Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 15, 2007

Pars Mutaf
Institut National des
Telecommunications
May 14, 2007

Private Information Queries: problem statement and overview
draft-mutaf-piqproblem-01.txt

Status of this Memo

Copyright Notice

Abstract

Private Information Queries (PIQ) is an Internet protocol that allows making a phone number query directly to the target cell phone. The target user can decide whether or not a phone number should be returned; in real-time and on a case-by-case basis.

PIQ may also be used for bootstrapping IKEv2 (Internet Key Exchange). Along with a phone number, the querier can securely obtain a fixed IP address e.g., a Mobile IPv6 home address, exchange certificates and

initiate IKEv2 with the target host.

Table of Contents

1. Introduction

The "phone book" that maps human names to telephone numbers is one of the oldest concepts in telephony. The phone book is however dead in cellular telephony, today. For privacy reasons, users do not publish their cell phone numbers. This privacy does not come without a cost. Users are dependent on their personal contact lists and have a hard time sharing their phone numbers; often through oral communication. This is very inconvenient. More importantly, there are many real-life situations where communication cannot even take place because the target user's phone number is unknown or lost and cannot be learned. Yet another problem currently is the "slow learning cell phone" problem. Thousands of new cell phones are bought everyday by young new users. A newly bought cell phone cannot be immediately used, since the contact list of the new user is initially empty. A phone number is learned on the occasion when user contact occurs; and not when actually needed.

Therefore, by current practice, privacy kills reachability. This is also not the right approach to privacy. Allowing phone number queries can contribute to better privacy. Today, phone numbers cannot be easily changed or revoked without losing reachability to legitimate users. Changing a phone number (or, a SIP URI) may contribute to better privacy (see for example [TDIG][DPN]). However redistributing a new phone number to legitimate users must be made easy in this case.

Phone number queries are therefore necessary, however privacy must be also be preserved. A user should be able to distribute phone numbers on demand, on a case-by-case basis and in real-time, under his/her control. The "Private Information Queries" (PIQ) protocol brings this solution. The target user's phone number is requested directly from the target user's phone. The target user decides in real-time whether or not a phone number should be returned depending on the querier's identity or other information.

This document focuses on "phone numbers" for their actual relevance and also for editorial simplicity. SIP URIs, IPv4/IPv6 addresses, Mobile IPv4/IPv6 home addresses, DNS names, e-mail addresses, and various combinations of these private informations can also be distributed using PIQ.

2. Abstract protocol operation

Private Information Queries (PIQ) is an abstract protocol. It can be used over any technology and over the Internet. It can be used over a short distance (upon user contact) or over very long distances i.e.

through the Internet. From user perspective, this service is not very different from a traditional phone book, except that the query must be approved by the target user. Figure 1 illustrates the abstract protocol operation.

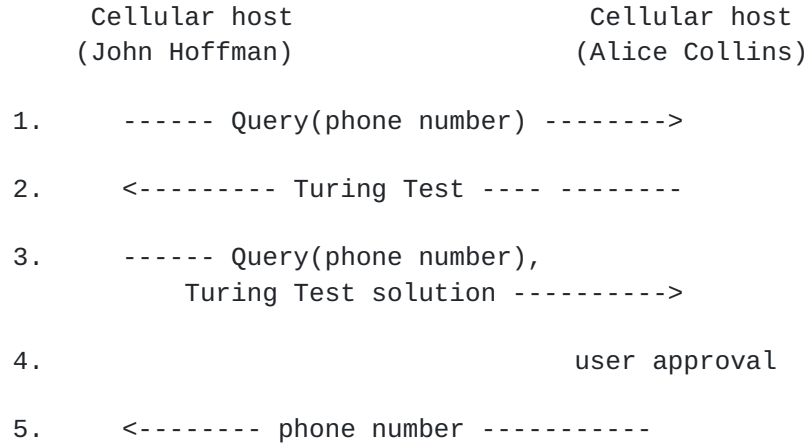

Figure 1

The query is sent directly to Alice Collins' host's IP address. Upon receipt of the private information query, the responder application displays a message:

```
John Hoffman requested your
phone number. Accept? [YES/NO]
```

The identity of the querier (i.e., John Hoffman in this example) must be verifiable. If not, the target user must be notified. The target user may know John Hoffman and may accept the request. Or, the target user may not know John Hoffman but may have an idea who he is and/or why he is trying to contact, and hence may accept the request (or not). The decision belongs to the target user. It is taken in real-time.

