IPSI Public Lecture Series 2011

Monday, Oct. 24	**Anestis Karasaridis, AT&T Labs Research** *“DNS Security”* The Domain Name System (DNS) is one of the most important network infrastructure services. It serves as the white pages for network resources and is used by almost every web, email and messaging application. DNS is also used as the base for new widely-deployed applications such as Voice over IP (VoIP) Telephony, Radio Frequency IDs (RFID), Content Distribution Networks (CDN), and Mobile voice and data services. Since security was not a primary concern in the design of the protocol, it is amenable to wide scale attacks that can lead to either denial of service or serious security violations (e.g., client redirection to illegitimate sites). Given that availability and reliability in many of the applications that depend on DNS are critical, DNS security is of outmost importance to any organization that provides network-based services. In this talk, we will provide an overview of following topics • Protocol overview and typical service architectures • Main protocol and implementation vulnerabilities • Monitoring and detection of various attacks • Prevention, protection and mitigation of attacks • DNSSEC and DNSCurve • DNS in next generation Mobile Services	4pm - 6pm Bahen Centre, 40 St. George Room 1130
Monday, Nov. 7	**Colin Mckay, Public Policy - Google** *“Discovery and Delight in Big Data”* Big data - extraordinary data sets, flexible computing architecture and precise algorithmic analysis - can shed light on difficult scientific problems. It can uncover associations among data trends and pinpoint inflection points. It can inform public policy decisions. Oh, and help focus your purchasing decisions. Trust, represented in part by data protection safeguards, is an essential part of the big data ecosystem. As our interactions with data-based services, sensor-based tools and integrated data networks multiplies, how does this ecosystem remain effective and trustworthy? Drawing on real life examples, this talk will discuss how big data is fueling innovation and revitalizing public policy.	4pm - 6pm Bahen Centre, 40 St. George Room 1200
Monday, Nov. 14	**Ashish Khisti, Electrical Engineering, University of Toronto**	4pm - 6pm Bahen Centre,

	“How Can Physical Layer Resources Increase Wireless Security “ Traditionally wireless networks have been considered to be a weak link in security of network systems. The broadcast nature of the wireless medium as well as the limited computation power of mobile devices make traditional cryptographic techniques vulnerable to various attacks in wireless systems. In this talk we will discuss a new emerging research area - Physical Layer Security (PHY-SEC). Unlike traditional cryptographic approaches, PHY-SEC exploits physical layer resources such as multiple-antennas, power-control mechanisms and time/frequency diversity to develop new methods for encrypting data. We will discuss both theoretical results as well as some potential applications of these techniques.	40 St. George Room 1190
Friday, Nov. 21	**Hong (Vicky) Zhao, Electrical Engineering, University of Alberta** **“***Multimedia Forensics for Traitor Tracing”* Recent development in multimedia and network technologies has raised the critical issue of protecting multimedia content and enforcing digital rights. To address the post-delivery protection of multimedia, digital fingerprinting is an emerging technology to identify users who have legitimate access to multimedia content but use it for unintended purposes. It provides proactive forensic tools to trace the illegal usage of multimedia by inserting unique identification information (" fingerprint ") into the content before distribution. However, the global nature of Internet enables a group of attackers to collectively and effectively remove traces of digital fingerprints. These attacks, known as collusion, pose serious threats to protecting the intellectual property rights of multimedia. Therefore, it is essential for multimedia fingerprinting to resist such multi-user collusion. In addition, in digital fingerprinting, different users have different objectives and they influence each other s decisions and performance. It is important to investigate how they interact with and respond to each other. Better understanding of behavior forensics can offer stronger protection of multimedia. This talk addresses various issues in digital fingerprinting and introduces recent advances in multimedia forensics for traitor tracing. First, different collusion strategies will be	4pm - 6pm Bahen Centre, 40 St. George Room 1190

	discussed and compared. Then, traitor tracing capability and collusion resistance of multimedia fingerprinting will be evaluated, which provides fundamental guidelines for anti-collusion fingerprint design. Finally, the fairness dynamics among colluders and the traitor-within-traitor behavior forensics will be formulated and analyzed.	
Monday, Nov. 28	**Abraham Drassinower, Law, University of Toronto** *"Copyright Infringement as Compelled Speech"* This paper offers a rights-based account of copyright law. Its central proposition is that a " work " subject to copyright is a communicative act. This proposition grounds two further propositions. The first is that, because a work subject to copyright is a communicative act, infringement of the right attendant on the work is best grasped as a disposing of another's speech in the absence of her authorization. Copyright infringement is wrongful because it is compelled speech. The paper develops this view of copyright infringement through analysis of the wrongfulness of unauthorized publication of unpublished works. In this vein, the paper considers, albeit briefly, the distinction between a privacy focus and a copyright focus on unauthorized publication. The second proposition is that, because a work is a communicative act, rights attendant on it must be consistent with the communicative rights of others, even - or especially - where such rights require unauthorized reproduction of a work for the purposes of responding to its author's communication. Copyright doctrine protects not an author's absolute rights over her work but only such rights as are consistent with the structure of the dialogue of which the work is but a part. The concept of the work as a communicative act thus traverses both the justification and the limitation of copyright. The paper concludes with some remarks on the implications of this construal of copyright law for our understanding of the public domain in particular and of copyright law generally. As distinct from a policy-driven incentive-based account, a rights-based account can help us broach the deep significance of copyright law as an effort to organize normatively an irreducible aspect of human interaction.	4pm - 6pm Bahen Centre, 40 St. George Room 1190