My research focus: implementation attacks
(a.k.a. projects where you can get electrocuted)

• Side channel attacks:
  • Power analysis
  • EM analysis
  • Cache attacks

• RFID security
Typical lab setup
**BATT out of Hell – Security Risks of After-Market Accessories**

---

**General Description**

- **Motivation**: End users install unverified aftermarket batteries in their phones. Can we design a malicious battery that attacks the phone via the power interface? What secrets can the battery steal? How can the battery exfiltrate data? can we do this with a standard battery if we install malicious firmware on its controller? How can we defend ourselves?

- **Approach**: Analyze the Rx and Tx paths of the attack, design and evaluate countermeasures.

- **Expected Benefit**: Awareness of a new, high-impact security risk on a popular device.
Spy in the Sandbox – Side-channel Attacks in Javascript

- **Motivation:** Unprivileged Javascript can use side-channel attacks to learn about the memory activity of the entire system.
- **Approach:** Analyze the capabilities of this attack method, find out what we can compromise (Kernel? Encryption? Network? Keylogging?) design and evaluate countermeasures.
For more info:
yos@bgu.ac.il

p.s. Join the BGU Cyber mailing list! http://cyber.bgu.ac.il/join