بسمه تعالی

سوالات طرح شده از مقاله انتخابی درس امنیت شبکه

سینا دهقانیسان

برای اینکه هدف سوالات طرح شده واضح باشد و خواننده دید کلی نسبت به موضوع داشته باشد، ابتدا در ادامه خیلی مختصر موضوع مقاله را توضیح داده و سپس سوالات در ادامه خواهند آمد.

هدف اصلی این مقاله ارائه مدلی است تا در شبکه‌های نظیر به نظیر (P2P) حریم خصوصی حفظ شود. چراکه در این شبکه‌ها، با نظارت بر محتوایی که هر نظیر[1] دانلود می‌کنند و همچنین با آپلود کردن، محتوایی را در اختیار دیگران قرار می‌دهد، به علایق آن کاربر پی برد. برای روشن‌تر شدن موضوع شبکه‌ی اشتراک فایلی را در نظر بگیرید، مانند BitTorrent ، که هر نظیر علاوه بر دانلود محتوای مطلوب خودش، محتوایی که دارد را برای دیگر نظیرها آپلود کند. پس می‌توان با نظارت بر اینکه کاربر چه محتوایی را دانلود کرده و چه محتواهایی را آپلود می‌کند (که نشان از در اختیار داشتن آن فایل‌ها توسط آن کاربر است) به علایق کاربر پی برد.

پیشنهاد می‌کنم جهت آشنایی اجمالی با مکانیزم یک شبکه نظیر به نظیر، عکس زیر را که از متن مقاله انتخاب شده است، مشاهده کنید:

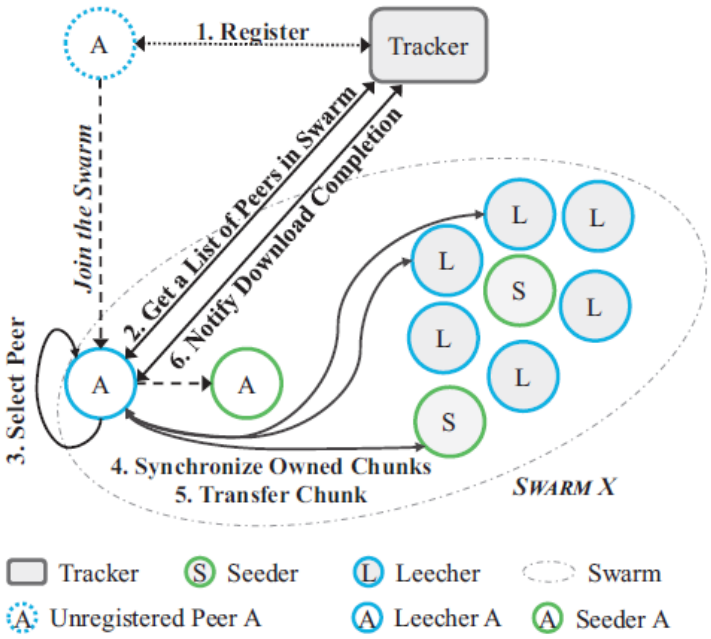

Fig. 2. Overview of the content download process on traditional P2P systems. First, peer A registers at the tracker to join the swarm of content X (swarm X). After registering, the peer starts as a leecher (still downloading) and requests from the tracker a list of peers (a subset) sharing that content. Until download completion, peer A selects peers from that list, synchronizes the chunks it owns with theirs, and transfers those available, if any, that it misses; the list of peers may be updated during content download. Upon download completion, peer A notifies the tracker to be known as a seeder.

[1] Peer

بسمه تعالی

سوالات طرح شده از مقاله انتخابی درس امنیت شبکه

سینا دهقانیسان

---

۱. راه حل‌هایی[۲] که در شبکه‌های نظیر به نظیر رایج، برای فراهم کردن حریم خصوصی استفاده می‌شوند، از چه تکنیک‌هایی استفاده می‌کنند؟

اکثر این راه حل‌ها از تکنیک‌هایی بهره می‌برند تا گمنامی (anonymity) یا انکارپذیری قابل قبولی (plausible deniability) را فراهم کنند. این راه‌حل‌ها همگی مصالحه‌ای[۳] بین کارایی و سطح حریم خصوصی دارند.

۲. دو مورد از روش‌هایی که گمنامی را فراهم می‌کنند، نام ببرید.

Onion routing و information slicing. این دو روش معمولا خیلی خوب گمنامی را فراهم می‌کنند اما کارایی[۴] کمتری دارند.

۳. دو مورد از روش‌هایی که انکارپذیری قابل قبولی را فراهم می‌کنند، نام ببرید و مختصرا توضیح دهید.

Request relaying: به این صورت عمل می‌کند که نظیرها درخواست‌ها را دست به دست می‌کنند تا مبدا و مقصد ارتباط مشخص نشود و یا حداقل نتوان با قطعیت مبدا و مقصد را تشخیص داد.

