Please see the attached course plan to help plan out your registration. You may also consult your Georgia Tech degree audit to view your degree plan. Please let us know if you may have any questions!

CS 6035 - Introduction to Information Security (core course) (Course Preview)

This course teaches the basic concepts and principles of information security, and the fundamental approaches to secure computers and networks. It's main topics include: security basics, security management and risk assessment, software security, operating systems security, database security, cryptography algorithms and protocols, network authentication and secure network applications, malicious malware, network threats and defenses, web security, mobile security, legal and ethical issues, and privacy.

CS 6210 - Advanced Operating Systems (Course Preview)

Introduction to graduate-level topics in operating systems using research papers, textbook excerpts, and projects. Provides students thorough comprehension of distributed and parallel computer systems. Advanced Operating Systems is a graduate-level course that addresses a broad range of topics in operating system design and implementation, including: operating system structuring; synchronization, communication and scheduling in parallel systems; distributed systems, their communication mechanisms, distributed objects and middleware; failures and recovery management; system support for Internet-scale computing. By tracing the key ideas of today's most popular systems to their origins in research, the class highlights key developments in operating system design over the last two decades and illustrates how insight has evolved to implementation.

CS 6238 - Secure Computer Systems (Course Preview)

Design principles of secure systems, authentication, access control and authorization, discretionary and mandatory security policies, secure kernel design, and secure databases.

CS 6250 - Computer Networks (Course Preview)

Design principles of secure systems, authentication, access control and authorization, discretionary and mandatory security policies, secure kernel design, and secure databases.

CS 6260 – Applied Cryptography (Course Preview)

This is an introduction to modern cryptography. We focus on the classical goals of cryptography such as data privacy, authenticity and integrity. Topics include pseudorandom functions and permutations, block ciphers, symmetric encryption schemes, security of symmetric encryption schemes, hash functions, message authentication codes (MACs), security of MACs, PKI, public-key (asymmetric) encryption, digital signatures, security of asymmetric encryption and digital signature schemes, secret sharing, threshold cryptography. You will learn how various cryptographic schemes work and will discuss how they are used in practice. But the main objective is more fundamental. The goal is to build the understanding of what "secure" is and how to evaluate and measure security. We try to understand what it means for a cryptographic scheme to be "secure" by studying definitions of security of various primitives. You will learn how to analyze security of a cryptographic scheme and determine whether or not it is secure.

CS 6262 - Network Security (Course Preview)

This course provides an introduction to computer and network security. Students successfully completing this class will be able to evaluate works in academic and commercial security and will have rudimentary skills in security research. The course begins with a tutorial of the basic elements of cryptography, cryptanalysis, and systems security and continues by covering several seminal papers and monographs in a wide range of security areas. **[Prerequisite – CS 6035]**

CS 6265 - Information Security Lab (Course Preview)

Computer systems and network vulnerabilities, information warfare, network and operating system security techniques, security analysis tools.

CS 6264 - Information Security Lab: System and Network Defenses (Course Preview)

This course will help students develop both in-depth knowledge and hands-on skills in a number of important cybersecurity areas. The lecture materials of each topic area are drawn from latest research papers and prototypes, and comprehensive projects are assigned to help students master each area. The main topics include:

- **Software security**: software vulnerabilities; program analysis techniques.
- **Malware analysis:** building a malware analysis environment; threat analysis; obtaining and sharing threat intelligence.

- **End-point security**: monitoring computer activities through system call hooking and virtual machine introspection; forensic analysis using system-wide record-and-replay technologies.
- **Network security**: vulnerabilities of network protocols; network monitoring, including network intrusion detection and alert correlation.
- **Web security**: browser security models; providing fine-grained access control to third-party scripts, and the security vulnerabilities of WebView.
- **Mobile security**: iOS and Android security models; Android malware and gray-ware; attack ecosystem including rooting attacks and third-party app stores.
- **Machine learning for security analytics**: using machine learning algorithms (deep learning) to automatically produce security models; how the machine learning process can be subverted by attackers and how to improve the robustness of machine learning.

