دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

مدرس درس: دکتر حمیدرضا شهریاری

تدریس‌یار: مهدی نیکوقدم

پاییز1402

نکته1: جواب تمرینات صرفا برای افزایش اطلاعات دانشجویان قرار داده شده است. برای سوالات ممکن است جواب‌های مختلفی درست باشد. در نتیجه در صورتی که مشاهده کردید که جواب تمرینات شما با پاسخی که قرار داده شده است دقیقا مشابه نیست نگران نباشید! همان‌طوری که گفته شد برای سوالات جواب‌های مختلفی جواب صحیح است و این پاسخ‌ها تنها پاسخ‌های صحیح نمی‌باشد. همان‌طوری که از اول ترم در پایین تمامی تمرینات نوشته شده است هدف افزایش یادگیری شماست و همین که دانشجو تلاشی در راستای به دست آوردن جواب کرده باشد ارزشمند است.

نکته2: جواب برخی سوالات به طور کامل نوشته شده است. برخی سوالات نیز با توجه به اینکه حالت تحقیقاتی داشته‌اند آورده نشده است. همچنین با توجه به این موضوع که برخی دانشجویان جواب‌های واقعا جالبی به سوالات داده‌اند. پاسخ آن‌ها به عنوان یک نمونه در این فایل آورده شده است تا نحوه پاسخگویی به سوالات را مشاهده کنید و بتوانید نحوه تفکر و فکر دیگر دوستانتون رو ببینین.

1. عبارت Computer Security به چه معناست ؟

حفاظت از یک سیستم اطلاعاتی خودکار به منظور حفظ یک‌پارچگی (integrity)، دسترس‌پذیری (availability)، و محرمانگی (confidentiality) اطلاعات سیستم (سخت‌افزار، نرم‌افزار، داده و ارتباطات.

2. تفاوت حمله، تهدید، و آسیب‌پذیری را توضیح دهید.

تعریف هر سه مورد و مقایسه آن‌ها

آسیب‌پذیری: نقص یا ضعف در طراحی، پیاده سازی، یا عملیات و مدیریت سیستم که می‌تواند برای نقض خط‌مشی امنیتی سیستم مورد سوء استفاده قرار گیرد.

تهدید: پتانسیل نقض امنیت، که زمانی وجود دارد که شرایط، قابلیت، اقدام یا رویدادی وجود داشته باشد که توانایی نقض امنیت را داشته باشد و باعث آسیب شود. یعنی یک تهدید یک خطر احتمالی است که ممکن است از یک آسیب پذیری سوء استفاده کند.

حمله: حمله به امنیت سیستم که از یک تهدید هوشمند ناشی می‌شود. یعنی یک اقدام هوشمندانه که تلاشی عمدی (به ویژه به معنای یک روش یا تکنیک) برای فرار از سرویس‌های امنیتی و نقض خط‌مشی امنیتی یک سیستم است.

3. منظور از حملات فعال و غیرفعال را توضیح دهید. تشخیص کدام حمله سخت‌تر است؟ توضیح دهید.

حمله Active: تلاش برای ایجاد تغییر در منابع سیستم و یا اثر گذاشتن بر روی عملیات سیستم. مانند: جعل هویت و ارسال دوباره پیام و تغییر.

حمله Passive: تلاشی برای یادگیری یا استفاده از اطلاعات از سیستم است که بر منابع سیستم تاثیر نمی‌گذارد. مانند: تحلیل ترافیک و یا شنود و رصد پیام ها .پیشگیری از حملات غیرفعال آسانتر و در مقابل برای حمالت فعال تشخیص و مقابله بهتر است.

