکرد بالای خود را از دست می‌دهد، توصیه می‌شود که یک سیستم عامل مبتنی بر یونیکس را به جای آن انتخاب کنید.

- مدل توسعه، باگها، امنیت و قابلیت اطمینان.

به ترتیب نگاهی به مدلهای توسعه سیستم عاملهای OpenBSD ، لینوکس و ویندوز می‌اندازیم تا بفهمیم که این مطلب چگونه روی قابلیت اطمینان و مسائل مربوط به امنیت اثر می‌گذارد.

## OpenBSD

OpenBSD کوچکترین سیستم است و شاید کوچکترین مدل توسعه را دارا باشد. و در مقایسه با لینوکس و ویندوز تعداد توسعه دهندگان کمتری دارد. توسعه دهندگان OpenBSD در مقایسه با لینوکس از نزدیک با یکدیگر هماهنگ شده‌اند. سیستم عامل OpenBSD یکی از امن‌ترین سیستم عاملهاست. خطوط آغازینی که در صفحه امنیت سایت OpenBSD تحت عنوان هدف آمده است، گویای این مدعاست. این خطوط عبارتند از:

((OpenBSD شدیدا به امنیت معتقد است. آرزوی ما این است که از نظر امنیت در صنعت در رتبه اول باشیم. (البته چنانچه تا کنون به این مرتبه نرسیده باشیم.) مدل توسعه آزاد ما، به ما این اجازه را می‌دهد که دید مصمم‌تری نسبت به افزایش امنیت، نسبت به Sun، SGI، IBM و HP و سایر فروشندگان سیستم‌عامل داشته باشیم. ما می‌توانیم تغییراتی را اعمال کنیم که سایر فروشندگان قادر به انجام آن نیستند. ))

آنها در این خطوط هدفشان را می‌گویند و می‌گویند: ((البته چنانچه تا کنون به این مرتبه نرسیده باشیم.)) و این نشان می‌دهد که آنها تا چه حد به هدف خود نزدیک شده‌اند. آنها ادعا نمی‌کنند که از هر سیستم رقیبی سریعتر هستند و قضاوت در مورد این مساله را به دیگران واگذار می‌کنند که آیا به هدف خود در این راستا دست یافته‌اند یا نه. آنها هر باگی را که پیدا می‌کنند به سرعت برطرف می‌کنند و این مساله آنها را به هدفشان نزدیکتر می‌کند. و چون آنها ادعا نکرده‌اند که امن‌ترین سیستم عامل هستند، پیدا شدن و برطرف کردن باگها، اعتبار قبلی آنها را زیر سوال نمی‌برد و لطمه‌ای در روند پیشرفت امنیت آنها ایجاد نمی‌کند. آنها به خوبی می‌دانند که امنیت مطلق وجود ندارد بلکه امنیت دارای یک روند تکمیلی است و به تدریج کامل می‌شود.

بنابراین آنها به اضافه کردن قابلیتهای جدید و توسعه توابع موجود ادامه می‌دهند و با این کار هر چه بیشتر به هدفشان نزدیک می‌شوند. برطرف کردن مشکلاتی که در سیستم پیدا می‌کنند از نظر آنها بیشترین اولویت را دارد. و جملاتی نظیر ((این مشکل در OpenBSD شش ماه پیش حل شد.)) را می‌توان در جاهایی نظیر BUGTRAQ بارها دید. و این نشان می‌دهد که فرآیند بررسی‌ها و حسابرسی‌های دقیق آنها موثر واقع شده است. از آنجائیکه این یک مساله داخلی است، ما نمی‌توانیم بفهمیم که مشکلاتی که پیش می‌آیند با چه سرعتی حل می‌شوند. ولی از طریق مثالهای خارجی نظیر باگهای مرتبط با IP Filter و Sendmail ما می‌دانیم که پاسخدهی آنها برای حل باگها سریع است. هر دوی این باگها مطالبی را در ارتباط با هر دو سیستم عامل OpenBSD و لینوکس روشن می‌سازند.

