1. Checkout Scenario

Assumptions:
There are only few security personnels or store managers available to check for each station of the self-checkout system. Most payments made at the counter are through credit cards.

Assets:
- *Grocery items* - high price and grocery products that are sold in the Kroger
- *Credit card information* - credit card information stored on the magnetic stripe

Threats:
- *Removal of tags* - Items with high price tag are usually tagged with an RFID (Radio Frequency Identification) chip to prevent shoplifting. However, such embedded could be removed before being checked out. The monitor system could not detect such shoplifting, which causes losses to the grocery shop.
- *Skimming devices* - A skimming device might be placed at the payment devices similar to the one used in the article [http://krebsonsecurity.com/2011/04/atm-skimmers-hacking-the-cash-machine/]. Credit card information are gathered by the attackers.

Countermeasures:
- *Separate counters* - Setup a counter managed by employees, payment of all high price tagged items should be paid at the counter only. A close example would be the electronic device counter at Meijer. As for grocery products, an object recognition system, [https://www.youtube.com/watch?feature=player_embedded&v=L4VR2z2n5Ec], could be implemented to check whether there are still items not being scanned. Although with some false position alarm, the system in general could prevent shoplifting.
- *Warning messages and checks* - Employees should randomly check for suspicious skimming devices that are attached to ordinary device. A picture of original payment device should be placed next to the payment device. A warning message of avoiding credit card sniffing should be displayed to customers. A real world example would be one in Singapore, where an animated warning message is played every time a user tries to draw money from ATM.

2. NSA Scenario
Assumptions:
All employees of NSA and private contractors working for NSA have clearances.

Assets:
- *Documents* - Sensitive and classified documents, mostly digital which can be easily copied and transported.

Threats:
- *Leaks* - Next Snowden leaking sensitive information to outsiders

Countermeasures:
- *Two-Person Authorization* - For every private contractors, he/she will be paired with one employee from the NSA. A two-person rule will be applied. The rule required that anyone copying data from a secure network onto portable storage media does so with a second person who ensures he or she isn't also collecting unauthorized data. [http://www.forbes.com/sites/andygreenberg/2013/06/18/nsa-director-says-agency-implementing-two-person-rule-to-

stop-the-next-edward-snowden/] Cameras, recorders, mobile phones, and any other unauthorized storage devices should be forbidden and guarded against. Metal detectors at doors would detect violators. Radio frequency (RF) emissions should be monitored, and Faraday cages could be incorporated to block RF emissions. None of these techniques is expensive.

- *Log events and monitor* - The NSA should monitor how many documents one accesses and at what rate, and then detect and limit this. Decent real-time monitoring and automated response to events would have detected both events early on and could have prevented most of each breach. Unusual events would be flagged.
- *Prevent Removable Media from Leaving the Building* - The NSA could put each thumb drive inside a large steel box, or it could replace the standard USB connectors and those of the computers with custom-designed connectors that are difficult to duplicate.
- *Periodic Security Audits* - An outside security audit performed quarterly or annually would have found the NSA's problems and, perhaps, fixed them in time to stop Snowden. Such an audit is quite common and considered good practice.

3. Grading Scenario

Assumptions:

There is one homework set released to the class. Homework solution are typed in word or pdf form.

Assets:

- *Self written homework answers* - students work on the homework individually even for difficult problems.

Threats:

- *Copied homework answers* - students might search online for solutions or copy the solutions from another student in the class or another students from the previous term.

Countermeasures:

- *Cross reference with all students in the current enrollment* - Since in our assumption that all homework are written digitally in word or pdf format, a similarity scoring algorithm could be implemented to check the similarity of two homework answers. Even with a size of 100+ * 100+, it shouldn't take long to compare as most of the "stopping words" are removed. The similarity scoring function could be a distance of two multi-dimensional vectors. Each word in the answer is recorded with its frequency and each documents are essentially become an normalized matrix. Other similarity scoring functions can be implemented such as Locality-sensitive hashing, like those algorithms taught in EECS 485.
- *Separate homework for each discussion session* - Furthermore, two or more homework set with similar problem could be released to students with different discussion session. This prevents students in different sections copy each other. More interestingly, if two students plan to cheat for homework, they have to be in the same discussion session. The likelihood of getting caught using the similarity scoring function is even higher.
- *Encourage cheating for homework* - Cheating might not be bad overall. For a cyber security class or economic class teaching game theory, to know how to prevent cheating, one has to know how to cheat cleverly.
- *Spear and shield* - Professor could divide the assignments into two parts, first part is allow extensive and creative cheating methods to be applied to the homework. Whereas the

second part is to prevent students' own cheating methods. One of the cipher implementation project in EECS 475 class is a concrete example to this. Students are given bonus points to implement an extremely complicated crypto system, which most of students did without knowing the need to break their own cipher later. Most of the students collaborated to work on one complicated cipher and later encountering difficult tim to break one's own cipher. It was a great experience to create and break cipher.

