



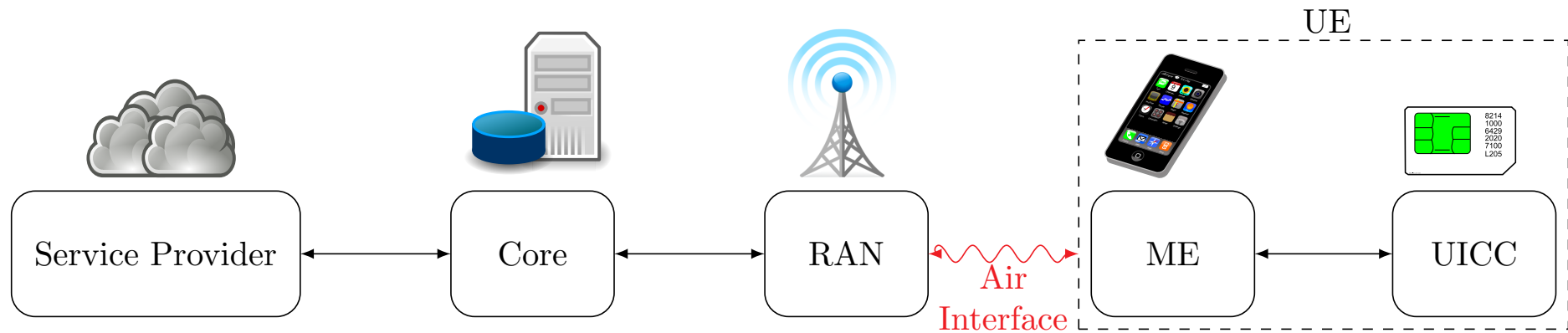
فصل ششم: امنیت در شبکه های مخابراتی


امنیت سیستم های کامپیوتری

ابوالفضل دیانت

آخرین ویرایش: ۸ خرداد ۱۴۰۳ در ساعت ۲۲ و ۷ دقیقه - نسخه 1.0.3

امنیت در شبکه‌های تلفن همراه



معماری کلان شبکه‌های تلفن همراه از پنج گروه عملکردی (Functionality Group) تشکیل شده: 

● UICC (Universal Integrated Circuit Card)

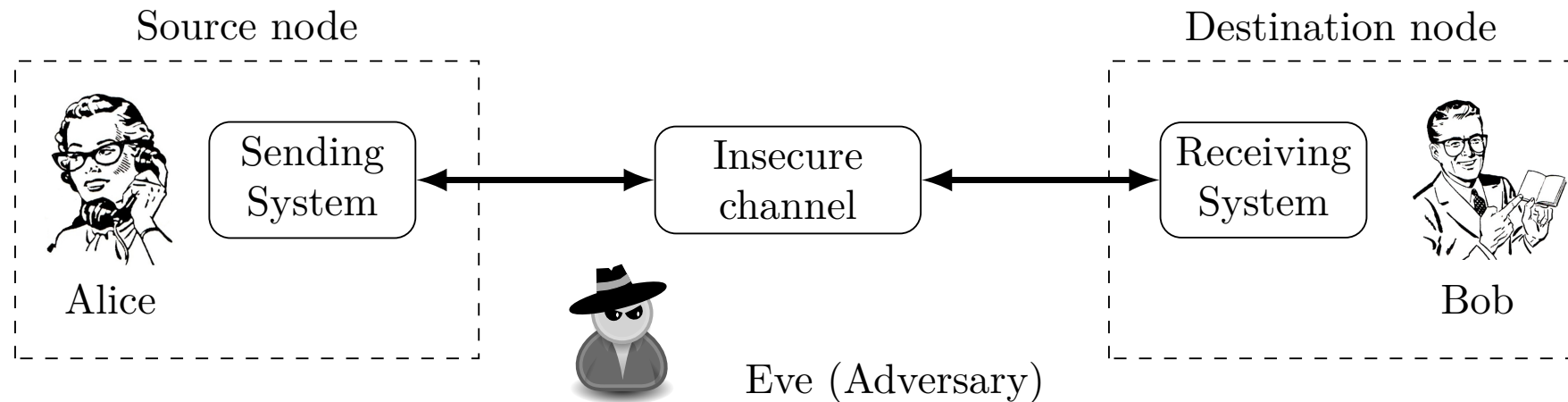
● ME (Mobile Equipment)

