



دانشگاه فردوسی مشهد



مبانی امنیت اطلاعات



تاریخ تحویل: ۱۴۰۳/۰۳/۱۶

Mini Project

دانشجویان محترم لطفا به نکته های زیر توجه کرده و آنها را رعایت کنید:

تحويل پروژه فقط از طریق سامانه آموزش مجازی دانشگاه (VU) امکان پذیر است.

از سورس کد های سایر گروه ها استفاده نکنید، در صورت اثبات کپی برداری -به هر دلیلی-، نمره تکلیف طرفین از ۱۰۰ نمره، **صفر (-۰-)** خواهد شد.

تحويل پروژه بعد از مهلت مشخص شده نمره ای نخواهد داشت.

فایل ارسالی حتما به صورت Zip بوده و نام گذاری فایل به صورت Fullname_Student.number_HWnumber.zip باشد.

"Evaluation, analysis and voting"



هدف:

این فاز پروژه شامل دو بخش اصلی است شامل ۱- ارزیابی، تحلیل و ایمن سازی ۲- رای گیری

شبکه های اجتماعی بزرگترین منابع اطلاعاتی جوامع بشری را دارا هستند به همین دلیل آن ها را به یکی از محبوب ترین گزینه ها در نظر مهاجمین برای دسترسی به اطلاعات افراد مبدل کرده است، تیم امنیت هر سازمان وظیفه تشخیص دارایی ها، ارزش آنها و آسیب پذیری ها را بر عهده دارد، پس از تشخیص آسیب پذیری می بایست متناسب با ارزش و نوع آن ها رویکرد مناسبی در برابر آن داشته باشد.

یکی از بخش هایی که امنیت ارتباطات و اطلاعات تاثیر به سزایی دارد با توجه به شرایط امروزه جامعه ما، انتخابات است. یکی از بزرگترین رویداد های تاثیرگذار در جامعه است که توسط دولت ها برگزار می گردد. همواره یکی از بزرگترین چالش های برگزاری این رویدادها برقراری امنیت آن می باشد که راه های گوناگونی برای آن ارائه شده است.





صورت پروژه:

همانطور که پیش تر گفته شد این بخش از پروژه شامل دو قسمت اصلی می باشد: ۱- ارزیابی، تحلیل و ایمن سازی ۲- رای گیری

۱ ارزیابی، تحلیل و ایمن سازی

این بخش در ادامه فاز نخست پروژه طرح شده است بدین صورت که شما به عنوان مسئول امنیت یک سامانه چت در گام نخست وظیفه بررسی دارایی ها، ارزش گذاری هر دارایی و همچنین تشخیص آسیب پذیری هایی که این سامانه امکان دارد متحمل شود را بر عهده دارید.

گام ۱: بررسی دارایی ها و ارزش گذاری

به منظور انجام این بخش مراحل زیر را طی کنید:

- **شناسایی دارایی ها:** فرآیند تعیین و فهرست بندی تمامی منابع و اجزای مهم سیستم که نیاز به حفاظت دارند.
- **ارزش گذاری دارایی ها:** ارزیابی و تعیین اهمیت و ارزش هر دارایی بر اساس تاثیر آن بر کسب و کار و عملکرد سیستم.
- **تشخیص آسیب پذیری ها:** شناسایی نقاط ضعف و نقص های موجود در سیستم که می توانند مورد سوءاستفاده قرار گیرند.
- **تحلیل آسیب پذیری ها:** ارزیابی و بررسی آسیب پذیری های شناسایی شده به منظور درک تاثیر و احتمال بهره برداری از آن ها و اولویت بندی برای اقدامات اصلاحی.
- **اقدامات لازم برای رفع آسیب پذیری:** پیاده سازی رویکرد های لازم برای مقابله با آسیب پذیری های تشخیص داده شده.

۲ رای گیری

گام ۱: شروع رای گیری

➤ **اعلان رای گیری:**

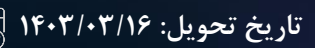
- مالک گروه پیغام "Voting" را با کلید خصوصی خود امضا کرده و بر روی کانال ارتباطی همگانی ارسال می کند.
- اعضا پس از دریافت پیام، پیغام "Voting ACK" را با کلید خصوصی خود امضا کرده و ارسال می کنند.

