Idea: A DPRIVE Document about Evaluating Privacy

Allison Mankin and Aziz Mohaisen
Verisign Labs
IETF91 - DPRIVE WG

References

- RFC 7258 – in DPRIVE charter
- RFC 6973
- draft-ietf-dprive-problem-statement
- The above are guide rails

Why an Evaluation Document?

- Advice for those who deploy
- Consider Section 2 of RFC 6973 (2 quotes)

  [A protocol] may make use of privacy and security features at lower layers of the protocol stack (Internet Protocol Security, Transport Layer Security, and so forth) to mitigate the risk of attack. But when deployed within a larger system or used in a way not envisioned at design time, its use may create new privacy risks.

  Furthermore, in many cases the privacy properties of a system are dependent upon the complete system design where various protocols are combined together to form a product solution

Initial Questions/Thoughts

- Set stage and then adapt questionnaire in Section 7 of RFC 6973?
- Stage Setting for DNS to include
  - Specific DNS "system setup"
  - Informal and formal privacy metrics, defined in DNS system
- Adaptations include focusing on only Pervasive Surveillance threat (RFC 7258)?

Privacy Terms

- RFC 6973 Entities
  - Attacker
  - Eavesdropper
  - Enabler
  - Individual
  - Initiator
  - Intermediary
  - Observer
  - Recipient
- RFC 6793 Data and Analysis
  - Correlation
  - Fingerprint
  - Item of Interest (IOI)
  - Personal Data
  - Undetectability
  - Unlinkability
- RFC 6793 Identifiability
  - Anonymity
  - Anonymity Set
  - Identifiability
  - Pseudonymity
- Supplemental Terms
  - Subject (cf. Individual)
  - Unobservability
  - K-anonymity
  - Side Channel (cf. Correlation)
  - Unfortunate Few

System Setup

- RFC 6973 Communications Model
  - Individual(s)
  - Initiator
  - Enabler
  - Intermediary
  - Recipient

  "Although recipients, intermediaries, and enablers may not generally be considered as attackers, they may…pose privacy threats (depending on the context)

- Per draft-ietf-dprive-problem-statement, particularly focus on Enablers
  - DNS Servers
  - DHCP provision of DNS server configuration?

System Setup (cont)

- Stub Resolver: minimal resolver not supporting referral, delegating resolution to a recursive resolver. *Initiator*
- Recursive Resolvers: a resolver that implements the recursive function of DNS, as well as providing cached DNS responses. *Enabler*
- Proxy/Forwarder: server in between stub resolver and recursive, or recursive and authority resolver, which doesn't implement primary DNS functionality, but forwards or directs queries. *Intermediary*
- Authoritative Name Server: *Enabler*
- Rogue Name Server: *Attacker*

System Setup:Threat

- Quoting from RFC 7258:

  Pervasive Monitoring (PM) is widespread (and often covert) surveillance through intrusive gathering of protocol artefacts [sic], including application content, or protocol metadata such as headers. Active or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols can also be used as part of pervasive monitoring. PM is distinguished by being indiscriminate and very large scale, rather than by introducing new types of technical compromise.

System Setup: Attacker Model

- Attacker Type-1: Pervasive Monitor
  - Passive Pervasive Monitor: an attacker able to monitor links carrying individual's traffic. This attacker does not try to be on the path of any particular individual. *Focus is on this Adversary?*
  - Active Pervasive Monitor: corresponding to "honest but curious" model of adversaries, an entity trying to actively breach privacy of users by getting on the path of a user's queries
    - Actions could include arranging to serve as intermediary
- Attacker Type-2: Malicious Monitor
  - Same attackers as above, with addition that attacker also controls one or more infrastructure elements, e.g. has malicious control of the recursive server

IOI and Personal Data in DNS Context

- Needed for evaluation setup, but ideally should refer to definitions in problem statement draft
- Item of Interest
  - Could be qname
  - Could be other items as well
- Personal Data
  - Of interest “on its own” or “in a context”
  - On its own: could be IP address of individual (or initiator) sending query
  - In a context: could be organization-level attributes such as an ASN, if such means “relating to an individual identified directly or indirectly” (RFC 6973)

Evaluating Privacy

- Anonymity: given an anonymity set *K*, a subject *S* is said to be anonymous if it is NOT identifiable in such set.
  - Informally, given a set of attributes of an individual S, the adversary is not able to uniquely identify S among the set K.
  - Formally, S is anonymous if the attributes of S are computationally *indistinguishable* from the distribution of attributes of all individuals in the anonymity set *K.*
- *Practical Notes*
  - This formal definition references anonymity, but in face treats privacy not as a binary property, but rather as a quantifiable continuous variable.
  - Measurement compares what is achieved against maximal (anonymity)
- Assumptions
  - Uniform attributes; and identification is bounded to a given set of attributes, such as IP address and qname
  - Adversary is computationally and resource-bounded, and not unbounded
- Draft's meat is to describe measuring privacy for a given system setup.

Sample Privacy Evaluations - Template

- Threat: Pervasive Monitor
- System: [what system is being protected, using defined system terms]
- Data and Analysis: [IOI, Personal Data, Fingerprinting etc.]
- Attacker Model: [Passive Pervasive Monitor, Active Pervasive Monitor, Malicious Monitor]

- Straw Man Evaluation
  - Of one or more mechanisms per evaluation
  - Identify type or types of privacy
  - Define probability that adversary cannot identify meaningful query given those mechanisms

Upcoming examples include only Passive Pervasive Monitors, and not the the others, pending discussion.

Sample Privacy Evaluation (i)

- Threat: Pervasive Monitor
- System: Individual using stub resolver and ISP recursive server (no intermediaries)
- Data and Analysis: Personal Data and IOI (source IP and qname)
- Attacker Model: Passive Pervasive Monitor

- Straw Man Evaluation
  - *Dummy Traffic:* O(10) queries to hide each meaningful query
  - Privacy type is Undetectability
  - High probability that adversary cannot identify meaningful query
  - P = 1 – 1/10

Sample Privacy Evaluation (ii)

- Threat: Pervasive Monitor
- System: Individual using stub resolver and ISP recursive server (no intermediaries)
- Data and Analysis: Personal Data and IOI (source IP and qname)
- Attacker Model: Passive Pervasive Monitor

- Straw Man Evaluation
  - *Mix Network:* "Mixes are … usually intended to resist an adversary that can observe all traffic everywhere"[1]
  - Privacy type is Unlinkability
  - Adversary not able to associate queries to individuals directly
  - Probability that two observations identify the same individual S is uniform in set K.

[1] P. Syverson, Why I'm Not an Entropist

Sample Privacy Evaluation (iii)

- Threat: Pervasive Monitor
- System: Individual using stub resolver and ISP recursive server (no intermediaries)
- Attacker Model: Passive Pervasive Monitor

- Evaluation (informal only)
  - *Encrypted Channels* (as in the TLS drafts)
  - Undetectability of individual is provided
  - Unlinkability of individual's artifacts (queries) is not
- RFC 6973 quote from start: "in many cases the privacy properties of a system are dependent upon the complete system design where various protocols are combined together to form a product solution"

Summary

- Proposed to leverage RFCs 6973 and 7258, as well as close tracking of problem statement
- Proposed strong motivation from RFC 6973 Section 2
- Illustrated DNS-specific system definitions
- Provided illustrative evaluation templates
- Draft to follow shortly