**describe the research questions**

How secure is the internet?

What exploits can adversaries use to hack into popular ssh and tls hosts?

**Contributions**

Numerical & tangible issues with modern internet security – inadequate randomness

0.75% TLS certificates share keys due to insufficient entropy 0.50% RS private keys able to be obtained from this

**methods**

three phases: discovering IP addresses accepting connections on TCP port 443 (HTTPS) or 22 (SSH); performing a TLS or SSH handshake and storing the presented certificate chain or host key; and parsing the collected certificates and host keys into a relational database (page 3)

**results**

Flaws in design by shifting responsibility to other layers, instead developers should fix problems they can

**Limitations**

techniques have likely only revealed a small fraction of the hosts prone to repeating DSA signature randomness. (p 15)