Good morning professors,

My name is Dan and this is my partner Huy, today we would like to present to you what we have been doing in the project named attack crawler for modern networked systems for 2 semesters

Our presentations is divided into many parts following this agenda

First of all – objectives are

+ Extract information of threads from the internet sources.

+Develop a crawler for collecting data of vulnerabilities

+Integrate the data into TTool

Timeline : Kỳ 1 : We studied and Model Stuxnet – SysML-Sec model

Kỳ 2 : Designed and implemented a client-server protocol for TTool and the crawler for exchanging information

Based on documents relating to stuxnet including w32 stuxnet dossier and Stuxnet under the microscope. We study deeply the behaviors of stuxnet and model it.

General – Execute – Inject Stuxnet to project files – Modify PLCs

SMB Microsoft server message block

To help TTool users and Crawler database exchange information. We designed and implemented a client-server protocol to connect them together. In addition, we also want to secure the exchanged information.

Because of that, we designed a clients-server protocol, this server is a multithread server, and the protocol us SSLsocket.

Message - Further, we also create a new structure name message which is a unified structure between client-server. Well talk about it in the next couple of slides

Protocol – How does it work ? – Blue lines – Request from users, red lines – Response from Server

Firstly, user select options from the search module interface ….

There are two type of message. Request message and answer message