Why IP Alerts May Require New Technology

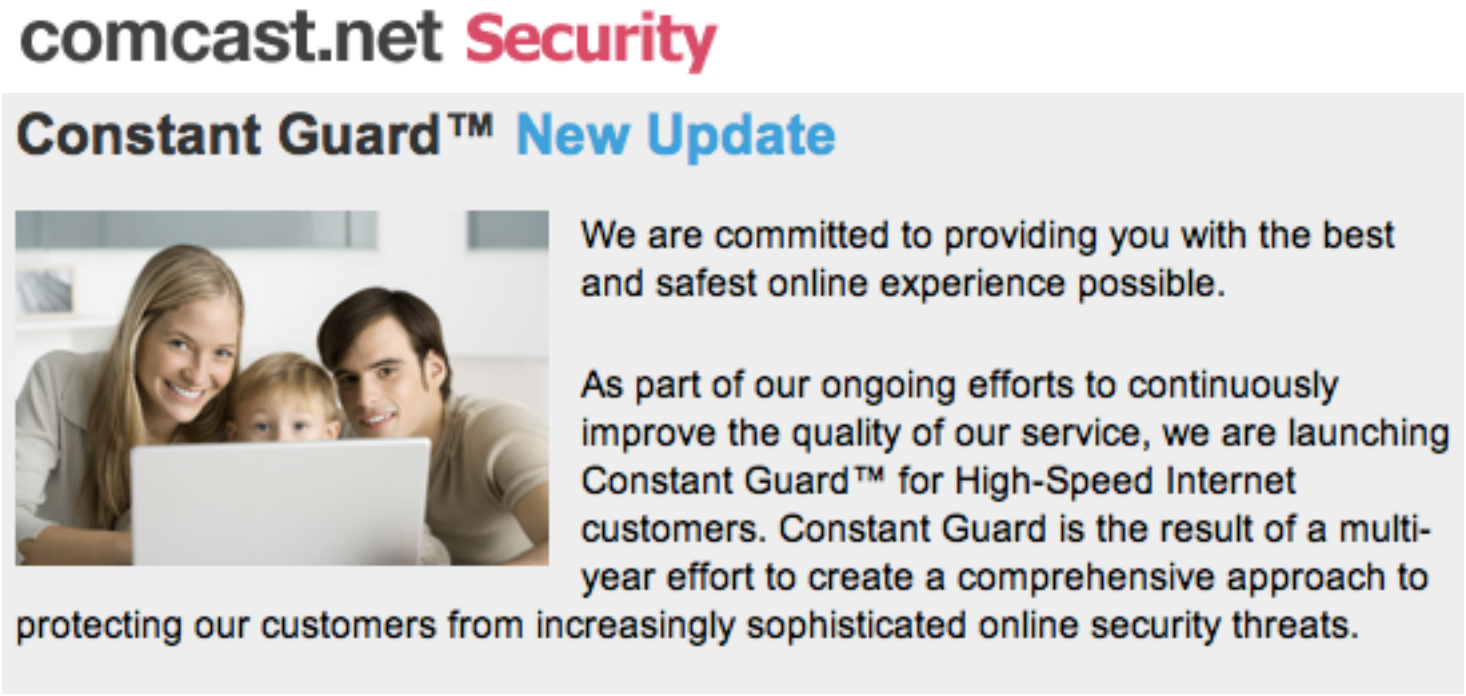
Nick Feamster
Georgia Tech

Nick Feamster

Georgia Tech Computer Science
Network Operations and Internet Security Lab
feamster@cc.gatech.edu
http://www.cc.gatech.edu/~feamster/
http://connectionmanagement.org/

- **Research:** Network security and operations
- **Goal:** Improve network availability and performance in the face of accidental or intentional degradations or faults
- **Areas**
  - **Security and trust:** spam filtering, phishing
  - **Transparency/Anti-censorship:** open information access
  - **Network Management:** fault diagnosis, provisioning
  - **Economics:** effects of tiered pricing for Internet connectivity
  - **Reliability:** fast recovery from failures

ISPs Already Help Users Fight Malware



- Comcast “Constant Guard”: Observes user traffic and notifies user about possible compromise
- **Notifying a user about possible piracy: Significantly different!**

Malware and Spam Detection: No Content Inspection Necessary!

