Security & Privacy

Botnets, configuration analytics, data sharing

DNS data sharing

- aggregated statistics; anonymized
- semantic interpretation of domain names
- hypothesis testing of (dis-)similarity of traffic
- Botnet master detection
- cannot secure US networks unless you secure the other parts of the world

Security & Privacy

Botnets, configuration analytics, data sharing

Configuration analytics

- quantify mis-configurations in firewalls and BGP
- organizations verify what they got is what they paid for
- compare policies across institutions and analyze differences

Security & Privacy

Botnets, configuration analytics, data sharing

Automated incident collection and analysis

- Automatically collect relevant data to a particular incident to be reported
- IODEF standard; SES
- trust fabric

Security & Privacy

Botnets, configuration analytics, data sharing

Participants

Basheer Al-Duwairi, Ahmed Al-Hammori, Ehab ElShaer, Sonia Fahmy, George Kesidis, Sherif Khattab, Engin Kirda, Ken Klingenstein, Vern Paxson, Zhi-Li Zhang