● شبکه دسترسی رادیویی (Radio Access Network)

● هسته شبکه (Core Network)

● ناحیه خدمات

چرا به احراز اصالت (Authentication) نیاز داریم؟

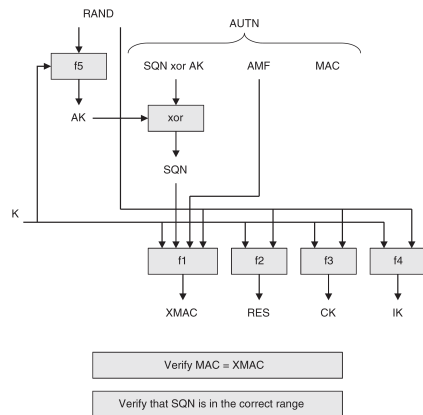
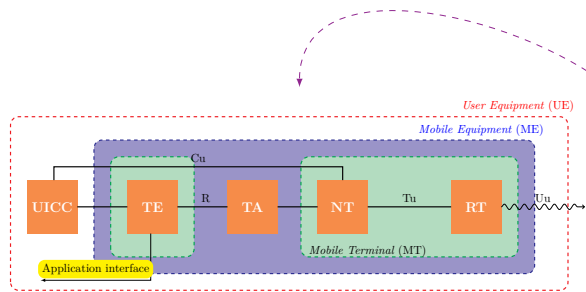


👉 برای محرمانه ماندن پیام می‌بایست از رمزگذاری (Encryption) استفاده کنیم، و برای آن نیاز به کلید داریم.

👉 استفاده از سازوکارهای برقراری کلید (Key Establishment) [۱، فصل ۱۲]:

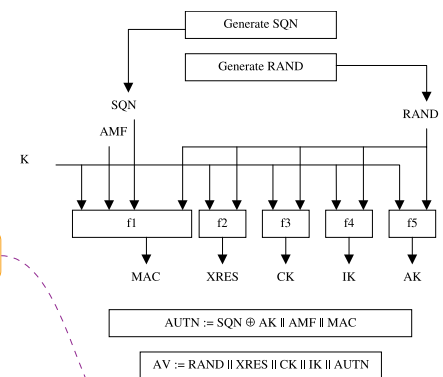
- تبادل کلید (Key Transport): یک سمت کلید را تولید کرده و در اختیار طرف مقابل نیز قرار می‌دهد.

- توافق کلید (Key Agreement): هر دو سمت، در فرایند تولید کلید مشارکت می‌کنند.



Verify AUTN,
Compute RES

Auth Vector
request from AuC
Generate Auth Vec:
(RAND, AUTN, IK, CK, XRES)



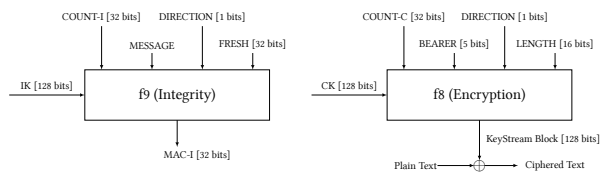
RAND	IK	CK	MAC	AK	RES	SQN	AMF
128	128	128	64	48	32-128	48	16