یک سیستم عامل هر چند که در حالت مینیمم نصب شود، شامل بسیاری از قسمتهایی می‌باشد که کد آنها توسط تولید کننده‌های دیگر تولید شده است. وقتی شما نرم‌افزارهای GNU و سرویس دهنده‌های TCP/IP را بررسی می‌کنید، می‌بینید که آنها واقعا بخشی از هسته سیستم عامل نیستند. و این ممکن است که بیشتر کد از منابع دیگر آمده باشد. نویسندگان واقعی کد مسوول پاسخگویی به باگهای گزارش شده آن هستند. نویسندگان OpenBSD و لینوکس بسیار علاقه‌مندند که این باگها توسط نویسندگان اصلی کد اصلاح شوند. چرا که با این روش، مشکل دوباره کاری و واگرایی درخت سورس پیش نمی‌آید. محصولی مانند IP Filter که معمولا به عنوان یک ماژول ثابت در کرنل کامپایل می‌شود، ممکن است نیاز به کمی تغییر داشته باشد. نویسندگان OS بطور طبیعی دوست دارند تغییراتشان را تا حد امکان کم کنند تا بتوانند که این محصولات را به همراه سیستم عامل خود عرضه کنند. تصور من این است که نویسندگان اصلی، به طور معمول به خوبی پاسخگو هستند. بسیاری از آنها آبروی حرفه‌ای خود را روی محصولات Open Source ای که تولید کرده‌اند گذاشته‌اند. مدل مجوز Open Source به نویسندگان سیستم عامل این اجازه را می‌دهد که مشکلات محصولات دیگر را در صورتی که نوسندگان اصلی آنها پاسخگو نبودند، خود برطرف کنند.

OpenBSD برخلاف لینوکس و خانواده ویندوز، یک سیستم واحد است که توسط یک گروه واحد تولید شده است و هر شش ماه در ماههای ژوئن و دسامبر به روز می‌شود. و هر نسخه آن دقیقا به موقع منتشر می‌شود. همه نسخه‌هایی که برای سکوهای سخت‌افزاری مختلف تولید می‌شود، در یک زمان و بر روی یک مجموعه CD منتشر می‌شوند. (لازم به ذکر است که تعداد سکوهای سخت افزاری OpenBSD به خاطر ارث‌بری از NetBSD زیاد است.)

OpenBSD یک رهبر قاطع به نام Theo de Raadt دارد و سایت تجاری آن www.OpenBSD.org می‌باشد. بین نسخه‌های مختلفی که release می‌شود، دو شاخه سورس همیشه توسعه می‌یابد و برای download آماده است. همچنین همیشه یک شاخه current وجود دارد که شامل آخرین نسخه‌ای است که جدیدترین تغییرات روی آن اعمال شده است که ناپایدار است و احتمالا دارای باگهای جدید است و همچنین بعضی از قابلیتهای جدیدی که به آن اضافه شده است، هنوز تکمیل نشده است. همچنین شاخه جداگانه‌ای شامل patchها وجود دارد. در این شاخه آخرین نسخه release برنامه که باگهای مهم آن برطرف شده است وجود دارد. یک mailing list برای باگها وجود دارد که شامل گزارش باگها و مسائل مرتبط با آنها می‌باشد. و همچنین یک mailing list در رابطه با امنیت و مسائل امنیتی وجود دارد.

برای محصولاتی که به عنوان بخشی از OpenBSD ارائه می‌شوند، mailing list امنیت، تنها منبع اطلاعات امنیتی است که به آن نیاز دارید. به عنوان مثال اگر در یک component که با آن کار می‌کنید، با باگی مواجه شدید، برای پیدا کردن راه حل آن به سایت مربوطه مراجعه کنید و در صورت پیدا نکردن راه حل، آن باگ را گزارش کنید.

