Security Day

Security papers 2011/2012

Registration URL:-

https://docs.google.com/spreadsheet/viewform?formkey=dFBHVXR4QTFXQ1JMVE1zb0hYNEM1UkE6MQ#gid=0

Registration Deadline: 05-05-2012

Delivery Date: 28-05-2012

Description:

1- Each team must select one of the mentioned security topics below.
2- Each team minimum has (5) members and maximum (6) members.
3- Each team must present a paper as the format mentioned below.
4- Each team will make a presentation about the paper within 10 mins.
5- The best (5) papers & presentation simultaneously will take an honor certificates.
6- The best paper in each topic will be announced in a "THANK YOU" list.
7- All students will share in the evaluation.
8- All students must attend all presentations in his track.
9- All presentations will be presented in the same day. All presentations will be divided in two tracks. Each track will contain 10 topics.
10- In the delivery day you must deliver three hard copies of your paper.
11- Each paper will be evaluated from 3 examiners and then the average will be calculated. This average will be multiplied by a factor of students' evaluations,

Security topics:

1- Cloud computing security.
2- Wireless security.
3- Cellular network security.

Prof.Dr. Mohamed Hashem

T.A. (Mirvat El-Qutt – Heba Khaled - Eslam Gamal - Mohamed Saber – Yara Medhat – Ahmed Mahany)

4- Secure socket layer.
5- Transport Layer security
6- E-mail security.
7- Web security
8- IP security.
9- Elliptic curve security.
10- Trust management.
11- VANET management.
12- Ad-Hoc network management.
13- E-payment security.
14- Database security.
15- Intrusion detection systems.
16- Sensors and actuators security.
17- Wireless hacking tools.
18- Social networks security.
19- Web single sign-on systems.
20- Cybercrime.

Paper format:

1- Paper between (4-6) pages of size A4 arranged in two columns format.
2- The top of the first page must contain title security topic, team names, mails and name of university and faculty.
3- The header of all pages must contain the title of selected security topic.
4- The footer of all pages must contain course name and page number.
5- The paper must **AT LEAST** contain the following sections. You can add more sections as you like
    a. Abstract.
    b. Keywords.
    c. Introduction.
    d. Scientific Background.

Prof.Dr. Mohamed Hashem

T.A. (Mirvat El-Qutt – Heba Khaled - Eslam Gamal - Mohamed Saber – Yara Medhat – Ahmed Mahany)

e. Conclusion.
f. References.

6- Paper Font is times new roman. Title of your paper is font 24. Names, mails, university and faculty with size 16. Titles like (abstract, introduction…) with size 14 and normal text with size 12.

7- This is an example of the required paper format.

Untraceable RFID Tags via Insubvertible Encryption

Giuseppe Ateniese
The Johns Hopkins University
ateniese@cs.jhu.edu

Jan Camenisch
IBM Research
jca@zurich.ibm.com

Breno de Medeiros
Florida State University
breno@cs.fsu.edu

ABSTRACT

We introduce a new cryptographic primitive, called *insubvertible encryption*, that produces ciphertexts which can be randomized without the need of any key material. Unlike plain universal re-encryption schemes, insubvertible encryption prevents against adversarial exploitation of hidden channels, by including certificates proving that the ciphertext can only be decrypted by authorized parties.

The scheme can be applied to RFID tags, providing strong protection against tracing. This enables post-sale applications of manufacturer-issued RFID tags while preserving the privacy of consumers. The functionality required of the RFID tags is minimal, namely that they be re-writable (many-writable). No cryptographic capabilities are required of the tags themselves, as the readers perform all necessary computations.

Categories and Subject Descriptors: K.6.5 [**Security and Protection**]

General Terms: Algorithms, Security.

Keywords: Universal re-encryption, bilinear maps, RFID

since unlike the latter, they do not require precise reader-tag alignment, making inventory management more efficient. Similarly, the unit-specific feature of RFID tags allows for finer inventory control by, for instance, supporting automated verification of expiration dates.

On the other hand, RFID tags may pose a substantial issue to privacy by enabling distance tracking of specific product units beyond the point-of-sale. For instance, an RFID tag attached to a bottle of medicine or to food packaging would likely not be removed by the user—in fact, there may exist incentives for users to hold on to the RFIDs in the products they buy: One such instance, is that RFID tags could be used to enable more efficient product safety recalls. Over time, consumers might carry enough RFIDs on their body or belongings, and for long enough time, that the movements of each person could be tracked at a distance.

A separate reason for concern is that the "forward channel" of RFID readers can broadcast the value of tag contents several hundred feet away during the reading process. This exacerbates both concerns of individual privacy—a possible scenario would be an eavesdropper situated outside the customs hall in an airport—as well as corporate confidentiality