Who, What, Where and How
An Insider's View to Participating in the Security Community

John Kristoff jtk@cymru.com

Editorial Note

I can't but help reflect on the security community history, present and future in a limited, personal way. My perspective likely differs at least slightly from many of my colleagues.

Security Community Players

- System administrators including network engineers

- Security coordinators, incident response teams (IRTs)

- Developers, software and hardware, vendors or not

- Government and law enforcement

- Professional journalists

- Researchers

  - Often a catch-all group if none of the above fit

- ...and hopefully no miscreants

The FIRST.org Party

- One of the longest running, best known parties

- Team constituency, rather than individuals

- Good international CERT/CSIRT participation

- In-person events (AGMs and TCs) not bad

- Professionally managed, hardened infrastructure

- Membership fee and sponsorship supported

- first-teams@ list posting not for the leak averse

- Team constituency, rather than individuals :-(

The nsp-security Party

- Vetted, limited number of individuals per ISP/NSP

  - Rules are imperfectly flexible

- ISP/NSP network-level event security coordination

- Volunteer run and operated, no cost to play

- Mailing list, IRC and open tracks at *NOGs

- Lots of excellent data sharing in the 2000's

- Little bit of a "boys club"

- Many modern-day parties arose from success here

The ops-trust Party

- Envisioned to be nsp-security++

  - Eliminate NSP focus, retain strong vetting

- Now fosters self-forming "trust groups"

  - Susceptible to death by secret lists syndrome

- Web-based participant directory, portal and wiki

- Nominee refutations infrequent, but an issue

- Small, but motivated group of stewards

- Success diluted by alternatives and interest

The YASML and ii Parties

- Malware-oriented mailing lists

- One vets individuals similar to nsp-security

- Another invites individuals based on referral

- Good places for malware sharing

- Some good analysis and insight discussion occurs

The REN-ISAC Party

- Higher education and R&E focused

- Cost-recovery based

- Insight, feeds, tools and services part of the deal

- Limited international participation

- One of the most successful parties, few drawbacks

The Conficker Cabal Party

- Specifically interested in Conficker worm variants

- Arose along with large-scale sinkhole coordination

- Wide participation from registries and registrars

- Containment and remediation was the stated goal

- Sometimes business and glory got in the way

- Demonstrated two things...

  - Security community can come together

  - Security community doesn't always play nice

Some Other Parties

- Volunteer groups

  - e.g. SANS ISC, Dragon Research Group

- System or event specific

  - e.g. DNS-OARC, Flashback Working Group

- Government, Law Enforcement

  - e.g. GFIRST

- Industry supported

  - e.g. BTF, Underground Economy Conference

How to Get Invited to Play

- Do something useful

  - Be a contributing participant in a community

  - Get data, synthesize it, analyze it, write about it

  - Develop a tool

  - Host a niche forum or community resource

- Gain the respect of an existing player

- Rant widely (not recommended)

The Open Parties

- IETF, ISOC and ICANN (more or less)

- *NOGs

- Social media and blogs

- Mailing lists (see seclists.org for a good sample)

- Sometimes the best stuff is in the open

- Secret parties often formed after a publicized issue

Email lists

- By far the medium of choice

- Practically always in clear text

    - Very few do "always-on" encrypted email

- The data leak movement hasn't altered behavior

- Outsourced email services causes consternation

- Lists are cheap and fast, and that's two out of three

Other mediums

- IRC – old school, imperfect, but widely used

- Jabber – has its advocates, but limited use

- Web forums – unlike miscreant forums, little used

- VoIP – some use, can be unwieldy for large groups

- In-person events – expensive, but high-value

Traffic Light Protocol (TLP)
https://en.wikipedia.org/wiki/Traffic_Light_Protocol

- Sometimes used in discussing sharing restrictions

- RED – personal for named recipients only

- AMBER – limited distribution

- GREEN – community wide

- WHITE – unlimited

Common Secret Club Problems

- How do you find out about a secret club?

  - Ask around, try not to sound like a miscreant?

- Application dilemma:

  - Participants are not publicized

  - Who do you put down for references?

- Collusion, subpoena and compliance bogey men

  - Any form of the word "membership"

  - Centralized list archives

- Vetting discrepancies

Should It Be All About Trust?

- A high degree of trust is desired

- Not all the good folks trust or like each other

- A lot of energy is spent on trust issues

- Very few documented trust violation issues

- Many folks lack an invite due to too few vouches

- Trust yes, community building heck yes

He Who Has the Gold...

- What you should consider about your community

  - Who is in charge? One person or organization?

  - Would the admin give up control? Have they?

- With control comes many advantages

  - Insight

  - Access

  - Cred

- Old timers know this and are leery of new ventures

Ruled By Many

- Do good work or talk about how to do good work?

- Shared control and consensus prone to gridlock

- Policy process expends much energy and goodwill

- Often easier to just do something and adjust later

- A good ruler isn't necessarily bad

- Especially if their focus is on effective collaboration

People and Personalities

- Many communities characterized by some players

- In-fighting between players drives people away

- Navigating your way can be tricky

- Negotiation and cooperation skills needed

- Online and offline interactions often incongruent

- Why not just be friendly with everyone?

Security Community Nits

- New security communities with the same people

- Replies to "Who has a contact at...?" off-list

- List posts that should have gone to a abuse@

- Nicknames and identity obfuscation

- The fear of being left out

- Similarly, the fear of not being in control

- Administrivia

List Participation Advice

- It is OK to not join or to leave a list

- "Rule of two", two calm responses, then move on

- Assume what you post will eventually leak

- Your participation will be all some know you by

Security Community Fodder

- All the added secrecy doesn't seem to have helped

- Some sharing has increased, some has decreased

- Matriculation of new people to the parties is slow

- Growth of the professional community participant

- The real, hard work is being diluted and fractured

- Too much jockeying for position

- I'd gladly trade in-person events for lists

Focus Your Time and Energy

- Discuss less, inform more

- Less RSS, Twitter and social media

- More papers, coding and research

- Posturing is for marketeers, build new relationships

- Strive for perfection, but it's OK to accept less

- Keep an IDID list

Read Good Works

- ACM, IEEE, USENIX journals and papers

  - my preference generally

- Blogs, Twitter, RSS, "trade rags", social media

  - I literally never read them

  - Except if someone I know says "check this out"

  - Or if it's my turn to man the Twitter feed

- Books

  - I prefer the classics (e.g. Stevens)

- Ask me about what else I like to read

Parting Thought

You being here at FIRST 2012 is AWESOME!
Now follow through.

contact

- Never hesitate to send feedback to:

jtk@cymru.com

PGP key 0xFFE85F5D

http://www.cymru.com/jtk/