ECE 544/644-Trustworthy Computing

Final Project –Topics and Guidelines

Goals: The goal of the final project is to pursue research in a specific narrow topic in trustworthy computing, learn how to write a good research proposal and improve your presentation skills. The project will be done in groups of **four students**.

Please be cognizant of the fact that this project includes more than surveying a topic. You need to propose a "semi-new" concept. Do not be afraid to dare, even if the proposed concept is not new, but you defend it well and layout a good plan, you will get the full credit. This is NOT a MS or PhD proposal in which the topic has to be entirely unexplored. We will emphasize in our grading the fact that you have written the proposal well, explained your goals, the literature is surveyed well (not comprehensive, but what you surveyed is done well) and the proposed concept is exposed clearly. It is highly important to correlate your ideas with the existing works by showing concrete citations. Any work that cogs well with the existing work will be given high value.

In this document we provide a list of suggested topics as well as guidelines for the proposal writing. **Please read the rest of the document carefully.**

We will provide more details on Phase I, Phase II, Phase III and the presentation.

1. Suggested Research Topics

Here is a list of suggested general topics which include applications of trustworthy computing as well as technology developments. You are welcome to pick your own topic.

1. Cyber security mitigation techniques for critical infrastructures such as banking and finance, communications, emergency services, energy, food chain, health, mass gatherings, transport and water (pick a specific industry segment)
2. Secure software distribution
3. Security in Emergency Situations (e.g. DIORAMA system)
4. Payment via Mobile Phones
5. Secure body sensor devices
6. Security in implantable devices

7. Secure healthcare web services
8. Secure Instant Messaging
9. Virtual Private Network for TCP and/or UDP packets using your own cryptographic code
10. Secure Wearable Device (e.g. Apple Watch, Android Watch)
11. Secure message distribution system in Green Buildings (e.g. computer energy managed building)
12. Secure power distribution systems
13. Secure Assistive Technology (e.g. PERCEPT)
14. Cyber forensics
15. Security in vehicular networks
16. Mobile evidence preservation and examination
17. Watermarking and intellectual property theft
18. Network traffic analysis, traceback and attribution
19. Network incidents response, investigation and evidence handling
20. Biometrics related to cyber security
21. Security for Internet of Things
22. Cloud security
23. Content Protection and Digital Rights Management
24. Security and privacy in Social Networks

Please use the IEEE Explore database through the UMASS library. It includes a vast repository of papers with a powerful search engine.

Phase 0: By October 2nd email the TA tao@ecs.umass.edu Please pick three topics as soon as possible since the topics will be given following first in first served policy. We will try to accommodate your first choice. We will post the topics for all groups by October 5th

Phase I: By October 14th submit through moodle a topic that you picked including a number of sentences (up to ½ page) that describe the topic as *well as a list of preliminary references (conference and journal papers, books, web sites, etc).*

ECE 644 students: include a detailed description of the system/application as detailed in the Appendix.

Phase II:

Each group will submit through moodle by November 11ths a preliminary report containing 6 pages that outlines your proposal along with sound background study needs to be submitted. The preliminary report should contain an abstract, specific aims, background and significance and proposed work.

Each group will have a 5-10 minutes presentation during class time on November 12th and November 17th (check the web site for your assigned slot).

ECE 644 students: implement a client-server architecture and submit it on Moodle (see details in the Appendix).

Phase III:

This is a final phase and each group will have a 15 minutes presentation outlining the improvement from the previous presentation and a comprehensive summary of your whole work. The presentations will take place December 3rd and December 8th (check the web for your assigned slot) and the final report is due on December 11th**.** The final report should be up to **15 pages.**

ECE664 students: we will have the final project review of the working demo on December 12th.

2. Proposal Format

The proposal will follow the NIH PHS 398 guidelines and includes the following sections:

1. Abstract
2. Specific Aims
3. Background and significance
4. Preliminary studies
5. Research design and methods
6. Implementation details or Test Bed
7. Literature cited

More description on each one of the sections.

