**Name : Otmane Laaziz**

**ID : 1124860**

**University of Bridgeport**

The security of devices and databases is very important for every person in the planet. Keeping our data safe that means our secrets and information are not tampered by strangers. Now adays it is very hard to make that happen. It is a big challenge for people and companies. The big cooperations spend billions of dollars every year to keep their devices safe to keep their clients happy and loyal. Hackers use different ways and strong tools to break to an organization’s servers and break them down and get what they want. In the field of security, we don’t believe the word elimination of danger, but we use mitigation. The reason why we use that because we use different strategies and different techniques to make bad guys who hunt information to select wrong way rather the correct way. Hackers spend hours, days, and could be years for breaking to a database of a specific organization. That’s why people must learn to be as an attacker to defense their organization.

Researchers look for safety ways to keep people devices safe. Professor Mohammad S. Obaidat explained in his presentation a new technique in passwords security. They call it keystroke dynamics. As we know many people don’t know how to use correct and safety passwords. Sometimes they use their birthday, favorite team, favorite food, or common words to create their passwords. The missing part here that all this information is sealed online. You can buy many gigabytes of this information and you start doing an attack called brute force attack or birthday attack to break your victim’s password. Many websites follow some conditions to not let users select weak passwords and make the create a strong one. People who interact with many platforms and different websites, it become very hard from them to memories all those passwords. That’s why they select easy one to remember.

The study that Professor Mohammed Obaidat present it uses Android operating system-based touch screen for conducting their experiment. Keystroke dynamics very common way to authenticate to a system. The good thing about KSD that doesn’t need extra devices and that what makes her cheaper and not expensive to get it. This strategy uses a combination of timing, and the no timing features.

They study shows a good result and the level of mistakes are very low. For example, if we look to false acceptance rate is 0,3%, and the level of false rejection is 1.5%. Also, the level of equal rate of 0.9%. Based on this numbers we can tell that the study has an excellent feedback rate. This will help in the future in eliminating most of the issues that were common in the past about passwords. It will participate in keeping any organization safe and not to let strangers break to people’s data. Professor Mohammed Obaidat showed that the KSD authentication based on two important phases. The first one is collecting data from user and storing that in the database and the second one is the enrollment.

Enrollment is based on capturing phase, extraction, preprocessing extract features, and storing.

Authentication is based on enrollment, comparison process, and confirmation.

For me the KSD is a very good study. It will help and make users safe from hacking by bad guys. All these useful tools with knowledge will decrease the number of hacking and stealing data.