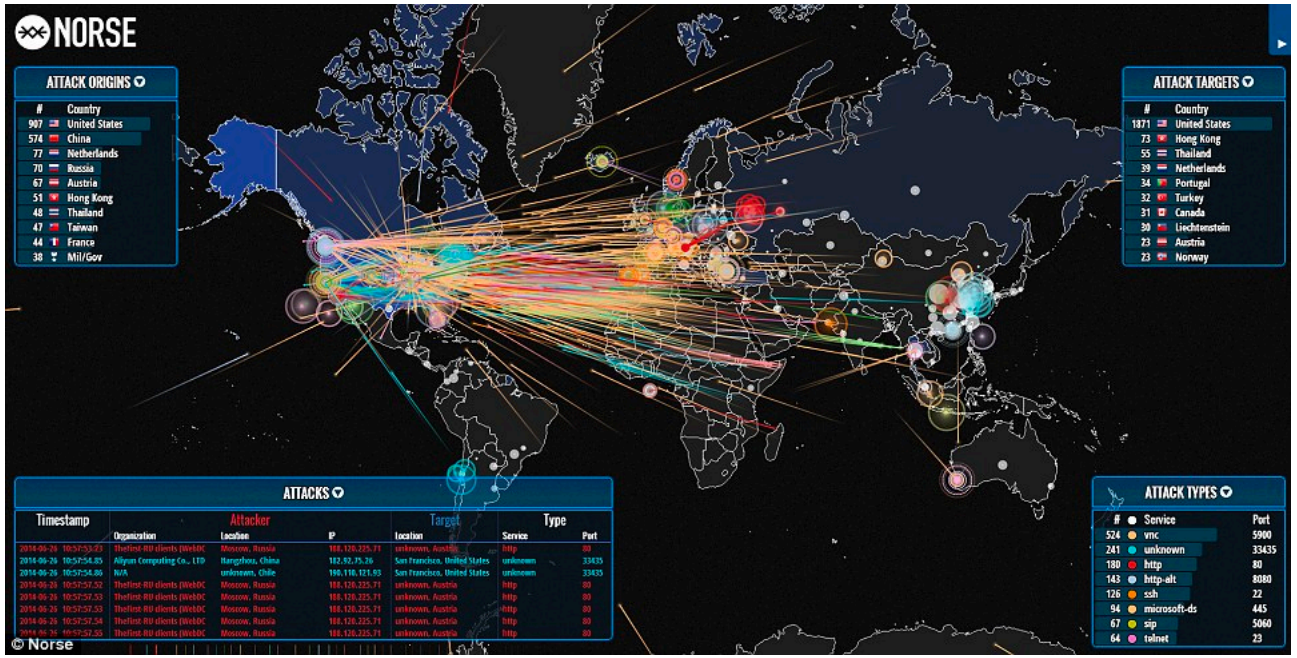
Network and Systems Security

Ang Chen

Department of Computer Science
Rice University

Challenge: Security



- What do we need to do to make sys/nets more secure?
  - Security as a first-class goal in sys/nets design

Discussed questions

- What are the key trends in sys/nets and what are their security implications?
- How can the SaTC and NeTS/CSR communities complement each other?
  - e.g., different mindsets, approaches
  - What can the NeTS/CSR community learn from the SaTC community? Vice versa. Cross-community collaboration?
  - How can we develop ”principled approaches” to security?
- What are the BIGGEST problems in this area?

Q1: Key trends + security implications

- 1. Dominance of end-to-end encryption
  - Traffic over TLS, good for privacy, harder to do DPI
  - Perhaps applications could "tag" extra data to packets
- 2. Dominance of datacenter networks
  - Most traffic sent over the public Internet → over datacenters
    - Extreme view: No public Internet, just access networks + datacenters
  - Security protections are easier to deploy, privacy is harder
- 3. Emergence of programmable networks
  - Programmable switches, Smart NICs, and FPGAs
  - Opens up new opportunities to deploy security "in-network"
  - Needs to anticipate new risks, too

Q2: Bridges across communities

- 1. Should we have CSR/NeTS session at Blackhat?
  - "Bug bounty" programs from NSF for networks+systems
  - Create incentives for "correctness"
- 2. Principled security
  - Security cannot be bolt-on from the top
  - Needs a systematic approach to securing the foundation
- 3. SaTC + CSR/NeTS
  - Science of attacks
    - "Design patterns" for attacks, independent of layers of the stack
  - Science of defenses
    - Developing foundations for security, understanding the tradeoffs

Q3: BIGGEST problems

- 1. Designing a secure foundation for sys/nets
- 2. Trust and trust management on top of this foundation
- 3. "Division of labor" for security (net vs. endpoint sys)
- 4. Systematic understanding ("sciences" of attacks/defenses)
- 5. Understand which types of research gets used in practice
- 6. Support from NSF+DARPA to drive real deployments