جامعة الملك عبدالله
للعلوم والتقنية
King Abdullah University of
Science and Technology

Course Syllabus: Contemporary Topics on Resilience - CS 394T

Division	Computer, Electrical and Mathematical Sciences & Engineering
Course Number	CS 394T
Course Title	Contemporary Topics on Resilience
Academic Semester	Fall
Academic Year	2022
Semester Start Date	08/29/2021
Semester End Date	12/14/2021
Class Schedule (Days & Time)	01:15 PM - 02:45 PM | Mon Wed

Instructor(s)				
Name	**Email**	**Phone**	**Office Location**	**Office Hours**
Paulo Esteves-Verissimo	PAULO.VERISSIMO@KAUST.EDU.SA	+966128087861		Office B5-2226 Hours - TBA

Teaching Assistant(s)	
Name	**Email**

Course Information	
Comprehensive Course Description	This advanced course exposes students to the field of resilient computing, as a key enabler of the design of cybersecure systems in the XXI century. Resilience is believed to become a central paradigm for achieving safety and/or cybersecurity of systems operation, since classic cybersecurity paradigms are becoming obsolete and insufficient, given the magnitude of the emerging challenges to computing systems. The outcomes of this course are very relevant to students envisioning

	their research within the scope of the recently created RC3 (Resilient Computing and Cybersecurity Center, rc3.kaust.edu.sa). The key for resilience lies on the fusion between dependability and security research, or understanding the need to simultaneously fight against cyber-attacks, accidental faults, design errors, and unexpected operating conditions, in an automatic and persistent way. We review the theoretical foundations that made possible this common body of knowledge based on paradigms like automation, tolerance, self-healing, adaptation. We study dependability and security of computer systems and communication networks --- with a slant toward distributed systems --- as well as algorithmic and architectural solutions to make them resilient under the allowed presence of accidental and malicious threats. Furthermore, we study how to build on that, in order to make these properties sustainable over time, under persistent and/or evolving threat scenarios. Concrete competences acquired are: theory including fundamental paradigms and architectures; knowledge of techniques and tools for the design and development of algorithms, resilient systems, and their components; and, finally, practical knowledge and experience in the application of the paradigms and tools in diverse situations and execution environments, from networked embedded systems to large-scale web systems.
Course Description from Program Guide	A course of current interest. Topics are not permanent and the content of the course will change to reflect recurring themes and topical interest. The content will be approved by the division.
Goals and Objectives	Objectives: This advanced course exposes students to resilient computing, drawing from the fusion between dependability and security research, as a paradigm for fostering robustness of computing systems in the face of a wide range of threats, by simultaneously fighting against cyber-attacks, accidental faults, design errors, and unexpected operating conditions, in an automatic and sustainable way. A solid training in resilient computing, dependability and security assumes extreme importance as a precursor of advanced studies and research in these areas. Likewise, on a shorter term, it prepares students for mastering the design and operation of systems supporting many critical operations of modern societies, including: mission-critical data centers; utility

	infrastructures such as power grid, telco, or process control; autonomous vehicles in land, air and space; fintech and blockchain; digital health. Outcomes: Concrete competences acquired are: theory including fundamental paradigms and architectures; knowledge of techniques and tools for the design and development of algorithms, resilient systems, and their components; and, finally, practical knowledge and experience in the application of the paradigms and tools in diverse situations and execution environments, from networked embedded systems to large-scale web systems. As such, students will be exposed to the following subjects, from theoretical foundations to system-level approaches, and will be challenged with devising solutions for problems, along the knowledge provided by these subjects. 1. Review of fundamental security and dependability concepts 2. Fault and Intrusion Tolerance (FIT) concepts and terminology 3. FIT foundations, frameworks, mechanisms and strategies 4. Modeling threats 5. Architecting fault-and-intrusion-tolerant systems 6. Protocols: Tolerating Intrusions 7. Protocols: Resilience to Persistent and Evolving Threats 8. Testing Attacks The syllabus of this curricular unit contributes both to the objectives of the unit as well as to the program objectives.
Required Knowledge	Introductory Computer Security and Dependability courses advised, and it is expected that students have at least introductory notions of: computational systems and computer networks; operating systems and distributed systems.
Reference Texts	Given the time closeness of these matters to the s.o.t.a., two published survey works will serve as textbooks, forming the thread of the course explanation in lecture: - Intrusion-Tolerant Architectures: Concepts and Design. P. Veríssimo, N. Neves, and M. Correia. An extended version of the paper in: Architecting Dependable Systems. R. Lemos, C. Gacek, A. Romanovsky (eds.), Springer-Verlag LNCS 2677 (2003). [ITACD]. - Intrusion-Resilient Middleware Design and Validation. P. Verissimo, M. Correia, N. Neves, P. Sousa. In Annals of Emerging Research in

