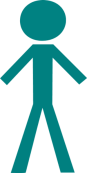
Availability:

استفاده از تاکتیک monitor:

فرد کارت خود را به دستگاه rfid reader می کشد( یا در دانشگاه حضور می یابد و موقعیت او از طریق GPS شناسایی می شود.) چون محیط در حال شلوغی است اطلاعات حضور ثبت نمی شود اما لوگ برداری می شود به طوری که فرایند ثبت بیش از 1 دقیقه طول نکشد.



محرک: عدم ثبت اطلاعات کارت (و یا موقعیت)

منبع تحریک: اطلاعات کارت (و یا موقعیت)

محیط: در حالت شلوغی

پاسخ: لوگ برداری شود

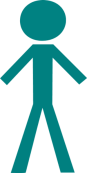
معیار پاسخ: نباید بیش از 1 دقیقه زمان ثبت طول بکشد تا در اطلاع رسانی مشکلی پیش نیاید

فراورده: فرایند ثبت حضور

شکل 1: کانکریت سناریو 1

استفاده از تاکتیک heart beat:

از دستگاه Rfid reader پیغام heartbeat نیامده است و محیط در حالت عادی است. به مسئول مربوطه خبر می دهیم و به سرویس ادامه می دهیم.



محرک: پاسخی از دستگاه نیاید

منبع تحریک: عنصر heart beat

محیط: در حالت عادی

پاسخ: به شخص بگوییم که از دستگاه دیگری استفاده کند. به مسئول مربوطه اطلاع دهیم.

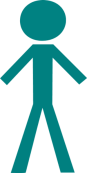
معیار پاسخ: اگر تا 3 بار جواب نیامد. اگر تا 20 ثانیه جواب نیامد.

فراورده: دستگاه rfid reader

شکل 2: کانکریت سناریو 2

استفاده از تاکتیک Condition Monitoring:

اطاعات کارت خوانده می شود ( کارت زده می شود) و یا فرد در مکان مورد نظر وارد می شود. جست و جو روی گروه ها صورت می گیرد اما گروهی پیدا نمی شود. محیط در حالت عادی است. به جای ثبت در جدول حضور از حضور log برداری می شود و به کار خود ادامه می دهد.



محرک: با توجه به اطلاعات دریافتی گروهی پیدا نشود

منبع تحریک: اطلاعات کارت (و یا موقعیت)

محیط: در حالت عادی

پاسخ: از حضور های بدون سرگروه لوگ برداری شود.

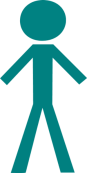
معیار پاسخ: نباید بیش از 10 دقیقه سیستم از کار بیافتد

فراورده: جدول حضور

شکل 3 : کانکریت سناریو3

استفاده از تاکتیک Passive Redundancy:

فردی در حال دیدن گروه ها است درخواست update ای نمی آید( یعنی صفحه به لود شدن ادامه می دهد). محیط در حالت عادی است و برای این که بیش از ده دقیقه در حال load شدن نباشیم به پایگاه داده کمکی وصل می شویم.



محرک: گروه ها هیچ حضوری را نشان ندهند

منبع تحریک: دیدن گروه ها

محیط: در حالت عادی

پاسخ: به پایگاه داده کمکی متصل شویم

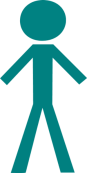
معیار پاسخ: نباید بیش از 10 دقیقه سیستم از کار بیافتد

فراورده: گروه ها

شکل 4: کانکریت سناریو 4

Degradation:

کارت زده می شود ( یا فرد در مکان وارد می شود و از طریق gps مکان یابی می شود) و اتصال به پایگاه داده ها برقرار نمی شود، محیط در حالت عادی است، حضورها را log بردادری می کنیم تا بیش از 1 دقیقه فرایند ثبت طول نکشد و به گروه ها آپدیت حضور را ارسال می کنیم تا با اتصال به پایگاه داده اطلاعات وارد شود.



محرک: اتصال به پایگاه داده برقرار نمی شود.

