                  Customer Management DNS Resource Records

Abstract

   Maintaining high Quality of Experience (QoE) increasingly requires
   end-to-end, holistic network management, including managed Customer
   Premises Equipment (CPE). Because customer management is a shared
   global responsibility, the Domain Name System (DNS) provides an ideal
   existing infrastructure for maintaining authoritative customer
   information that must be readily, reliably, and publicly accessible.

   This document describes four new DNS resource record types for
   encoding customer information in the DNS. These records are intended
   to better facilitate high customer QoE via inter-provider cooperation
   and management of customer data.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   A significant portion of today's Internet is comprised of residential
   access networks. These access networks, and their providers, are now
   critical infrastructure, and significant research is devoted to
   measuring residential broadband speed and reliability [SAMKNOWS].

   Unfortunately, Customer Premises Equipment (CPE) is one of the
   weakest links in the chain of network equipment connecting consumers
   to the Internet. Customers typically do not perform proactive
   maintenance, e.g., firmware updates, on their own CPE. In many
   cases, CPE is even deployed with default authentication credentials,
   a fact that has been exploited by various Internet-wide denial-of-
   service attacks [MIRAI].

   A central observation motivating this document is that customers
   simply cannot be trusted to manage their own networks, much less the
   path-critical CPE. Given the difficulty in maintaining the hygiene

and resilience of broadband access, CPE maintenance should instead be
treated as a shared global responsibility among Internet Service
Providers (ISPs).

Further complicating customer management is choice in ISP, which is
currently available to nearly half of US households. While customers
may switch providers, their biographical, billing, and technological
details remain constant. Therefore, service providers need
mechanisms to ensure that transitioning customers into and out of
their network is as seamless as possible from both a technical and
billing standpoint.

Finally, service providers, advertisers, and law enforcement agencies
have varying but important reasons to track unique users' behavior on
the Internet. While RFC 7043 [RFC7043] makes use of EUI48 and EUI64
Resource Record (RR) types to uniquely identify CPE devices and
better support third-party tracking, these mechanisms can be defeated
by the customer simply purchasing new CPE.

This document takes a holistic, end-to-end view of customer
management with the aim of enhancing customer QoE and overall network
security. To enable shared CPE maintenance, this document leverages
the Domain Name System (DNS), described in RFC 1034 [RFC1034] and
RFC 1035 [RFC1035], and introduces new RR types to aid network
management.

1.1. Terminology

   This document uses capitalized keywords such as MUST and MAY to
   describe the requirements for using the registered RR types. The
   intended meaning of those keywords in this document are the same as
   those described in RFC 2119 [RFC2119] and RFC 8174 [RFC8174].
   Although these keywords are often used to specify normative
   requirements in IETF Standards, their use in this document does not
   imply that this document is a standard of any kind.

2. Customer Management Resource Records

   The ubiquity of residential broadband Internet service affords myriad
   benefits to consumers, but also poses a daunting challenge for
   Internet Service Providers -- how to best manage sensitive customer
   identifiers and billing details, while ensuring the resilience and
   security of CPE devices on their network?

   This document introduces four new RRs to assist in the management of
   customer data by ISPs.

   This section describes the purpose and wire format of the new DNS
   RRs.

2.1. The PASSWORD Resource Record

   The PASSWORD RR facilitates remote management of CPE devices by
   providing the login credentials for the CPE in a single RR. These
   credentials are used by authorized service providers to authenticate
   to the CPE. Authenticated users can then install important software
   and configuration updates to benefit the security and health of the
   provider's network.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                           USERNAME                            |
   |                                                               |
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                           PASSWORD                            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
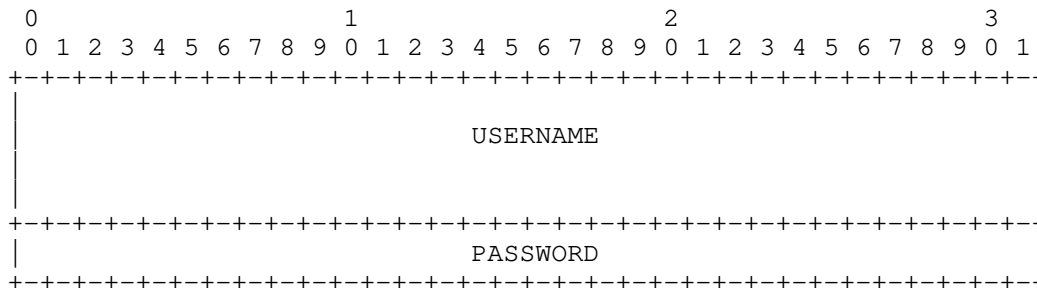
                     Figure 1: PASSWORD RDATA Format

   Where:

   USERNAME
      The <character-string> username of the account holder located at
      the CPE. In order to limit gratuitous expressions of
      individuality, usernames MUST be 16 or fewer ASCII characters and
      MUST NOT include punctuation.

