“Focus on Web Privacy”
Presented by Gunes Acar, Princeton University

Abstract:
We present two web-based attacks against IoT devices that can be performed by any malicious web page or third-party script, even when the devices are behind NATs. In our attack scenario, a victim visits the attacker's website, which contains a malicious script that communicates with IoT devices on the local network that have open HTTP servers. We show how the malicious script can circumvent the same-origin policy by exploiting error messages on the HTML5 MediaError interface and by carrying out DNS Rebinding attacks. We demonstrate that the attacker can gather sensitive information from the devices (e.g., unique device identifiers and precise geolocation), track and profile the owners to serve ads, or control the devices by playing arbitrary videos and rebooting. We propose potential countermeasures to our attacks that can be implemented by users, browsers, DNS providers, and IoT vendors.

Bio:
Gunes Acar is a postdoctoral research associate at Princeton University's Center for Information Technology Policy. His research interests involve web tracking measurement, anonymous communications, and IoT privacy and security.