آسیا
ICT

پای مصنوعی هوشمند به کمک بیماران سکته مغزی می‌آید

منبع: AERZTE ZEITUNG

ترجمه: سعید اکبریان

مهندسان دانشگاه تکنولوژی برلین موفق به ساخت یک پای مصنوعی هوشمند شدند که در آینده بیمارانی را که در اثر سکته‌های مغزی قادر به تکان دادن پاهای خود نیستند، یاری خواهد داد.

این پای مصنوعی هوشمند قادر به پیش‌بینی حرکت‌های پای بیمار است، به‌طوری که همانند پای طبیعی دستورات مغز به سلول‌های عصبی پا را توسط کامپیوتری شناسایی کرده و به دستورات آن به درستی عمل می‌کند.

«کریستیان فلایشر» (Christian Fleischer) مسوول انستیتو تکنولوژی انفورماتیک و میکروالکترونیک آلمان در مورد این گونه پاهای مصنوعی هوشمند می‌گوید: به کمک چندین سنسور که در پوست کشاله‌ران بیمار کار گذاشته می‌شود، سیگنال‌های الکتریکی قسمت فوقانی عضلات پای بیمار رجیستر می‌شود و به کامپیوتر کوچکی که بیمار همواره با خود حمل می‌کند، هدایت می‌شود.

معمولاً هر حرکت بیمار باعث تحریک قسمتی خاص از عضلات پای بیمار خواهد شد و موجب می‌شود و آن عضله بیشتر فعال شود و تغییرات سیگنالی که سنسورها در پای بیمار ایجاد می‌کنند باعث به حرکت در آوردن موتورهای الکتریکی می‌شوند و در نتیجه پای مصنوعی قادر به حرکت خواهد شد.

طبق اعلام مهندسان سازنده، این پای مصنوعی هوشمند زمانی خواهد توانست به وظایف خود عمل کند، که سلول‌های عصبی عضلات پای بیمار در اثر سکته و یا ضربه‌های مغزی صدمه ندیده باشند. طبق گفته‌های «کریستیان فلایشر» متاسفانه پای هوشمند برای بیمارانی که فلج کامل و یا سلول‌های عصبی آنها از بین رفته‌اند کاربردی نخواهد داشت.

وی امیدوار است: حداکثر تا شش ماه آینده این ایده جدید تست نهایی خود را به کمک تولیدکنندگان ابزار پزشکی و فیزیوتراپی به انجام برساند و در خط تولید قرار بگیرد.

در صورتی که تمام مراحل آزمایش پای مصنوعی هوشمند با موفقیت به پایان برسد، در آینده دوران معالجه بیماران سکته مغزی که دچار مشکلات حرکت پا شده‌اند، به‌شدت کاهش خواهد یافت.

مهندسان دانشگاه تکنولوژی برلین در نظر دارند: پس از پایان پروژه پای مصنوعی هوشمند، بازوی مصنوعی هوشمند را نیز طراحی کنند و به بیمارانی را که از محدودیت‌های حرکت دست و بازوی خود رنج می‌برند، کمک کنند.

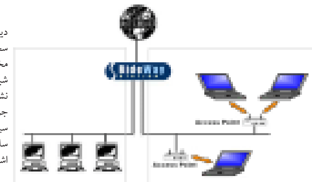
یکی از اعضای این تیم به نام «اندراس وگه» (Andreas Wege) از هم اکنون اقدام به طراحی یک نوع دستکش کرده است که شمایل آن بی‌شباهت به یک دستکش معمولی نیست که توانایی حرکت انگشتان دست را به راحتی دارد.

این دستکش هوشمند نه تنها برای کسانی که دچار سکته مغزی شده‌اند مناسب است، بلکه برای کسانی که بر اثر زخمی شدن شدید انگشتان خود قادر به حرکت آنها نیستند، نیز مناسب خواهد بود.

حرکت عضلات پا و یا دست‌ها باعث تقویت آنها خواهد شد، یکی از وظایف مهم پاها و دست‌های مصنوعی هوشمند در آینده نیز کمک به این امر خواهد بود.

