Op Sec Trust

Status and Comments
2014-06-24
Ops-T – Scalable Human Trust

• Human brain does “trust” in hardware
  – But, limited to tribes of ~100

• Mailman is not the right answer
  – So, Vixie created the ops-t “portal”

• We’ve beat the magic ~100 barrier
  – Currently ~40 “trust groups”
  – “Main” has ~700 members
  – “Crimeware” is even larger
Inhuman Trust Can Scale

• Require N in-vouches, M out-vouches
  – Have met in person more than once, worked with them, and gained a sense of trustworthiness - or - Have known for longer than two years, actively worked with them and gained trust through mutual actions. This individual has demonstrated the ability to maintain confidence of sensitive information.
  – I trust this individual to take actions that directly impact internet security operations in a positive manner. I believe others in this community can also trust this individual as someone who will take action.
  – If a user I vouched for is removed for violations of the list charter, my membership and trustworthiness can be reviewed by my peers and I will respect the decision of that OPSEC-Trust Steering Committee regardless of their recommendation.
Ops-T Status

• Had to do emergency 501(c)(3) incorporation and fundraising after server failure (major data loss) in June 2013
  — Emergency past; fundraising continues
• Operations Security Administration, Inc. (OSA)
  — Board is a bunch of system administrators
• The Board has no input on policy and relies on Stewards and TG Admins for all governance
Ops-T Technical Support

• Please use the ticket system:
  – technical@support.ops-trust.net
  – business@support.ops-trust.net

• E-mail to sysadmin@ops-trust.net is discouraged unless the issue you’re e-mailing us about requires no followup
Ops-T Initiatives

• Working with various parties to create other instances of the Ops-T portal system
  – These will eventually be federation-capable
  – Dave Dittrich (UW) team funded by DHS for this
• Invited Chris Clark of Verisign to bring in MISP
  – We do not love PHP, but the tent must be large
• Considering a CIF instance
• Considering a Zoo instance
Other Observations

• “Trust group” is our term.
  – So is “KMT” (*don’t ever say this!*)

• Barry, Jose, and JTK came up with the idea
  – Vixie merely wrote code, recruited sysadmins, and now serves as Treasurer and Sysadmin
  – BApril, Krassi, MorrowC, JTK, Jeroen are heroes who actually do everything these days
What (Not) To Do

• To get into the main T.G. you need to be active and known in the community. Work incidents, form professional friendships, earn a rep.
  – It’s invitation only (nomination + vouches)
• Other T.G.’s like ISOI are more issue-focused
  – Every T.G. has its own private wiki & mailinglists
• The security community now has, in Ops-T, a mature data sharing capability
  – You can stop reinventing it; join us and help out