ICANN's Identifier Systems Security, Stability and Resiliency Team

ITU Workshop on Child Online Safety – Lilongwe: July /20 /2016

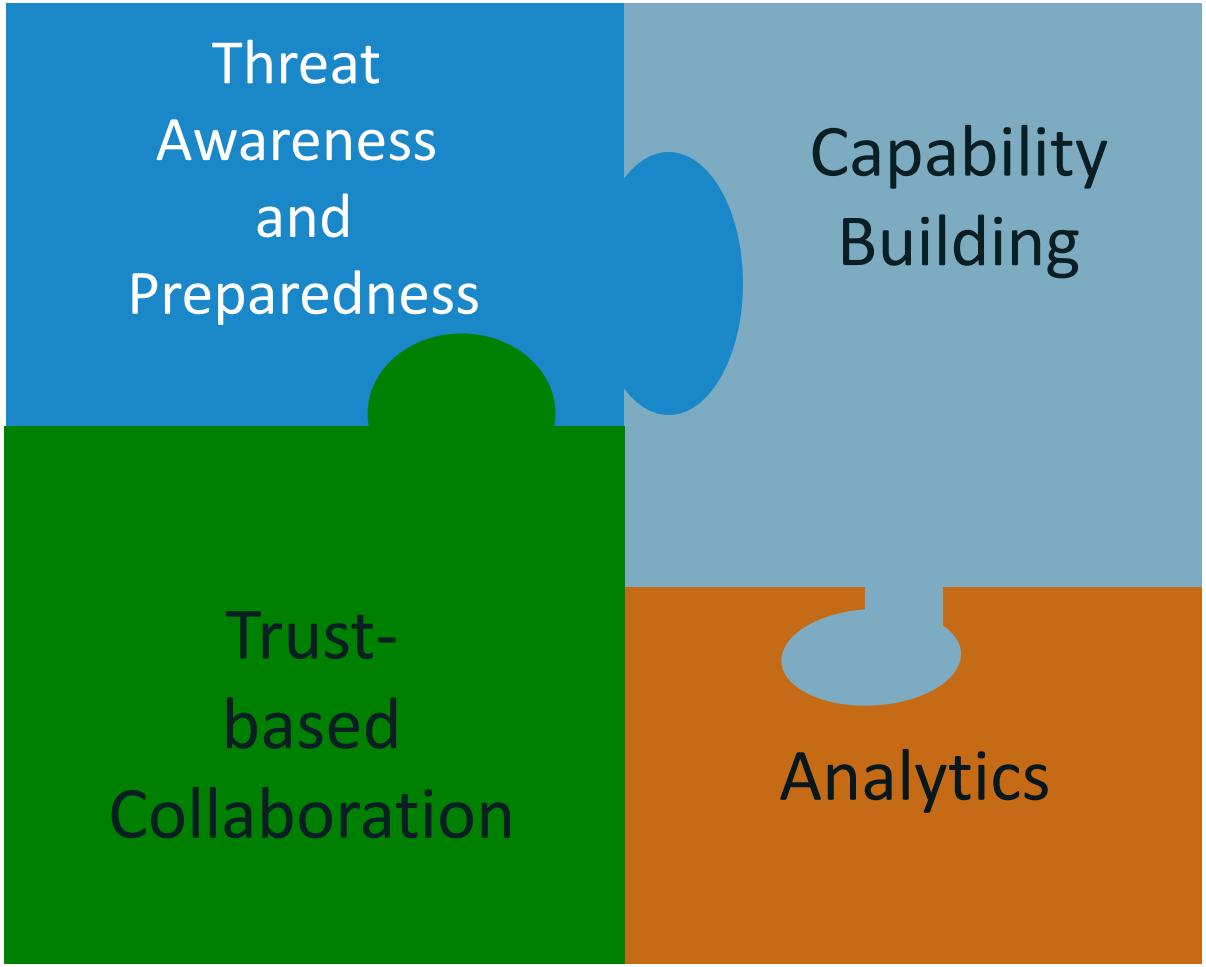
bob.ochieng@icann.org

What is ICANN?

