

پروتکل‌های تبادل کلید، احراز اصالت، تبادل
کلید توام با احراز اصالت (AKE) و تبادل کلید
و احراز اصالت مبتنی بر گذر واژه (PAKE)

محسن تورانی

toorani@ieee.org

دانشکده مهندسی برق

دانشگاه علم و صنعت ایران

دی ماه ۱۳۸۵

چکیده

در این گزارش در ابتدا اصول کلی پروتکل‌های مبادله کلید¹ تحت بررسی قرار می‌گیرند. همچنین برخی از پروتکل‌های کاربردی جهت احراز اصالت² و تعدادی از پروتکل‌هایی که مبادله کلید را همراه با احراز اصالت انجام می‌دهند، معرفی می‌شوند. سپس به معرفی پروتکل‌های مبادله کلید و احراز اصالت مبتنی بر گذر واژه خواهیم پرداخت و در پایان نیز به طور مختصر روش‌های مختلف تحلیل و معیارهای ارزیابی میزان امنیت یک پروتکل معرفی می‌شود.

کلمات کلیدی: پروتکل‌های مبادله کلید (KE)، پروتکل‌های احراز اصالت، پروتکل‌های مبادله کلید توام با احراز اصالت (AKE)، پروتکل‌های مبادله کلید و احراز اصالت مبتنی بر گذر واژه (PAKE)، حملات لغتنامه‌ای، روش‌های تحلیل پروتکل

¹ Key Exchange
² Authentication

فهرست مطالب

۴	مقدمه
۶	بخش اول: پروتکل‌های مبادله کلید
۶	۱-۱ مبادله کلید با استفاده از رمزنگاری متقارن
۷	۱-۲ مبادله کلید با استفاده از رمزنگاری کلید همگانی
۹	۱-۲-۱ پروتکل قفل داخلی
۱۱	۱-۲-۲ استفاده از امضای دیجیتال
۱۲	۱-۲-۳ ارسال پیام و کلید به طور همزمان
۱۳	۱-۳ پروتکل دیفی-هلمن
۱۵	۱-۳-۱ افزایش نفرات در پروتکل دیفی-هلمن
۱۶	۱-۳-۲ پروتکل هوقس
۱۷	۱-۴ پروتکل ایستگاه به ایستگاه
۱۹	بخش دوم: احراز اصالت
۱۹	۲-۱ احراز اصالت با استفاده از توابع یک راهه
۲۰	۲-۲ حملات لغت نامه ای و salt
۲۲	۲-۳ SKEY
۲۳	۲-۴ احراز اصالت با استفاده از کلید همگانی
۲۵	۲-۵ احراز اصالت توام با استفاده از پروتکل قفل داخلی
۲۶	۲-۶ SKID
۲۷	۲-۷ تصدیق صحت پیام
۲۹	بخش سوم: پروتکل‌های مبادله کلید توام با احراز اصالت
۳۰	۳-۱ پروتکل قورباغه دهان بزرگ
۳۰	۳-۲ پروتکل یاهاوم
۳۱	۳-۳ پروتکل نیدهام-شرودر

۳۴	پروتکل اتوی-ریس
۳۵	پروتکل کرپرس
۳۶	پروتکل نویمان-استابلین
۳۸	DASS-پروتکل
۳۹	پروتکل دنینگ-ساکو
۴۱	پروتکل وو-لام
۴۳	بخش چهارم: پروتکل‌های مبادله کلید و احراز اصالت مبتنی بر گذر واژه
۴۹	SPEKE-پروتکل
۵۱	DH-EKE-پروتکل
۵۲	A-EKE-پروتکل
۵۳	B-SPEKE-پروتکل
۵۵	PAK-X-پروتکل
۵۵	OKE-پروتکل
۵۵	SNAPI-X-پروتکل
۵۷	AMP-پروتکل
۵۷	SRP-پروتکل
۵۸	DH-BPAKE-پروتکل
۵۸	۴-۱۱ ویژگی‌های مطرح در طراحی و ارزیابی پروتکل‌های PAKE
۶۱	بخش پنجم: مروری بر روش‌های تحلیل و ارزیابی پروتکل‌ها
۶۶	نتیجه گیری
۶۷	فهرست منابع مورد استفاده
۶۸	فهرست مراجع