- **Domains:** Can detect using lookup features
- **Spam:** Can detect using sending behavior
  - Source ISP of sender
  - Geography (distance traveled)
  - Time of day
- **Malware:** Can detect using network statistics
  - Coordinated behavior across “bots”
  - Correlation with attack traffic

DNS Domain Reputation (How Constant Guard Works)

- Domain registration and resource record establishment **occur before attacks take place**
- DNS infrastructure for scam domains is located in **different address space regions and autonomous systems** than the infrastructure for legitimate domains.
- **Early lookup patterns** for a newly registered malicious domain differ significantly from the patterns for a legitimate domain

SNARE: Spatio-Temporal Network Level Automated Reputation Engine

- Can detect spam with state-of-the-art accuracy based on features from a single packet
- **No content inspection: Packet headers only!**

Technology Review
PUBLISHED BY MIT

A Better Way to Shoot Down Spam

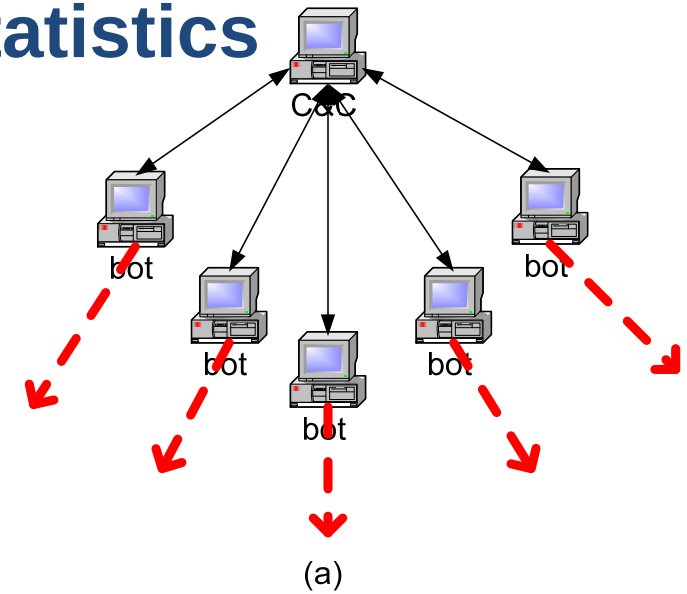
Junk mail can now be identified based on a single packet of data.

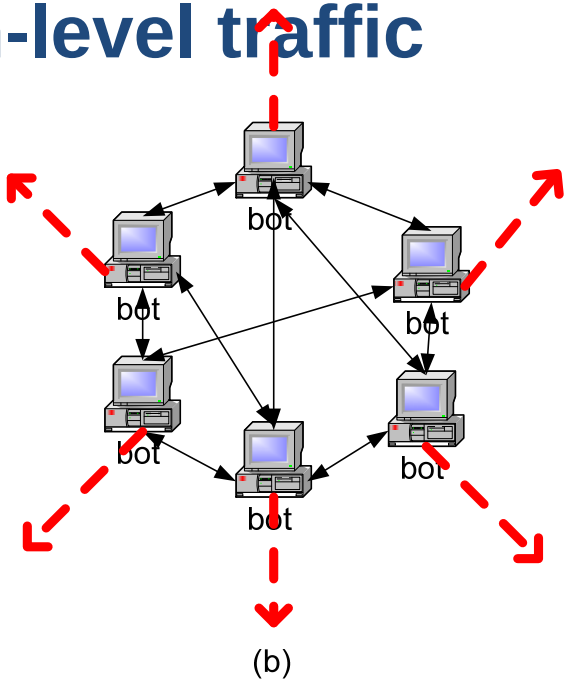
By Rachel Kremen WEDNESDAY, JULY 29, 2009

New software developed at the Georgia Institute for Technology can identify spam before it hits the mail server. The system, known as SNARE (Spatio-temporal Network-level Automatic Reputation Engine), scores each incoming e-mail based on a variety of new criteria that can be gleaned from a single packet of data. The researchers involved say the automated system puts less of a strain on the network and minimizes the need for human intervention while achieving the same accuracy as traditional spam filters.

Botnet Detection: Coordination

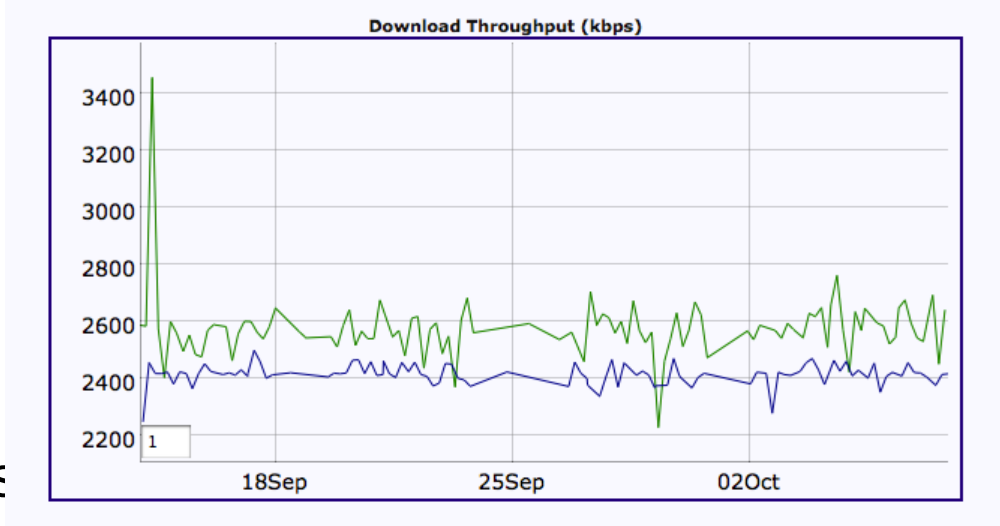
- A **coordinated group** of **malware** instances that are **controlled** by a botmaster via some C&C channel
  - Hosts that have similar C&C-like traffic *and* similar malicious activities
- **Can be detected with high-level traffic statistics**





