MARYVILLE UNIVERSITY

JOHN E. SIMON SCHOOL OF BUSINESS

MASTER OF SCIENCE

SECURE SOFTWARE DEVELOPMENT

SKILLSERVE Education Partner

MARYVILLE UNIVERSITY

UGPG GLOBAL

Artificial Intelligence and Cybersecurity:

Intelligent systems increasingly rely on AI and machine learning in the modern era; therefore, possessing the knowledge and abilities necessary to defend these systems against cyber threats is critical. The study of secure software development and AI security is relevant in this context. AI security encompasses measures to protect the integrity of AI algorithms, thwart data manipulation and sabotage, and avert data poisoning risks. Additionally, it ensures the safety of applications that employ AI. It is critical to have developers proficient in AI security, given that AI systems frequently deal with sensitive data. These skills are necessary to safeguard user privacy, construct AI models resistant to adversarial assaults, and guarantee the reliability, trustworthiness, and responsibility of AI-driven judgments. Acquiring proficiency in AI security not only safeguards our data but also provides developers with access to novel employment prospects and places them at the vanguard of technological progression.

With the ongoing revolution of AI across multiple sectors, expertise in AI security will become an exceedingly sought-after competency. Through the integration of AI security into secure software development practices, developers can proactively identify and address emergent challenges within the ever-evolving realms of cyber threats and technology. Proficiency in this area is of the utmost importance to guarantee that the ongoing advancements of AI and machine learning in numerous industries do not compromise the privacy and security of users.

Master of Science in Secure Software Development:

The Master of Science in Secure Software Development, with its focus on AI Security, is an advanced program for professionals aspiring to excel in cybersecurity. The degree offers stackable certificates, focusing on Systems Architecture Security and Secure Software Development, and provides innovative content and access to industry experts. Learners will delve deeply into cryptography, AI-enhanced cybersecurity, and machine-learning algorithms to analyze and process encrypted data. This 30-credit hour degree is designed to be completed in 15 months.

Format

The MS in Secure Software Design program blends practical skills and theoretical knowledge, focusing on cybersecurity fundamentals and their real-world application. Graduates will be prepared for advanced cybersecurity roles and adept at addressing contemporary cyber threats.

The program caters to those aiming to innovate in secure system development, artificial intelligence, and integrating theory with industry-relevant skills in the rapidly evolving cybersecurity field. Coursework includes a mix of hands-on learning, including projects, interactive discussions, and labs. This academic experience is supplemented with virtual online experts from around the US.

Curriculum

The MS in Secure Software Design coursework is organized with student achievement in mind. With flexible, 8-week terms, students undertake an accelerated schedule, with opportunities to earn three graduate certificates in **Secure Software Development, Systems Architecture Security,** and **Artificial Intelligence Security.** Students also have an opportunity to earn academic credit through an internship experience.

Course and Program Overview:

Term	Course Sequence
Fall 1 Term	SSD 600 Secure Software - Foundation Course*
Fall 2 Term	SSD 610 Development Cybersecurity Standards & Risk * SSD 640 Information Security Architecture
Spring 1 Term	SSD 620 Practical Cryptography SSD 650 Cryptography & Protocols*
Spring 2 Term	SSD 630 Security Assurance
Summer (Optional)	SSD 699 Internship
Fall 1 Term	SSD 660 Security Architecture SSD 665 Computer Vision
Fall 2 Term	SSD 675 Voice Analysis for Security SSD 685 AI Security
December 2025 Graduation	

Program Duration and Weekly Time Commitment
The MS in Secure Software Design is offered in a 15-month format, with an expected weekly time commitment of approximately 45 hours per week based on the average time students report in the SSD program. Of course, the time commitment will vary across students.

Target Student Profile
The typical target student is in their early 20s who has received a BS in a computer science field, but the program also works for more senior professionals. For example, in the graduate certificate format, 45% of the students are in their 30s, while 30% are 40 or older.

Career Development
As an F-1 visa student in this STEM-eligible MS in Secure Software Development degree program, students are eligible for Optional Practical Training (OPT) for up to three years of work in the US after graduation. Additionally, they have the opportunity for Curricular Practical Training (CPT) during their studies, allowing them to undertake internships or employment related to their field.

Both OPT and CPT provide valuable real-world experience in your study area. The program provides training for early career students to pursue jobs such as software security engineer, application security analyst, security consultant, and security architect. With the growing importance of cybersecurity, the demand for these professionals will likely continue to increase. The salary range for professionals in secure system design varies depending on factors such as location, experience, and the specific industry they work in. On average, salaries in the US range from around $60,000 to upwards of $150,000 per year.