آشنایی با استانداردهای امنیت شبکه‌های محلی بی سیم

مهندس امیر عباس سپهربند



در این قسمت بررسی روش‌ها و استانداردهای امن‌سازی شبکه‌های محلی بی‌سیم مبتنی بر استاندارد IEEE ۸۰۲/۱ را آغاز می‌کنیم. با طرح قابلیت‌های امنیتی این استاندارد می‌توان از محدودیت‌های آن آگاه شد و این استاندارد را برای موارد خاص و مناسب مورد استفاده قرار داد. استاندارد ۸۰۲/۱۱ سرویس‌های مجزا و مشخصی را برای تأمین یک محیط امن بی‌سیم در اختیار قرار می‌دهد. این سرویس‌ها اغلب توسط پروتکل Wired Equivalent Privacy (WEP) تأمین می‌گردند و وظیفه آنها امن‌سازی ارتباط میان مخدوم‌ها و نقاط دسترسی بی‌سیم است. درک لایه‌ای که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌ای دارد، به‌عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه‌های دیگر، غیر از لایه ارتباطی بی‌سیم که مبتنی بر استاندارد ۸۰۲/۱۱ است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه بی‌سیم به‌معنی استفاده از قابلیت درونی استاندارد شبکه‌های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.

قابلیت‌ها و ابعاد امنیتی ۸۰۲/۱۱

در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌های بی‌سیم بر اساس استاندارد ۸۰۲/۱۱ می‌کند WEP است. این پروتکل با وجود قابلیت‌هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه‌های بی‌سیم را به‌نحوی، ولو سخت و پیچیده، فراهم می‌کند. نکته‌ای که باید به خاطر داشت اینست که اغلب حملات موفق صورت گرفته در مورد شبکه‌های محلی بی‌سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به‌عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می‌گذارد، هرچند که فی‌النفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه‌های بی‌سیم انجام می‌گیرد از سویی است که نقاط دسترسی با شبکه سیمی دارای اشتراک هستند. به‌عبارت دیگر نفوذگران بعضاً با استفاده از راه‌های ارتباطی دیگری که روی مخدوم‌ها و سخت‌افزارهای بی‌سیم، خصوصاً مخدوم‌های بی‌سیم، وجود دارد، به شبکه بی‌سیم نفوذ می‌کنند که این مقوله نشان دهنده اشتراکی هرچند جزیی‌ای میان امنیت در شبکه‌های سیمی و بی‌سیم است که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه‌های محلی بی‌سیم تعریف می‌شود:

" Authentication
" Confidentiality
" Integrity

Authentication

هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی‌سیم است. این عمل که در واقع کنترل دسترسی به شبکه بی‌سیم است. این مکانیزم سعی دارد که امکان اتصال مخدوم‌هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

Confidentiality

محرمانگی هدف دیگر WEP است. این بعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه‌های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال روی شبکه محلی بی‌سیم است.

Integrity

هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه خصوصاً میان مخدوم‌های بی‌سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها بسترها و شبکه‌های ارتباطاتی دیگر نیز کم و بیش وجود دارد.

خدمات ایستگاهی

بر اساس این استاندارد خدمات خاصی در ایستگاه‌های کاری پیاده‌سازی می‌شوند. در حقیقت تمام ایستگاه‌های کاری موجود در یک شبکه محلی مبتنی بر ۸۰۲/۱۱ نقاط دسترسی موظف هستند که خدمات ایستگاهی را فراهم کنند. با توجه به اینکه امنیت فیزیکی به‌منظور جلوگیری از دسترسی غیر مجاز بر خلاف شبکه‌های سیمی، در شبکه‌های بی‌سیم قابل اعمال نیست استاندارد ۸۰۲/۱۱ خدمات هویت‌سنجی را به‌منظور کنترل دسترسی به شبکه تعریف می‌کند. سرویس هویت‌سنجی به ایستگاه کاری امکان می‌دهد که ایستگاه دیگری را شناسایی کند. قبل از اثبات هویت ایستگاه کاری، آن ایستگاه مجاز نیست که از شبکه بی‌سیم برای تبادل داده استفاده کند. در یک تقسیم‌بندی کلی ۸۰۲/۱۱ دو گونه خدمت هویت‌سنجی را تعریف می‌کند:

- Open System Authentication
- Shared Key Authentication

روش اول، متد پیش فرض است و یک فرآیند دو مرحله‌ای است. در ابتدا ایستگاهی که می‌خواهد توسط ایستگاه دیگر شناسایی و هویت‌سنجی شود یک فریم مدیریتی هویت‌سنجی شامل شناسه ایستگاه فرستنده، ارسال می‌کند. ایستگاه گیرنده نیز فریمی در پاسخ می‌فرستد که آیا فرستنده را می‌شناسد یا خیر. روش دوم کمی پیچیده‌تر است و فرض می‌کند که هر ایستگاه از طریق یک کانال مستقل و امن، یک کلید مشترک سری دریافت کرده است. ایستگاه‌های کاری با استفاده از این کلید مشترک و با بهره‌گیری از پروتکلی موسوم به WEP اقدام به هویت‌سنجی یکدیگر می‌کنند. یکی دیگر از خدمات ایستگاهی خاتمه ارتباط یا خاتمه هویت‌سنجی است. با استفاده از این خدمات دسترسی ایستگاهی که سابقاً مجاز به استفاده از شبکه بوده است، قطع می‌شود.

در یک شبکه بی‌سیم، تمام ایستگاه‌های کاری و سایر تجهیزات قادر هستند ترافیک داده‌ای را "بشنوند" - در واقع ترافیک در بستر امواج مبادله می‌شود که توسط تمام ایستگاه‌های کاری قابل دریافت است. این ویژگی سطح امنیتی یک ارتباط بی‌سیم را تحت تأثیر قرار می‌دهد. به‌همین دلیل در استاندارد ۸۰۲/۱۱ پروتکلی موسوم به WEP تعبیه شده است که روی تمام فریم‌های داده و برخی فریم‌های مدیریتی و هویت‌سنجی اعمال می‌شود. این استاندارد در پی آن است تا با استفاده از این الگوریتم سطح اختفا و پوشش را معادل با شبکه‌های سیمی کند.

