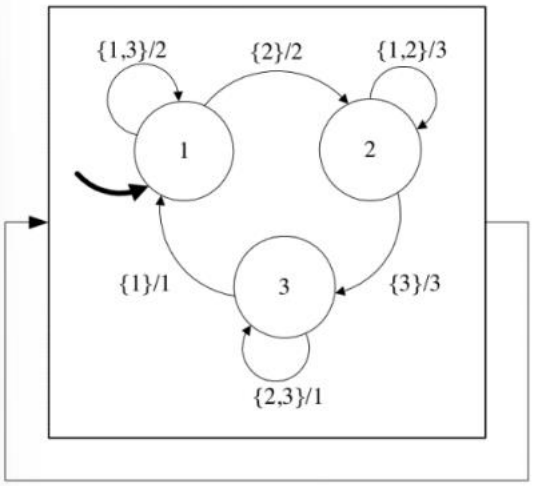
تمرین سری 4 امبدد

عرفان رفیعی اسکویی – 98243027

پارسا نوری – 98243067



سوال1)

الف) و ج) بله، ماشین خوش ساخت و برساختنی است به این دلیل که در هر state حتی اگر input ما unknown باشد، output ما مشخص است و در determined میباشد.

ب) نماد خروجی 10 واکنش اول به صورت زیر است:

(2,3,1,2,3,1,2,3,1,2)

سوال2)

Root of trust :

برنامه ها و منابع سخت افزاری اغلب به عنوان های قابل اعتماد یا غیر قابل اعتماد طبقه بندی می شوند.

قابل اعتماد یک برنامه با امتیازات بیشتری است: توانایی تغییر مکان‌های حافظه خاص، دسترسی به دستگاه‌های IO، و غیره.

برنامه‌های غیرقابل اعتماد اجازه ندارند مستقیماً برنامه‌های مورد اعتماد را اجرا کنند، اگر بتوانند، ممکن است بتوانند سطح بالاتری از اعتماد را برای خود به دست آورند که منجر میشود برنامه نامعتبر عملیاتی را انجام دهد که مجوز آن را ندارد.

سیستم باید بتواند سطح اعتماد یک برنامه را قبل از دادن وضعیت قابل اعتماد بودن یا نبودن به آن برنامه را تعیین کند. می توان از امضای دیجیتالی برای برنامه استفاده کرد تا مشخص شود که از یک منبع قابل اعتماد آمده است یا خیر. با این حال، public key مورد استفاده برای بررسی امضای دیجیتال برنامه، خود باید قابل اعتماد باشد و باید مطمئن باشیم که دشمن کلید عمومی را تغییر نداده است تا بتواند امضاها(signature) ها را جعل کند. قابل اعتماد بودن کلید عمومی مستلزم ارزیابی سطح اعتماد منبع آن است که حتما باید قابل اعتماد باشد.

در نهایت، ارزیابی اعتماد باید به ریشه ای از منبع اصلی نرم افزار قابل اعتماد در سیستم برگردد. که به این ریشه در اصطلاح root of trust میگوییم.

Smart card :

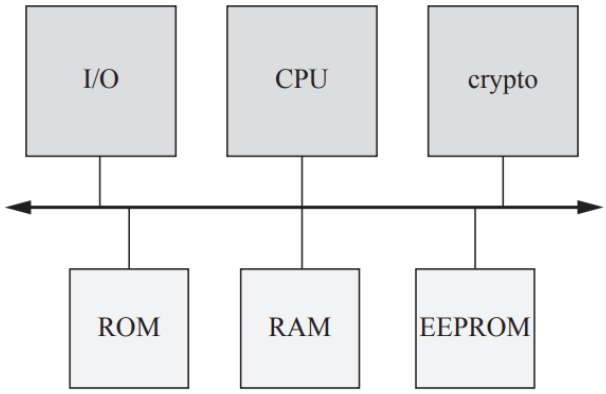
کارت های هوشمند به طور گسترده ای برای تراکنش هایی که شامل پول یا سایر اطلاعات حساس است استفاده می شود. یک تراشه کارت هوشمند باید چندین محدودیت را برآورده کند: باید ذخیره سازی ایمن برای اطلاعات فراهم کند.

باید اجازه دهد برخی از اطلاعات آن تغییر کند.

باید در سطوح انرژی بسیار پایین کار کند.

و باید با هزینه بسیار کم ساخته شود.

شکل زیر معماری یک کارت هوشمند معمولی [NXP14] را نشان می دهد:



تراشه کارت هوشمند است طراحی شده است تا فقط زمانی که یک منبع تغذیه خارجی اعمال می شود کار کند. واحد I/O به تراشه اجازه می دهد تا با یک ترمینال خارجی صحبت کند. هم می توان از کنتاکت های الکتریکی سنتی و هم ارتباطات غیر تماسی استفاده کرد.

CPU برای محاسبات به RAM دسترسی دارد اما از حافظه nonvlatile نیز استفاده می کند. یک ROM 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. برای این حافظه nonvolatile به دلیل هزینه بسیار پایین، از یک ROM قابل گرامر قابل پاک شدن الکتریکی (EEPROM) 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.

: TrustZone

ARM TrustZone [ARM09] به ماشین‌ها اجازه می‌دهد که طوری طراحی شوند که با تعداد unit های زیاد بتوانند در یکی از دو حالت عادی یا ایمن کار کنند. پردازنده‌های دارای TrustZone یک بیت وضعیت NS دارند که تعیین می‌کند در حالت secure یا normal کار کند. BUS ها، کنترل‌کننده‌های DMA و کنترل‌کننده‌های cache نیز می‌توانند در حالت امن کار کنند.

سوال3)

ZigBee defines two layers above the PHY and MAC layers:

The NWK layer provides network services and the APL layer provides application-level services.

The ZigBee NWK layer forms networks, manages the entry and exit of devices to and from the network, and manages routing. The NWK layer has two major components. The NWK Layer Data Entity (NLDE) provides data transfer services;

The NWK Layer Management Entity (NLME) provides management services. A Network Information Base (NIB) holds a set of constants and attributes. The NWK layer also defines a network address for the device.

The NWK layer provides three types of communication: broadcast, multicast, and unicast. A broadcast message is received by every device on the broadcast channel.

Multicast messages are sent to a set of devices. A unicast message, the default type of communication, is sent to a single device.

The devices in a network may be organized in many different topologies. A network topology may be determined in part by which nodes can physically communicate with each other but the topology may be dictated by other factors.

A message may, in general, travel through multiple hops in the network to its destination. A ZigBee coordinator or router performs a routing process to determine the route through a network used to communicate with a device. The choice of a route can be guided by several factors:

Number of hops or link quality. The NWK layer limits the number of hops that a given frame is allowed to travel.

The ZigBee APL layer includes an application framework, an application support sublayer (APS), and a ZigBee Device Object (ZDO). Several application objects may be managed by the application framework, each for a different application. The APS provides services interface from the NWK layer to the application objects. The ZigBee Device Object provides additional interfaces between APS and the application framework.