Verify RES, decide
allowed algorithms

Allowed algorithms
IK, CK

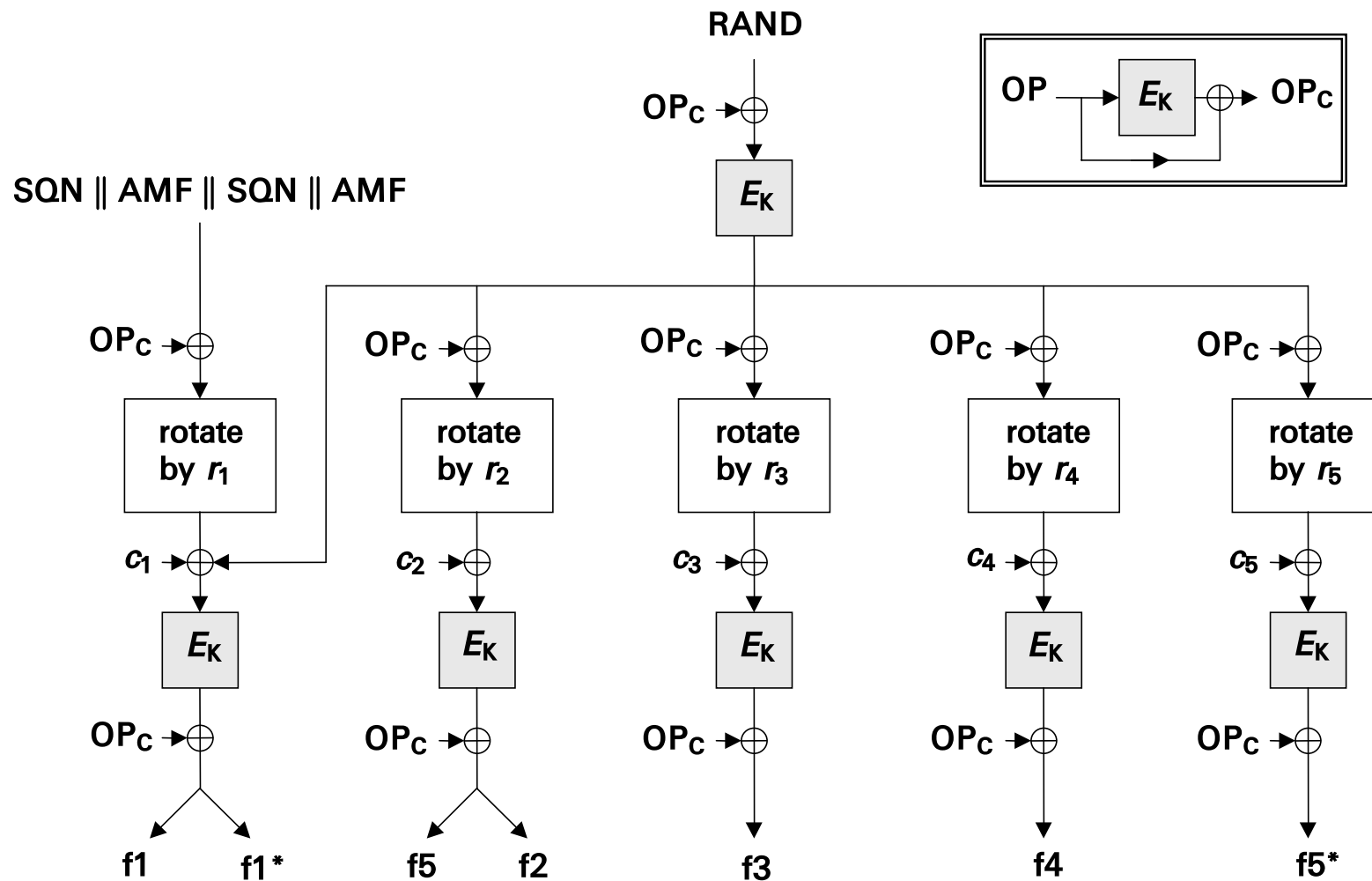
Decide algorithms,
Start Integrity

Verify MAC and
security capabilities




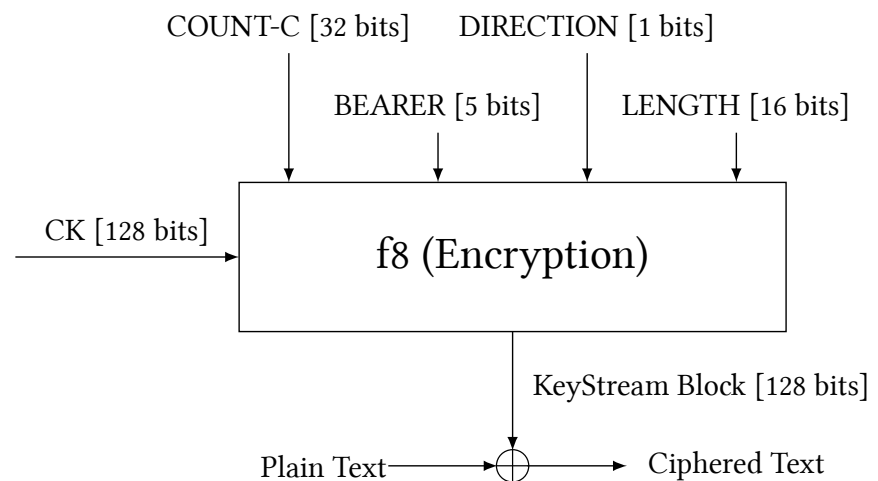
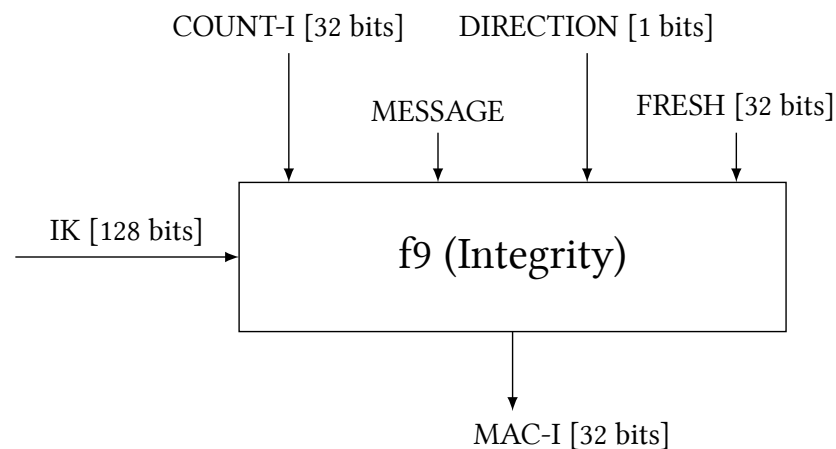
security mode command
selected algorithms, security capabilities

نمایی از توابع MILENAGE



الگوریتم‌های تامین امنیت در UMTS (ادامه)

