RESUME

Richard E. Newman

CISE Department, CSE-E301, PO Box 116120
University of Florida
Gainesville, FL 32611-6120
352.392.1488 office/1220 fax/1200 secretary
http://www.cise.ufl.edu/ nemo

2016 NW 17th Lane
Gainesville, FL 32605
352.373.5191/2118 fax
nemo@cise.ufl.edu

Education:

- B.A. 5/81, Mathematics, New College, Sarasota, FL
- M.S. 5/83, Computer Science, University of Rochester, Rochester, NY
- Ph.D. 5/87, Computer Science, University of Rochester, Rochester, NY

Employment:

- Asst. Professor, UF, 8/86-present
- Consultant for Intellon Corp., Ocala, FL, 9/99-present
- Consultant for Raytheon Systems Company, St. Petersburg, FL, 5/98-8/98, 6/00-9/00
- Senior Scientist, UNISTRY Associates, Inc., 11/95-present
- Consultant for Xerox Corp. WRC, Webster, NY, 9/83-12/83
- Summer Intern, Xerox Corp. WRC, Webster, NY, 5/82-8/82, 5/83-8/83

Professional Memberships:
IEEE, IEEE-CS, ACM, ACM SIGSAC, ACM SIGCSE, ACM SIGACT, ACM SIGOPS, ACM SIGCOMM, ACM SIGOIS, NEA
Honors and awards:

- University Superior Accomplishment Award for Faculty Service, University of Florida, 1995-1996
- Superior Accomplishment Award, Academic Affairs, University of Florida, 1996.
- Teaching Improvement Program Award, College of Engineering, University of Florida, 1995.
- ACM Teacher of the Year, CISE Department, 1994-1995.
- Distinguished Service Key, Alpha Phi Omega National Service Fraternity, 1991.
- Faculty of the Year, CIS Department, 1989-1990.
- Member, Upsilon Pi Epsilon Computer Science Honorary Fraternity, 1989-present.

Recent Publications:

1. Jyh-haw Yeh, Randy Chow, and Richard Newman, "Key Generation and Safe Session Key Distribution for Interdomain Access Control," submitted to ACM Trans. on Information and Systems Security, 1999

2. Johnson, Theodore and R. E. Newman-Wolfe, "A Comparison of Fast and Low Overhead Distributed Priority Locks," Journal of Parallel and Distributed Computing

3. Lee, C. W., R. Chow and R. Newman, "A QoS Routing Model for Active Networks," Proc. 5th International Conference on Computer Science and Informatics, Washington, D.C., February, 2000.

4. Newman, R., M. V. Hoyt, T. Swanson, P. Broccard, M. Sanders and J. Winner, "Design of LAN-Lock, A System for Securing Wireless Networks," Proceedings of the Fifteenth Annual Computer Security Applications Conference, pp. 170-177, Phoenix, AZ, Dec. 6-10, 1999.

5. Jyh-haw Yeh, Randy Chow, and Richard Newman, "A Dynamic Interdomain Communication Path Setup in Active Network," Proceedings of the First International Working Conference on Active Networks, pp. 274-284, Berlin, Germany, June 30-July 2, 1999.

6. Newman, R., L. Dyson and O. Sabina, "Authentication and Key Exchange for Mobile Groupware Users," Proceedings of the SPIE Conference on Mathematics of Data/Image Coding, Compression, and Encryption, 3456, San Diego, CA, July 1998.

7. Yeh, S., R. Chow and R. Newman, "Key Assignment for Enforcing Access Control Policy Exceptions," Proceedings of the International Symposium on Internet Technology, pp. 54-59, Taipei, Taiwan, April 1998.

8. Eksioglu, O., R. Newman and R. Chow, "The Design and Implementation of Packet-Level Access Control Security Scheme (PASS)," Proceedings of the International Symposium on Internet Technology, pp. 266-271, Taipei, Taiwan, April 1998.

9. Newman, R. E., R. Chow and J. Lin, "Efficient Link Access Protocols for High Delay Shared Laser Links," Proceedings of the SOQUE International Symposium on Lasers, New Orleans, LA, December 1997.

10. Yeh, S., R. Chow and R. Newman, "Interdomain Access Control with Policy Routing," Proceedings of the 6th IEEE Workshop on Future Trends in Distributed Computing, pp. 46-52, Tunis, Tunisia, October 1997.

