Networking/Security Research
Faculty

- James C. Browne
- Mohamed Gouda
- Simon S. Lam
- Al Mok
- Lorenzo Alvisi
- Mike Dahlin
- Greg Plaxton
- Harrick Vin
We also collaborate with

- Gustavo de Veciana (ECE)
- Vijay Garg (ECE)
- Adnan Aziz (ECE)
- San-Qi Li (ECE/Santera Systems, Dallas)
- Andrew Whinston (Business School)
- Prabhudev Konana (Business School)
- Mootaz Elnozahy (IBM, Austin)
- Nishanth Sastry (IBM, Boston)
- Chung Kei Wong (Inktomi, CA)
- Thomas Woo (Bell Labs)
- Krishan Sabnani (Bell Labs)
- Ray Miller (Univ. Maryland)
- Nancy Lynch (MIT)
- Nick Maxemchuk (Columbia U.)
- Ken Calvert (Univ. Kentucky)
- Richard Yang (Yale Univ.)
- Anish Arora (Ohio State U.)
- Jorge Cobb (UT-Dallas)
- Ted Herman (Univ. of Iowa)
- David Yau (Purdue Univ.)
- Udaya Shankar (Univ. Maryland)
- Carl Gunter (Univ. Penn.)
- . . .
Current Research Interests

- Mohamed Gouda
  - network security services
  - self-stabilizing protocols

- Simon S. Lam
  - network security services
  - Internet congestion control
  - protocol design for dynamic P2P networks
Network Security Services (Lam, Gouda)

- scalable and reliable group key management (Keystone)
  - key graph/tree idea
- efficient signing and verifying for lossy packet flows (Flowsign)
- digital signature algorithm (eFFS)
  - fast signing and verifying
  - adaptive, incremental verification

*Issues of efficiency, scalability, and latency in addition to authenticity, confidentiality, integrity, ...*
Internet Congestion Control (Lam)

- TCP-friendly congestion control for streaming media

- a theory of window-based unicast congestion control
  - CYRF family of algorithms guaranteed to converge to fairness and efficiency
  - analysis of throughput, TCP-friendliness, transient behavior
Protocol Design for Dynamic P2P Networks (Lam)

- optimal distribution tree for Internet streaming media
  - distributed algorithm
  - congestion controlled streaming media
  - bandwidth measurement protocols

- other topics in progress
Model Checking for Security of Software Systems (Browne)

- Integrated model checking for information flow, self-stabilization, safety, and liveness properties

- Current research on integration of model checking extended to component-based development of software systems
Real-Time Virtual Resource as Temporal Firewall (Mok)

- RTVS (Real-Time Virtual Resource) is a resource abstraction that supports the composition of applications with timeliness properties when multiple applications share a resource in an open system environment.
- By decoupling timeliness properties from resource sharing policies, RTVS sets up a temporal firewall between applications.
TINMAN – an Architecture for Assuring Resource Bound Security (Mok)

- Resource usage prediction by source code analysis
- Resource usage certification by theorem proving
- Runtime monitoring by automated event insertion

⇒ 100% coverage

“Check the verifiable & monitor the unverifiable”