CS 6300 - Software Development Process (Course Preview)

This course provides an in-depth study of the process of developing software systems, including the use of software processes in actual product development, techniques used to ensure quality of the software products and maintenance tasks performed as software evolves. By the end of the course, students will understand the role of software processes in the development of software and will have experienced several types of processes, from rigid to agile. Students will also become familiar with a variety of modern technologies and development techniques and understand their connection to software processes.

CS 6400 - Database Systems Concepts and Design (Course Preview)

This course presents an example of applying a database application development methodology to a major real-world project. All the database concepts, techniques, and tools that are needed to develop a database application from scratch are introduced. In parallel, learners in the course will apply the database application development methodology, techniques, and tools to their own major class team project. In addition, this course will include instruction in the Extended Entity Relationship Model, the Relational Model, Relational algebra, calculus and SQL, database normalization, efficiency and indexing. Finally, techniques and tools for metadata management and archival will be presented.

CS/ECE/PUBP 6727 - Practicum

The primary objective of PUBP/CS 6727 is in-context learning by allowing students to apply cyber security principles and techniques to a real-world problem. The course requires that students explore a substantial scope/size cyber security problem, and design, implement, and evaluate a solution for it that has practical applicability. Students are responsible for choosing a problem that is addressed by the practicum project, but it must be approved by the course instructor. A project may be inspired by problems that arise in a student's work place, but it must be completed with sufficient academic rigor. Typically, narrowly scoped and short term tasks that a student works on at his or her job do not meet the requirements of the practicum project. The purpose of the practicum is to offer some freedom in the project you choose, but also ensure that you can apply the knowledge gained in the program to produce the desired outcome. Since students are able to work on different problems based on their interest, there is no one written problem description other than the prerequisites. Although each student explores a cyber-security problem individually, there is also a shared learning component of the course. This will be achieved by requiring that a group of students in the course meet virtually each week where each student will present his or her progress on the project and receive feedback from the instructors/TAs and fellow students. The instructors will also outline weekly goals via Canvas to ensure that students make consistent progress. The main learning objectives of the course include:

1. Define key cyber security requirements for a system or environment that relies on or is impacted by information technology
2. Explore the threat model and choose threats against which security requirements must be met
3. Understand and evaluate existing techniques/solution relevant to the problem
4. Design, develop and implement a solution (software system or policy requirements) that can help address the security problem more effectively
5. Carefully evaluate the effectiveness of the solution and any tradeoffs that must be considered in its application.

Since this course is a capstone, it is expected that students have completed most of their coursework prior to registering for it. However, exceptions may be granted by the instructors based on a student's past experience and the nature of the practicum project.

CS/ECE 6747 - Advanced Topics in Malware Analysis (Course Preview)

This course covers advanced approaches for the analysis of malicious software, the investigation of cyber-attacks, and explores recent research and unsolved problems in software protection and forensics. The goal of this course is to engage in critical discussion around key research topics in software security and forensics. This course will cover: Binary Program Analysis Principles, Binary Software Security, Software Forensics and Cyber Attack Response. Students will be required to study published research papers from the top-tier academic venues in computer security and cyber forensics. Why take this course? You are interested in learning the fundamental principles of dissecting malware, vulnerability finding/defense, and cyber-attack triage. You aim to study the limitations of existing defense mechanisms and how to overcome them. You want to read cutting-edge research publications on these topics.

CS 6750 - Human Computer Interaction (Course Preview)

(Only for students in the Policy specialization. Information Security and ECE students cannot enroll in this course. This course is an elective that is not listed in the degree plan but will be applied to your program of study if completed.)

This course is an introductory course on human-computer interaction. It does not presuppose any earlier knowledge of human-computer interaction, computer science, or psychology. The class covers three broad categories of topics within human-computer interaction: (a) the principles and characteristics of the interaction between humans and computers; (b) the techniques for designing and evaluating user-centered systems; and (c) current areas of cutting-edge research and development in human-computer interaction.

CS 8803/ECE 8833/PUBP 8833 – Enterprise Cybersecurity Management (Course Preview)

This course is intended for students with an interest in designing and leading cybersecurity organizations or operating in functions that need to work closely with security teams. Beginning with a focus on strategy and guiding principles, the course then moves into organizational structure and specific roles and duties required to address the cybersecurity needs of different organizations. Core concepts of risk management are introduced and used to frame modules on cyber risk management and oversight. Finally, cyber risk governance is studied with a focus on both internal oversight structures and Board-level interaction.

