Prof. Ari Trachtenberg, Fall 2018

**When:** Mondays/Wednesdays 12:20-2:05pm

**Pre-requisites:** EC521, or consent of the instructor

**Description:** As our lives increasingly integrate with computerized systems – be they pacemakers, smartphones, or semi-autonomous vehicles – so too does our dependence on cybersecurity research and practice. These devices, with their assorted subsystems and sensors, endemically leak information about their activity and the activity of their users through *side-channels*, the unplanned channels of information arising from the specific implementation rather than the design of the device. As opposed to yesteryear’s engineers, who typically focused on natural and inadvertent failure modes, today’s engineers must increasingly design for malicious adversaries intent on studying and exploiting these channels, sometimes with state-level resources. To remain relevant, the informed engineer must constantly remain on the forefront of innovation in this area.

This course will cover advanced topics at the state-of-the-art of modern cybersecurity, focusing on *side-channels and their uses* in three broad directions:

- Theoretical concepts reinforced with practical hands-on exercises,
- Reading, implementing, and presenting results from the literature,
- Tackling open problems in the field in project groups.

Potential Topics:

- **Channels:** timing (software, crypto, ntp), power, network (voice-over-IP, SSL, web), sensors (fingerprinting, location, keylogging), storage (RAM, flash), binary (reversing, analysis), cache (flush, speculative execution), stack (overflows, return-orientation), UI (hijacking), wifi (packets-in-packets, signal corruption, SSID, SDR)

- **Tools:** machine learning, natural language processing

- **Applications:** Android, ransomware, malware, practical crypto, anomaly detection, cryptocurrency

Students are expected to have background knowledge from a solid graduate-level cybersecurity course, including a technical understanding of ethics, operating systems, networking, and system and application programming.

Key-press picture courtesy of Xiaohui Ma’s MS project. Graph courtesy of work by Klausner, Boyle, Wu, Starobinski, and Trachtenberg. Microrprinting courtesy of US government (and Wikipedia).