Abstract

It should contain a summary of the whole work along with general motivation. It should also briefly discuss the advantages of your system.

Phase III: *One page is recommended.*

A. Specific Aims

List the broad, long-term objectives and the goal of the specific research proposed, e.g., create a novel design, solve a specific problem, challenge an existing paradigm or develop new technology.

Phase III: *One page is recommended*

B. Background and Significance

Briefly sketch the background leading to this proposal, critically evaluate existing knowledge. State concisely the importance of the research described in this proposal by relating the specific aims to the broad, long-term objectives. If the aims of the application are achieved, state how scientific knowledge will be advanced.

Phase III: *Three to five pages are recommended.*

C. Preliminary Studies

In this project our preliminary studies part will be minimal, unlike the “real” NIH applications (in “real: NIH applications this is the most important part that established the experience and competence of the investigator to pursue the proposed project). Describe here one or more papers that are the most similar to the proposed approach which you will provide in the next section.

Phase III: *Three to five pages are recommended.*

D. Research Design and Methods

Describe the research design conceptual framework, procedures, and analyses to be used to accomplish the specific aims of the project. Include how the data will be collected, analyzed, and interpreted. Describe any new methodology and its advantage over existing methodologies. Describe any novel concepts, approaches, tools, or technologies for the proposed studies. Discuss the potential difficulties and limitations of the proposed procedures and alternative approaches to achieve the aims.

Phase III: *Two to three pages are recommended.*

E. Implementation Details or Test Bed

You should come up with a system architecture or software design.

ECE544 students: implementation details of a “proof of concept” are mandatory, whereas the implementation is not.

ECE644 students: your project needs to include an implementation.

Implementation guidelines are presented in the Appendix.

Phase III: Two to three *pages are recommended.*

Appendix: Implementation Guidelines for ECE644

In this Appendix we introduce an example of a system/application along with its interfaces. This example will guide you how your chosen system/application should be developed for this project.

Example System/Application

DIORAMA is an electronic system that provides situational awareness during a disaster triage and evacuation process. The system was developed by 5G mobile evolution lab (for details see diorama.ecs.umass.edu). DIORAMA provides secure communication between the unit leader and responders in the field.

The following information is exchanged between the unit leader and the responders:

1. From the unit leader to responders
   a. Start rescue
   b. Stop rescue
2. From the responders to the unit leaders
   a. Acknowledgements to unit leader commands:
      i. Roger
      ii. Negative
   b. Location and priority of a victim found in the disaster site. The Priority which reflects the victim's severity of injury can be red, yellow, green or black.

The system is designed and implemented as **client –server architecture**. The server side program will be used by the unit leader and the client side will be used by the responder. Every message exchanged between the unit leader and the responder needs authentication and confidentiality services. We will choose a combination of security schemes and algorithms learned from the course to accomplish the required security services.

The system should implement the following interfaces and components:

- *sendCommand(command)*, which sends the encrypted command from the unit leader to the responders.
- *sendFeedback(acknowledgement),* which sends the encrypted acknowledgement from the responder to unit leader.
- *sendVictimInfo(location, priority),* which sends the encrypted information about victim location and priority.

For DIORAMA system we implemented security services as well as attack models.

Notes for your system/application:

1. You should describe your system in details, describe the information exchanged between the client and the server, describe the interfaces and components that you develop as well as the attack model and security services implemented
2. Deploy at least one client and one server. They can be setup on the same machine.
3. Provide a description of the proposed testing plan (attack case) and results. Put the attack program into your system, test your system with it and submit the output from your testing cases
4. You can use any programming languages. However, support will be provided only for Java/C#/Python.

Grading Policy

1. Program Listing
   works correctly ------------- 50%
   in-line documentation -------- 10%
2. Documentation
   quality of design and creativity ------------ 30%
3. Thoroughness of test cases ---------- 10%