## لینوکس

Linus Torvalds کرنل لینوکس اصلی را نوشت. وی "Linux" را به عنوان نشان تجاری ثبت کرد و هنوز هم رهبری لینوکس را بر عهده دارد. برخلاف OpenBSD ، سیستم عامل لینوکس یکتا نیست و توزیعهای مختلفی ازآن وجود دارد. سورس کرنل سیستم عامل که شامل آخرین نسخه آن است در آدرس www.kernel.org نگهداری می‌شود. در home page این سایت چنین آمده است: ((لینوکس از جنس سیستم عامل Unix است که از آغاز توسط Linus Torvalds و تیمی از هکرهای شبکه نوشته شده است. این سیست عامل با هدف اجابت ویژگیهای Unix و POSIX نوشته شده است.))

یک دوجین سایت اینترنتی وجود دارد که به لینوکس اختصاص دارد. که گذشته از سایت مربوط به کرنل سیستم، معلوم نیست که کدامیک از سایتها از بقیه اداری‌تر است. چنین به نظر می‌اید که کرنل سیستم عامل بطور پیوسته از چند جهت تحت توسعه قرار دارد و بطور همزمان بیش از یک نسخه در حال توسعه است. نسخه‌های 2.2.0 تا 2.2.19 بین 25 ژانویه 1999 و 25 مارچ 2001 منتشر شدند. نسخه‌های 2.3.0 تا 2.3.51 و نسخه‌های 2.3.99-pre1 تا 2.3.99-pre9 بین 11 می 1999 و 23 می 2000 منتشر شدند. نسخه‌های 2.4.0 تا 2.4.6 بین 4 ژانویه 2001 تا 3 جولای 2001 منتشر شدند. که همه این نسخه‌ها از کرنل 2.2 استفاده می‌کنند. کرنل 2.3 چندان متداول نشده است و گامی مقدماتی برای توسعه کرنل 2.4 می‌باشد. کرنل 2.4 شامل چندین تغییر اساسی است و بعضی از توزیعهای لینوکس کم کم شروع کرده‌اند که از کرنل 2.4 استفاده کنند.

لینوکس معمولا بصورت توزیعهای مختلف وجود دارد که هر توزیع شامل یک روتین نصب است که کرنل لینوکس را به همراه دارد و علاوه بر آن پاره‌ای ابزارهای استاندارد و هر چیزی که به نظر تولید کننده توزیع لازم بوده است، را شامل می‌باشد. در سایت www.linux.com می‌توانید لینکهایی را ببینید که به سایتهای download شش توزیع معروف لینوکس متصل هستند. این شش توزیع مختلف عبارتند از: Caldera، Debian ، Slackware، TurboLinux، Red Hat و SuSE. Debian و Slackware و TurboLinux به نظر می‌آید که از نسخه‌های اخیر کرنل 2.2 استفاده می‌کنند در حالیکه Cladera و Red Hat و SuSE از کرنلهای 2.4 استفاده می‌کنند. توزیعهای دیگری نیز وجود دارد از جمله Corel و Mandrake. همچنین توزیعهایی وجود دارد که از دگرگونی توزیعهای دیگر بدست آمده‌اند مثل Trustix که نسخه‌ای از توزیع Red Hat است.

EnGarde یک توزیع ایمن از لینوکس است که بر پایه توزیعهای دیگر لینوکس نمی‌باشد. مقایسه دقیق بین این توزیع و سیستم عامل OpenBSD می‌تواند جالب توجه باشد. در حالیکه OpenBSD بصورت انحصاری و بطور پیش فرض telnet، FTP، NFS و خدمات مرتبط با RPC را غیر فعال کرده است، EnGarde همه آنها را کاملا حذف کرده است و کل محتویات CD نصب آن تنها 134MB است. OpenSSH و OpenSSL که توسط تیم OpenBSD تولید شده اند، به عنوان جایگزینی برای telnet و FTP برای انتقال و مدیریت فایل از راه دور بطور ایمن، استفاده می‌شوند. سیستم انتقال استاندارد میل یونیکس به نام Sendmail، که دارای باگهای

تاریخی است، با سیستم ایمن‌تر Postfix تعویض شده است. روند نصب سیستم، این انتخاب را به کاربر می‌دهد که بطور خودکار سرویس دهنده‌های web، mail، DNS، IMAP و POP را فعال کند ولی بطور پیش فرض همه آنها خاموش هستند. IMAP و POP و همچنین httpd بطور خودکار با SSL تنظیم می‌شوند. رابط مدیریت وب SSL به نحوی قرار گرفته است که سرور می‌تواند راه‌اندازی و اجرا شود بدون آنکه صفحه کلید یا مانیتور متصل شده داشته باشد.

