به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

ایمن نگه داشتن گذرواژه‌ها در حضور کلیدنگار هوشمند

Passwords Safekeeping in Presence of a Smart Keylogger

بهنام مومنی

زمان: شنبه ۹ آبان ماه ۱۳۹۴ ساعت ۹:۱۵

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهارم، سالن خوارزمی (۴۰۴)

یکی از قابلیت‌های سامانه‌های پایه‌ی امروزی پشتیبانی از چندین کاربر برای اجرای برنامه‌ها و حفاظت از داده‌های آن‌ها در برابر یکدیگر است. ولی به طور معمول در زمانی که یک نفر از رایانه‌ای استفاده می‌کند، قابلیت چندکاربری آن‌گونه که باید به‌کارگرفته نمی‌شود. در نتیجه همه‌ی برنامه‌ها با یک کاربر و یک سطح دسترسی اجرا شده و اگر یکی از آن‌ها، همچون مرورگر وب، آلوده گردد مهاجم می‌تواند به همه‌ی پرونده‌های کاربر در آن رایانه دسترسی پیدا کند. این مشکل آنگاه شدیدتر می‌شود که مهاجم با نصب کلیدنگار رفتار کاربر را زیر نظر می‌گیرد و هنگامی که کاربر می‌خواهد دستوری را با سطح دسترسی بالاتر، همچون دسترسی ریشه در لینوکس، اجرا نماید از گذرواژه‌ی وی با خبر می‌شود.

در نتیجه مهاجم با اندکی درنگ می‌تواند به دسترسی ریشه در رایانه‌ی آلوده‌شده هم دست پیدا کند. در این صورت حفاظت از پرونده‌های گوناگون با استفاده از قابلیت چندکاربری کارایی خود را از دست می‌دهد. در این ارایه روشی برای توسعه‌ی یک برنامه‌ی مدیریت گذرواژه معرفی می‌شود که می‌تواند با بهره‌گیری از قابلیت‌های لینوکس از فاش شدن گذرواژه‌ها، حتی در حضور یک مهاجم هوشمند، جلوگیری کند. منظور از مهاجم هوشمند فردی است که با آگاهی کامل از روش معرفی‌شده در این جلسه می‌تواند هر برنامه‌ی دلخواهی را بر روی رایانه‌ی قربانی و البته با سطح دسترسی کاربر معمولی اجرا کند.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.