

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL



Making Network Sense of the encryption problem Roundtable



Head of GCHQ NAC



NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under related Freedom of Information legislation. Refer disclosure requests to GCHQ on [REDACTED]

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20360501

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

GCHQ metadata

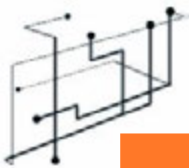
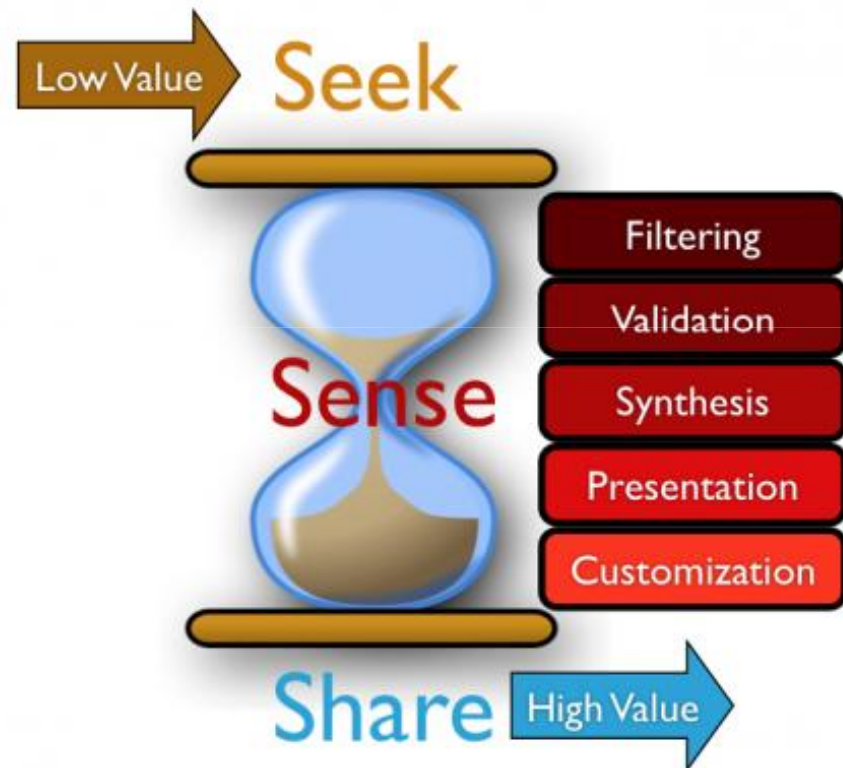
- GCHQ now creating metadata on:
 - SSL / TLS
 - IKE
 - OpenVPN
 - SSH
 - SQUEAL signatures (Various crypt packages)
- Data available in BEARDED PIGGY and/or the CLOUD



TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

How can Network Analysis help ?

- Can NAC help make sense using network knowledge of the volumes of data to isolate that which we want to decrypt...