	Information Assurance, Security and Privacy Services, H. Rao and S. Upadhyaya (Eds.), Elsevier 2008. [IRMDV]. These will be complemented by a repository of several dozens of additional research and design papers, split in thematic modules and available from the course web, containing both the seminal works in the area over the years, as well as of the most recent, s.o.t.a. frontier works, so that students, in self-reading (pointed to from the lectures) or as part of reading assignments, may consolidate the notions obtained in the lectures.
Method of evaluation	**65.00**% - Homework /Assignments **30.00**% - Final exam **5.00**% - Active participation
Nature of the assignments	Reading Assignments (research papers to read and write a short essay about, with a structure oriented to creating a critical and creative researcher's mind) and group projects (a 2-phase project, destined to be a PoC of the value of the resilience concepts learned, results presented and defended in class by each group; students can and should constructively criticize each others' projects). If there is a sufficient split of PhD and advanced MSc students enrolled, I am considering a methodology of differentiated grading methods for PhD and MSc students. Pedagogically, this achieves a better mapping with the objectives of these two classes of students.
Course Policies	Unless during allowed group work, copying or allowing someone to copy homework solutions, machine problems, and exam solutions, from other students in the class, or from other sources is considered plagiarism and is treated very seriously by the Program of Computer Science and CEMSE. The usual penalty for a first cheating offense is a grade of zero on the homework or exam. The penalty for a second offense, or a particularly severe first offense, is an F in the course. All cheating cases are reported to the department. Multiple offenses can result in suspension or dismissal from the CS program or from the university. Please further refer to the KAUST policy on Academic Integrity.
Additional Information	

Tentative Course Schedule
(Time, topic/emphasis & resources)

Week	Lectures	Topic
1	Mon 08/30/2021	Introduction Introduction of instructor. Introduction to the course:

	Wed 09/01/2021	objectives, program outline, bibliography, grading. " Motivation by example: the case for intrusion tolerance. Intrusion-Tolerant Architectures: Concepts and Design (ITACD).
2	Mon 09/06/2021 Wed 09/08/2021	Foundations of Intrusion Tolerance (FIT): concepts and terminology "Review of fundamental security and dependability concepts : Classical fault tolerance and security, Dependability as a common framework, Open problems. Trust and trustworthiness; Fault models: AVI attack-vulnerability-intrusion. " Intrusion-Tolerant Architectures: Concepts and Design (ITACD); DSSA: chap.6 and 16. FIT methodologies, frameworks and mechanisms "Methodologies for FIT: error processing and fault treatment; intrusion detection and processing; vulnerability and intrusion forecasting. Wrapping-up: a metaphor for FIT. FIT frameworks and mechanisms: Secure and fault-tolerant communication, Software-based intrusion tolerance, Hardware-based intrusion tolerance, Auditing and intrusion detection, Automatic intrusion processing. " ITACD
3	Mon 09/13/2021 Wed 09/15/2021	Fault and Intrusion Tolerance strategies FIT Strategies: Fault Avoidance vs. Fault Tolerance, Confidential Operation, Perfect Non-stop Operation, Reconfigurable Operation, Recoverable Operation, Fail-Safe. Example Intrusion-Tolerant Networks and Architectures. Example Intrusion-Tolerance mechanisms. ITACD FIT Systems Paradigms "Review of basic dist. sys. paradigms: review of distributed systems models.; ordering, coordination and consistency. FIT paradigms: intrusion detection; self-enforcing vs. TTP; Byzantine protocols (agreement, multicast, consensus, atomic broadcast). Review of Replication management (partition-free and partitionable settings); review of General State Machine Replication and Quorums." IRMDV; ITACD; DSSA: chap.2 and 7
4	Mon 09/20/2021 Wed 09/22/2021	FIT Systems Paradigms "Review of basic dist. sys. paradigms: review of distributed systems models.; ordering, coordination and consistency. FIT paradigms: intrusion detection; self-enforcing vs. TTP; Byzantine protocols (agreement, multicast, consensus, atomic broadcast). Review of Replication management (partition-free and partitionable settings); review of General State Machine Replication and Quorums." IRMDV; ITACD; DSSA: chap.2 and 7 FIT Systems Paradigms "Review of Replication management (partition-free and partitionable settings); review of General State Machine Replication and Quorums (contd.). Intrusion tolerance paradigms (cont.): Byzantine State Machine Replication; Byzantine quorums; Threshold cryptography; Secret sharing (general, proactive); Information dispersal; Fragmentation and scattering; Erasure codes; randomisation; indulgence; separation of exec and agreement; trusted-trustworthy comp.; convergence functions; timing functions. " IRMDV; ITACD; Reading Module Mod. 1. DSSA: chap.7 and 12
5	Mon 09/27/2021	FIT Systems Paradigms "Review of Replication management (partition-