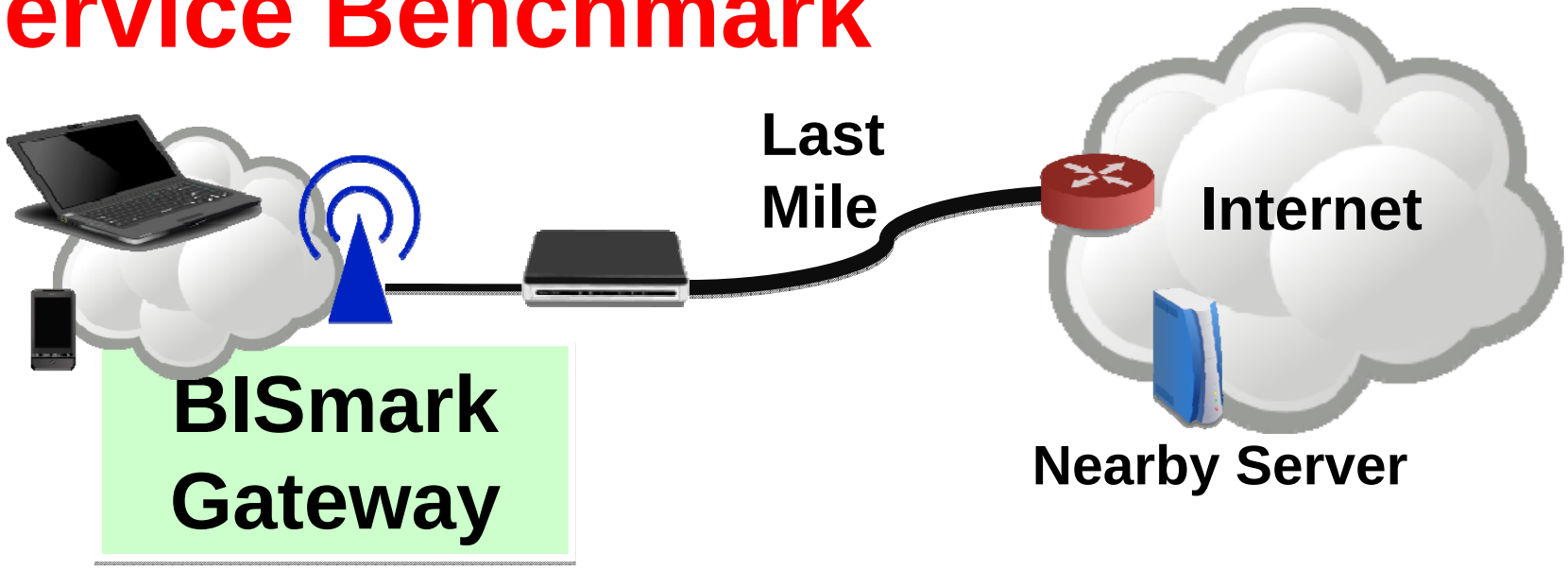
ISPs Have Other Interests, Too

- **Bandwidth constraints:** Access network performance is already strained
  - Content pirates may be significant bandwidth “hogs



- **Vested interests:** Some ISPs are now becoming content providers

BISmark: Broadband Internet Service Benchmark



- **Goal:** Better transparency for network performance
- OpenWrt firmware with custom measurement suite
  - Periodic active measurements of access link, home network
  - Metrics: Throughput, latency, jitter
- Current hardware: Netgear 3700v2 router
  - Planned support for other hardware platforms

Summary

- ISPs don’t need to inspect content to perform common security/management tasks
- Detection of piracy is not a natural extension
- ISPs may have other interests
  - Can incentives be better aligned?

Nick Feamster
feamster@cc.gatech.edu

http://projectbismark.net