به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

گمنامی در شبکه‌های نظیر به نظیر

A Protocol to Improve Privacy and Security of Anonymity Networks

مهدی سلطانی

زمان: شنبه ۲۲ شهریور ماه ۱۳۹۳ ساعت ۳ عصر

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

با رشد کاربردهای شبکه‌های کامپوتری، اهمیت حفظ حریم خصوصی به صورت روز افزونی در حال افزایش است. یکی از جنبه های مهم حفظ حریم خصوصی، گمنامی - به معنای مخفی نگه داشتن هویت طرفین ارتباط -است. امروزه یکی از پرکاربردترین گونه های پروتکل‌های گمنامی، شبکه مخلوط‌کن‌ها هستند. به طور کلی مخلوط کن برای فراهم آوردن گمنامی، الگوی بیتی و ترتیب پیام‌های ورودی را چنان تغییر می‌دهد که ناظر خارجی قادر به مربوط کردن پیام‌های ورودی و خروجی نباشد. در کنار شبکه مخلوط‌کن‌ها، برای ایجاد شبکه‌های گمنامی با تاخیر کم، پروتکل مسیریابی پیازی به وجود آمد که شبکه گمنامی تـُر، یا همان نسل دوم شبکه‌های پیازی به عنوان پرکاربردترین شبکه‌ی گمنامی با تاخیر کم، بر اساس این پروتکل به وجود آمده است. هدف اصلی تـُرعموماً برقراری ارتباط یک کاربر به صورت گمنام با یک کارپذیر بدون نیاز به ایجادهر گونه تغییری در سمت کارپذیر است. درمقابل راهکارهای ارائه شده برای ایجاد گمنامی، حملاتی نیز به این پروتکل‌ها وارد شده است، مانند حملات زمان‌سنجی، حمله‌ی تکرار، حملات برچسب‌گذاری، حملات مخلوطی، حملات ماقبل، حملات سطح پروتکل و حملات تحلیل ترافیک. در این ارائه، تلاش خواهد شد تا با ایجاد تغییراتی در پروتکل تُر، این پروتکل را در برابر حملات تحلیل ترافیک و حملات سطح پروتکل مقاوم‌تر سازیم.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.