بهبود معیار پوشش کد برای کشف آسیب پذیری در پروتکل‌های شبکه دارای حالت توسط فازینگ ترکیبی

حمید رضایی رهورد* محمد مهدی سالخورده حقیقی**

*کارشناس ارشد شبکه، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه سجاد، مشهد

**هیئت علمی، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه سجاد، مشهد

چکیده

فازینگ نرم‌افزار، روشی برای یافتن آسیب‌پذیری‌های امنیتی در برنامه‌های کاربردی است. در این روش با ارسال داده‌های تصادفی به برنامه، سعی می‌شود مواردی پیدا شود که منجر به رفتارهای نامطلوب و خطاهایی همچون خرابی حافظه یا دسترسی‌های غیرمجاز شود. یکی از روش‌های پیشنهادی برای بهبود و اثربخشی فازینگ، استفاده از تحلیل نمادین و اجرای پویا-نمادین است. در این روش علاوه بر تولید داده‌های تصادفی، از تحلیل منطقی برنامه و اجرای نمادین آن برای تولید داده‌هایی استفاده می‌شود که بتوانند مسیرهای جدیدی از اجرای برنامه را پوشش دهند. در این پژوهش نشان داده‌ایم که می‌توان از روش اجرای پویا-نمادین برای فازینگ پروتکل‌های شبکه استفاده نمود و همچنین این فرایند را بهبود بخشید. بدین منظور اولین چارچوب برای فازینگ ترکیبی پروتکل‌های شبکه طراحی و پیاده‌سازی شده است. نتایج بر روی دو سرویس dcmtk و dnsmasq نشان می‌دهد که فازینگ ترکیبی در معیار پوشش کد نسبت به فازینگ سنتی عملکرد بهتری دارد. پوشش شاخه در سرویس dcmtk مقدار ۲.۷۱ درصد نسبت به AFLNet بهبود داشته است که توانسته عملکرد منفی NyxNet نسبت به AFLNet را مثبت نماید. همچنین پوشش شاخه در سرویس dnsmasq نسبت به AFLNet مقدار ۳۷.۷۲ درصد و نسبت به NyxNet مقدار ۱۱.۸۲ درصد بهبود داشته است.

واژگان کلیدی: آزمون فازینگ, آزمون پروتکل های شبکه, آسیب پذیری, اجرای نمادین, اجرای پویا-نمادین

نویسنده مسئول: مهدی سالخورده حقیقی
haghighi@sadjad.ac.ir