Cybersecurity and Privacy
Session co-chairs: Daniela Oliveira and David Brumley

How do we engineer systems that are both secure and respectful of user privacy? Our societal dependence on computers makes this question extremely relevant, but also nuanced. Perhaps surprisingly, we know how to engineer highly secure, privacy-respecting systems. First, an engineer rigorously states the security and privacy goals of the system. For example, typical goals include the confidentiality of system data, and the systems' integrity and availability.

Second, the engineer defines what type of threats the system should be resilient to. For example, will an adversary attempt to infect the system through software vulnerabilities in applications? Or will he attempt to compromise the integrity of the operating system, which manages how applications access hardware resources? Worse still, is the adversary targeting the hardware, the lowest level of abstraction? Attacks on the hardware render all security solutions residing at operating system and application-level useless. The attacker could also discover side-channels, such as the system's electromagnetic radiation to discover cryptographic keys. Further, the attacker can leverage weaknesses in network protocols designed in the 60s and still used today to compromise system availability.

Third, the engineer proves the system design achieves the security goals in the presence of the adversary. Finally, he implements the system and formally verifies the implementation is correct. Rigorous models and proofs, however, are performance expensive and problem specific. You get what you pay for, and highly secure systems are not cheap.

Further, the Internet Era exposes the challenge of protecting people's privacy, such as personal information, life habits, social networks, heath conditions and personal beliefs. Who owns and can profit from people's data? How can people delete or hide information from the Internet? Or should they? Isn't it rewriting history?

In practice the question is often not how to build a secure system, but how to engineer a system that is as secure as possible given practical construction constraints. New systems are almost always built on top of existing hardware, operating systems, software, and network protocols that provide fixed capabilities and have both known and unknown weaknesses. A well engineered system follows a defense in depth strategy that incorporates both layered protection and mechanisms for detecting and mitigating the effects of successful attacks. For example, a web server handling credit card numbers may use a network firewall to restrict access to only authorized computers, an intrusion detection system for detecting suspicious behaviors, and a secure communication protocol with its clients to encrypt the credit card numbers.

The best results come when security and privacy are engineered in from the beginning. Experience shows that retrofitting security and privacy measures into existing systems is difficult and often results in relatively weak security guarantees.

Finally, the user is often just as important to security and privacy as the technology. Users make decisions on what to share, what links to click, and what software to install. A recent surge in research shows that existing systems often have unintuitive security and privacy mechanisms, ultimately making the user the weakest link. Research has also shown user-centric designs help the user to make good security and privacy decisions.

In this session, Dr. Payne will start off with a talk that describes the various security and abstraction levels of modern systems, and security consequences at each layer. Dr. Roesner will then describe the role of the user, and how we can design interfaces that help them make better security decisions, with a focus on mobile platforms. Next, Dr. Fu's talk will address security within medical devices. Medical devices have different characteristics, and highlight different challenges to a security engineer. Finally, Dr. Vagoun will conclude the session with a talk on the US government's view about the challenges and frontiers in engineering cybersecurity.