هیچ انتخابی برای آنکه EnGarde را به عنوان workstation نصب کنید وجود ندارد و به سختی می‌توان آنرا روی تنها یک ماشین نصب کرد. این سیستم عامل شامل سیستم intrusion detection هم مبتنی بر host و هم مبتنی بر شبکه می‌باشد. از بعضی جهات امنیت EnGarde فراتر از OpenBSD رفته است ولی EnGarde یک سیستم عامل همه منظوره به حساب نمی‌آید.

تنظیماتی که سیستم عامل EnGarde بطور default انجام می‌دهد، حتی از OpenBSD بهتر است ولی در عوض کد سیستم عامل OpenBSD با کیفیت بالاتری تولید شده است. برای آنکه یک سیستم خوب و مطمئن درست کنیم می‌توانیم سیستم عامل OpenBSD را نصب کنیم، سپس تنظیمات سیستم عامل EnGarde را روی آن اعمال کنیم. بدین معنی که هر سرویسی که OpenBSD آنرا فعال می‌کند و EnGarde آنرا غیر فعال می‌کند، غیر فعال بکنیم و نیز هر سرویسی که OpenBSD آنرا شامل می‌شود ولی EnGarde آنرا شامل نمی‌شود، حذف کنیم.

بر خلاف OpenBSD که بصورت یک پروژه واحد تولید می‌شود، کرنل لینوکس و برنامه‌های آن در پروژه‌های جداگانه‌ای تولید می‌شوند.

توسعه کرنل لینوکس اساسا یک کار داوطلبانه و غیر تجاری است. بعضی از توزیعهای لینوکس تجاری نیستند ولی بعضی دیگر نظیر Caldera و Red Hat و Turbo Linux تجاری هستند و با ارائه سیستم عامل خود، از فروش سرویسهای پشتیبانی همراه، و نیز با گرفتن هزینه رسانه و هزینه ثبت مشتری، سود می‌برند.

همه توزیعهای لینوکس در حال حاضر یک نسخه از سیستم عامل خود را روی اینترنت قرار داده‌اند که به رایگان قابل download است ولی معمولا هزینه خرید CD های آن، از هزینه download نیز کمتر است.

## ویندوز و مایکروسافت

برخلاف OpenBSD و لینوکس که اساسا تجاری نیستند، مایکروسافت بزرگترین شرکت تولید کننده نرم افزار در جهان است و صد در صد تجاری است. بعید است که مایکروسافت کاری را انجام دهد بدون آنکه کوچکترین اثرات آنرا در نظر گرفته باشد. حتی کمکهای بشر دوستانه‌ای هم که این شرکت انجام می‌دهد، صرفا در راستای موفقیت در بازار تجاری با بدست آوردن یک چهره خوب در نزد مردم است.

برخلاف OpenBSD که کمتر از خودش تعریف می‌کند و بیشتر سکوت می‌کند، مایکروسافت مرتبا به تعریف و تمجید از محصولات خود می‌پردازد. مایکروسافت با ستیزه جویی سعی در فروش محصولاتش دارد و از ادعاهایی که در مورد مزایای محصولاتش می‌کند، خجالت نمی‌کشد. از جمله ادعاهایی نظیر: امنیت، قابلیت اطمینان، کنترل کامل روی نصب سیستم در مقیاس بزرگ و ... که در مجموع ادعاهایی بی اساسند.

مایکروسافت ادعا می‌کند که سیستمهایش ایمن هستند که این ادعا چیزی بیش از یک شعار تبلیغاتی نمی‌باشد. حتی پس از آنکه صدها و بلکه هزاران باگ مرتبط با امنیت در Windows NT پیدا شد، باز هم مایکروسافت دست از ادعای خود برنداشته است.