نکته‌های در تجارت الکترونیک

داریوش بلادی

چه نکاتی را به هنگام خرید Online باید به خاطر داشت؟

برای انجام یک خرید مطمئن از طریق اینترنت رعایت برخی نکات بسیار مهم است. در اولین مرحله انتخاب، یک فروشگاه که در مورد آن شناخت داریم یا انجام تحقیقات لازم قبل از خرید می‌تواند به انتخاب درست کمک کند. فروشگاه‌های معتبر عموماً آدرس پستی، تلفن و مشخصات خود را به‌طور دقیق روی وب سایتشان معرفی می‌کنند. بررسی این مشخصات و تطبیق آنها با سایت‌هایی که دارای فهرستی از لیست‌های شکایت علیه سایت‌های اینترنتی (مانند bbb.org) هستند برای درک وضعیت سایت می‌تواند مورد استفاده قرار گیرد. همچنین بررسی گواهی اعتبار سایت که نشان دهنده همکاری فروشگاه با سایت‌های دارای برنامه حفظ امنیت خریداران می‌باشند نیز دارای اهمیت است. بعد از انتخاب فروشگاه مطالعه و بررسی دقیق شرایط و تعهدات اطلاعات لازم در مورد نحوه ارسال کالا، زمان ارسال، قابلیت بازپس فرستادن خرید و نحوه محاسبه پول برگشتی، نحوه تبدیل ارز و هزینه‌های مربوطه به آن نیز ضروری است. حتما آدرس پست الکترونیکی و تلفن واحد پشتیبانی خریدار را داشته باشید. باید دقت شود که آیا خرید از یک فروشگاه و یا شرکت انجام می‌گیرد یا از طریق یک فروشنده و یک سایت حراجی. زیرا حقوق شما در قبال خرید از یک فروشنده شخصی و یا یک شرکت و فروشگاه متفاوت است. در سیستم پرداخت به‌وسیله کارت‌های اعتباری صادر کنندگانی مانند Mastercard & Visa فروشندگان و پذیرندگان این کارت‌های اعتباری را ملزم کرده اند که دارندگان کارت‌ها را از کلیه مسوولیت‌ها در قبال خریدها مبرا سازند. از امنیت سایتی که اطلاعات کارت خود را در آن وارد می‌کنید کاملا مطمئن شوید. برای این منظور می‌توانید به شروع آدرس سایت (URL) دقت کنید چنانچه این آدرس با https:// آغاز شده باشد می‌توانید از امنیت ارسال اطلاعات کارت اعتباریتان مطمئن گردید با این وجود اگر همچنان احساس امنیت در انتقال اطلاعات کارت خود را ندارید از طریق تلفن یا فاکس جهت ارسال آن اقدام کنید. اگر از طریق سایتی که از شما می‌خواهد نام و رمز عبور برای خرید ایجاد کنید از این رمز عبور باید با دقت حفاظت کنید و هرگز آن را در اختیار شخص ثالث قرار ندهید. پس از انجام هر خرید اطلاعات مربوط به خرید و آدرس سایت محل خرید را نگهداری کنید.

اکثر سایت‌ها بعد از انجام معامله یک نامه الکترونیکی که در آن جزییات خرید مانند قیمت، تعداد و ... درج شده به آدرس الکترونیکی شما خواهند فرستاد.

این نامه‌ها را چاپ کرده و نگهداری کنید.

چین سال آینده
مقررات جدیدی برای استفاده از اینترنت اجرا می‌کند

چین از سال آینده میلادی مقررات جدیدی برای استفاده از اینترنت اجرا می‌کند و پلیس این کشور بر فعالیت ارایه‌کنندگان خدمات اینترنتی نظارت خواهد کرد.

وزارت امنیت عمومی چین، اعلام کرد که مقررات جدید استفاده از اینترنت از اول مارس سال آینده میلادی (۱۰ اسفند) در این کشور به اجرا گذاشته خواهد شد.

چین با پایگاه‌های اینترنتی غیراخلاقی، شرط بندی و با برخی از پایگاه‌های دیگر مبارزه می‌کند و محدودیت‌هایی برای استفاده از کاربران اعمال می‌کند.

چین طبق مقررات استفاده از اینترنت، بیش از دو هزار پایگاه غیراخلاقی اینترنتی را در یک سال تعطیل کرده است.

"وو خه پینگ" سخنگوی وزارت امنیت چین روز جمعه به خبرنگاران، گفت مقررات جدید مربوط به جلوگیری از انتشار ویروس‌های رایانه‌ای و پیام‌های اینترنتی غیر اخلاقی و فعالیت‌های ناهنجار از طریق این شبکه است.

مقررات جدید از ارایه‌کنندگان خدمات اینترنتی در چین خواسته است که این موارد را مراعات کرده و از امنیت اینترنت حفاظت کنند، ضمن آنکه پلیس باید بر کار آنها نظارت داشته باشد.

براساس این مقررات که توسط این مقام وزارت امنیت چین تشریح شد، فناوری‌های رایانه‌ها همچون سیستم‌های نظارت بر رایانه‌ها و فناوری‌های اطلاع رسانی و غیره باید به صورت استاندارد مورد استفاده قرار گیرد.

وی تاکید کرد که آزادی افراد نباید به‌واسطه اجرای این مقررات محدود شود و تا زمانی که از اینترنت تحت مقررات استفاده می‌شود، نباید به آزادی و حریم خصوصی کاربران بی احترامی شود.

