دانشکده مهندسی کامپیوتر

روش‌های رسمی در مهندسی نرم‌افزار

تمرین سری اول

علی صداقی

۹۷۵۲۱۳۷۸

۱ سوال اول

نیازمندی‌های ضروری یک کانال ارتباطی بین دو Process و مشخص کردن ویژگی‌های Safety و Security:

برای پاسخ به این مسئله سه روش Inter Process Communication (IPC) یعنی Shared Memory، Message Passing و Socket را در نظر می‌گیریم. نیازمندی‌های مشترک این سه روش را ذکر می‌کنیم.

- Data transfer rate: برای ایجاد تبادل اطلاعات سریع
- Full duplexing: دو پردازه همزمان هم ارسال کنند هم دریافت
- Async / Sync: جلوگیری از بلاک شدن قسمت‌های دیگر، همگام سازی ارتباطی که نیازمند ترتیب زمانی است.
- Latency: تاخیر در ارسال پیام زیاد نباشد.
- Bandwidth: پردازه‌های زیادی بتوانند همزمان از کانال استفاده کنند و ظرفیت کانال پر نشود.

Safety properties: در این ویژگی‌ها سیستم نباید باعث خسارات جبران پذیر شود. اگر موارد زیر رعایت نشود ممکن است هزینه بسیاری متحمل شویم و فاجعه رخ دهد.

- Data integrity (end to end): اطلاعات در هنگام جابجایی تغییر نکنند. تغییر اطلاعات می‌تواند منجر به تصمیمات غلط شود که می‌تواند فجایعی به همراه داشته باشد.
- Data leaking avoidance: از بین رفتن اطلاعات در کاربردهای بحرانی می‌تواند منجر به فاجعه شود.

Security properties: تضمین امنیت داده، تعیین سطوح دسترسی و ... جزو این دسته هستند.

- Mutual exclusion: دو پردازه به طور همزمان به یک منبع دسترسی نداشته باشند.
- Data encryption: داده به صورت رمزنگاری شده در کانال عبور کند.
- Channel access: اطلاعات درون کانال قابل شنود نباشد.

۲ سوال دوم

Automatic Teller Machine (ATM) را می‌توان در دامنه کاربری بانک‌داری (Banking) در نظر گرفت.

Entities:

- Display
- Keyboard
- Card reader
- Cash dispenser
- Printer
- Customer
- Card
- Operator
- Bank
- Bank account (weak entity)

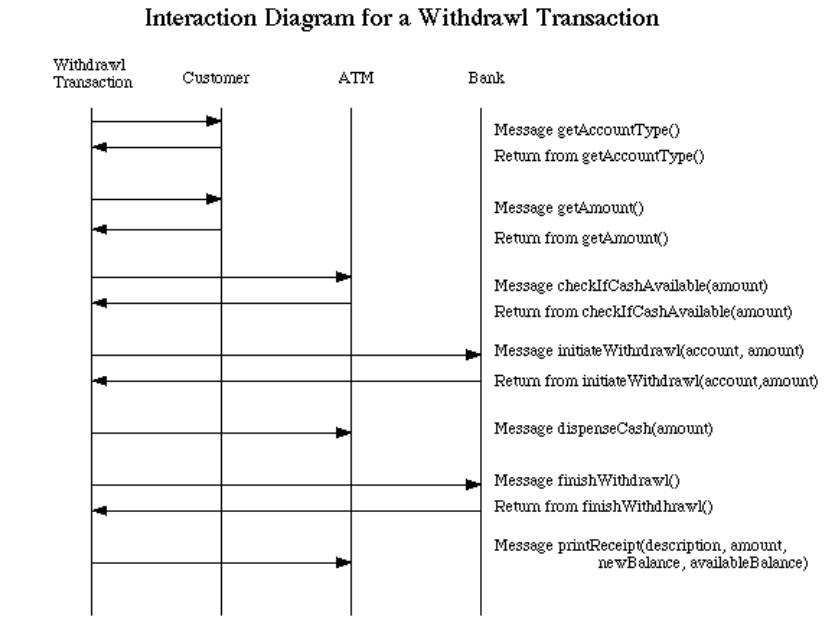
Events (Transactions):

