به نام خدا

تمرین چهارم امنیت داده و شبکه

نیم‌سال دوم ۱۴۰۴-۱۴۰۳

دانشکده مهندسی کامپیوتر

دانشگاه صنعتی شریف

موضوع **امنیت شبکه**

موعد تحویل **سه‌شنبه ۱۶ خرداد ۱۴۰۴**

طراحی تمرین توسط **رضا سعیدی - متین آقامیرکریمی - مبین آقامیرکریمی**

۱. در طرح امضا زیر جهت وارسی اصالت پیام‌ها، یک عملگر p در نظر گرفته شده است که ویژگی‌های خاصی دارد. برای یک ورودی x، یافتن x از روی $p(x)$ امکان پذیر نیست. در این سیستم، پیام‌ها از مجموعه $M = \{1, 2, \ldots, n\}$ انتخاب شده و پروسه‌های زیر برای امضا و تأیید امضا تعریف شده است:

- **تولید کلیدها:** ابتدا یک رشته بیت تصادفی $a \in \{0,1\}^n$ تولید می‌شود. سپس برای بدست آوردن کلید عمومی، عملگر p به صورت پیاپی بر روی a اعمال می‌شود تا مقدار b به دست آید. به عبارت دیگر، کلید عمومی b به صورت زیر محاسبه می‌شود:

$$p^n(a) = b$$

که در آن $p^n(a)$ به معنای اعمال عملگر p به تعداد n بار روی a است. در این صورت a کلید خصوصی و b کلید عمومی خواهد بود.

- **امضای پیام:** برای امضای پیام $i \in M$ عملگر p به تعداد $n - i$ بار روی a اعمال می‌شود و خروجی این اعمال به عنوان امضا برای پیام i در نظر گرفته می‌شود. به عبارت دیگر، امضای پیام i به صورت زیر محاسبه می‌شود:

$$p^{n-i}(a) = \sigma_i$$

- **وارسی امضا:** برای تأیید صحت امضا σ_i روی پیام i با استفاده از کلید عمومی b، باید بررسی شود که آیا رابطه زیر برقرار است یا نه:

$$p^i(\sigma_i) = b$$

آ. نشان دهید که اگر یک مهاجم امضای یک پیام را داشته باشد، می‌تواند امضای پیام‌های دیگری را نیز تولید کند. این جعل برای کدام پیام‌ها ممکن است؟

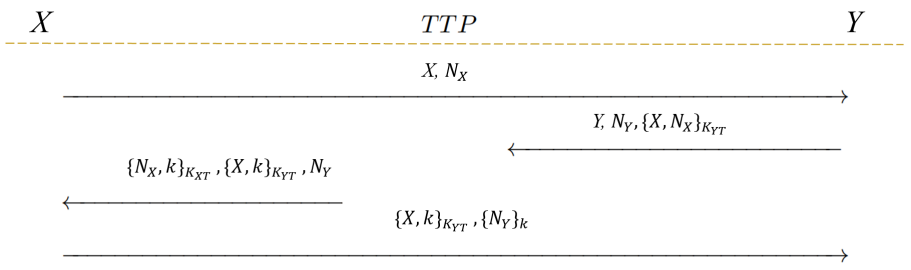
ب. برای اصلاح این سیستم به طوری که امنیت آن برای امضاهای یک‌بار مصرف تضمین شود، چه تغییراتی باید در روش و ساختار آن ایجاد گردد؟

۲. فرایند زیر را به عنوان پروتکلی جهت احراز هویت و توافق کلید در نظر بگیرید. (N_x و N_Y مقادیر نانس می‌باشند)

ویژگی‌های بیان شده زیر را در پروتکل بررسی کنید:

- امکان اجرای حمله تکرار
- احراز تازگی کلید توسط هر یک از طرفین
- احراز اصالت طرفین و تایید کلید (اطمینان از دریافت کلید توسط طرف مقابل و زنده بودن آن)

در صورت وجود هرگونه آسیب‌پذیری، پروتکل را به گونه‌ای اصلاح کنید که تمامی ویژگی‌های امنیتی فوق را تأمین نماید.



۳. C، S و KDC [۱] اعضای دامنه[۲] کربروس هستند. زمانی که C درخواست بلیط برای S کند، KDC یک کلید موقت $K_{C,S}$ را ایجاد می‌کند. با توجه به این که KDC کلید $K_{C,S}$ را می‌داند، می‌تواند تمام ترافیکی که با این کلید رمزنگاری می‌شود را رمزگشایی کند.