حملات فعال. شناسایی حملات غیرفعال بسیار دشوار است زیرا هیچ‌گونه تغییری در داده‌ها وجود ندارد. به طور معمول، ترافیک پیام به شکل ظاهراً عادی ارسال و دریافت می‌شود و نه فرستنده و نه گیرنده آگاه نیستند که شخص ثالثی پیام‌ها را خوانده یا الگوی ترافیک را مشاهده کرده است. با این حال، جلوگیری از موفقیت این حملات معمولاً با استفاده از رمزگذاری امکان‌پذیر است. بنابراین، تاکید در برخورد با حملات غیرفعال بر پیشگیری است تا تشخیص.. در حالی که شناسایی حملات غیرفعال دشوار است، اقداماتی برای جلوگیری از موفقیت آنها در دسترس است. از سوی دیگر، جلوگیری از حملات فعال کاملاً دشوار است، زیرا انجام این کار مستلزم محافظت فیزیکی از کلیه امکانات و مسیرهای ارتباطی در هر زمان است. در عوض، هدف شناسایی آنها و بهبودی از هرگونه اختلال یا تاخیر ناشی از آنهاست. از آنجایی که تشخیص اثر بازدارنده دارد، ممکن است به پیشگیری نیز کمک کند.

4. حملات زیر را توضیح دهید و بیان کنید که در کدام دسته از حملات قرار می‌گیرند.

- حمله جعل هویت

منظور از حمله جعل هویت یا حمله نقاب این است که در یک ارتباط بین دو موجودیت فرد مهاجم بتواند خودش را به جای یکی از موجودیت‌های قانونی جا بزند و به عنوان یک موجودیت قانونی با او تبادل اطلاعات کند.

- حمله تکرار

منظور از حمله تکرار این است که در یک ارتباط مهاجم از پیام‌های تکراری و بیات استفاده کند. به عنوان مثال فرض کنید که آلیس در تاریخ 9 آبان 1402 از باب درخواست 5 میلیون تومان را داشته و باب این پیام را دریافت کرده و این میزان پول را برای آلیس ارسال کرده است. حال مهاجم این پیام را شنود کرده و در تاریخی دیگر به عنوان مثال 9 آذر 1402 مجدد این پیام رو بدون هیچگونه دستکاری برای باب ارسال کند. در این صورت اگر باب تازگی پیام را چک نکند. تکراری بودن پیام مشخص نخواهد شد.

- حمله دستکاری

منظور از حمله دستکاری این است که مهام پیامی را که بین دو موجودیت رد و بدل می‌شود را تغییر دهد و در واقع صحت و یکپارچگی پیام را از بین ببرد.

- حمله شنود

منظور از این حمله این است که مهاجم یک حمله غیرفعال انجام دهد و صرفا بر روی بستری که دو موجودیت با هم تبادل پیام می‌کنند قرار گیرد و پیام‌های تبادل شده را بدون هیچگونه دستکاری مشاهده کند.

- حمله منع سرویس

منظور از این حمله این است که مهاجم با ایجاد درخواست‌های زیاد و پی در پی باعث شود فعالیت یکی از موجودیت‌های درگیر در تبادل اطلاعات مختل شود و امکان سرویس دهی نداشته باشد. معمولا این حمله بیشتر زمانی اتفاق می‌افتد که یکی از موجودیت‌های درگیر در ارتباط یک خدمات‌دهنده یا همان سرور باشد.

5. در مورد سوال موارد زیر **تحقیق** کنید و توضیح دهید که هر کدام زیر مجموعه کدام مورد دیگر است.

- data leakage
- privacy
- anonymity
- untraceability
- confidentiality

6. فرض کنید که DES(a,k) رمزنگاری متن ساده a را با کلید k با استفاده از سیستم رمزنگاری DES را نشان دهد. همچنین فرض کنید c = DES(a,k) و cc= DES(a', k') که در آن منظور از (') مکمل بیتی میباشد. ثابت کنید $cc = 'c$

نمونه اولیه پاسخ

ابتدا دو رابطه مهم را که بر اساس خواص XOR داریم را بررسی کنیم:

رابطه ۱:

$$a' \oplus b' = 1 \oplus b \oplus 1 \oplus b = a \oplus b$$

رابطه ۲:

$$a' \oplus b = 1 \oplus a \oplus b = (a \oplus b)'$$

حال روابط خود DES را بررسی می‌کنیم:

$$L_i = R_{i-1} \xrightarrow{yields} L_i' = R_{i-1}'$$

$$R_i' = L_{i-1}' \oplus f(R_{i-1}', k_i') \overset{***}{\rightarrow} L_{i-1}' \oplus f(R_{i-1}, k_i) \xrightarrow{\text{رابطه } 2} (L_{i-1} \oplus f(R_{i-1}, k_i)' = (R_i)'$$

قسمت قرمز در رابطه بالا اینگونه نتیجه گرفته شده‌است که ورودی‌های تابع f دو مقدار R' و K' هستند و سپس R' از یک عمل Expansion می‌گذرد که عملی خطی است یعنی اگر خروجی آن‌را $EXP(R')$ در نظر بگیریم در اینصورت داریم:

$$EXP(R') = EXP(R)$$

چون صرفا بیت‌ها تکرار شده‌اند. در نتیجه وقتی که $EXP(R')$ و K' به عمل XOR می‌رسند طبق رابطه شماره یک به نتیجه زیر می‌رسیم:

$$f\left(R', k'\right) = f(R, k)$$

طبق اثبات بالا با ورودی‌هایی که مکمل بیتی هستند، خروجی هر مرحله نیز مکمل بیتی می‌شود. یعنی جواب به صورت دیاگرام زیر است:

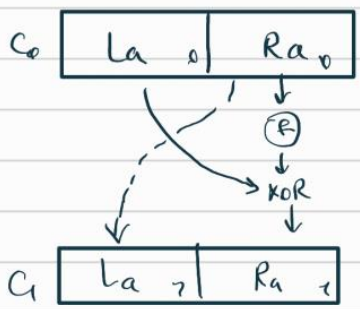
می‌بینیم که دو خروجی هم مکمل بیتی هم هستند.

نمونه دوم پاسخ

$DES(a, K) = C$ $\qquad$ $a \text{ XOR } 1 = a'$

$K \text{ XOR } 1 = K'$

$DES(a', K') = C_c$ $\qquad$ $\hookrightarrow C \text{ XOR } 1 = C' \overset{?}{=} C_c$



از آن جایی که در تمامی دورهای DES یک عملیات یکسان تکرار می‌شود اگر ثابت کنیم که در یک مقدم سازی در مرحله‌ی اول از DES از بین نمی‌رود (یعنی مقدم خروجی دور اول برابر است با خروجی مقدم های ورودی های دور اول) آن گاه می‌توانیم نتیجه بگیریم که عملیات مقدم سازی در کل الگوریتم DES حفظ می‌شود

پس اگر نتیجه بگیریم که $FRound(a_0, K_0)' = FRound(a_0', K_0')$ ← یعنی اجرای یک دور از فیستل آن گاه فرض مسأله را هم ثابت کرده‌ایم.

$F(a, K) = L_{a_1} R_{a_1}$

$L_{a_1} = R_{a_0}$ $\quad$ $R_{a_1} = L_{a_0} \text{ XOR } f(R_{a_0}, K_0)$

$F(a', K') = L''_{a_1} R''_{a_1} \rightarrow L''_{a_1} = R_{a_0'}$ $\quad$ $R''_{a_1} = L_{a_0'} \text{ XOR } f(R_{a_0'}, K_0')$

$$(L_{a_1})' = L''_{a_1}$$

از آن جایی که $L''_{a_1} = R'_{a_0}$ و $L_{a_1} = R_{a_0}$ می‌توان مشاهده کرد که عملیات متمم‌سازی در سمت چپ و خروجی دور فیستل منتقل شده فقط باید ثابت کنیم که $(R_{a_1})' = R''_{a_1}$

یعنی

$$\longrightarrow \left[L_{r_0} \text{ XOR } f(R_{a_0}, K_0)\right]' = L'_{a_0} \text{ XOR } f(R'_{a_0}, K'_0)$$