encryption (AE) ciphers to the standards could prevent this attack in the future. Besides this cryptographic weakness, HTML emails also play an important role.

While it is possible to port Efail-like attacks to any data standard supporting backchannels, HTML makes the attack particularly easy. HTML emails and especially remote content loading (e.g. images, style sheets) can be used for user tracking and were known to be a privacy issue for many years. While it is quite common for privacy advocates to disable HTML in emails completely, most non-technical users insist on HTML emails because they value rich typesetting in their day-to-day work. This raises some questions:

Is HTML the way to go for future typesetting of emails? Are there safer alternatives?

What is a safe subset of the HTML standards that allows rich typesetting, but without allowing user-tracking or Efail-like attacks?

How to enforce this safe subset in existing emails clients?

3.8 How to Design Browser Security and Privacy Alerts

Lynsay Shepherd (Abertay University – Dundee, GB) and Karen Renaud (University of Abertay – Dundee, GB)

Main reference Lynsay A. Shepherd, Karen Renaud: "How to design browser security and privacy alerts", CoRR, Vol. abs/1806.05426, 2018.
URL http://arxiv.org/abs/1806.05426

Browser security and privacy alerts must be designed to ensure they are of value to the end-user, and communicate risks efficiently. We performed a systematic literature review, producing a list of guidelines from the research. Papers were analysed quantitatively and qualitatively to formulate a comprehensive set of guidelines. Our findings seek to provide developers and designers with guidance as to how to construct security and privacy alerts. We conclude by providing an alert template, highlighting its adherence to the derived guidelines.

3.9 REASON – A programmable architecture for secure browsing

Stefano Calzavara

Joint work of Stefano Calzavara, Riccardo Focardi, Niklas Grimm, Matteo Maffei
Main reference Stefano Calzavara, Riccardo Focardi, Niklas Grimm, Matteo Maffei: "Micro-policies for Web Session Security", in Proc. of the IEEE 29th Computer Security Foundations Symposium, CSF 2016, Lisbon, Portugal, June 27 - July 1, 2016, pp. 179–193, IEEE Computer Society, 2016.
URL https://doi.org/10.1109/CSF.2016.20

The REASON project is a research proposal which I wrote with the goal of improving the security architecture of web browsers. More specifically, REASON aims at replacing the traditional Same Origin Policy (SOP) of web browsers with a programmable security monitor amenable for formal verification.

Preliminary evidence of the effectiveness of the proposal was given in a paper at CSF'16, where a small fragment of the architecture was designed and implemented. This talk will discuss the main motivations behind REASON, its benefits and a few ideas on how to implement it on top of existing browsers.