

# Curriculum Vitae

## Chin-Tser Huang

### CONTACT INFORMATION

Mailing address: 1300 S. Pleasant Valley Rd #128, Austin, TX 78741 USA  
Phone: (Home) (512) 383-9086  
(Office) (512) 471-9711  
Email: [chuang@cs.utexas.edu](mailto:chuang@cs.utexas.edu)  
Homepage: <http://www.cs.utexas.edu/users/chuang/>

### EDUCATION

- 1998 – present      **The University of Texas at Austin**, Austin, Texas  
Ph.D. candidate in Computer Sciences
- Expected graduation date: May 2003
  - Dissertation title:  
*Hop Integrity: Architectures and Protocols*
  - Advisor: Mohamed G. Gouda
  - GPA : 4.0 / 4.0
- 1996 – 1998      **The University of Texas at Austin**, Austin, Texas  
M.S.C.S. in Computer Sciences
- GPA : 4.0 / 4.0
- 1989 – 1993      **National Taiwan University**, Taipei, Taiwan  
B.S. in Computer Science and Information Engineering

### WORK EXPERIENCE

- 1998 – 2002      **The University of Texas at Austin**, Austin, Texas  
Research Assistant
- Network security protocol design and verification
- 1995 – 1996      **Institute of Information Science, Academia Sinica**, Taiwan  
Research Assistant
- Intelligent Chinese Information Retrieval System Design
- 1993 – 1995      Deployed Army, Taiwan  
Personnel Officer and Database Administrator
- Personnel database management

## RESEARCH INTERESTS

- Network Security
- Network Protocol Design and Verification
- Distributed Computing

## TEACHING EXPERIENCE

1997 – 2002

**The University of Texas at Austin**, Austin, Texas

Teaching Assistant in Department of Computer Sciences for courses:

- Communication Networks (graduate course CS386), Spring 1998, Spring 2000, and Spring 2002
- Computer Networks (undergraduate course CS356), Summer 1998, Fall 2000, Summer 2001, and Fall 2002
- Compilers (undergraduate course CS378), Summer 1998
- Foundations of Computer Sciences (undergraduate course CS307), Fall 1997
- Introduction to Computer Sciences (undergraduate course CS304), Summer 1997

## AWARDS AND HONORS

- 10/2002      Student travel fellowship, Luminy Seminar on Self-Stabilization, Marseille, France.
- 06/2001      Student fellowship, Graduate School, the University of Texas at Austin.
- 06/2000      Student fellowship, Graduate School, the University of Texas at Austin.

## PROFESSIONAL SERVICES

- Student Member, IEEE Computer Society.
- Student Member, Association for Computing Machinery.
- Referee, Journal of Information and Computation.
- Referee, the 8<sup>th</sup> International Conference on Network Protocols (ICNP 2000).
- Secretary to Program Chair, the 19<sup>th</sup> International Conference on Distributed Computing Systems (ICDCS 1999).
- Secretary to Program Chair, the 6<sup>th</sup> International Conference on Network Protocols (ICNP 1998).

## PUBLICATIONS

### JOURNAL PAPERS:

1. Chin-Tser Huang, Mohamed G. Gouda, E. N. Elnozahy, “Convergence of IPsec in Presence of Resets”, submitted to *Journal of High Speed Networks* for publication.
2. Mohamed G. Gouda, Chin-Tser Huang, “A Secure Address Resolution Protocol”, *Computer Networks*, Vol. 41, No. 1, January 2003.
3. Mohamed G. Gouda, E. N. Elnozahy, Chin-Tser Huang, Tommy M. McGuire, “Hop Integrity in Computer Networks”, *IEEE/ACM Transactions on Networking*, Vol. 10, No. 3, June 2002.