Recent Grants and Contracts:

- "Information Hiding," $ 85,000, PI, 8/10/01-5/31/02, NRL via ITT.
- "Interdomain Access Control Using IDPR & Active Network Technology," $ 197,400, Co-PI (PI Chow), 8/21/98-8/20/00, NSA.
- "A High Performance Algorithmics Laboratory," $1,236,350 (pending), Researcher (PI Sanguthevar), 8/1/00- 7/31/05, NSF.
- "Design and Implementation of Robust Micro-controller for Real-time Systems," $1,181,000, Co-PI, (PI Lee), 3/4/98-3/3/01, US Army.
- "TAMA Protocol Simulation Studies," $61,000, Co-PI (PI Latchman), 8/21/99-12/31/01, Intellon Corp.
- "Multilevel Secure Database System in an MSL Network," $47,000, PI, 8/16/00-8/8/01, Raytheon, Inc.
- "Integrated Process and Product Development," $63,000, PI, 8/16/97-8/8/01, Raytheon, Inc.
- "Protection of Naval Computers against Denial-of-Service Attacks," $60,000, PI, 1996-1998, ONR/UNISTRY Associates, Inc.

- “Enforcing Inter-Domain Access Control with IPv6,” $100,000, (co-PI, Chow PI), 1996-1998, NSA
- “High-speed Block Synchronization and Forward Error Correction,” $25,000, (PI), 1995-1996, SCTC/NASA/FAU
- “Virtual SERC: An Experiment in Enterprise Integration,” $31,000, 1995-1996, NSF.
- “A Distributed Group Decision Support Tool,” $18,000, 1995-1996, SERC.
- “Interdomain Authentication and Authorization for Large Information Systems,” with R. Chow, $50,000, 1995-1996, NSF.
- “Computer and Communication Network Security,” with R. Chow, $422,000, 1994-1997, US Army.
- “Space Communication Technology Center: Digital Signal Handling and Satellite Networking,” (PI of University of Florida portion of $5,000,000 NASA Center for Commercial Development of Space, with co-PIs S. Miller, H. Latchman, R. Chow, R. Shrestha), $1,102,000, 1991-1997, NASA.

Brief Descriptions of Selected Projects:

- Information Hiding
  For over a decade I have been investigating various aspects of information hiding. Facets of this area include Traffic Analysis Prevention (TAP), which was my starting point with Balaji Venkatraman. At first, we and others (including Dr. Latchman and others working on a project sponsored by BellSouth) were studying LAN and WAN traffic, trying to model it using traces from the UF College of Engineering backbone and other points. Soon Balaji and I became interested in new methods of preventing traffic analsis, and eventually culminated in analysis of network covert channels. More recently, I have been working with Drs. Ira Moskowitz and Li-Wu Chang of the Naval Research Laboratory on information theoretic aspects of steganography, and with Dr. Paul Syverson of NRL on information theoretic aspects of TAP.
- WAN Security
  With Dr. Randy Chow and several graduate students over the past several years, I have considered problems in providing for secured access between processes in different administrative domains. Some of the issues that arise include policy routing, key distribution, identification and authentication, authorization, policy mapping, connection acceptance and establishment, in addition to the usual issues of cryptographic protection of the communications between the processes. We have also investigated the use of Active Networks for discovery and prevention of spoofing and other types of network attacks. One of my first doctoral students, Steve Greenwald, worked with me on the definition of a security model for limited sharing of resources in a multiple AD environment (the DisCom model).
- Distributed Systems
  I have investigated a number of issues in this area from distributed locks and performance (with Theodore Johnson) to reliable multicast and garbage collection, distributed databases and consistency for groupware systems that is somewhat weaker than the transaction-based consistency typical of distributed databases. With a few graduate students over the years, we have implemented systems for fault-tolerant site servers (sharing the same LAN and network file system) with remote clients (where the largest costs are in sending messages between the client and the server site rather than sending them within the server site), and for fault tolerant distributed services, where the servers are in fact site servers and there are high costs

for sending messages between sites. The main problem in the latter environment is obtaining useful failure information, and we devised a protocol that uses heartbeats and counter machines to give each host perceived state information about other hosts that could then be used to drive group membership and multicast configuration information. With others, I developed and analyzed a protocol for identification and strong mutual authentication between mobile users and servers when the users do not carry memory with them (other than the usual names and password one could expect).

- LAN security
  Several projects with Raytheon Systems Company have focussed on securing LANs in various ways. Our first projects considered wireless LANs (the RayLink product was their business motivation), and I supervised an undergraduate team that used the Layered Service Provider (LSP) available for WinSock2 to introduce PCMCIA hardware-based cryptographic mechanisms (Fortezza cards with X.509 certificates and Fortezza encryption) for establishing private communications first between a pair of laptops, then between laptops and a wired network through an access point and a guard. In order to minimize the impact on off-the-shelf applications, we had to provide for some external initialization of the smart card as well as key distribution, etc. A particularly sticky point was handling communications between hosts without Fortezza hardware on the wired LAN and laptops on the WLAN through the guard without disrupting communication connections. The two more recent projects with them have centered around developing a system for database-driven network vulnerability assessment, and currently, enforcement of multilevel secure (MLS) policies in a multiple single level (MSL) environment, using a COTS DBMS and PKIX.