   PASSWORD
      The <character-string> password associated with the USERNAME. In
      order to keep the RR size to a minimum, passwords longer than 32
      bits are NOT supported.

   Hosts on which multiple accounts exist SHOULD have separate PASSWORD
   RRs for each account.

2.2. The CREDITCARD Resource Record

   The CREDITCARD RR stores the billing details of the primary account
   holder located at the hostname associated with the CPE. Upon gaining
   a new subscriber, an ISP enters their billing details in a CREDITCARD
   RR so that it MAY be queried as needed for automated billing
   purposes. In addition, any outside entity with whom the customer

develops a recurring payment plan MAY query this RR for payment
details as well. Storing payment information in an RR, rather than
in the databases of disparate organizations with varying data
security postures, helps reduce attack vectors available to malicious
actors seeking this data.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                                                               |
|                          CARDNUMBER                           |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            EXPIRE                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           CHECKSUM                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                    Figure 2: CREDITCARD RDATA Format

Where:

CARDNUMBER
        The <character-string> 16-digit credit card number used for
        billing by the host's service provider. This field MUST NOT
        contain punctuation or spaces; only numeric digits
        represented in ASCII are allowed. Because this field is 16
        digits in length, users MUST NOT use American Express cards.

EXPIRE
        A <character-string> specifying the two-digit month and two-
        digit year in which the credit card expires. This field MUST
        NOT contain punctuation or spaces; only numeric digits
        represented in ASCII are allowed.

CHECKSUM
        In order to protect against bit errors occurring in the
        CARDNUMBER field, this RR type MUST use error checking as
        follows: Luhn's algorithm is employed as a simple checksum to
        validate that none of the 16 digits were corrupted in
        transit. Starting with the leftmost digit, we add this
        digit's value to a running total; for every second digit
        (beginning with the second-from-left digit), we add twice its
        value to the running total. This algorithm continues until
        all 16 digits have been exhausted. With this partial sum in

        hand, we solve for the value x such that x added to our
        partial sum is congruent to 0 modulo 10, and store x in the
        CHECKSUM field.

        When a CREDITCARD RR is queried, the recipient simply
        computes Luhn's algorithm in the same manner as described
        above, and validates that their computed value of x matches
        that stored in the CHECKSUM field.

        Note that this novel use of Luhn's algorithm MAY have
        applications outside of the CREDITCARD RR.

2.3. The SSN Resource Record

   The SSN RR maps hostnames to the US Social Security number and birth
   date of a user located at that host. For CPE behind which multiple
   users reside, a separate SSN RR SHOULD be entered into the DNS for
   each user. When residential broadband service becomes available
   outside of the United States, those countries SHOULD adopt
   identifiers that are compatible with the US SSN in order to ease
   administrative burden on the DNS and multinational service providers.

   During tax preparation season, the United States Internal Revenue
   Service WILL query the SSN RR to verify residency and proof of
   hostname ownership. In addition, the SSN RR MAY be used in
   conjunction with the CREDITCARD RR to automate the collection of back
   taxes owed.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            SOCIAL                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          BIRTHDATE                            |
|                                                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

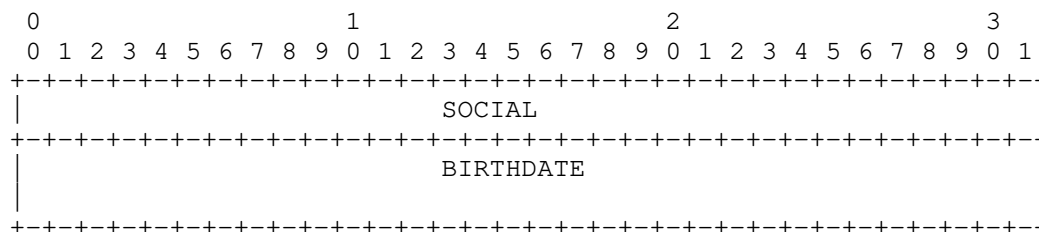   Figure 3: SSN RDATA Format

   Where:

   SOCIAL
        The Social Security number of the user associated with the
        host, formatted as a 32-bit unsigned integer in network byte
        order.