گام ۲: ارسال و انجام رای گیری

➤ **ارسال poll:**

- مالک گروه یک نظرسنجی (poll) چند گزینه ای را طراحی کرده و آن را با کلید خصوصی خود امضا می کند.
- نظرسنجی شامل سرتیفیکیت مالکیت گروه است که اعتبار مالک را تایید می کند





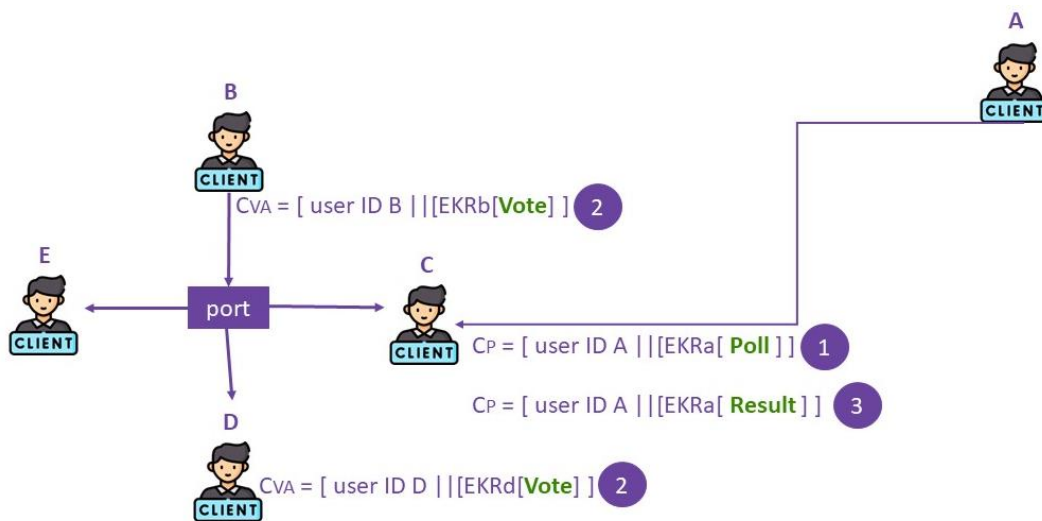
شکل ۱: شروع رای گیری



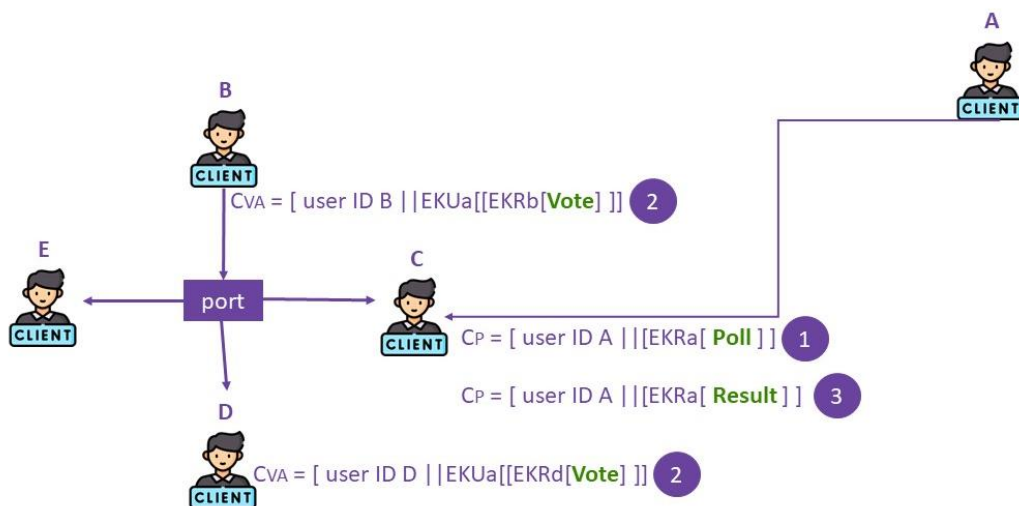


شروع رای گیری شامل مراحل زیر است:

- ❖ ارسال پیام "Voting" توسط مالک گروه
- ❖ ارسال پاسخ کاربران با پیام "Voting ACK"



شکل ۲: رای گیری شفاف



شکل ۳: رای گیری محرمانه





دانشگاه فردوسی مشهد



مبانی امنیت اطلاعات



تاریخ تحویل: ۱۴۰۳/۰۳/۱۶

نکات قابل توجه

- مهلت تحویل تکلیف، ساعت ۲۳:۵۹ روز شنبه مورخ ۱۴۰۳/۰۴/۱۶ می باشد.
- دانشجویان گرامی تا تاریخ مشخص شده فرصت دارند تا فایل های زیر را در سامانه مجازی درس در بخش **final project** آپلود نمایند.
- تهیه گزارش کتبی (مستندات) از فرآیند پیاده سازی و اجرا الزامی است.
- فایل های ارسالی شامل مستندات و کد های اجرایی می باشد.
- این تکلیف به صورت گروهی در قالب گروه های دو نفره تعریف شده و قابل انجام است و مشخصات اعضای گروه باید در مستندات ذکر شود.

چه عواملی باعث می شود از این فعالیت نمره کسب نکنید:

- عدم تحویل فایل ها در سامانه vu
- مشاهده شباهت بیش از حد معقول
- عدم تسلط به موضوع در جلسه ارائه