About Maryville University

Maryville University is a nationally recognized private institution that offers a comprehensive and innovative education focused on student learning, outcomes, and success. The Chronicle of Higher Education named Maryville as the second fastest-growing private university in the US and has been honoured as an Apple Distinguished School three times, holding that honour continuously since 2016. Maryville has been recognized for its Digital World Program, which allows students to personalize their education in an enhanced technology environment. Its data science programs, on ground and online, are ranked #17 in the United States. Its online MBA in Cybersecurity and BS in Cybersecurity are ranked in the top 10 in the US. Maryville University is now a National Center of Academic Excellence in Cyber Defense, as designated by the National Security Agency (NSA). Their Cybersecurity Center of Excellence offers both undergraduate and graduate programs in cybersecurity, both online and on-campus. The CCOE unites academic excellence with real-world experience to prepare their students for a successful career in cybersecurity.

About St. Louis

Maryville University, located in west St. Louis County and just 20 miles from downtown, sits in the heart of a major metropolitan region. More than 2 million people call St. Louis home—for nearly as many good reasons. Take a ride to the top of the 630-foot-tall Gateway Arch, and you'll see why St. Louis is known as the Gateway to the West. While there are hundreds of urban and suburban parks in the vicinity of Maryville University, you can't miss the 1,371-acre Forest Park with its world-class Saint Louis Zoo, Saint Louis Art Museum, Missouri History Museum, the Saint Louis Science Center and James S. McDonnell Planetarium, and the World Chess Hall of Fame. During the summer, Forest Park hosts Broadway musicals at Muny Opera, the nation's largest and oldest outdoor theater, and you can catch performances of the St. Louis Shakespeare Festival under the stars. There is no bigger sports town in America than St. Louis. If music is what you are looking for, St. Louis offers one of the top live music scenes in the Midwest. The Grammy-award-winning St. Louis Symphony, Opera Theater of Saint Louis, and dozens of venues, festivals, and concerts offer everything from blues, country, rock, hip-hop, and everything in between. The city is also home to the National Blues Museum. The city is home to seven Fortune 500 companies, including Centene (#25), Emerson Electric (#207), Reinsurance Group of America (#257), Edward Jones (#333), Graybar Electric (#378), Olin (#410), and Ameren (#480), which provide employment opportunities and contribute to the city's economic growth. St. Louis has a low cost of living compared to other major cities in the United States, making it an affordable option for international students. With its academic excellence, cultural diversity, and affordability, it's easy to see why St. Louis is a popular destination for international students.

Admissions Requirements:

1. Bachelor’s degree in computer science, or related field
2. Complete Admission Application
3. Personal Statement
4. Proof of English Proficiency: Official test scores with a test date within two years of application. Students must meet one of the following minimum requirements:
    a. TOEFL 79 overall with no sub score lower than 18.
    b. IELTS 6.0 overall with no sub score lower than 5.5.
    c. PTE academic score of 54.
    d. DET score of 105.

5. Official transcripts from the baccalaureate degree-granting institution (converted, where relevant, to U.S.-based GPA system).
    a. Minimum 3.0 cumulative GPA on a 4.0 scale

Admittance

Upon admittance in the program, students must submit the following:

6. $250 Tuition Deposit
7. Intent to Enroll Form
8. Evidence of Financial Ability (https://studyinthestates.dhs.gov/students/prepare/financial-ability)

Timeline:

Spring 2024	
February	Information Sessions for Prospective Students Begin
March	Priority application open: March 1
March – April	**Student Actions:** - Sit for English Proficiency exams (TOEFL/IELTS/PTE/DET) - Request Transcript Evaluation - Compose Personal Statement
May	Online Application deadline: May 1
Summer 2024	
May - June	Admission decisions communicated by June
June	Student Actions: - Pay $250 Tuition Deposit - Submit Intent to Enroll Form - Pay $350 I-901 SEVIS Fee
June	Maryville issues the Form I-20, "Certificate of Eligibility for Nonimmigrant (F-1) Student Status – For Academic and Language Students."
June – July	**Visa Application Process** **Student Actions:** - Review the Study in the States website - Complete the Form DS-160 online – including a photo - Gather I-20, SEVIS fee receipt, Form DS-160 printed copy, and Passport - Prepare for Visa Application Interview - Schedule an Interview at the U.S. Embassy or Consulate - Pay the Visa Application Fee of $185 - Receive your F-1 visa
July	**Preparing for St. Louis** **Student Actions:** - Make travel arrangements - Make accommodation and living arrangements - Connect with classmates!
Fall 2024	
August	Attend International Student Orientation Classes Begin
Summer 2025	
	Optional Internship Experience
Fall 2025	
December	Graduation Ceremony at Maryville University

Appendix: Course Descriptions

Secure Software Development

This course is designed to provide students with a comprehensive understanding of secure software development principles and practices. Students will learn how to identify and mitigate common security vulnerabilities throughout the software development lifecycle. The course will cover topics such as threat modelling, secure coding practices, security testing, and secure deployment strategies. Through a combination of lectures, hands-on exercises, and real-world case studies, students will gain the knowledge and skills necessary to develop secure software applications.