   BIRTHDATE
         A 64-bit timestamp representing the number of seconds past the
         Unix Epoch that the individual described by this RR was born.
         Because the Unix Epoch predates the birth of all Internet
         users, this field provides a sufficient range of values for
         ISPs to describe their subscribers. The 64-bit timestamp field
         is also "future proof", avoiding the Year 2038 problem and
         ensuring SSN RR applicability into the foreseeable future.

2.4. The SSNPTR Resource Record

   The SSNPTR RR provides the reverse functionality of the SSN RR; it
   maps Social Security numbers to hostnames. Every individual for whom
   an ISP provides service, not only primary account holders, SHOULD
   have an SSNPTR RR entry in the DNS.

   One benefit provided by the SSNPTR RR is the ability to conduct some
   population census functions remotely. For example, consider a
   residential ISP with SSNPTR RRs for each of its subscribers.
   Performing SSNPTR queries for all of their SSNs returns the host at
   which those individuals are located, allowing for the trivial
   association of family members behind the same CPE device. Further,
   these hosts can then be geolocated using an IP geolocation service or
   LOC RR [RFC1876], providing the ability to determine municipal
   populations and thereby inform decisions about appropriations and
   appropriate public policies.

    0   1   2   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+
   /   DNAME   /
   +-+

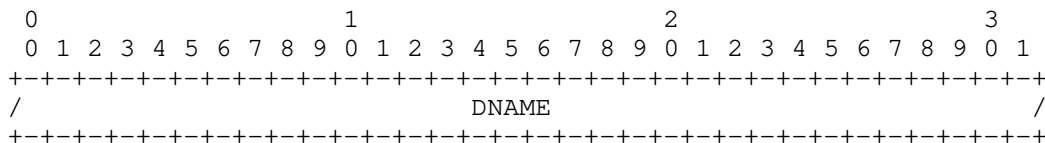   Figure 4: SSNPTR RDATA Format

   Where:

   DNAME   A <domain-name> that points to a location in the domain name
            space.

3. Related RR Types

   The practice of introducing new RR types to the DNS to support
   functionality that is either only tangentially related or wholly
   unrelated to name resolution is well established.

[RFC2539] describes the Diffie-Hellman KEY RR type, which is used to
conveniently store public key parameters for a domain. The SRV RR
type [RFC2782] combines name resolution with transport- and
application-layer details, providing a "no-fuss" way for network
administrators to advertise the location of specific services. The
Name Authority PTR (NAPTR) RR [RFC2915] recognized and corrected the
lack of POSIX Extended Regular Expression support in the DNS,
allowing for DNS-based automobile parts identification systems
[RFC3402] among other use cases. Having established the DNS's role
in encryption in [RFC2539], the IPSECKEY RR resurrected the since-
obsoleted ability to store public key parameters for the purposes of
IPsec encryption [RFC4025]. [RFC4255] codified the natural inter-
dependency between the Secure Shell (SSH) protocol [RFC4253] and DNS
by providing the SSHFP RR type, which is used to verify the host key
of a server.

Extending the idea of distributing public key parameters via DNS,
[RFC4398] introduced the CERT RR type to publish X.509 and PGP
certificates. [RFC4701] introduces the DHCID RR type to solve the
problem of Fully Qualified Domain Name (FQDN) collisions when Dynamic
Host Configuration Protocol (DHCP) clients make DNS updates after
obtaining a DHCP lease. The TLSA RR type [RFC6698] is used to
associate a TLS certificate with a domain, leveraging DNSSEC as the
binding, and the CAA RR type [RFC6844] specifies the Certificate
Authority allowed to issue certificates for a domain. The EUI48 and
EUI64 RR types specified in [RFC7043] seek to eliminate boundaries in
the TCP/IP model by creating, in essence, A records for MAC
addresses.

4. IANA Considerations

   This document has no IANA actions.

5. Security Considerations

   DNSSEC [RFC4033] SHOULD be used in conjunction with the PASSWORD,
   CREDITCARD, SSN, and SSNPTR RR types to provide data integrity.
   Employing DNSSEC ensures that the data contained in these RRs
   originates from an authoritative source and is not, for example, an
   attacker attempting to provide invalid login credentials in response
   to a legitimate request for a PASSWORD RR.

6. References

6.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <https://www.rfc-editor.org/info/rfc2119>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

6.2. Informative References

   [CAMEL]   Hubert, B., "The DNS Camel", March 2018,
              <https://blog.powerdns.com/2018/03/22/
              the-dns-camel-or-the-rise-in-dns-complexit/>.