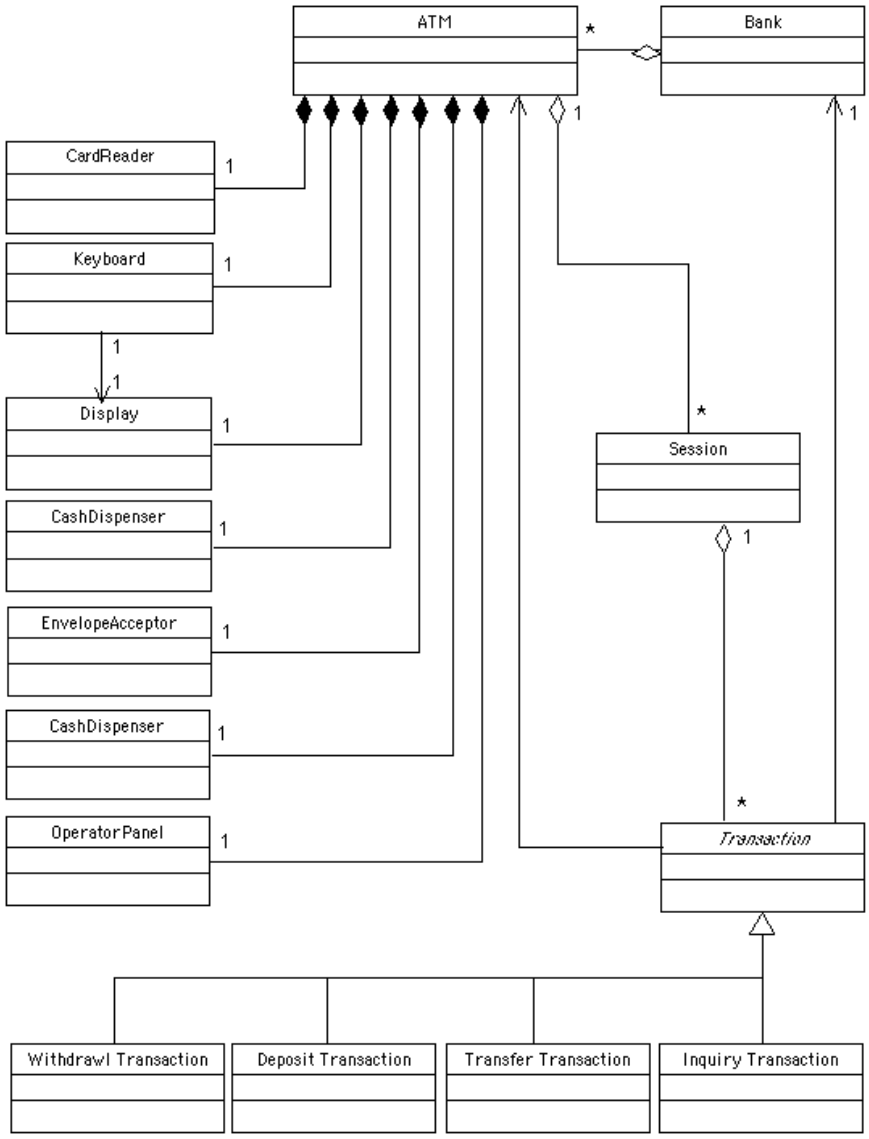
- Deposit
- Cash withdraw
- Transfer
- Balance inquiry

Properties:

- Card:
  - Card ID, Type, Bank
- Bank account:
  - First name, Last name, Creation date, Balance
- Transaction:
  - Time, ID
- Cash withdraw:
  - Amount
- Transfer:
  - Destination card, amount

Relationships:





ویژگی مهم امنیتی "ورود به اکانت" است که به وسیله کارت و رمز بانکی صورت می‌گیرد.

مورد دیگری که امنیت در آن مهم است "تراکنش" است. قبل از هر تراکنشی نیاز به احراز اصالت (Authentication) است. همچنین کلیه ارتباطات باید تحت شبکه و پروتکلی امن صورت گیرد.

با توجه به اینکه در ATM بحث مال و اموال انسان‌ها در میان است و این سیستم به نوعی Safety Critical است بایستی بسیاری از ویژگی‌ها و عملیات‌ها Verify شوند. برخی از این موارد شامل: ورود به اکانت با رمز و کارت، انجام صحیح تراکنش، Atomic بودن و ...

توصیف محیط: بدنه و سخت افزار دستگاه ATM که شامل صفحه نمایش، کیبورد و ... است. کاربر که از دستگاه استفاده می‌کند. پول نقد درون دستگاه، کاغذ رسید، دوربین امنیتی، بدنه محافظتی دستگاه و ...

محدودیت‌های نرم افزار به محیط:

کاربر (محیط) زمانی می‌تواند تراکنش انجام دهد که کارت داشته باشد.

کاربر (محیط) علاوه بر کارت (محیط) نیازمند رمز است.

تراکنش باید به صورت صحیح انجام شود تا به کاربر رسید داده شود.

تراکنش باید به صورت صحیح انجام شود تا به کاربر پول نقد داده شود.

محدودیت‌های محیط به نرم افزار:

دستگاه نیازمند پول (محیط) است تا کاربر بتواند برداشت وجه کند.

دستگاه نیازمند کاغذ (محیط) برای چاپ رسید است.

دستگاه نیازمند کیبورد (محیط) برای دریافت دستورات است.

کاربر نیازمند رسیدن نوبت برای استفاده از دستگاه است (صف ایستادن)

قسمت‌هایی که نیازمند صوری سازی (Formalization) هستند:

قسمت احراز اصالت و ورود به حساب با کارت و رمز باید به صورت فرمال بیان شود. در غیر این صورت ممکن است کاربری بدون کارت یا رمز وارد حساب شخص دیگر شود و ضرر مالی ایجاد کند. ویژگی ای که در این جا باید فرمال شود کارت بانکی و رمز است.

تمامی تراکنش‌ها شامل برداشت وجه، انتقال، موجودی و ... بایستی صوری سازی شوند. زیرا در غیر این صورت ممکن است کاربر پول خود را در تراکنشی که انجام نشده از دست دهد و ضرر مالی ببیند. یا حتی ممکن است برداشت وجه کند ولی از موجودی کم نشود و بانک ضرر ببیند. ویژگی که در این مورد باید فرمال شود موجودی کاربر است.

منابع:

Requirements for Example ATM System (gordon.edu)