	Wed 09/29/2021	free and partitionable settings); review of General State Machine Replication and Quorums. Intrusion tolerance paradigms (cont.): Byzantine State Machine Replication; Byzantine quorums; Threshold cryptography; Secret sharing (general, proactive); Information dispersal; Fragmentation and scattering; Erasure codes; randomisation; indulgence; separation of exec and agreement; trusted-trustworthy comp.; convergence functions; timing and clock synchronisation functions. " IRMDV; ITACD; Reading Module Mod. 1; DSSA: chap.2 and 7 Modeling and Architecting Intrusion-Tolerant Systems "Models and assumptions, Architectural notions, A Reference FIT Architecture. FIT Middleware Design strategies. Algorithm design under several models. Advanced architecting concepts for FIT systems: architectures with hybrid trustworthiness; recursive building of trust & trustworthiness." IRMDV; ITACD; Mod. 2
6	Mon 10/04/2021 Wed 10/06/2021	Modeling and Architecting Fault-and-Intrusion-Tolerant Systems "Models and assumptions, Architectural notions, A Reference FIT Architecture. FIT Middleware Design strategies. Algorithm design under several models. Advanced architecting concepts for FIT systems: architectures with hybrid trustworthiness; recursive building of trust & trustworthiness." IRMDV; ITACD; Mod. 2 Tolerating Intrusions Intrusion-Tolerant Protocols (Arbitrary failure architectures): Byzantine atomic broadcast and consensus; information dispersal; Byzantine quorums; BFT State Machine Replication (BFT and variations). BFT Implementation Techniques. IRMDV; ITACD; Mod. 3
7	Mon 10/11/2021 Wed 10/13/2021	Tolerating Intrusions Intrusion-Tolerant Protocols (Arbitrary failure architectures): Byzantine atomic broadcast and consensus; information dispersal; Byzantine quorums; BFT State Machine Replication (BFT and variations). BFT Implementation Techniques. IRMDV; ITACD; Mod. 3 Trusted Components and Architectures Components and Architectures. Trusted Components: TPM, Trusted Platform Module; Hardware-based Secure Firewall; pitfalls and enhancements of IDS and SIEM; Automatic Remediation. IRMDV; ITACD; Mod. 4
8	Mon 10/18/2021 Wed 10/20/2021	Tolerating Intrusions "Intrusion-Tolerant Protocols (controlled failure and TTP architectures): quorums with controlled failure models; coordination service TTPs. Intrusion-Tolerant Protocols (hybrid architectures): local trusted components (ex. USIG); distributed trusted components (ex TTCB)." IRMDV; ITACD; Mod. 3
9	Mon 10/25/2021 Wed 10/27/2021	FIT Systems Example FIT projects and systems IRMDV; ITACD; Mod. 4
10	Mon 11/01/2021 Wed 11/03/2021	Invited Seminar Presentation and discussion of projects, phase 1
11	Mon 11/08/2021 Wed 11/10/2021	Invited Seminar Review of selected subjects.

12	Mon 11/15/2021 Wed 11/17/2021	Resilience to Persistent and Evolving threats "Limitations of distributed systems models. Limitations and enhancements of BFT protocol resilience. The makings of resilience: hardening, automation, diversity, adaptivity, sustainability. Intrusion tolerance paradigms (contd.): exhaustion failure; reactive and proactive recovery; exhaustion safety. Limitations and vulnerabilities of some current FIT paradigms: attackers work in real time; attackers pick the weakest link. Attack-resilient application scenarios: a case for hybrid distributed systems models." IRMDV; Mod. 5
13	Mon 11/22/2021 Wed 11/24/2021	Resilient Systems Example Threat Resilient IntTol Systems. IRMDV; Mod. 5 Resilience to Persistent and Evolving threats "Intrusion tolerance paradigms (contd.): diversity and obfuscation; proactive resilience. Proactive Resilience Application scenarios." IRMDV; Mod. 5
14	Mon 11/29/2021 Wed 12/01/2021	Resilient Systems "Example Threat Resilient IntTol Systems. Proactive/Reactive Recovery systems." IRMDV; Mod. 4, 5 Validating Threats and Vulnerabilities "Importance of Assumption Coverage. Attack Profiling. Vulnerability Assessment by attack injection." IRMDV; Mod. 6
15	Mon 12/06/2021 Wed 12/08/2021	Invited Seminar: Validating Threats and Vulnerabilities.
16	Mon 12/13/2021	Presentation and discussion of projects, phase 2"

Note

The instructor reserves the right to make changes to this syllabus as necessary.