نمای کلی از ورودی‌های توابع f_8 و f_9 



IDS

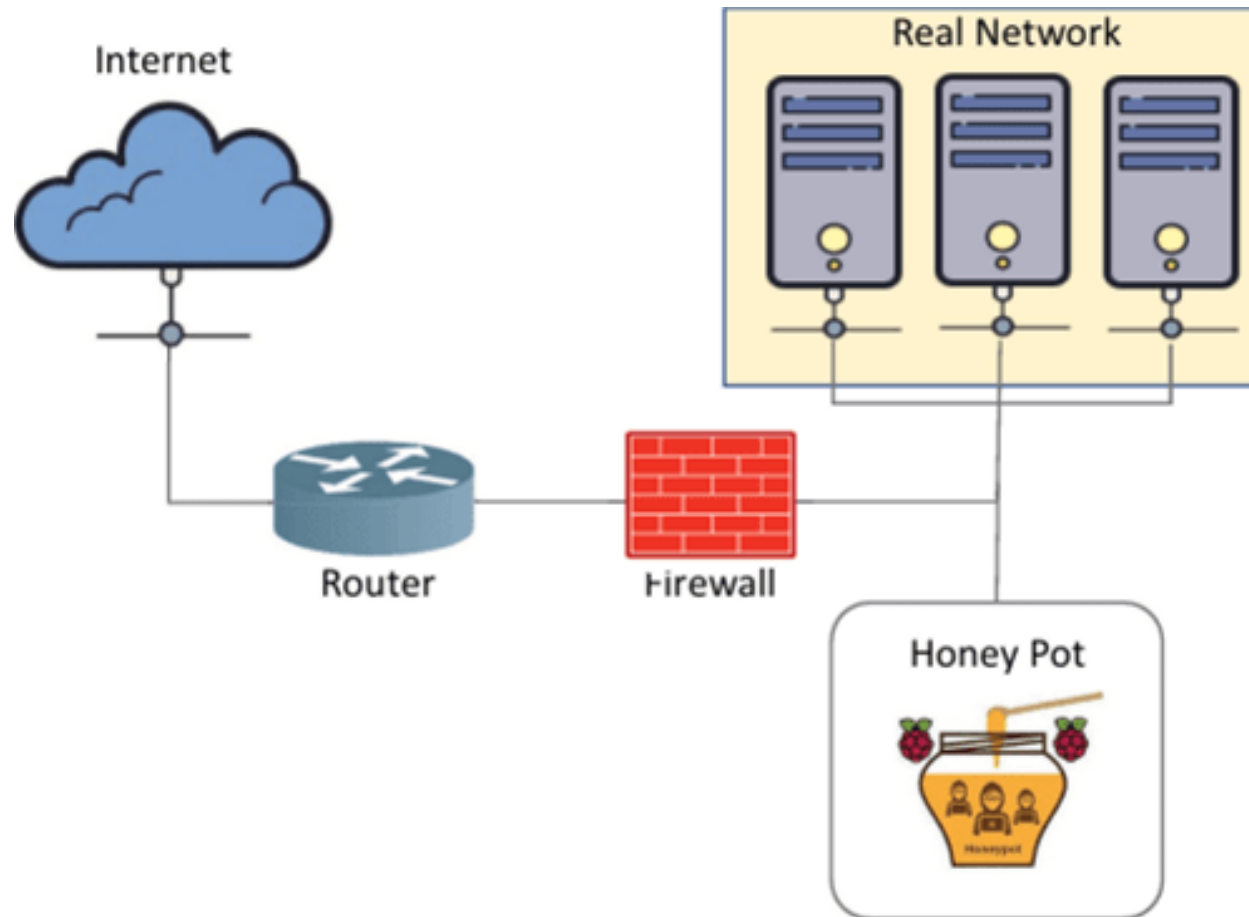
راه کارهای مواجهه با حملات

📌 راه کارهای مواجهه با حملات:

- جلوگیری از حمله: مثل استفاده از دیوار آتش (Firewall)
- تشخیص حمله: مثل بکارگیری IDS (Intrusion Detection System)
- به ترکیب و همکاری این دو نیز باید فکر کرد، مثل IPS (Intrusion Prevention System)
- فریب حمله گر: ایده های جذابی به مانند تله عسل (Honeypot)



تله عسل (Honeypot)