مردم عادی و حتی بسیاری از صنایع کامپیوتری درک کمی نسبت به مساله امنیت دارند. بیشتر مردم دوست دارند این طور فکر کنند که امنیت حالتی است که می‌توان بطور مطلق به آن رسید و پس از رسیدن به امنیت می‌توان همه چیز را فراموش کرد. کمتر کسانی خود را برای این باور صحیح آماده کرده‌اند که امنیت یک پروسه در حال حرکت است که به تدریج کامل می‌شود و همواره نسبی است و برای همراه بودن با آن به کار و تلاش مداوم نیاز است. مایکروسافت در شکل‌گیری طرز فکر غلط اکثریت مردم، نقش بسزایی داشته است. این شرکت به مردم به دید خریدار نگاه می‌کند و به آنها می‌گوید که محصولات مایکروسافت را بخرند تا به امنیت برسند.

وقتی سیستمی که ویندوز روی آن نصب شده است مورد حمله و آسیب واقع می‌شود، بعضی از صاحبان این سیستمها خود را مقصر می‌دانند در حالیکه مقصر اصلی خود مایکروسافت است که به مشتریانش چنین تلقین کرده است که سیستم آنها مطلقا ایمن است.

## ▪ نتیجه گیری

سیستم عامل OpenBSD به عنوان یکی از پیشگامان امنیت در بین سیستم عاملهای همه منظوره شناخته شده است. این سیستم عامل بطور قابل ملاحظه‌ای امن‌تر از توزیعهای استاندارد لینوکس است. توزیعهای استاندارد لینوکس، لیست نسبتا بزرگی از باگهای مرتبط با امنیت را با خود به همراه دارند. هر چند که این باگها به سرعت برطرف می‌شوند، ولی بیشتر کاربران سیستمهای خود را به سرعت به روز در نمی‌آورند.

چه در OpenBSD و چه در لینوکس، به خاطر ساختار ماژولار و مستقل سرویسها و به خاطر اینکه هر سرویس تنها از یک یا دو پورت بطور معمول استفاده می‌کند، حذف و اضافه کردن سرویسها آسان است و بنابراین احتمال لطمه خوردن به سیستم کم است و لذا امنیت سیستم زیاد است.

هر چند که OpenBSD از اکثر نسخه‌های لینوکس امن‌تر است، ولی در عوض برنامه‌های کاربردی کمتری را پشتیبانی می‌کند. در هر حال در جائیکه مسائل امنیتی و مسائل مربوط به firewall ها، proxy ها، رمزنگاری و VPN بیشترین اهمیت را دارد، OpenBSD انتخاب اول است.

سیستم عامل‌های خانواده ویندوز اگرچه می‌توانند از سرویسهای امنیتی زیادی بهره ببرند، ولی نصب ویندوز با انتخاب گزینه‌های پیش فرض از نظر امنیتی وحشتناک است و سیستم به هیچ وجه امن و قابل اطمینان نیست. بعضی از ماشینهای ویندوز هیچ وقت امن نمی‌شوند و همیشه طعمه‌های خوبی برای حمله‌کنندگان به حساب می‌آیند. همه روزه باگهای جدیدی در سیستم عامل ویندوز پیدا می‌شود. حتی در نسخه‌های قدمی این سیستم عامل هم هنوز باگهایی آشکار می‌شود.

سرورهای ویندوز بدون هیچ شک و تردیدی حتما باید بوسیله firewall های خارجی حفاظت شوند. حتی با وجود حفاظت خارجی باز هم باگهای زیادی در این سیستم عامل وجود دارد که باعث می‌شود که حمله کنندگان بتوانند از بیرون شبکه به درون آن راه یابند و لطماتی را به سیستمها وارد آورند که firewall ها هم نمی‌توانند جلوی این لطمه‌ها را بگیرند.

در مقایسه با لینوکس و بخصوص در مقایسه با سیستم عامل OpenBSD ، ویندوز در اتصال به اینترنت از امنیت کمی برخوردار است. بطوریکه امروزه بعضی شرکتهای بیمه مبلغ بیشتری را برای بیمه کـردن سیسـتمهای وینـدوز نسبت به سیستمهای مبتنی بر یونیکس می‌گیرند.