منبع تحریک: دریافت اطلاعات کارت (و یا موقعیت)

محیط: در حالت عادی

پاسخ: ابتدا حضورها را ارسال کنیم و حضورها را لاگ کنیم تا بعدا با اتصال پایگاه داده ذخیره کنیم.

معیار پاسخ: نباید بیش از 30 دقیقه سیستم از کار بیافتد

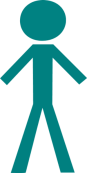
فراورده: پایگاه داده

شکل 5 : کانکریت سناریو 5

قابلیت تعامل

Orchestrate:

باید از یک ورک فلو با کنترل پیچیدگی ها کمک بگیریم چرا که ارتباط با سیستم دانشگاه چه در تایید هویت افراد در هنگام ثبت نام و چه در گرفتن اطلاعات درسی پیغام های پیچیده ای دارد.



محرک: نام و شماره دانشجویی یا شماره استاد و رمز ارسال می شود.

منبع تحریک: سیستم ما

محیط: سیستم ها از قبل شناسایی شده اند

پاسخ: سیستم دانشگاه اطلاعات را گرفته هویت فرد تایید یا رد می شود

معیار پاسخ: پردازش اطلاعات مبادله شده در 95 درصد مواقع درست است.

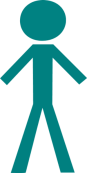
فراورده: سیستم دانشگاه

شکل 6 : کانکریت سناریو 6

قابلیت تغییر

Use an intermediary:

اگر برنامه نویسی بخواهد منبع داده ی جدیدی به سیستم اضافه کند(مثلا یک شبکه ی سنسور)، به مشکل بر می خورد. اگر واسطی تعریف کنیم که امکان گرفتن اطلاعات از منابع مختلف را فراهم کند و اجازه دهد بخش ورودی منابع از بخش تجزیه تحلیل جدا شود و بتوان منابع جدید داده را نیز اضافه کرد. همینطور برنامه نویس بخواهد یک بخش آموزشی به سیستم اضافه کند و نیازمند سیستم ذخیره سازی مانند google drive است. باید سرویس های ذخیره سازی را برایش تعریف کنیم تا بتواند از آن ها استفاده کند. همچنین امکان اضافه کردن نیز وجود داشته باشد.



محرک: افزودن ورودی های جدید ( مانند راه انداختن شبکه ی سنسور و گرفتن اطالات از آن ها)

منبع تحریک: برنامه نویس

محیط: در حال اجرا

پاسخ: با استفاده از یک intermediary تعریف شده از قبل تغییرات اعمال و تست می شود

معیار پاسخ: در 1 ماه

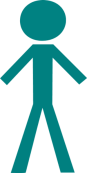
فراورده: آبجکت مربوط به گرفتن داده های ورودی برای سیستم پیشنهادات

شکل 7: کانکریت سناریو 7

تاکتیک های امنیت

Authenticate actors:

اگر گوشی های هوشمند اثر انگشت را پشتیبانی می کنند می توان برای بالا بردن امنیت از این روش نیز به صورت مکمل استفاده کرد. در دستگاه های rfid نیز می توان سخت افزار اثر انگشت را اضافه نمود.



محرک: می خواهد به عنوان استاد به سیستم وارد شود

منبع تحریک: یک دانشجو

محیط: سیستم آنلاین

پاسخ: باید اثر انگشت چک شود.

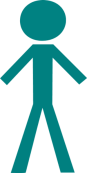
معیار پاسخ: جلوی تهدید گرفته می شود.

فراورده: سرویس هایی که فقط استاد می تواند استفاده کند

شکل 8: کانکریت سناریو 8

Encrypt data:

برای شناسایی افراد از سیستم دانشگاه باید در دو سمت از کلیدی برای رمزگشایی استفاده شود تا ارتباط امن بماند و هویت افراد تضمین شود.



محرک: میخواهد اطلاعات تشخیص هویت دریافتی به/از سیستم دانشگاه را دریافت کند

منبع تحریک: هکر

محیط: سیستم آنلاین

پاسخ: داده رد و بدل شده رمز نگاری شود

معیار پاسخ: اطلاعات محرمانه اساتید به خطر می افتد

فراورده: اینترفیس مربوط به دانشگاه

شکل 9: کانکریت سناریو 9