با هدف فریب حمله‌گر و جمع‌آوری بدافزارها

فقط در حد شبیه‌سازی (کم‌تعامل) و یا سامانه واقعی (پر تعامل)

IDS (Intrusion Detection System) یک چارچوب با قابلیت تشخیص، آشکارسازی و واکنش

به فعالیت‌های غیرمجاز و نابهنجار (Abnormal) به سامانه مورد بررسی (حملات). در واقع IDS نقش دزدگیر را در سامانه‌های امنیتی است.

اهداف و وظایف IDS:

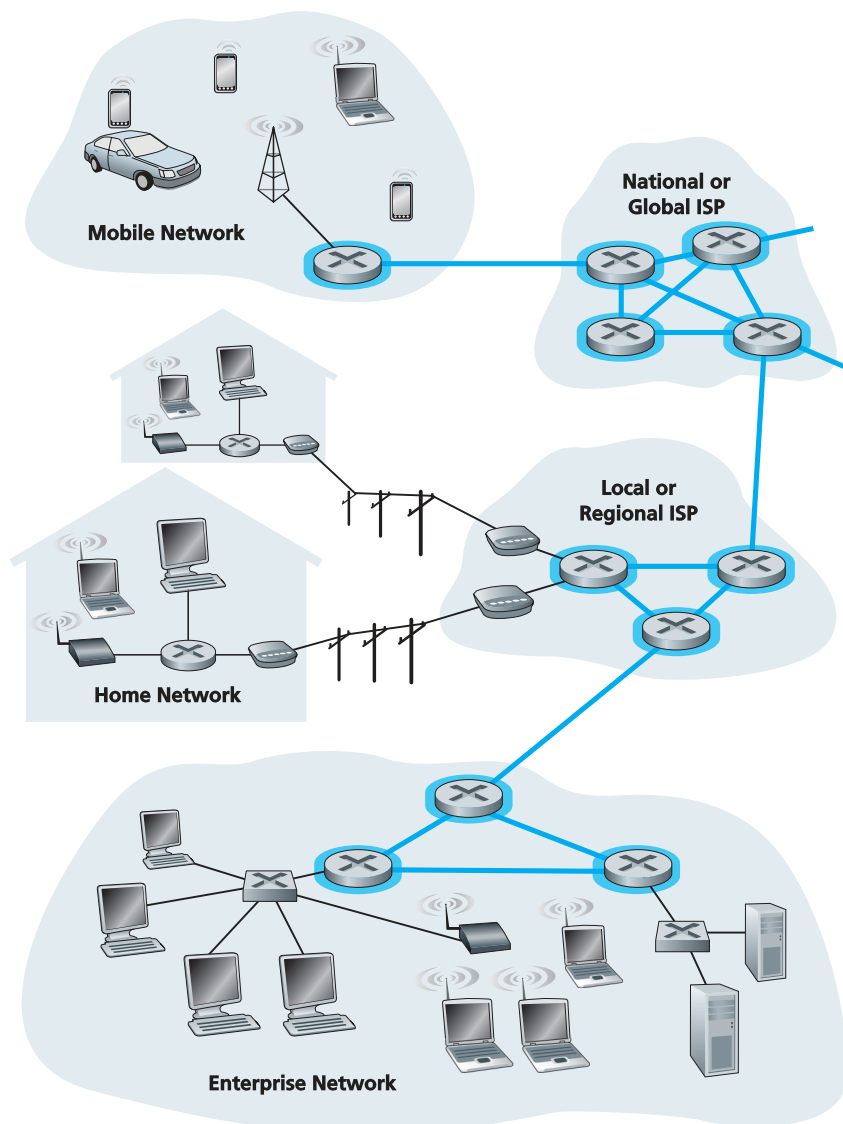
✓ نظارت و تحلیل فعالیت و رفتار نهادهای (Entity) (مشتری، سامانه‌ها و ...)