Content interest disguise: به این صورت است که نظیرها علاوه بر محتوای مطلوبشان، محتوای دیگری نیز دانلود می‌کنند تا علاقه‌ی اصلی آن‌ها مشخص نشود.

این دو روش ضعیف‌تر هستند اما کارایی بهتری دارند.

---

[۲] Solution

[۳] Trade-off

[۴] Performance

بسمه تعالی

سوالات طرح شده از مقاله انتخابی درس امنیت شبکه

سینا دهقانیسان

۴. چرا در شبکه‌های نظیر به نظیر حق نشر[۵] به وضوح نقض می‌شود؟

حق نشر به این دلیل نقض می‌شود زیرا یک نظیر پس از دریافت کامل تکه‌های[۶] یک فایل و تجمیع آن‌ها متوجه محتوای فایل شده. همچنین پس از دانلود، سریعا به tracker اطلاع داده می‌شود که این فایل در دسترس است و در نتیجه‌ی آن، فایلی که حق نشر دارد مجددا در شبکه توزیع می‌شود.

۵. یکی از اساسی‌ترین موادری که در ارتباط با نقض حق نشر در شبکه‌های نظیر به نظیر اتفاق می‌افتد چیست؟

یکی از رایج‌ترین و همچنین اساسی‌ترین مشکلاتی که در شبکه‌های نظیر به نظیر اتفاق می‌افتد این است که کاربر فایلی را دانلود می‌کند که حق نشر آن محفوظ است، اما نظیری که آن فایل را برای اولین بار در شبکه توزیع کرده، این حق نشر را نقض کرده است. در نتیجه کاربر ثانویه که آن فایل را دانلود کرده نیز ناخودآگاه و غیرارادی حق نشر را نقض می‌کند (در صورتی که شاید واقعا مایل به این کار نبوده باشد!).

۶. یک مدل بدگمان (Mistrustful) بر چه فرضی استوار است و مزیت چنین مدلی چیست؟

یک مدل بدگمان در شبکه‌های نظیر به نظیر برا این فرض استوار است که همه نظیرها در شبکه غیرقابل اعتماد هستند. در نتیجه، با این فرض، نظیرها نیازی به برقراری یک لینک قابل اعتماد (trustful) برای اشتراک‌گذاری محتوا ندارند و براحتی می‌توانند فرآیند اشتراک‌گذاری را آغاز کنند.

---

[۵] Copyright

[۶] Chunk

بسمه تعالی

سوالات طرح شده از مقاله انتخابی درس امنیت شبکه

سینا دهقانیسان

---

۷. در شبکه‌های توزیع محتوای نظیر به نظیر، هر کاربر در دو نقش می‌تواند در فرآیند اشتراک‌گذاری شرکت کند، آن‌ها را نام برده و توضیح دهید.

Seeder : نظیری که محتوایی را در اختیار دارد و می‌خواهد آن را به اشتراک بگذارد و نقض حریم خصوصی برایش اهمیتی ندارد.

Commoner : نظیری که فقط با تضمین اینکه حریم خصوصی‌اش حفظ می‌شود، در فرآیند اشتراک‌گذاری شرکت می‌کند.

۸. برای تامین حریم خصوصی، چگونه می‌توان از IP Address برای گروه‌بندی نظیرها استفاده کرد؟

می‌توان تعدادی از نظیرها که آدرس IP مشابهی دارند (بطور مثال کاربران یک ISP در یک محدوده IP دارند) را به عنوان یک نظیر در نظر گرفت، که به این کار IP address aggregation می‌گویند.

همچنین تعدادی از نظیرها که از یک آدرس IP استفاده می‌کنند (مثلا پشت NAT قرار گرفته‌اند) را با استفاده از ترکیب (IP, Port#) از هم تفکیک کرد، که به این کار IP address multiplexing می‌گویند.

۹. مکانیزم Request backoff چیست و چه عملکردی دارد؟

این مکانیزم مشخص کننده‌ی تاخیری است که بین درخواست‌های قطعه‌های مختلف یک فایل باید وجود داشته باشد. این تاخیر باعث می‌شود تا تعداد قطعاتی که در کمترین زمان ممکن دریافت می‌شوند، بیشینه شود.

۱۰. پیشامدهای مختلف request backoff چیست؟ (فرض کنیم که نظیر A، درخواست دهنده و نظیر B، تامین‌کننده درخواست است.)

Refusal : درخواست توسط B رد می‌شود چون نمی‌تواند آن را تامین کند.

بسمه تعالی

سوالات طرح شده از مقاله انتخابی درس امنیت شبکه

سینا دهقانیان

Cancellation : درخواست توسط A لغو می‌شود (به هر دلیلی نمی‌خواهد/نمی‌تواند فایل را دانلود کند.)

Acceptance : درخواست پذیرفته شده و از B به A منتقل می‌شود.

Interruption : درخواست پذیرفته شده و انتقال داده نیز شروع شده است، اما به دلیلی (مثلا مشکلات شبکه‌ای) انتقال داده قطع می‌شود.

Disposal : هیچ درخواستی مبادله نشده است.