CS 6261/PUBP 8803 – Security Incidence Response (Course Preview)

Through analysis of real world cyber security incidents and reports, students will learn the background information and skillsets necessary to operate as an effective cyber security operations staff member and leader. Specific topics include: cyber security topics primer, and incident response procedures (including host and network based forensics).

ECE 6320 – Power Systems Control & Operations (Course Preview)

Introduction to methods used in the real time operation and control of power systems as well as to the hardware and software technology of energy management systems (EMS).

ECE 6347 - Introduction to Cyber-Physical Electric Energy Systems (Course Preview)

This course provides an introduction to cyber-physical infrastructure for protection and control of electric energy systems, communication protocols and standardization and present practices for cyber security. The course covers the cyber-physical infrastructure for protection of EES, the cyber-physical infrastructure for communications and control of EES, the methods used to protect the cyber-physical infrastructure for protection of EES against attacks, the methods used to protect the cyber-physical infrastructure for communications and control of EES against attacks, and applicable standards and best practices.

ECE 8813 - Introduction to Cyber-Physical Systems Security (Course Preview)

The course covers introductory topics in cyber-physical systems security. The goal is to expose students to fundamental security primitives specific to cyber-physical systems and to apply them to a broad range of current and future security challenges. Much of the course is taught with the focus on one instance of cyber-physical systems - Industrial Control Systems (CPSs). However, students will be expected to generalize the concepts for other cyber-physical systems.

ECE 8823 - Cyber Physical Design and Analysis (Course Preview)

Cyber-physical systems are systems comprising both a physical part and a software part, whereby the physical part of the system sends information about itself to the software part, and the software sends information, usually in the form of commands, to the physical part. The development of cyber-physical systems, therefore, requires knowing a mix of competencies relative to physical systems, on the one hand, and software systems, on the other hand. Because physical systems have "a life of their own", and they can often harm operators (think airplanes, medical devices, or cars) and/or cost a fortune to repair (think power grid and centrifuges), the development of programs that control these systems cannot rely much on "trial and error". This course introduces the tools and models that will allow attendees to develop high confidence in the resulting system's proper operation prior to any operational test. Included are tools for model-based systems engineering, and cyber-physical system verification and validation currently in use by the CPS industry. Numerous examples will be considered, from aerospace, automotive, medical devices, etc. The frequent presence of human operators is also acknowledged and discussed in-depth. Various verification and validation formalisms (formal methods) are described and applied to simple examples.

ECE 8843 - Side-Channels and Their Role in Cybersecurity (Course Preview)

The primary objective of this course is to provide an in-depth treatment of digital and analog side-channels and their use for attacks and defenses in cyber security. Upon completion of the course, the student will have a high degree of confidence in discussing the fundamental mechanisms of side-channel creation, analysis, and application to various cybersecurity problems, and have competence in considering these mechanisms during software and hardware development.

INTA 6103 – International Security (Course Preview)

This course focuses on the intersection of international relations and security policy. Students will examine theoretical foundations of key policy debates. Readings will cover theories of war, the security dilemma, deterrence and coercion, grand strategy, terrorism, democratic peace, Asia, Europe, balance of power, and ethnic conflict. The objectives are to introduce and critique the main theories of international conflict, and to discuss specific threats. This course does not focus on in-depth historical study of discrete events or U.S. national security policies, per se. Rather, primary emphasis is placed on analyzing these issues systematically to uncover the implicit assumptions and logic behind decisions to threaten or to use force, and to tie these assessments to real-world concerns and contemporary policy debates.

INTA 6450 – Data Analytics and Security

Explores use of big data techniques to problems at the national and international levels. Topics may include cybersecurity, surveillance, economic development, behavioral prediction, and manipulation.

INTA 6742 - Modeling, Simulation, and Military Gaming (Course Preview)

Computer modeling and simulation offers a unique perspective on events because of the ability to hold some variables constant and change others, and run a scenario repeatedly searching for underlying themes. Computer simulation has been used as an analytical tool in the natural sciences, business, commerce, government, and politics. This course focuses on the creation and application of computer simulations to model strategic international events concerning warfare. The course is project-based, requiring computing and international affairs students to work together in multidisciplinary teams to analyze specific questions utilizing computer-based modeling and simulation tools (largely, but not exclusively "NetLogo").