- Intrusion Detection Systems
  I have worked in the area of detection of denial-of-service (DoS) attacks as well as system resource availability monitoring for several years now. Part of this work was done with UNISTRY Associates, Inc. on an architecture for detection, coordination, and response to resource outages perceived or incipient. This system has layered defense to detect both misuse and anomalies in the network event stream and in the system event stream. It also monitors resource availability to catch nonmalicious loss as well as otherwise undetected attacks. Coordinators may create static or dynamic detectors and monitors, and may execute responses in real time. Policy is enunciated by a single configuration file formed as a rule base, depending on an extended event set and conditions. Complex detection (e.g. temporal correlation) is carried out by a net of intermediate detectors. The system is extensible and distributed.

- Satellite Communications
  Several years ago Dr. Chow and I worked over an extended period of time on a host of problems associated with directional point-to-point links in a somewhat predictable dynamic environment (satellites with laser crosslinks). Some of our aims in the system were to develop robust topology selection and routing algorithms (the laser transceivers could be redirected to form a changing topology, but both ends would have to point at each other long enough to acquire each other in order to establish the link – this poses particularly interesting problems when the network is partitioned, which I solved in both theoretical and practical ways). With two master's students, we designed, verified, and implemented successfully the node control software used with experimental, high-speed laser links built by ThermoTrax in San Diego, CA. The system was delivered to Rome Labs. In addition to the wide range of interesting problems we encountered and solved in that project, I also worked as the Associated Director of the NASA Center for Space Communication Technology. The main focus of the SCTC was on high quality video compression and transmission over Ka band satellite links. I headed a team at UF that performed some measurements on Ka band links using the ACTS satellite (we did some modeling of the error arrival process to establish its qualities of burstiness or not), devised

efficient forward error correction (FEC) techniques combined with block synchronization that could withstand very long burst errors.

- Protocols for Powerline Data Transmission
  I have been consulting with Intellon Corporation, which is a leader in CEBus technology (low-speed data transmission for home automation over the home power lines) that is moving into the area of LAN speed data transmission over home power lines (PowerPacket is the trademarked name). The UF team analyzed and simulated various medium access control methods (with physical parameters that seemed to change on a weekly basis) to determine the best way for nodes to compete for access. We had to consider collision probabilities and costs of collisions (when no reliable collision detection is available) along with expected delay for attempted channel access under two competing access schemes, each with a large number of parameters. We compared the channel data rates and access latencies to other LANs, and then obtained delivery latency distributions to determine packet loss rates for multimedia traffic of various types. Then we devised means of providing controlled access for multimedia streams, and determined the residual capacity in the network for bursty data under various traffic pattern scenarios. I also worked with them on the issues and specification for system security, since the powerline network traffic may be visible to more than one residence. Finally, we considered various backoff schemes, first finding the optimal number of slots for a given number of contenders, then simulating various ways for nodes to back off under observed network loads (not just when a node suffers a collision, for instance). The chipset for this system is shipping now, and we are beginning work on another system that I can't talk about further.

- Groupware/Middleware
  A pet project over the past decade has been UF-DCS, for Distributed Conferencing System. Early on, a few graduate students and I devised some groupware applications (Ensemble, an object-oriented concurrent graphics editor, and MACE, a fine-grained, concurrent text editor) and incorporated them into DCS.v1. With some experience using DCS.v1, and in my goal of extending the system to handle the problems encountered in WANs, we started DCS.v2. This effort has focussed more on the infrastructure and less on groupware applications per se. In it, we have developed a collection of services we believe are needed to support persistent groups of collaborators over a WAN. These include reliable database services (our consistency requirements are less than typical databases due to the lack of transactions and the way we manage changes), authentication and secure communications, access control services, conference control services, application management, notification services, and decision support services. The last one is less a necessity and more of a philosophical inclusion in the system, following from the principles of DCS.v1 that the users of the group should be able to specify how their group worked in terms of actions that affected the group, and that a wide range of policies should be supported by the system. In short, the access control services do not permit a requested action to be taken without calling a group-modifiable decision procedure. In many cases, this is just a rubber stamp "yes," but in many cases, it requires a vote of some subset of the group membership, either on-line or off-line. Going from the hardwired but parametrized version of this in v1 to the more general approach of v2 has been challenging, and I believe it represents a different paradigm for resource allocation and for access control.