### CONFERENCE PAPERS:

4. Chin-Tser Huang, Mohamed G. Gouda, E. N. Elnozahy, “Convergence of IPsec in Presence of Resets”, to appear in *Proceedings of the 2<sup>nd</sup> International Workshop on Assurance in Distributed Systems and Networks*, May 2003.
5. Mohamed G. Gouda, Chin-Tser Huang, E. N. Elnozahy, “Key Trees and the Security of Interval Multicast”, *Proceedings of the 22<sup>nd</sup> International Conference on Distributed Computing Systems*, July 2002.
6. Chin-Tser Huang, E. N. Elnozahy, Mohamed G. Gouda, “Hop Integrity and the Security of Routing Protocols”, *Proceedings of the 3<sup>rd</sup> Annual IBM Austin Center for Advanced Studies Conference*, Austin, February 2002
7. Chin-Tser Huang, Mohamed G. Gouda, “An Anti-Replay Window Protocol with Controlled Shift”, *Proceedings of the 10<sup>th</sup> IEEE International Conference on Computer Communications and Networks*, Phoenix, October 2001.
8. Mohamed G. Gouda, Chin-Tser Huang, Anish Arora, “On the Security and Vulnerability of PING”, *Proceedings of the 5<sup>th</sup> Workshop on Self-stabilizing Systems*, Lisbon, Portugal, October 2001.
9. Mohamed G. Gouda, E. N. Elnozahy, Chin-Tser Huang, Eunjin Jung, “An Overview of Hop Integrity”, *Proceedings of the 2<sup>nd</sup> Annual IBM Austin Center for Advanced Studies Conference*, Austin, February 2001
10. Mohamed G. Gouda, E. N. Elnozahy, Chin-Tser Huang, Tommy M. McGuire, “Hop Integrity in Computer Networks”, *Proceedings of the 8<sup>th</sup> IEEE International Conference on Network Protocols*, Osaka, Japan, November 2000. (This paper was voted as the best paper in the conference.)
11. Mohamed G. Gouda, Chin-Tser Huang, Eric Li, “Anti-Replay Window Protocols for Secure IP”, *Proceedings of the 9<sup>th</sup> IEEE International Conference on Computer Communications and Networks*, Las Vegas, October 2000.

## INVITED TALKS

1. Chin-Tser Huang, Mohamed G. Gouda, E. N. Elnozahy, “Convergence of IPsec in Presence of Resets”, presented in Luminy Seminar on Self-Stabilization, Marseille, France, October 2002.
2. Mohamed G. Gouda, Chin-Tser Huang, “The Theorem of Convergence”, presented in Dagstuhl-Seminar 00431 on Self-Stabilization, Schloss Dagstuhl, Wadern, Germany, October 2000.

## REFERENCES

1. **Mohamed G. Gouda** (Ph.D. Dissertation Advisor)

Mike A. Myers Centennial Professor  
Department of Computer Sciences  
The University of Texas at Austin  
Phone: (Office) (512) 471-9532, (Fax) (512) 471-8885  
Email: [gouda@cs.utexas.edu](mailto:gouda@cs.utexas.edu)  
Address: Department of Computer Sciences  
The University of Texas at Austin  
Austin, TX 78712-1188 USA

2. **Simon S. Lam**

Professor and Regents Chair  
Department of Computer Sciences  
The University of Texas at Austin  
Phone: (Office) (512) 471-9531, (Fax) (512) 471-8885  
Email: [lam@cs.utexas.edu](mailto:lam@cs.utexas.edu)  
Address: Department of Computer Sciences  
The University of Texas at Austin  
Austin, TX 78712-1188 USA

3. **Aloysius K. Mok**

Quincy Lee Centennial Professor  
Department of Computer Sciences  
The University of Texas at Austin  
Phone: (Office) (512) 471-9542, (Fax) (512) 471-8885  
Email: [mok@cs.utexas.edu](mailto:mok@cs.utexas.edu)  
Address: Department of Computer Sciences  
The University of Texas at Austin  
Austin, TX 78712-1188 USA

## ABSTRACTS OF SELECTED PUBLICATIONS

### Convergence of IPsec in Presence of Resets

Chin-Tser Huang, Mohamed G. Gouda, E. N. Elnozahy

*Proceedings of the 2nd International Workshop on Assurance in Distributed Systems and Networks*, Providence, Rhode Island, May 2003

IPsec is the current security standard for the Internet Protocol IP. According to this standard, a selected computer pair  $(p, q)$  in the Internet can be designated a “security association”. This designation guarantees that all sent IP messages whose original source is computer  $p$  and whose ultimate destination is computer  $q$  cannot be replayed in the future (by an adversary between  $p$  and  $q$ ) and still be received by computer  $q$  as fresh messages from  $p$ . This guarantee is provided by adding increasing sequence numbers to all IP messages sent from  $p$  to  $q$ . Thus,  $p$  needs to always remember the sequence number of the last sent message, and  $q$  needs to always remember the sequence number of the last received message. Unfortunately, when computer  $p$  or  $q$  is reset these sequence numbers can be forgotten, and this leads to two bad possibilities: unbounded number of fresh messages from  $p$  can be discarded by  $q$ , and unbounded number of replayed messages can be accepted by  $q$ . In this paper, we propose two operations, “SAVE” and “FETCH”, to prevent these possibilities. The SAVE operation can be used to store the last sent sequence number in persistent memory of  $p$  once every  $K_p$  sent messages, and can be used to store the last received sequence number in persistent memory of  $q$  once every  $K_q$  received messages. The FETCH operation can be used to fetch the last stored sequence number for a computer when that computer wakes up after a reset. We show that the following three conditions hold when SAVE and FETCH are adopted in both  $p$  and  $q$ . First, when  $p$  is reset, at most  $2K_p$  sequence numbers will be lost but no fresh message sent from  $p$  to  $q$  will be discarded if no message reorder occurs. Second, when  $q$  is reset, the number of discarded fresh messages is bounded by  $2K_q$ . In either case, no replayed message will be accepted by  $q$ .

