POTENTIAL RESEARCH PROJECTS

I. Potential Project Topics

Students may select one of the pre-defined research topics or come up with their own idea. Depending on the topic, students may forge a team with two/three persons, or work individually (the scope will be adjusted accordingly).

A) Choose your own research project: This is great! Students are encouraged to propose their own original ideas. A well-prepared research project proposal is invaluable and evaluated very positively. Indeed, a self-proposed research project, if the proposal is accepted, may supersede the survey/scouting (because it will itself include a "related work section" for your idea) report and receive extra credits.

The main content of the proposal should include the following:

- A summary of the research problem you plan to study.
- Motivation of the proposed problem (i.e., why do you study this problem).
- Description of the technique(s) you plan to use to address the problem.
- Justification about why you believe you can solve the problem.
- Expected result and a plan for validation.
- A reference list with at least 5-10 relevant papers.
- The page limit for your proposal is 10 pages excluding references and well-marked appendix.

Remark: Students with original ideas will be given an extra week to submit their proposal provided that they contact with the instructor beforehand.

B) Select a pre-defined project: There are several interesting and challenging research projects with a great potential to create a real-life impact. Each of these projects may potentially turn into a MS thesis, seed a PhD thesis or at minimum good research papers.

Potential topics include but not limited (more will be described with slides) to the following:

Privacy-preserving Searches for Computing Clouds: Enabling searches on the encrypted data without decrypting it has countless applications including but not limited to privacy for "Big Data" applications. This project focuses on the implementation and evaluation of recent Searchable Encryption (SE) methods to enable privacy-preserving searches on computing clouds.

Evaluation of Encryption Methods for Medical Information Systems: Digital medical information systems store highly sensitive patient data, and it is legal requirement to keep it secure (e.g., via encryption). Recently, Chaos-based cryptosystems are recommended to encrypt medical images of patients or raw medical data by claiming high efficiency (i.e., encryption speed) as a differentiating factor over traditional encryption methods. This project questions these claims by investigating whether well-implemented standard encryption methods and stream-ciphers can outperform aforementioned methods.

Inter-car Security: Autonomous driving and smart-cities require that vehicles communicate with each other and city infrastructure (e.g., traffic lights, centers) in a secure, efficient and reliable manner. Especially, rapid authentication of messages exchanged among vehicles and infrastructures is a vital need.
This project focuses on the design and implementation of time-valid real-time authentication mechanisms for inter-vehicular networks.

**Intra-car Security:** Intra-car networks are comprised of internal vehicle components such as Electrical Control Units (ECUs), sensors, actuators and digital interfaces that exist in modern automobiles. Recently, several attacks have been discovered and successfully realized on intra-car networks. The objective of this project is to design and analyze efficient authentication and encryption methods to counter these attacks.

**Security Mechanisms for Internet-of-Things and Systems (IoTS):** Billions of heterogeneous devices and systems are being interconnected and cooperate to meet the ever growing demands of industry and consumers. These devices include low-end wireless sensors, mobile devices (e.g., smart-phone), automobiles (consider inter-vehicular networks as a part of IoTS) and also resourceful control centers. Scalable and efficient key exchange and distribution is an important need to provide security and privacy in IoTS. This project explores the recent self-certified key exchange methods and their implementations/evaluations.

**Node Replication Attacks in Wireless Sensor Networks (WSNs):** Secure routing and voting mechanisms in WNSs require that each sensor device has a unique identifier (ID) (e.g., each sensor has one vote right, or sensor A routes packages to only sensor B). Node replication attacks clone sensors in a wireless network to disrupt routing and voting mechanisms. For instance, after the replication of sensor A, it has more vote right than required and several packages will be artificially routed to sensor B (probably depleting the battery of sensor B). This project aims designing and simulating new security mechanisms to combat with node replication attacks via time-released cryptography.

**Digital Forensics and Secure Logging in Computer Systems:** Audit logs are an integral part of modern computer systems due to their forensic value. Protecting audit logs on a physically unprotected machine in hostile environments is a challenging task, especially in the presence of active adversaries (who compromise the device and recovers keys from it). This project investigates the feasibility of strengthening some existing compromise-resilient secure logging mechanisms via strongly unforgeable signatures.

**II. Format, Deliverables and (Tentative Grading)**

Each report for the research project must have a title page, main content, and references. The proposal should be single-column, 1 inch margins, 11-point size, and single-spaced.

The title page should include:

- the title of the paper
- group member name(s) and email address(es)
- course name, number, and instructor's name
- a maximum 300-word abstract
- three to five keywords.
There are two reports to be delivered for the research project (and three for self-proposed research ideas with extra-credits). One is interim report and another is final report. The evaluation of these reports are as follows (it is subject to change):

**Interim Report (%30 percent plus %2 extra point):**

The main content of the interim report should at least include the following:

- **Introduction**
  - (2 points) Discuss the background and motivation of your work.
  - (2 points) Summarize the research problem
  - (1 points) Summarize the proposed approach to the problem and the results

- **Related work**
  - (5 points) Discuss research related to yours and make comparison if there are closely related work.

- **Your approach (10 points)**
  - Describe your approach in detail. You may present your result in any way you want as long as you believe it's convincing and clear.

- **Progress on Implementation if it is implementation heavy (10 points)**

- **References**
  - (2 points) List all the citations referenced in your paper. You will lose 1 points for each dangling reference (i.e., the reference not cited in the main text).

**Final Report (%70 percent plus %10 percent extra point):**

- **Introduction**
  - (4 points) Discuss the background and motivation of your work.
  - (4 points) Summarize the research problem
  - (6 points) Summarize the proposed approach to the problem and the results

- **Related work**
  - (10 points) Discuss research related to yours and make comparison if there are closely related work.

- **Your approach**
  - (20 points) Describe your approach in detail. You may present your result in any way you want as long as you believe it's convincing and clear.

- **Validation and implementation (22 points)**
  - Prove or demonstrate the effectiveness and/or efficiency of your approach. You may do this through theorems, experiments, etc.

- **References (4 points):** List all the citations referenced in your paper. You will lose 1 points for each dangling reference (i.e., the reference not cited in the main text).

- **Bonus points**
  - (10 points) The instructor may give up to 10 points extra credit to well presented papers with original contributions.