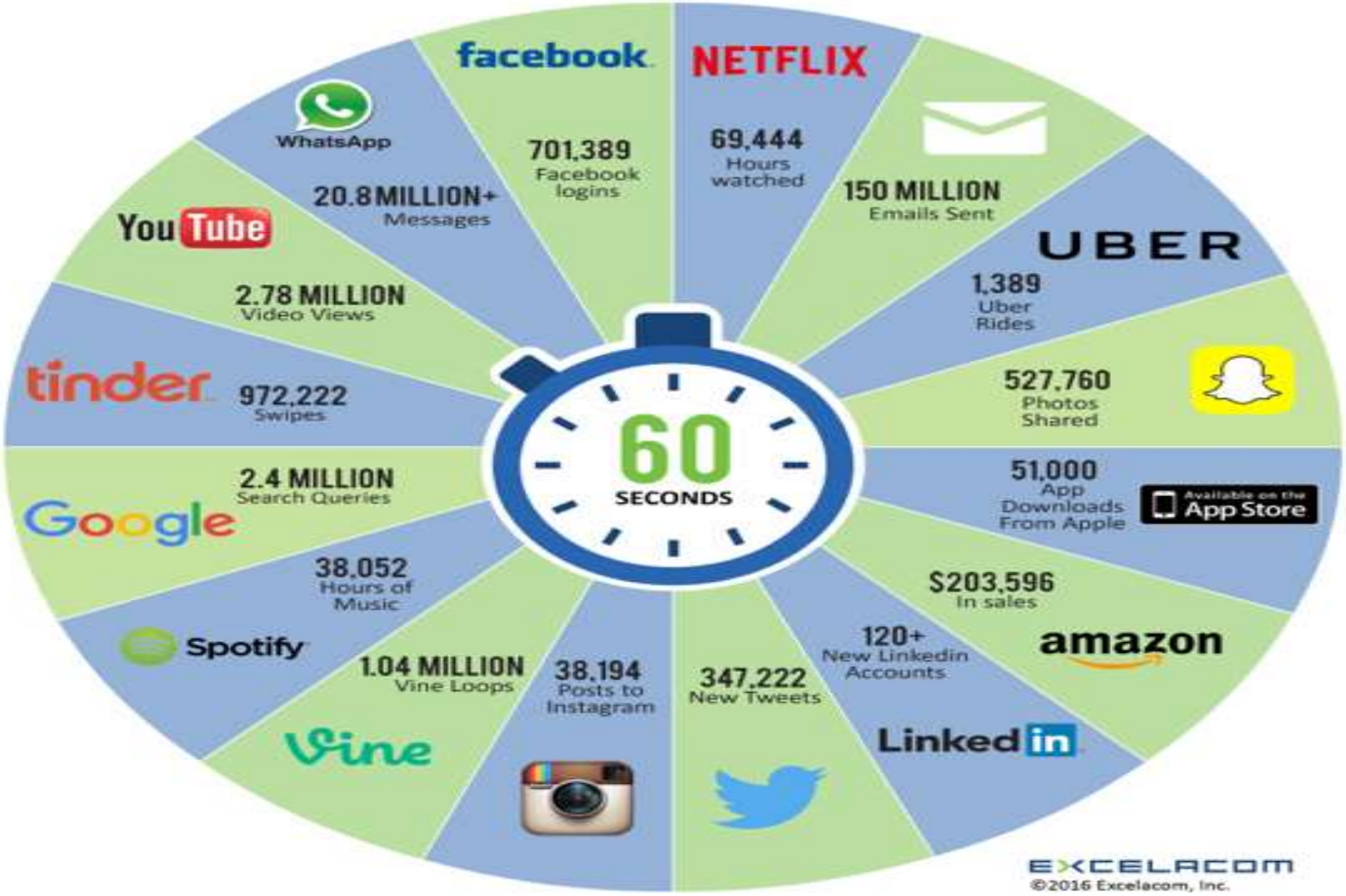
The Internet Corporation for Assigned Names and Numbers (ICANN) is a global multistakeholder, private sector-led organization that manages Internet resources for the public benefit

- ICANN coordinates the top-level of the Internet's system of unique identifiers via global, multistakeholder, bottom-up consensus policy processes, with the outcome of those processes implemented via the IANA Functions.