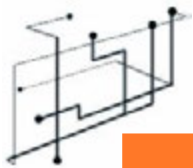
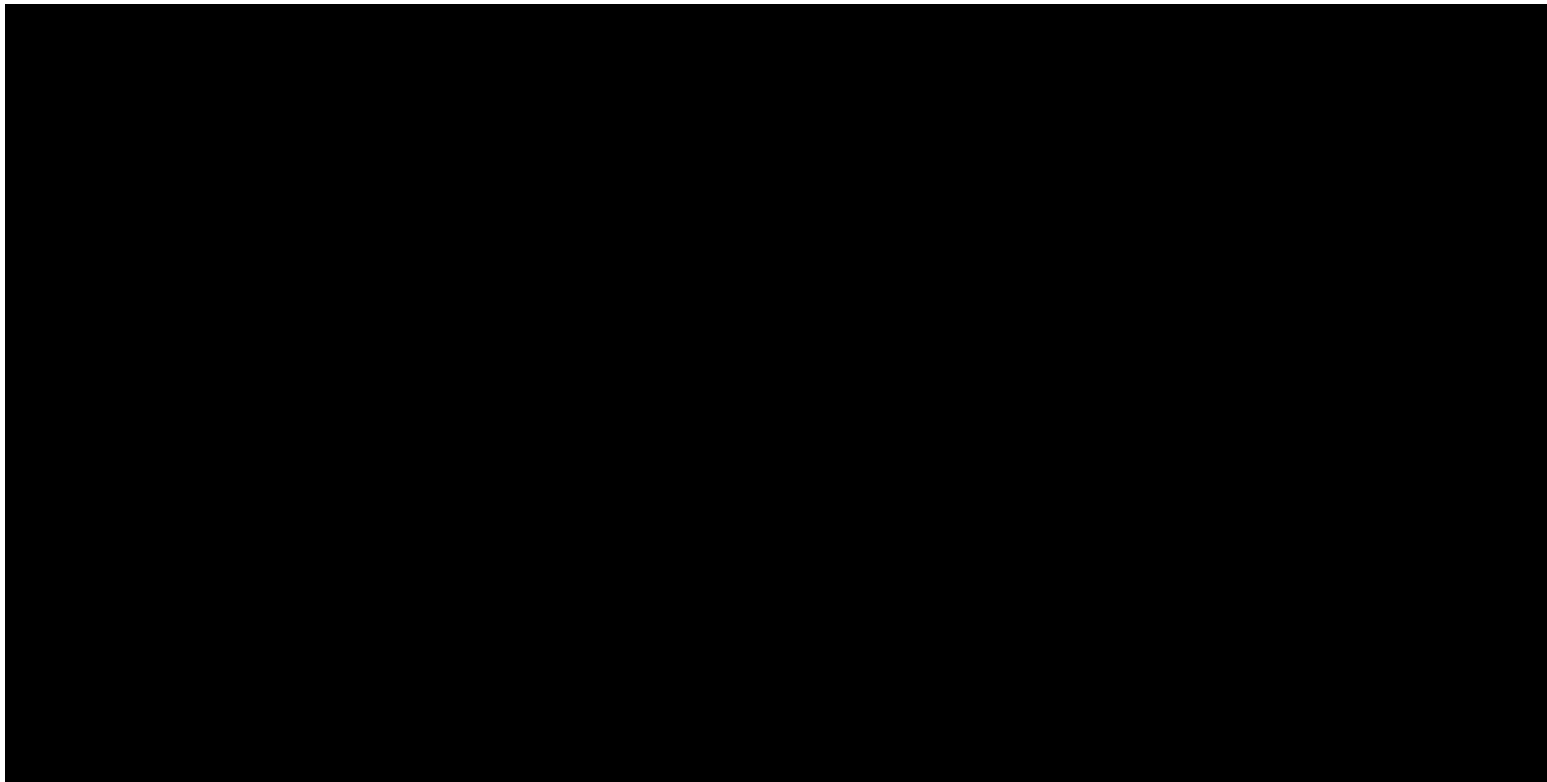
NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

The Seed Approach

- Intercepted documentation reveals details of VPN set up...



NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ or [REDACTED]

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

The Seed Approach

- Turn Seed IP into network block
- Query on network block against metadata
- Chain outwards / fuzzy subnet logic
- Basis of NTAT developed tradecraft:
 - IRASCIBLE HARE
 - IRASCIBLE RABBIT
 - IRASCIBLE MOOSE
 - IRASCIBLE EMITT

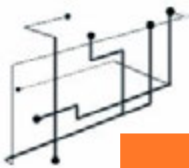


This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

Known usage

- Target known to use encryption
 - Identify target subnet
 - Select on subnet against metadata
- Or...
 - Start with an AS – look for most interesting wheel
 - BELGACOM - AS6774 – known to run GRX links to MNO over VPN



NAC
NETWORK ANALYSIS CENTRE

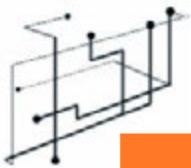
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ c [REDACTED]



TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

Network Knowledge enrichment

- Internet Registry information
- IP Geolocation
- DNS
- Data derived from network device configuration files (routers/Firewalls etc)
- Network information on surrounding IPs (i.e. rest of subnet is MNO related)
-



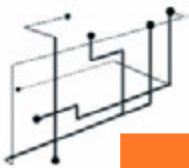
NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

Access Optimisation

- A given role of Network Analysis is optimising access for a given problem – in this case enabling two-ended collection
- Or..... Identifying opportunities to get at the data before it is encrypted therefore no need to make sense of encrypted data.
Can do this both:
 - Passive
 - Active



NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ [REDACTED]

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

Your Idea's Please



NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]