Learning Objectives:

1. Understand the fundamental concepts of secure software development.
2. Identify common security vulnerabilities in software applications.
3. Apply secure coding practices to mitigate vulnerabilities.
4. Conduct threat modelling to identify potential security threats.
5. Implement security testing techniques to validate software security.
6. Apply secure deployment strategies to protect software in production.

Cybersecurity Standards & Risk

This course provides students with a comprehensive understanding of cybersecurity standards, risk management, and compliance related to the use, processing, storage, and transmission of data. Students will learn about laws, regulations, controls, and best practices governing the protection of personal information and data. The course will teach risk assessment, data privacy, security controls, compliance frameworks, and incident response topics. Through lectures, case studies, and hands-on exercises, students will learn to manage cybersecurity risks and effectively ensure compliance with relevant standards. Prerequisite: SSD 600

Learning Objectives:

1. Understand the fundamentals of cybersecurity standards and risk management.
2. Identify and assess cybersecurity risks related to data use, processing, storage, and transmission.
3. Implement security controls to mitigate identified risks.
4. Compliance with relevant laws, regulations, and compliance frameworks governing data privacy and protection.
5. Develop incident response plans to handle cybersecurity breaches and violations.

Practical Cryptography

This course provides a comprehensive introduction to practical cryptography, covering fundamental concepts, techniques, and applications. Students will gain a solid understanding of cryptographic principles and their practical implementations. The course explores the historical context of cryptography, the importance of cryptographic protocols, the role of hash functions, and the significance of Kerckhoff's Principle. Students will develop the necessary skills to analyze and design secure cryptographic systems through lectures, interactive discussions, and hands-on exercises. Prerequisite: SSD 600

Learning Objectives:

1. Explain the importance of cryptography in modern information security and its role in protecting data confidentiality, integrity, authentication, and non-repudiation.
2. Understand the historical context and evolution of cryptography, including the impact of World War II and advancements during the digital age.
3. Describe the properties and applications of hash functions and apply them for data integrity and password storage.

4. Analyze and compare symmetric encryption algorithms, including modes of operation, and evaluate their strengths and limitations.
5. Comprehend public-key cryptography, including the concepts of asymmetric encryption, key management, and digital signatures.
6. Discuss the significance of Kerckhoffs' Principle and understand the difference between security through obscurity and open design.
7. Evaluate the security of cryptographic protocols, such as SSL/TLS, SSH, and IPsec, and analyze their strengths, weaknesses, and vulnerabilities.
8. Demonstrate knowledge of key management and distribution techniques, including key generation, storage, distribution, and revocation.
9. Identify cryptanalysis techniques, such as brute force and differential cryptanalysis, and understand countermeasures against them.
10. Explain side-channel attacks, such as timing attacks and power analysis, and discuss mitigation strategies.
11. Discuss emerging topics in cryptography, including post-quantum cryptography, homomorphic encryption, zero-knowledge proofs, and their practical implications.
12. Apply cryptographic principles and techniques to real-world scenarios, such as secure communication protocols, authentication mechanisms, and data protection.

Security Assurance

This course is designed to equip students with the knowledge and skills necessary to locate and identify system vulnerabilities and assess security needs systematically. Students will learn methods and techniques to identify potential vulnerabilities in system designs and evaluate the effectiveness of security measures. Through hands-on exercises and case studies, students will gain practical experience in conducting security assessments and validating system security against organizational security requirements. Prerequisite: SSD 600

Learning Objectives:

1. Understand the concept and importance of security assurance.
2. Identify and locate system vulnerabilities through systematic assessments.
3. Evaluate system designs for potential security vulnerabilities.
4. Validate a system's security to ensure it meets organizational security needs.
5. Apply security testing techniques to assess system security.
6. Develop skills in reporting and communicating security assessment findings.

