به نام خدا

تمرین چهارم درس سیستم‌های نهفته بی‌درنگ

نیمسال دوم ۱۴۰۱-۱۴۰۲

سوال اول)

الف)

تعریف← well-formed مدلی است که دو حالت زیر را نداشته باشد:

۱- یک جواب unique نداشته باشد.

۲- جواب نداشته باشد.

حالا برای تمامی state ها بررسی میکنیم:

در وضعیت 1 یالی که به همین وضعیت بر میگردد ورودی 1 و 3 خروجی 2 می‌دهند.

*در وضعیت1 یالی که به سمت وضعیت2 می‌رود ورودی 2 خروجی2 می دهد و این یک مسیر درست است.

در وضعیت 2 یالی که به همین وضعیت بر میگردد ورودی 1 و 2 خروجی 3 می‌دهند.

**در وضعیت2 یالی که به سمت وضعیت3 می‌رود ورودی 3 خروجی3 می دهد و این یک مسیر درست است.

در وضعیت 3 یالی که به همین وضعیت بر میگردد ورودی 3 و 2 خروجی 1 می‌دهند.

***در وضعیت3 یالی که به سمت وضعیت1 می‌رود ورودی 1 خروجی1 می دهد و این یک مسیر درست است.

طبق * و ** و*** نتیجه میگیریم که این مدل یک مدل well-formed است.

ب)

حال مسیر پیدا شده در بخش قبل 1,2,3 بود را اجرا میکنیم:

2,3,1,2,3,1,2,3,1,2

ج)

با روش must/may انالیز میتوان گفت که این استیت ماشین constructive است زیرا بدون دانستن ورودی خروجی برای ما مشخص است.بطور مثال همواره خروجی از حالت 1 به باقی حالتها مقدار 2 است.

سوال دوم)

الف) root of trust :

برنامه ها و منابع سخت افزاری اغلب به عنوان قابل اعتماد یا غیرقابل اعتماد طبقه بندی می شوند. یک برنامه مورد اعتماد دارای امتیازات بیشتری است: توانایی تغییر مکان‌های حافظه خاص، دسترسی به دستگاه‌های ورودی/خروجی، و غیره. برنامه‌های غیرقابل اعتماد نیز مجاز به اجرای مستقیم برنامه‌های مورد اعتماد نیستند، در صورت امکان، ممکن است بتوانند سطح اعتماد بالاتری را برای خود به دست آورند و به برنامه غیرقابل اعتماد اجازه می‌دهند تا عملیاتی را انجام دهد که برای آن‌ها مجوز ندارد و مجوزی برای آن‌ها ندارد.
سیستم باید بتواند سطح اعتماد یک برنامه را قبل از دادن وضعیت قابل اعتماد به آن برنامه تعیین کند. می توان از امضای دیجیتالی برای برنامه استفاده کرد تا مشخص شود که از یک منبع قابل اعتماد آمده است. با این حال، کلید عمومی مورد استفاده برای بررسی امضای دیجیتال خود باید قابل اعتماد باشد و باید مطمئن باشیم که دشمن کلید عمومی را تغییر نداده است تا بتواند امضاها را جعل کند. قابل اعتماد بودن کلید عمومی مستلزم ارزیابی سطح اعتماد منبع آن است که پس از آن باید قابل اعتماد باشد.
در نهایت، ارزیابی اعتماد باید به ریشه ای از منبع اصلی نرم افزار قابل اعتماد در سیستم منجر شود. برای ایجاد root of trust می توان از چندین روش استفاده کرد. یک روش قرار دادن نرم افزار امضا شده و کلید عمومی مرتبط در سخت افزار غیرقابل تغییر است.

ب)Smart card :

کارت های هوشمند به طور گسترده ای برای تراکنش هایی که شامل پول یا سایر اطلاعات حساس است استفاده می شود. یک تراشه کارت هوشمند باید چندین محدودیت را برآورده کند:

باید ذخیره سازی ایمن برای اطلاعات فراهم کند. باید اجازه دهد برخی از آن اطلاعات تغییر کند. باید در سطوح انرژی بسیار پایین کار کند. و باید با هزینه بسیار کم ساخته شود.

