Who + What + Where

The Internet and Security Ops Community
Personal note

Many of my colleagues can reasonably disagree with some of the choices and reflections I make on the following slides. What follows is a casual, if imperfect, look at some communities that have been useful to many operators over the years.
Typical key players

- Those with “root” on interesting components
  - ISP/network (router) engineers
  - DNS admins
  - content providers
- Protocol designers and software implementers
- Researchers
  - often a catch-all, especially for security folk
- Policy wonks and loud mouths, for better or worse
Becoming a player without a net

- Be an active participant in a volunteer group
- Get data, synthesize or analyze it, then publish
- Host a niche mailing list
- Be a miscreant (not recommended)
Communities on lists

• Most activity takes place on “real” mailing lists
• IRC and Jabber are common supplements
• Some communities are secret, private or restricted
  • many good ones are open, but can be noisy
• Most have colorful histories and persons involved
• Recommendation:
  • read and search the archives before posting
*NOG*

- Network Operator Group (NOG)
  - often as part of the regional NIC
- Face-to-face meetings are common
  - for business, relationship building, learning, fun
NANOG

• Recurring and “hot” topics in networking
• Moving from MERIT to community control
• Meetings, best in person, are a useful resource
• List is noisy, but high-value nuggets occasionally
  • “bans” do happen
• List personality often != meat space personality
IETF

• Stewards of Internet protocols past, present, future
• Wide array of “working groups” to participate in
• Most work done on various mailing lists
• Lots of good RFCs you should consider reading
• ID to RFC can be inexorably time consuming
• Appeals to protocol developers
  • but some operationally-relevant informational and BCP work frequently occurs
FIRST.org

- Organized around “teams”, not individuals
- Good international CERT/CSI RT participation
- AGMs and TCs are generally well received
- Mailing list has a history of trust/privacy lapses
- PGP and cert for lists and web, but limited usage
nsp-security

• One of the first informal and private netop lists
• Spawned to help ISPs coordinate DDoS response
• Avoided FIRST “teams” concept
• Largely restricted to those with “enable”
  • some exceptions, but rules kind of squishy
• Vetting requires two vouches, not from same org
• Somewhat arbitrary two person per org limit
  • again, with some squishy exceptions
• Very effective in early 2000's (e.g. Slammer)
YASML, ii

- Malware analysis oriented lists
- One has a vetting model similar to nsp-security
- The other managed largely by a single maintainer
- Common activities include:
  - sample and exploit sharing
  - reverse engineering and outreach help
ops-trust

• Intended to be an improved nsp-security
• More formal participation guidelines, wider appeal
• Hasn't turn out the way I anticipated
  • and not exactly as I wanted
• Hasn't had much of an impact yet, time will tell
• Nice GUI for membership directory and vetting
• Sub-groups for threat / issue specific projects
• Might go non-profit ala DNS-OARC or FIRST
linuxbox and isoI

• If not invited to the cool kids party, start your own
• Various lists, some private and a conference
• Motivation and personality seemed specious
• As more “known” ops participate, credibility rises
DNS-OARC

- DNS-oriented operations focus
- Sponsored by ISC (maintainers of BIND)
- Non-profit, funded by membership dues
- Provides some funded infrastructure
  - data sharing capability, ticketing, monitoring
- ICANN proposed DNS-CERT contention
REN-ISAC

- Only for R&E security community
  - R&E is clue rich and an interesting place to be
- Initially no cost, now membership dues required
- Provides alerting, support, data feed services
- Yearly meeting, mailing lists, IRC and “tech bursts”
Other communities of note

- UNISOG, precursor to REN-ISAC
- Internet2-associated (e.g. multicast, IPv6, netguru)
- EDUCUASE
- Various securityfocus mailing lists
- Various vendor specific lists (e.g. *-nsp@puck)
- Various protocol specific lists
Other events and venues

- Cisco Networkers
- Interop
- DEFCON, Black Hat, CanSecWest, etc.
- USENIX, ISOC, ACM and IEEE events
- Chicago local gatherings
  - e.g. 2600, 2621, chisec, student groups
- Training versus education
Reading matter

• ACM, IEEE, Usenix journals and papers
  • my preference generally
• Blogs, Twitter, RSS, “free magazines”
  • I literally never read any of them
  • except if someone I know says “look at this”
• Books
  • I read few computer books now-a-days
  • many I love as references though (e.g. Stevens)
Advice for participation

• Participate
• Rule of two, two calm responses, then move on
• Get to know people from other countries
• Travel some
• Avoid babble, make it something substantive