Contact Information

- **Instructor:** Dr. Gabriel Ghinita
  - **Email:** Gabriel.Ghinita@umb.edu (preferred contact)
  - **Web:** [http://www.cs.umb.edu/~gghinita](http://www.cs.umb.edu/~gghinita)
  - **Phone:** (617) 287-6479
  - **Office:** Science Building, 3rd Floor, Room 88 (S-3-88)

- **TA:** Evan Donato
  - **Email:** Evan.Donato001@umb.edu
Course Info

- **Office Hours**
  - Tue & Thu 5:30-7:00pm
  - By appointment (send email)

- **Class URL**
Textbook

by Charlie Kaufman, Radia Perlman, and Mike Speciner,
Prerequisites

- Introduction to System Administration
  - IT341

- If you take IT341 later, you will lose the credits of this course!
Grading

- Final exam (40%) – hands-on

- 6 lab assignments
  - 10% each
  - Assignments are either individual or in teams of two
  - In either case, submit your own (or own team) work only!
  - No plagiarism please – see student code of conduct

- Attendance is mandatory
Course Materials

- Class URL

- Blackboard
  - Discussion forums

- Make sure you create Unix course accounts
  - IT443-1 (evening session) or IT443-2 (afternoon session)
Course Rules & Conventions

- Security starts with good organization/administration!

- Course-related emails
  - Subject line **MUST BEGIN** with [IT443]

- Homework submission in digital form
  - Follow **EXACTLY** instructions
  - File names and directory structure **EXACTLY** as requested
  - File permissions must be correctly set: g+w, o-r
  - Ensure your files belong to correct grader group!
University Policies

- **Student Conduct**: Students are required to adhere to the University Policy on Academic Standards and Cheating, to the University Statement on Plagiarism and the Documentation of Written Work, and to the Code of Student Conduct as delineated in the University Catalog and Student Handbook. The Code is available online at: https://www.umb.edu/editor_uploads/images/life_on-campus/

- **Accommodations**: Section 504 of the Americans with Disabilities Act of 1990 offers guidelines for curriculum modifications and adaptations for students with documented disabilities. If applicable, students may obtain adaptation recommendations from the Ross Center for Disability Services, CC-UL Room 211, (617-287-7430). The student must present these recommendations and discuss them with each professor within a reasonable period, preferably by the end of Drop/Add period.
Course Outline

- **Network Basics**
  - Network layers, headers, services, …
  - TCP/IP, MAC, DNS, ARP, …
- **Cryptography Basics**
  - Secret key encryption, Public key encryption, Hash functions
  - Doesn’t cover theoretical foundation
- **Authentication**
  - Password, challenge/response, mutual authentication, …
- **Public Key Infrastructure**
  - PKI architecture, certificates, …
Course Outline

- **IPsec**
  - Secure IP layer protocol
- **SSL/TLS**
  - Secure transport layer protocol
- **Firewall**
  - Prevent attacks, iptables, …
- **Intrusion Detection System**
  - Host-based IDS and network-based IDS
- **Email Security**
Lab Outline

- Will use SEED VM with VMWare Wkstn
- Understanding network packets
  - IP prefix, DNS service
- Encryption/decryption
  - File encryption (openssl)
  - Distinguish cryptographic algorithms
- Password cracking
  - Dictionary attack, john-the-ripper
- Network attacks
  - SYN flood, ARP poisoning
Lab Outline

- Implementing certificates
  - Set up https service
- Configuring a firewall
  - iptables
- System monitoring
  - Remote logging
- Intrusion detection
  - Snort
- SQL injection
Security Objectives (CIA)
Security Objectives (CIA)

- **Confidentiality** — Prevent/detect/deter improper disclosure of information

- **Integrity** — Prevent/detect/deter improper modification of information

- **Availability** — Prevent/detect/deter improper denial of access to services provided by the system
OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”

- Defines a systematic way of defining and providing security requirements

- It provides a useful, if abstract, overview of concepts we will study
Aspects of Security

3 aspects of security:

security attack
- Any action that compromises the security of information owned by an organization

security mechanism
- A process that is designed to detect, prevent, or recover from a security attack

security service
- Counter security attacks: make use of one or more security mechanisms to provide the service
Threat Model and Attack Model

- Threat model and attack model need to be clarified before any security mechanism is developed

- Threat model
  - Assumptions about potential attackers
  - Describes the attacker’s capabilities

- Attack model
  - Assumptions about the attacks
  - Describe how attacks are launched
Passive Attacks

Darth reads the contents of the message from Bob to Alice through the Internet or other communication facility.
Active Attacks

Darth

Capture message from Bob to Alice; later replay message to Alice

Internet or other comms facility

Bob

Alice
Security Mechanism (X.800)

- **Specific security mechanisms:**
  - ciphers, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization

- **Pervasive security mechanisms:**
  - trusted functionality, security labels, event detection, security audit trails, security recovery
Security Service

- Enhance security of data processing systems and information transfers of an organization
- Intended to counter security attacks
- Using one or more security mechanisms

- Often replicates functions normally associated with physical documents
  - For example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed
Security Service

- **Authentication** - assurance that communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** – protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication
- **Availability** – resource accessible/usable