✓ تشخیص الگوهای منطبق با حملات (شناخته شده یا هوش مصنوعی)

✓ شناسایی و ردیابی: بررسی Logها

✓ پاسخ‌گویی و واکنش به حمله: به مانند آلارم دادن

تعریف (ادامه) IDS (Intrusion Detection System)



دلائل استفاده از IDS:

- تشخیص حمله
- جلوگیری از تکرار حمله
- جلوگیری از کامل شدن حمله
- فراهم سازی اطلاعات مهم از حمله و امکان عیب یابی

اولین تلاش ما ثبت کل وقایع یک سامانه بود، که به آن فرایند Audit می گفتیم (دهه ۷۰ و دهه ۸۰)

سامانه های IDS مبتنی بر میزبان (HIDS): نخست در IDS می خواهیم فرایند ثبت و تحلیل به صورت خودکار

و هوشمندانه صورت پذیرد. یعنی تمرکز بر روی میزبان (Host) است.

• ناهنجاری (Abnormality): هر کاربر یک سری ویژگی های مشخصی دارد (نرخ تایید، مدت نشست و ...).

پس من می توانم یک پروفایلی از رفتار نرمال کاربر را درست کنم.

• سوء استفاده (Misusing): الگوهای سوء استفاده را پیدا کنیم و یک تطابق انجام دهیم.

نکته


در ناهنجاری می گوییم چه چیز نرمال است، غیر از آن حمله است. در سوء استفاده می گوییم چه چیز با حمله تطابق دارد.



انواع خطا

تصمیم گیری		
رد H_0	قبول H_0	
خطای نوع اول	تصمیم درست	H_0
تصمیم درست	خطای نوع دوم	H_1
		واقعیت


خطای نوع اول (مثبت کاذب): میزبان سالم، به اشتباه ناهنجار تشخیص داده شود. 

خطای نوع دوم (منفی کاذب): میزبان ناهنجار، به اشتباه سالم تشخیص داده شود. 

📖 در دهه ۱۹۹۰ وقتی شبکه‌های رایانه‌ای آمد (ARPANET)، ما نیز به سراغ سامانه‌های NIDS مبتنی بر شبکه رفتیم.

📖 همان دو رویکرد قبلی، اما در سطح ترافیک شبکه بیاید:

- ناهنجاری (Abnormality): الگوی ترافیک سالم
- سوء استفاده (Misusing): باید الگوی بسته‌های مختلف حملات

تعدادی Agent داریم که در کل بخش‌های سیستم قرار می‌گیرد. 

ترکیبی از NIDS و HIDS 

نقش تصمیم‌گیری هوشمندانه در میان چند عامل 

- [1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. Discrete Mathematics and Its Applications, CRC Press, 1996.

فهرست اختصارات

واژه‌نامه انگلیسی به فارسی

واژه‌نامه فارسی به انگلیسی