Information Security Architecture

In this course, students will evaluate information security and its importance in protecting the confidentiality, integrity, and availability of systems and information. The students will develop the skills to discern the different security needs of various stakeholders, evaluate the robustness of security designs, and design security controls to protect information assets. Prerequisite: SSD 600

Learning Objectives:

1. Understand the concept of information security architecture and its role in protecting systems and information.
2. Evaluate the security needs of various stakeholders and discern their requirements.
3. Assess the robustness of security designs to ensure their effectiveness.
4. Design and implement security controls to protect information assets.
5. Apply risk management principles to prioritize and address security vulnerabilities.
6. Develop skills in analysing security requirements and communicating security architecture recommendations.

Cryptography & Protocols

In this course students will learn the fundamentals of cryptography and its application in security protocols. These protocols allow systems to achieve information security, privacy, and trust. Students will learn mathematical concepts and cryptographic tools to analyze and understand the strengths and shortcomings of such security protocols and will develop an understanding of how to improve insecure Systems. Prerequisite: SSD 600.

Learning Objectives:

1. Understand the fundamentals of cryptography and its role in security protocols.
2. Analyze and evaluate the strengths and weaknesses of security protocols.
3. Apply mathematical concepts and cryptographic tools to assess security protocols.
4. Identify vulnerabilities and shortcomings in insecure systems.
5. Develop skills to enhance the security of protocols through cryptographic mechanisms.
6. Apply theoretical knowledge to real-world scenarios and case studies.

Security Architecture

This course aims to provide students with a comprehensive understanding of the key concepts and techniques involved in designing secure system architectures. Students will learn about the fundamental principles and best practices for building secure systems and explore the key technologies used in secure system architecture. The course will also emphasize the importance of staying informed about emerging technologies and their potential impact on security. Through lectures, discussions, case studies, and practical exercises, students will develop the knowledge and skills necessary to design robust and secure system architectures while keeping pace with evolving technology trends. Prerequisite: SSD 600

Learning Objectives:

1. Understand the principles and fundamentals of secure system architecture.
2. Identify and analyze security requirements for system architecture design.
3. Apply key technologies and tools used in secure system architecture.
4. Evaluate and select appropriate security mechanisms for different system components.
5. Develop the ability to stay informed about emerging technologies and their security implications.
6. Apply theoretical knowledge to practical scenarios and real-world case studies.

Computer Vision

This course is designed to introduce students to the exciting field of computer vision, which is a subfield of artificial intelligence (AI) that focuses on enabling computers to interpret and understand visual information from the world. Students will learn the fundamental concepts, techniques, and tools used in computer vision, enabling them to develop basic computer vision applications. Prerequisite: SSD 600

Learning Objectives:

1. Understand the core concepts of computer vision.
2. Apply image processing techniques to manipulate and enhance images.
3. Implement basic computer vision algorithms for object detection and tracking.
4. Develop simple computer vision applications using popular libraries and frameworks.
5. Gain insights into the ethical and practical considerations of computer vision.

Voice Analysis for Security

This course delves into the field of voice analysis, emphasizing its importance in security applications. Students will learn the fundamentals of voice analysis, including speech recognition, speaker identification, and how these techniques are used in security-related contexts such as biometric authentication and fraud detection. Prerequisite: SSD 600

Learning Objectives:

1. Understand the basics of human voice production and characteristics.
2. Analyze and process voice data for various security applications.
3. Implement voice recognition and speaker identification algorithms.
4. Apply voice analysis techniques to biometric authentication and fraud detection.
5. Explore ethical considerations and privacy concerns in voice analysis for security.

AI Security

This course explores the critical intersection of artificial intelligence (AI) and security. Students will learn about the vulnerabilities, threats, and countermeasures associated with AI systems. The course covers topics such as adversarial attacks, secure model deployment, and ethical considerations in AI security. Prerequisite: SSD 600

Learning Objectives:

1. Understand the fundamentals of artificial intelligence and its security implications.
2. Identify and mitigate common vulnerabilities and threats in AI systems.
3. Implement security measures for AI model development and deployment.
4. Analyze ethical issues related to AI security and privacy.
5. Explore real-world case studies and best practices in AI security.

SSD 699 Internship

This course is designed to provide students with a structured academic framework for their internship experience. It connects theories with real-world practices, enabling students to apply and expand their academic knowledge. This hands-on experience allows for valuable insights into the daily operations and challenges of a professional environment in their field of study. Students will participate in reflection discussions and self-assessments and complete a cumulative presentation. Prerequisite: Permission of instructor.

MARYVILLE UNIVERSITY

ST. LOUIS

Master of Science in Secure Software Development

For further information on this program please contact SkillServe and UGPG Global at hello@skillserve.us

SkillServe and UGPG are education services companies appointed by Maryville University to assist with overseas student recruitment and onboarding.

SKILLSERVE Education Partner

MARYVILLE UNIVERSITY

UGPG GLOBAL