tutorial outline

• The Kaminsky Attack on DNS
  – An inspiring and elegant off-path attack
  – We use figures from the blog post by Steve Friedl
  – http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

• A brief overview of DNSSEC
  – DDoS attacks and DNS key choices (Roland)

• DNSSEC’s zone enumeration problem (and NSEC5)
  – We use slides from my joint work on NSEC5 with Dimitris Papadopoulos, Leonid Reyzin, Moni Naor, Sachin Vasant, Asaf Ziv

• DNS privacy? Or traffic analysis on Encrypted DNS
  – Haya Shulman’s attack: https://www.ietf.org/mail-archive/web/dns-privacy/current/pdfWqAlUmEl47.pdf