The Turing test ensures that a user cannot be disturbed with a bogus query without making some annoying mental effort. The effort needed to deny a request is, however, negligible. Pushing on the NO button of the phone will probably take less than a second (fast as a reflex and immediately forgotten). This feature makes the attack highly unspectacular hence defeats it. The attacker suffers but the impact is negligible. Turing test is also an effective defense against machine-generated Denial-of-Service attacks. The most common and popular Turing test is currently [CAPTCHA]. Its difficulty can be adaptively tuned by the target host. Once the target user's phone

number is learned, next time he/she can be contacted directly, i.e., without facing a Turing test.

Along with a PI (Private Information) query, the querier may also send a very short text (for example limited to 15-20 characters) providing a clue about his identity and motivations for requesting a phone number. The target user may allow or dissallow clues. An example clue is "found cred. card". The responder, who indeed lost his credit card can return a phone number although the querier is unknown. Another example clue is "forgot phone (carol)". The target user may expect a call from Carol, but Carol may be using a friend's cell phone (because she forgot her phone or has no battery power). Or, in some critical situations, a cell phone may be lost or broken. The lost person may borrow another person's phone and use PIQ to retrieve a target phone number. The person may provide a clue about his/her identity if necessary.

3. Mapping human names to IP addresses

Similarly to a traditional phone book, the target user can be identified by a human name or possibly a pseudonym.

The big difference from the traditional phone book is that the target human name must be resolved to an IP address instead of a phone number. The PI query will be sent or relayed to this address so that the target user can approve it in real-time.

Solutions to this problem are out of this document's scope.

4. Name collisions

A user who has a very common name (e.g. John Smith), may receive more frequent and mostly useless PI queries. The user can mostly drop such requests by pushing on the NO button of his phone, which should not be considered difficult.

With the traditional phone book, the querier can filter the returned results using some other information about the target user e.g. the street address, company, etc. PIQ may adopt a similar solution. Along with a Turing test, the target host may return some information helping the querier make the right choice. If the target user is unlikely to be the right person, the querier can give up the query and avoid solving an unnecessary Turing test.

5. Security considerations

A regional PKI (Public Key Infrastructure) formed by the cellular operators in the same area e.g., a country, may be used for user identity and public key certification. A user's identity and public key may be certified by the operator, and hosts may be configured with trusted operators' public keys. Although not secure over a global scale, a regional PKI can be enough for all PIQ users living in the same region.

PIQ may also be used for bootstrapping IKEv2 (Internet Key Exchange). Along with a phone number, the querier can securely obtain a fixed IP address e.g., a Mobile IPv6 home address, exchange certificates and initiate IKEv2 with the target host.

6. IANA considerations

This is an informational document.

7. Conclusion

"Private Information Queries" (PIQ) replaces the traditional "phone book" with an end-to-end protocol. A phone number query is made to the target phone directly. User distributes phone numbers on demand, on a case-by-case basis and in real-time. This ease of distribution contributes to reachability and also privacy. A phone number can be changed or revoked more comfortably. A legitimate user who lost contact with the target user, can always request a new phone number using PIQ.

8. Acknowledgements

Comments by Albert Manfredi, Olaf Kolkman and Christian Huitema helped better formulate the problem and the general solution.

9. Informative References

[CAPTCHA] "URL: http://en.wikipedia.org/wiki/CAPTCHA".

[DPN] "Disposable phone numbers, URL: http://dpn.sourceforge.net/".

[TDIG] "Tossable digits, URL: http://www.tossabledigits.com/".

Author's Address

Pars Mutaf
Institut National des Telecommunications

Email: pars.mutaf@int-evry.fr

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).