آ. با فرض این که KDC نمی‌تواند ترافیک بین C و S را تغییر دهد، C و S چطور می‌توانند یک کلید مشترک به نام K' بین خود تبادل کنند به طوری که KDC نتواند آن را بدست آورد؟

ب. اگر KDC امکان تغییر ترافیک بین C و S را داشته باشد چگونه می‌تواند راه حل ارائه شده شما در بخش اول را تهدید کند؟

ج. فرض کنید C, S به طور همزمان عضو دو دامنه کربروس باشند. به طوری که:

- دامنه ۱: $KDC1$ که کلید $K_{C,S,1}$ را ایجاد کرده است
- دامنه ۲: $KDC2$ که کلید $K_{C,S,2}$ را ایجاد کرده است

با فرض این که $KDC1$ و $KDC2$ امکان تبانی ندارند ولی می‌توانند ترافیک بین C و S را تغییر دهند، C و S چطور می‌توانند یک کلید مشترک به نام K' بین خود تبادل کنند به طوری که $KDC2$ و $KDC1$ نتواند آن را بدست آورد؟

۴. در رابطه با حملات منع خدمت به سوالات زیر پاسخ دهید.

آ. به طور کلی حملات منع خدمت در سه دسته زیر تقسیم می‌شوند، هر یک را خلاصه توضیح دهید.

- Volumetric Attacks
- Protocol Attacks
- Application Layer Attacks

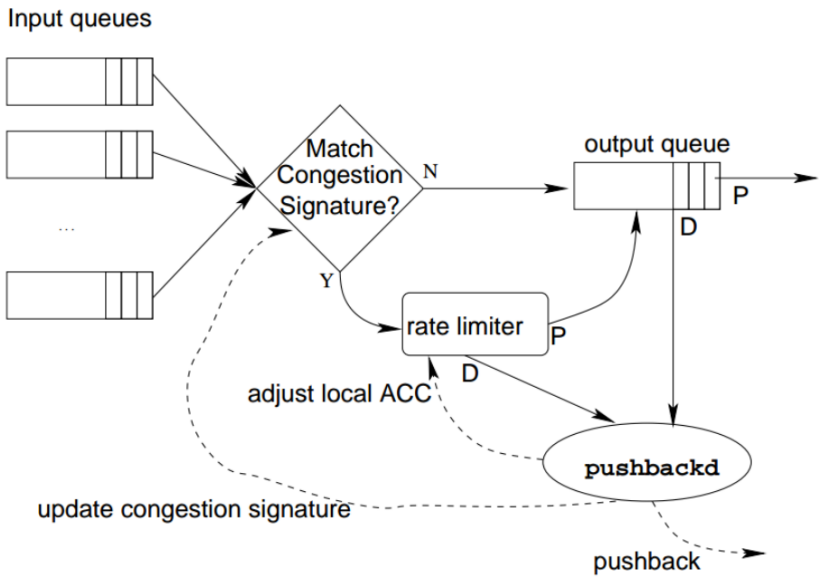
ب. یکی از رویکردهای مقابله با حملات منع سرویس، استفاده از رویکرد Push Back در مسیریاب‌ها است که در مقاله Ioannidis به بررسی و پیاده‌سازی این مکانیزم پرداخته شده است. معماری داخلی مسیریاب و نحوه به کارگیری این مکانیزم در شکل ۱ نشان داده شده است. با مطالعه و بررسی این مقاله به سوالات زیر پاسخ دهید.

i. چگونه مسیریاب، ترافیک مخرب را در طول یک حمله DDoS شناسایی و نرخ آن را محدود می‌کند؟ (فرآیند محدودیت نرخ را نیز توضیح دهید).

ii. چرا مکانیزم Push Back به جای اتکا به کنترل ازدحام مبتنی بر جریان‌ها[۳]، از کنترل ازدحام مبتنی بر تجمیع[۴] استفاده می‌کند؟

iii. بخش‌های مختلف پیام‌های درخواست، پاسخ و وضعیت Push Back را توضیح دهید.