   [MIRAI]   Antonakakis, M., April, T., Bailey, M., Bernhard, M.,
              Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.,
              Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma,
              Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N.,
              Thomas, K., and Y. Zhou, "Understanding the Mirai Botnet",
              Proceedings of the 26th USENIX Security Symposium, August
              2017, <https://www.usenix.org/system/files/conference/
              usenixsecurity17/sec17-antonakakis.pdf>.

   [RFC1034] Mockapetris, P., "Domain names - concepts and facilities",
              STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987,
              <https://www.rfc-editor.org/info/rfc1034>.

   [RFC1035] Mockapetris, P., "Domain names - implementation and
              specification", STD 13, RFC 1035, DOI 10.17487/RFC1035,
              November 1987, <https://www.rfc-editor.org/info/rfc1035>.

   [RFC1876] Davis, C., Vixie, P., Goodwin, T., and I. Dickinson, "A
              Means for Expressing Location Information in the Domain
              Name System", RFC 1876, DOI 10.17487/RFC1876, January
              1996, <https://www.rfc-editor.org/info/rfc1876>.

   [RFC2539] Eastlake 3rd, D., "Storage of Diffie-Hellman Keys in the
              Domain Name System (DNS)", RFC 2539, DOI 10.17487/RFC2539,
              March 1999, <https://www.rfc-editor.org/info/rfc2539>.

   [RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for
              specifying the location of services (DNS SRV)", RFC 2782,
              DOI 10.17487/RFC2782, February 2000,
              <https://www.rfc-editor.org/info/rfc2782>.

   [RFC2915] Mealling, M. and R. Daniel, "The Naming Authority Pointer
              (NAPTR) DNS Resource Record", RFC 2915,
              DOI 10.17487/RFC2915, September 2000,
              <https://www.rfc-editor.org/info/rfc2915>.

   [RFC3402] Mealling, M., "Dynamic Delegation Discovery System (DDDS)
              Part Two: The Algorithm", RFC 3402, DOI 10.17487/RFC3402,
              October 2002, <https://www.rfc-editor.org/info/rfc3402>.

   [RFC4025] Richardson, M., "A Method for Storing IPsec Keying
              Material in DNS", RFC 4025, DOI 10.17487/RFC4025, March
              2005, <https://www.rfc-editor.org/info/rfc4025>.

   [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and
              S. Rose, "DNS Security Introduction and Requirements",
              RFC 4033, DOI 10.17487/RFC4033, March 2005,
              <https://www.rfc-editor.org/info/rfc4033>.

   [RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH)
              Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253,
              January 2006, <https://www.rfc-editor.org/info/rfc4253>.

   [RFC4255] Schlyter, J. and W. Griffin, "Using DNS to Securely
              Publish Secure Shell (SSH) Key Fingerprints", RFC 4255,
              DOI 10.17487/RFC4255, January 2006,
              <https://www.rfc-editor.org/info/rfc4255>.

   [RFC4398] Josefsson, S., "Storing Certificates in the Domain Name
              System (DNS)", RFC 4398, DOI 10.17487/RFC4398, March 2006,
              <https://www.rfc-editor.org/info/rfc4398>.

   [RFC4701] Stapp, M., Lemon, T., and A. Gustafsson, "A DNS Resource
              Record (RR) for Encoding Dynamic Host Configuration
              Protocol (DHCP) Information (DHCID RR)", RFC 4701,
              DOI 10.17487/RFC4701, October 2006,
              <https://www.rfc-editor.org/info/rfc4701>.

   [RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication
              of Named Entities (DANE) Transport Layer Security (TLS)
              Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August
              2012, <https://www.rfc-editor.org/info/rfc6698>.

   [RFC6844] Hallam-Baker, P. and R. Stradling, "DNS Certification
              Authority Authorization (CAA) Resource Record", RFC 6844,
              DOI 10.17487/RFC6844, January 2013,
              <https://www.rfc-editor.org/info/rfc6844>.

   [RFC7043] Abley, J., "Resource Records for EUI-48 and EUI-64
              Addresses in the DNS", RFC 7043, DOI 10.17487/RFC7043,
              October 2013, <https://www.rfc-editor.org/info/rfc7043>.

   [SAMKNOWS]
              Crawford, S., "SamKnows: The Internet Measurement
              Standard", <https://samknows.com/>.

Acknowledgements

Authors' Addresses

   Erik C. Rye
   CMAND
   1 University Circle
   Monterey, CA 93943
   United States of America

   Email: rye@cmand.org

   Robert Beverly
   CMAND
   1 University Circle
   Monterey, CA 93943
   United States of America

   Email: rbeverly@cmand.org