4. Original Scenario

- The Courtyards student apartment, that is located on north campus, charges its residents $30 lockout charge after office hour.
- Such accident does occur frequently. It is most annoying for 1 bedroom and 2 bedroom floor plan residents because either they do not have a roommate or the roommates are unavailable to help them to gain access to the apartment.
- The door key is a magnetic stripe card instead of usual metal key.
- According the resident handbook of the Courtyards student apartment, there is no charge for lockout if it is caused by the malfunction of the magnetic card. All cards look identical to avoid being abused by others.
- The Courtyards student apartment does not have a database of residents' ID photos. Only name, ID (passport number, drivers license), birthday and cellphone number are recorded in their contract book. Because about 75% of the residents are international students. As a result, ID is rarely verified as individuals are not likely to remember one's passport number.
- All residents' large parcels or packages deliveries are kept on the floor in the main lease office. Anyone walking in or pass the office is able to acquire at least one other resident's basic information, including full name, contact number on the item tags, almost 71.4% (5 days out of 7 days) of the time.
- Assuming that more than 50% of the time, birthday is publicly viewable on Facebook.
- Assuming that each resident knows at least one other resident that's available in the Courtyards when he/she gets locked out.

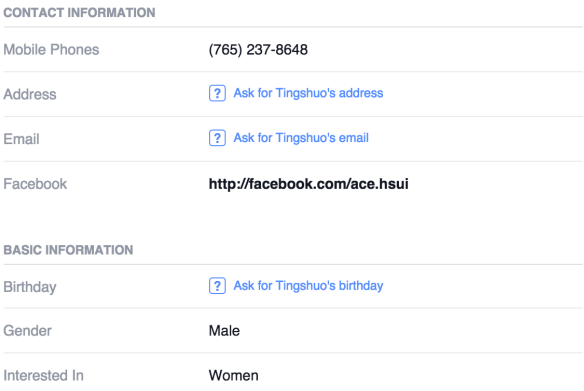
Assets:

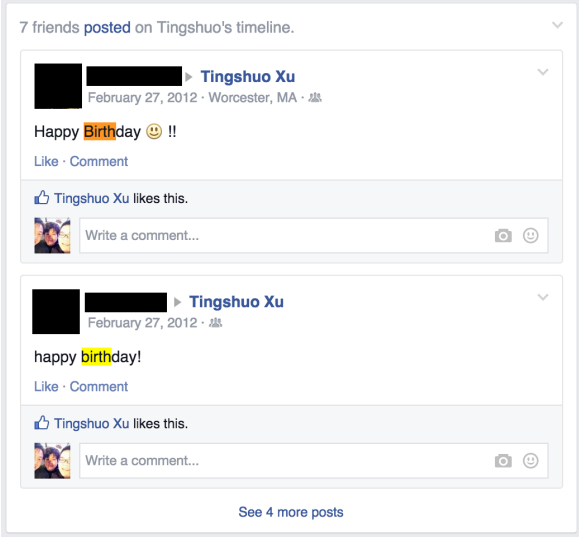
- Service charge - The $30 after office hour lockout charge.
- Unauthorized access - The unauthorized access right to at least one of the apartment.

Threats:

- Identical card - Suppose Alice, who stays in N331, gets locked out. She could borrow Bob's card and demagnetize the card with a fridge magnet. She calls the after office hour service number at the Courtyards. The person in charge will verify Alice's identity in the main office. Since Alice is the actual resident in N331, the person in charge will re-magnetize Bob's card with Alice's access information. Alice is able to gain her access back to her apartment with Bob's card. Alice return Bob's card. Then, right after Alice gained her way back to her apartment. Bob reports to the main office that his card is malfunctioning and demands a repair. Hence, Alice is able to gain her access back to her apartment while avoiding the $30 after office hour lockout charge. *This hack has been tested last time I got locked out >.< shhhhh…
- K-Anonymity - In extension to first threat, a random resident, victim, basic information - full name and cellphone number - can be easily obtained from the labels of package boxes. Furthermore, birthday information can be extracted from Facebook in many ways. A great segment of Facebook users makes their birthday publicly viewable. So, this is not difficult to get. Suppose, you are friends with the victim on Facebook, even if the victim does not make

day of birth viewable publicly, the attacker can deduct victim's birthday from friends messages posted on the wall, like the one attached. ** This has been authorized by Tingshuo Xu for this homework ONLY.**





Hence, theoretically, it is possible to bypass the verification details in the main lease office at the Courtyards student apartment to gain unauthorized access to victim's apartment. This attack is back traceable because of the CCTV in the office (remember to hack that first!). Furthermore, this attack can be extended further to any random attacker if the attacker finds the digital home lock system is implemented by Salflok and fake any magnetic stripe card to look like the one in this link [http://www.locktech.be/site/misc/Saflok_generic_keycards_b.jpg].

Countermeasures:

- Unique ID on the card - To prevent abuses after office hour service, charge $30 regardless the type of services. However, this could potentially increase the dissatisfaction of the residents as the service charges goes up. Instead, a single line of printing could change the situation. Since, there are only a few hundreds of residents in the apartment, a hashed alphanumeric string, like ones on the enterprise member card, printed on the card could help the person in charge in the office to verify each resident's identity.
- Photo ID in the database - To prevent the extended attack to the Courtyards student apartment is to create a new database with recent photo ID of all residents in it. Every time when the person in charge will check resident's photo against the person request for a key replacement or repair. So, in addition to the hashed string appear on the magnetic stripe card, real identity of the person is checked and verified against the photo ID in the database. We can not guarantee the database will never be hacked, but this will make the hack much harder.