[1] Key Distribution Center
[2] Realm
[3] Flow-Based Congestion Control
[4] Aggregation-Based Congestion Control



شکل ۱: معماری داخلی مسیریاب و به کار گیری مکانیزم Push Back

۵. در شکل ۲، ساختار شبکه‌ای یک شرکت خصوصی را نشان داده‌ایم که مهندس امنیتی این شرکت درصدد پیکربندی دیواره آتش است. نیازمندی‌هایی تعریف شده است که براساس آن‌ها می‌بایست ترافیک‌هایی از دیواره آتش عبور کنند. حال با توجه به نیازمندی‌های تعریف شده، قواعد خواسته شده را در دیواره آتش تعریف کنید.

(آ) اطمینان حاصل کنید که بخش فناوری اطلاعات می‌تواند درخواست‌های HTTP/HTTPS را ارسال کند.

(ب) قوانین ضد جعل مبدا را برای دپارتمان‌ها، DMZ و شبکه خارجی تعریف کنید. (یعنی یک گره نتواند بسته‌ای را با آدرس IP ای ارسال کند که در محدوده IP آن شبکه نیست.)

(ج) اطمینان حاصل کنید که درخواست‌های HTTPS از شبکه خارجی، فقط به وب‌سرور ناحیه DMZ هدایت شوند.

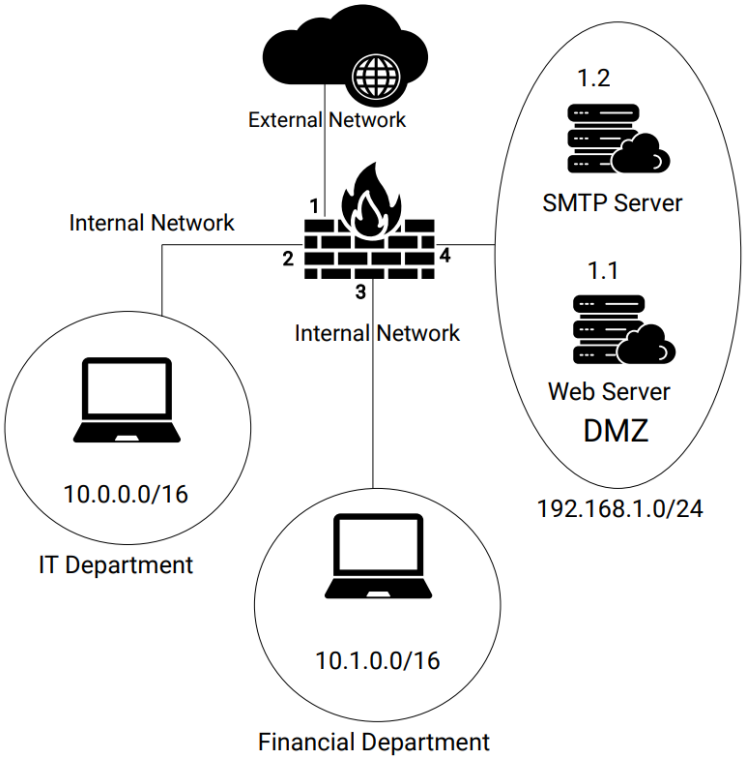
(د) پروتکل‌هایی مانند SSH، FTP، GOPHER و ... از سمت شبکه خارجی به DMZ باید مسدود باشند و تنها ترافیک وب و ایمیل فعال باشد.

(ه) امکان برقراری SSH را برای بخش فناوری اطلاعات فعال کنید تا محتوا و کد وب‌سرور را به‌طور ایمن مشاهده و به‌روزرسانی کند.

(و) اطمینان حاصل کنید که هر دو بخش فناوری اطلاعات و امور مالی می‌توانند ایمیل‌های خود را با استفاده از پروتکل امن IMAP دریافت کنند.

Flag	Protocol	DST Port	SRC Port	DST IP	SRC IP	Act	Int#
Any	Any	Any	Any	Any	Any	Block	Any
SYN	TCP	22	Any	192.168.1.1	10.1.0.0/16	Block	3, 4

جدول ۱: نمونه‌ای از قواعد تعریف شده در دیواره آتش



شکل ۲: شبکه فرضی شرکت

۶. دو عامل اول $p = 23, q = 11$ در الگوریتم RSA انتخاب شده است.

آ. کلید عمومی و خصوصی را با در نظر گرفتن $e = 3$ بدست آورید.

ب. پیام $m_1 = 4$ را امضا کنید.

ج. نشان دهید $\sigma_2 = 48$ امضای معتبر برای پیام $m_2 = 31$ است.

د. اگر σ_1 امضای m_1 باشد، آیا $\sigma_1 \times \sigma_2$ امضای معتبر برای $m_3 = 124$ است؟