## **A Secure Address Resolution Protocol**

Mohamed G. Gouda, Chin-Tser Huang

*Computer Networks*, Vol. 41, No. 1, January 2003

We propose an architecture for securely resolving IP addresses into hardware addresses over an Ethernet. The proposed architecture consists of a secure server connected to the Ethernet and two protocols: an invite-accept protocol and a request-reply protocol. Each computer connected to the Ethernet can use the invite-accept protocol to periodically record its IP address and its hardware address in the database of the secure server. Each computer can later use the request-reply protocol to obtain the hardware address of any other computer connected to the Ethernet from the database of the secure server. These two protocols are designed to overcome the actions of any adversary that can lose sent messages, arbitrarily modify the fields of sent messages, and replay old messages. Finally, we argue that this architecture and its secure protocols can be used for securely discovering general resources on the Web.

## **Hop Integrity in Computer Networks**

Mohamed G. Gouda, E. N. Elnozahy, Chin-Tser Huang, Tommy M. McGuire

*IEEE/ACM Transactions on Networking*, Vol. 10, No. 3, June 2002; a preliminary version appeared in *Proceedings of the 8<sup>th</sup> IEEE International Conference on Network Protocols*, Osaka, Japan, November 2000

A computer network is said to provide hop integrity iff when any router  $p$  in the network receives a message  $m$  supposedly from an adjacent router  $q$ , then  $p$  can check that  $m$  was indeed sent by  $q$ , was not modified after it was sent, and was not a replay of an old message sent from  $q$  to  $p$ . In this paper, we describe three protocols that can be added to the routers in a computer network so that the network can provide hop integrity. These three protocols are a secret exchange protocol, a weak integrity protocol, and a strong integrity protocol. All three protocols are stateless, require small overhead, and do not constrain the network protocol in the routers in any way.

## **Key Trees and the Security of Multicast**

Mohamed G. Gouda, Chin-Tser Huang, E. N. Elnozahy

*Proceedings of the 22<sup>nd</sup> International Conference on Distributed Computing Systems, Vienna, Austria, July 2002*

A key tree is a distributed data structure of security keys that can be used in two ways by a group of users. First, any user in the group can use the group key in the key tree to securely broadcast data items to all other users in the group. The cost of each secure broadcast is one encryption. Second, the key tree can be maintained efficiently when a user leaves the group, or when a new user joins the group. The cost of maintaining a key tree when a user leaves or joins the group is  $O(\log n)$  encryptions, where  $n$  is the number of users in the group. In this paper, we describe a third use of key trees where any user in the group can use the different keys in the key tree to securely multicast data items to different subgroups within the group. We show that the cost of securely multicasting a data item to a subgroup whose users are “consecutive” is  $O(\log n)$  encryptions. We also show that the cost of securely multicasting a data item to an arbitrary subgroup is  $O(n/2)$  encryptions. However, this cost can be reduced to one encryption by introducing an additional key tree to the group. Finally, we present a calculus for identifying user subgroups in a group with multiple key trees.

## **An Anti-Replay Window Protocol with Controlled Shift**

Chin-Tser Huang, Mohamed G. Gouda

*Proceedings of the 10<sup>th</sup> IEEE International Conference on Computer Communications and Networks, Phoenix, October 2001*

The anti-replay window protocol is used to secure IP against an adversary that can insert (possibly replayed) messages in the message stream from a source computer to a destination computer in the Internet. In this paper, we discuss this important protocol and point out a potential problem faced by the protocol, in which severe reorder of messages can cause the protocol to discard a lot of good messages. We then introduce a controlled shift mechanism that can reduce the number of discarded good messages by sacrificing a relatively small number of messages. We use simulation to show that the modified protocol is more effective than the original protocol when a severe reorder of messages occurs. In particular, we show that the modified protocol reduces the number of discarded good messages by up to 70%.