IP anonymization at .nz

Sebastian Castro – Chief Scientist

CENTR Jamboree 2018

Moscow, Russia

IP anonimization for DNS traffic

- DISCLAIMER
  - This is based on a design for a product that was never developed
  - Not a production system
  - Untested

ISP DNS Capture product

- We designed a product to be placed at ISPs in New Zealand
- Value proposal
  - You allow us to capture DNS traffic in front of your resolver
  - We provide you with analytics about usage, response time, query loss, security incidents
- Legal advice
  - IP addresses seen at an authoritative nameserver can't be mapped to individuals (as all of them should be resolvers with a user population > 1)
    - Based on the interpretation of the NZ Privacy laws, might not fit GDPR and EU legislation
  - For an ISP resolver, that's not the case, we need IP anonymization

Capture workflow

- Device captures DNS queries and responses
  - In 15 minute intervals
  - PCAP format
  - Into disk
- PCAP files get anonymized
  - Source address for queries, destination address for responses
  - Prefix-perserving anonymization
  - Using a key picked by the ISP manager
    - Keys can be rotated if they desire
    - We don't know the key
    - Tool to keep track of past keys
- Converted file gets transferred to the registry for analysis
  - Allowed us to identify anomalies based on user without knowing the user
  - Aggregated calculations per domain: popularity ranking based on time and other properties
- If a security incident is detected, we can report back to ISP with the anonymized IP
  - They can use the corresponding key to de-anonymize the address and contact the user

IP anonymization tools

- Crypto-PAn
  - Written in C++ by team at Georgia Tech
  - One-to-one mapping
  - Prefix-preserving
  - Consistent
  - Uses AES algorithm and requires a key
  - Only suitable for IPv4
- IP::Anonymous
  - Perl port of Crypto-PAn
  - Written by John Kristoff from Northwestern University
- ipcrypt
  - Python and Go version written by Jean-Phillipe Aumasson
  - One-to-one mapping of IPv4 addresses
  - Uses a 4-byte block cipher inspired from SipHash
  - Requires a 16-byte secret key

IP anonymization tools, continued

- ipcipher
  - An effort from Bert Hubert @ PowerDNS
  - https://github.com/PowerDNS/ipcipher
  - Collects the current state of pseudo-anonymization for IP addresses
  - Covers IPv4 and IPv6
  - Not a lot of tools available

Open Questions

- Anonymization versus pseudo-anonymization
- Key management
- Other values apart from addresses in a packet
  - Reverse lookups
  - Leaked queries containing personal information


InternetNZ