MGT 6727 - Privacy for Professionals (Course Preview)

This course takes a multi-disciplinary approach to the study of privacy––a current topic of great international interest for those in technology, policy, law, and/or business. It prepares students to work professionally in the privacy field, with an emphasis on U.S.-based law and practice. Course topics include introduction to privacy, federal and state regulators and enforcement of privacy law, principles of information management, online privacy, the California Consumer Privacy Act, information security and data breach notification laws, European Union privacy laws, medical privacy, financial privacy, education privacy, workplace privacy, privacy issues in civil litigation and government investigations, and emerging issues. The professor draws on his extensive experience in business, government, technology, and law to address current privacy debates.

PUBP 6501 - Information Policy & Management Information Policy & Management (Course Preview)

The course is an introduction to the role of information and knowledge in modern private and public organizations. It covers theoretical aspects of information seeking, gathering and use in organizations as well as knowledge creation and its role in management. The course also addresses the practical implementation of organization information strategies using information technology. Information security and cybersecurity are integrated into the framework of a learning and knowledge-oriented organization and general information policy rather than considered a separate concern. The first part of the course introduces the issues of organization strategy and its relation to information. The second part focuses on the notion of organizational learning. The third part focuses on the applications of information technology in government, especially related to various aspects of e-government. The final section focuses on new approaches to knowledge management in the public sector.

PUBP 6502 - Information and Communications Policy

The course is a survey of communication and information policy issues that covers the changing industrial organization of fixed and wireless telecommunications, internet, broadcasting, cable and social media. It covers late 19th, 20th and 21st century telecommunications in the U.S. and includes international institutions and the global political economy of communications. Using the tools of historical political economy, students will learn about the evolution of the information and communication industries, the impact of technological change on those industries, and the changing regulatory institutions associated with the rise and decline of various systems. The course covers issues such as antitrust actions against major businesses; network neutrality; radio spectrum policy, and content regulation on platforms.

PUBP 6725 - Information Security Policies (core course) (Course Preview)

This course introduces students to the policy and management aspects of cybersecurity. It is divided into four modules. The first involves basic concepts and definitions regarding policy, governance, and threats; the second deals with cybersecurity management and policy at the organizational level; the third deals with cybersecurity public policy at the national level; the fourth deals with cyber conflict, policy and diplomacy at the transnational level. This course situates cybersecurity in the overall Internet ecosystem.

PUBP 8813 - Public Policy for the Digital World (Course Preview)

Understand the public policy issues posed by the digital transformation, using a political economy framework. Students will learn to identify the component parts of the digital ecosystem and recognize the technical and economic interdependencies among them. They will learn the basics of political economy theory and use it to propose and critically analyze public policy interventions in areas such as artificial intelligence; the digitization of money; Internet governance; data governance and privacy; platforms, competition, and content moderation; and digitization's role in geopolitical competition among nation-states.

PUBP 8823 - Geopolitics of Cybersecurity (Course Preview)

This course will provide students with a framework for interpreting power politics in and through cyberspace. The organizing assumption of the course is that classic concepts from international relations remain useful for understanding modern technologies, but they must be combined in new ways to explain the potential for exploitation and subversion at scale. The course provides tools for analyzing cyber power, which is organized deception via information systems for strategic advantage. Cyber power differs in important ways from military power, bargaining power, and soft power. Different political logics are often combined in practice, which creates complex strategic tradeoffs. Students will learn how to analyze these tradeoffs in modern cyber campaigns and in the use of cyber power for national security objectives.

Policy Track Students *ONLY* – Flexible Core options

CS 6750 - Human-Computer Interaction – (Course Preview)

(Only for students in the Policy specialization. Information Security and ECE students cannot enroll in this course. This course is an elective that is not listed in the degree plan but will be applied to your program of study if completed.)

This course is an introductory course on human-computer interaction. It does not presuppose any earlier knowledge of human-computer interaction, computer science, or psychology. The class covers three broad categories of topics within human-computer interaction: (a) the principles and characteristics of the interaction between humans and computers; (b) the techniques for designing and evaluating user-centered systems; and (c) current areas of cutting-edge research and development in human-computer interaction.