وزارت امنیت عمومی چین همچنین اعلام کرد از ماه سپتامبر تا نوامبر امسال ۵۹۸، سایت اینترنتی ارایه‌کننده خدمات غیر قانونی و غیر اخلاقی در این کشور را تعطیل کرده است.

بیش از ۸۰، درصد از رایانه‌های چین در سال‌های اخیر به دلیل انتشار ویروس‌های مختلف مختل شده است. چین ۱۰۳، میلیون کاربر اینترنت دارد.

ترفندهای ویندوزی

سید عماد میرکریمی

چگونگی ایجاد پسورد برای محافظت از پوشه‌ها در ویندوز XP

آیا شما به طور مشترک از یک کامپیوتر استفاده می‌کنید و می‌خواهید پوشه هایتان امنیت بیشتری داشته باشند؟

برای ایجاد پسوردی که از پوشه‌ها محافظت می‌کند دو روش وجود دارد.

روش اول: اگر شما برای نام کاربری خود پسورد دارید می‌توانید از این پسورد برای محافظت از پوشه‌های خود استفاده کنید. اما در غیر این صورت روش زیر را دنبال کنید: روی پوشه ای که می‌خواهید محرمانه بماند راست کلیک کرده و گزینه Properties را انتخاب کنید (یا کلیدهای Alt و دابل کلیک را به طور همزمان فشار دهید.) سپس روی کلید sharing کلید کرده و گزینه (Make this folder private) را تیک دار کنید.

و در آخر کلید Apply را بزنید. اگر شما برای نام کاربری خود پسوردی نداشته باشید، کاردی ظاهر می‌شود که از شما سوال می‌کند آیا می‌خواهید پسوردی بسازید؟

اگر می‌خواهید پوشه را محرمانه کنید باید حتما این کار را انجام دهید بنابراین روی گزینه yes کلیک کنید. از این پس برای ورود به دسک تاپ کامپیوتر و استفاده از آن باید از پسوردتان استفاده کنید.

پس از کلیک گزینه yes باید پسورد خود را تایپ کنید و سپس آنها را تصدیق کنید. سپس روی دکمه (create password) کلیک کنید و در آخر پنجره پسورد را ببندید.

در آخر کلید ok پنجره propertiest را بزنید. اکنون هر کسی که وارد سیستم شما شود نمی‌تواند بدون اطلاع از پسورد شما به آن فایل دسترسی پیدا کنید.

معرفی نرم افزار

FlashDWG - DWGtoFlashConverter

این نرم افزار نیز به شما امکان تبدیل فرمت‌ها DWG را به فرمت Flash یا همان SWF می‌دهد. بنا براین در محیطی متفاوت طرح‌های خود را می‌توانید به عرضه گذارید.

DWGSee: دیگر برای مشاهده فایل‌های DWG نیازی به بازکردن نرم افزار سنگین AutoCad نیست به آسانی و سرعت با این نرم افزار ACDSee مانند به مدیریت، نمایش و چاپ انواع فرمت‌های DWG, DXF و DWf نرم افزار AutoCad بپردازید.

تمامی این نرم افزارها با فرمت‌های ساخته شده توسط AutoCad 14 تا ۲۰۰۶ سازگاری دارند.

لینک دانلود محصولات شرکت AutoDWG:

DWG to Image Converter 2.9.522 Download AutoDWG

AutoDWG DWG2PDF Converter 2.690 Download

AutoDWG DWG to Flash Converter 1.10 Download

Download AutoDWG DWGSee 2006 1.881

منبع: P30world

آسیا
ICT
Asia

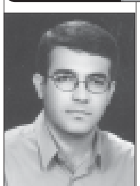
کنکوری‌ها سلام

۸۸۸۹۷۸۹۴

۰۹۱۲۱۲۵۶۲۳۹ کروبی

A.s.i.a - K.o.n.k.o.r - A.s.i.a - K.o.n.k.o.r «تحت نظارت استاد کروبی، مدرس باسابقه شیمی» A.s.i.a - K.o.n.k.o.r - A.s.i.a - K.o.n.k.o.r

زبان انگلیسی



مدرس: آقای اسماعیل زاده

نحوه قرار گرفتن صفت

صفت به دو صورت می‌تواند در جملات انگلیسی به کار برده شود

۱- صفت می‌تواند در جمله، قبل از اسم و برای توصیف آن به کار رود.