CPU برای محاسبات به RAM دسترسی دارد اما از حافظه غیرفرار نیز استفاده می کند. یک رام ممکن است برای ذخیره کدی که قابل تغییر نیست استفاده شود. ممکن است کارت بخواهد برخی از داده‌ها یا برنامه‌ها را تغییر دهد و آن مقادیر را حتی در صورت عدم استفاده از برق حفظ کند. یک رام قابل برنامه ریزی با قابلیت پاک شدن الکتریکی (EEPROM) اغلب برای این حافظه غیرفرار به دلیل هزینه بسیار پایین آن استفاده می شود. مدار تخصصی استفاده می شود تا به CPU اجازه می دهد تا به EEPROM بنویسد تا اطمینان حاصل شود که سیگنال های نوشتن حتی در طول عملیات CPU پایدار هستند [Ugo86]. یک واحد رمزنگاری، همراه با یک کلید که ممکن است در ROM یا سایر حافظه های دائمی ذخیره شود، رمزگذاری و رمزگشایی را فراهم می کند.

ج)Trust Zone:

ARM TrustZone [ARM09] به ماشین‌ها اجازه می‌دهد تا با واحدهای زیادی طراحی شوند که می‌توانند در یکی از دو حالت عادی یا ایمن کار کنند. پردازنده‌های دارای TrustZone یک بیت وضعیت NS دارند که تعیین می‌کند در حالت امن یا عادی کار کند. گذرگاه‌ها، کنترل‌کننده‌های DMA و کنترل‌کننده‌های کش نیز می‌توانند در حالت امن کار کنند.

سوال سوم)

NWL: لایه NWK خدمات شبکه را ارائه می دهد. لایه NWK تعداد hop هایی را که یک فریم معین مجاز به حرکت است، محدود می کند. لایه NWK خدمات شبکه و لایه APL خدمات در سطح برنامه را ارائه می دهد.

لایه ZigBee NWK شبکه‌ها را تشکیل می‌دهد، ورود و خروج دستگاه‌ها را به شبکه و از شبکه مدیریت می‌کند و مسیریابی را مدیریت می‌کند. لایه NWK دو جزء اصلی دارد. نهاد داده لایه NWK (NLDE) خدمات انتقال داده را ارائه می دهد. نهاد مدیریت لایه NWK (NLME)

خدمات مدیریتی را ارائه می دهد. یک پایگاه اطلاعات شبکه (NIB) مجموعه ای از ثابت ها و ویژگی ها را در خود جای داده است. لایه NWK همچنین یک آدرس شبکه برای دستگاه تعریف می کند. لایه NWK سه نوع ارتباط را فراهم می کند: پخش، چندپخشی و یونیکست. یک پیام پخش توسط هر دستگاه در کانال پخش دریافت می شود. پیام های چندپخشی به مجموعه ای از دستگاه ها ارسال می شوند. یک پیام unicast، نوع پیش‌فرض ارتباط، به یک دستگاه ارسال می‌شود. دستگاه های موجود در یک شبکه ممکن است در توپولوژی های مختلف سازماندهی شوند. یک توپولوژی شبکه ممکن است تا حدی تعیین شود که توسط آن گره ها می توانند به طور فیزیکی با یکدیگر ارتباط برقرار کنند، اما توپولوژی ممکن است توسط عوامل دیگر دیکته شود. به طور کلی یک پیام ممکن است از طریق چندین پرش در شبکه به مقصد خود برسد. هماهنگ کننده یا روتر ZigBee یک فرآیند مسیریابی را برای تعیین مسیر از طریق شبکه ای که برای برقراری ارتباط با یک دستگاه استفاده می شود، انجام می دهد. انتخاب یک مسیر را می توان با عوامل متعددی هدایت کرد: تعداد پرش یا کیفیت پیوند. لایه NWK تعداد پرش هایی را که یک فریم مشخص مجاز به سفر است محدود می کند.

APL: لایه APL خدمات در سطح برنامه را ارائه می دهد. APS رابط خدماتی را از لایه NWK به اشیاء برنامه ارائه می دهد.

لایه ZigBee APL شامل یک چارچوب برنامه کاربردی، یک زیرلایه پشتیبانی برنامه (APS) و یک شی دستگاه ZigBee (ZDO) است. چندین شی برنامه ممکن است توسط چارچوب برنامه مدیریت شوند که هر کدام برای یک برنامه متفاوت است. APS رابط خدماتی را از لایه NWK به اشیاء برنامه ارائه می دهد. ZigBee Device Object رابط های اضافی بین APS و چارچوب برنامه فراهم می کند. ZigBee تعدادی پروفایل برنامه را تعریف می کند که یک برنامه خاص را تعریف می کند. شناسه برنامه توسط ZigBee Alliance صادر می شود. فایل برنامه کاربردی شامل مجموعه ای از توضیحات دستگاه است که ویژگی ها و وضعیت دستگاه را نشان می دهد. یکی از عناصر توضیحات دستگاه نیز به خوشه ای اشاره می کند که از مجموعه ای از ویژگی ها و دستورات تشکیل شده است.

سوال چهارم)