ISSSR Team: Areas of Operation



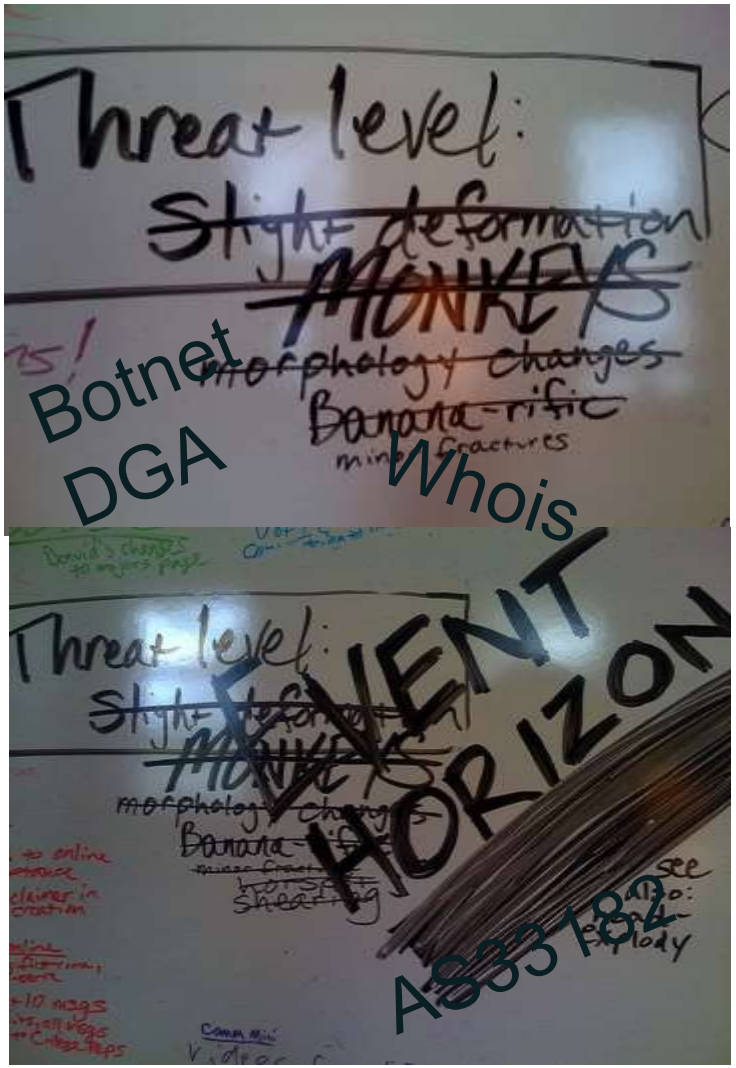
2016 What happens in an INTERNET MINUTE?



Threat Awareness

ICANN's ISSSR Team exchanges or acts on threat intelligence or incidents involving global Internet identifiers to mitigate threats

- DNS Coordinated Vulnerability Disclosure
- Tactical response to attacks
- Collaborative incident response



https://www.flickr.com/photos/opacity/

Capability Building

The IS SSR Team

- Provides technical training to ccTLD operators or public safety communities
  - Registry operations
  - DNSSEC
  - Investigating identifier systems abuse
- Collaborates on cybersecurity matters with security communities
  - APWG, MAAWG, DNS OARC…
- Shares cybersecurity subject matter expertise with legislation or policy makers or government agencies

Analytics

ICANN's ISSSR Team studies identifier system abuse or performance using event or reputation data

- Security threats e.g., spam, phishing, C2, malware…
- Whois accuracy
- DNS security, stability, resiliency

Trust-based Collaboration

ICANN's ISSSR team engages with cybersecurity and public safety communities

- To identify or mitigate identifier system abuse
- Share information related to identifier system misuse

Team also acts as a trusted introducer between DNS and information security communities

https://www.flickr.com/photos/slagheap/

How Does Trust-based Collaboration Work?

- Private- and public sector investigators cooperate 24x7 using trusted communications channels
- Information sharing
  - Malware, phishing, spam samples
  - Host names, URLs, addresses, geo-location
  - Activities of persons of interest (e.g., social media posts)
  - Points of contact (targets, victims, operators, investigators)
- Coordination or hand off
  - Mitigating DDoS by squelching sources
  - Providing evidence of AUP violation to operator for action

Trust is Earned

- New participants earn nominations from existing members and are vetted prior to admission
  - Personal references,
  - Prior collaboration and
  - Reputation
- Individuals put own reputation and membership at risk when they nominate
- Strict codes of conduct
- Self-policing model

Is trust-based collaboration effective?

Yes. It reduces the attack surface in several ways:

- Sharing “data feeds” forms the bases for action
- Sharing malware samples expedites remediation
- Sharing intelligence improves dossiers on suspected criminal actors
- Reduces time from threat identification to containment or mitigation
- Gives participating law enforcement agents insights other than direct complaints

Thank you