مثال:

It is a nice (صفت) book (اسم)

They are good (صفت) students (اسم)

۲- همچنین صفت می‌تواند در جمله بعد از افعال ربطی (Linking Verbs) در جمله قرار گیرد.

افعال ربطی عبارتند از:

be/ become / remain / stay/ appear/ seem/ sound/ feel/ look/ smell/ taste/ get/ grow/

The air looks (فعل ربطی) beautiful (صفت)

The fish tasted (فعل ربطی) nice (صفت)

I am (فعل ربطی) fine (صفت)

ترتیب قرار گرفتن صفات قبل از اسم

گاهی اوقات بیش از یک صفت برای توصیف اسم در جمله به کار می‌رود. نحوه قرار گرفتن صفات مختلف قبل از اسم به ترتیب زیر است:

تعریف (a / an / the) + صفت کیفیت (nice / good) + اندازه (big / small) + رنگ (blue / red) + ملیت (French) + جنس (silk / cotton)

مثال:

A good small blue French cotton shirt (اسم)

ترتیب بیان صفت

از این ترکیب برای بیان صفت استفاده می‌شود در اول جمله معمولاً ضمیر نامعین it قرار می‌گیرد که در جمله معنا نمی‌شود و به این ترتیب است:

It + be(is / was) + صفت + for + مفعول + to + فعل به صورت مصدر با to

در ترکیب فوق، گاهی اوقات عبارت (مفعول + for) بر حسب لزوم حذف می‌شود.

همچنین از صفات زیر در ترکیب فوق می‌توان استفاده نمود.

Necessary / important/ possible/ impossible/ bad/ hard/ good/ easy/ difficult /...

مثال:

It is necessary (صفت) for us to learn (فعل مصدر با to) English.

It is hard (صفت) to swim (فعل مصدر با to) in the river.

قید

قید کلمه‌ای است که معمولاً فعل را توصیف می‌کند.

The students are reading (فعل) carefully (قید)

در جمله بالا carefully قید می‌باشد زیرا چگونگی انجام کاری را بیان می‌کند.

نکته: کلمات fast (تند و سریع) و hard (سخت)، late، low هم صفت و هم قید می‌باشند.

He has bought a fast (صفت) horse (اسم)

The train goes (فعل) fast (قید)

نکته: چنانچه کلمات hard و late به انتهای آنها ly اضافه شود به قید تکرار تبدیل می‌شوند.

ترتیب قید در جمله: اگر در جمله بیش از یک قید داشته باشیم ترتیب آنها را در جمله به قرار زیر است:

اول قید حالت، دوم قید مکان، سوم قید زمان

مثال:

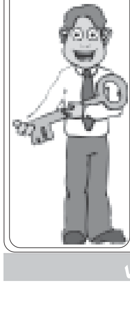
My friend walked quickly (قید حالت) in the park (قید مکان) yesterday (قید زمان)

ترجمه: به منظور یادگیری و یادآوری بهتر، تمرین‌ها و سوالات تستی مباحث این جلسه در شماره بعدی به چاپ خواهد رسید.

برنامه ریزی
فرد به فرد
یا گروهی

مختص موسسات
و مدارس
و آموزشگاه‌ها

اگر فقط بخواهید
کلید طلایی موفقیت
در دستان شماست



باکی بخونم؟

کجا بخونم؟

چطور بخونم؟

چه کتابی بخرم؟

چه رشته‌ای بزنم؟

جواب شما
در روزنامه آسیا

با آسیا تماس
بگیر
بهت می‌گم

(مشاوره تلفنی)
۸۸۸۹۷۸۹۴