Independent Submission
Request for Comments: 6593
Category: Experimental
ISSN: 2070-1721

C. Pignataro
J. Clarke
G. Salgueiro
Cisco Systems

1 April 2012

Service Undiscovery Using Hide-and-Go-Seek for the Domain Pseudonym System (DPS)

Abstract

With the ubiquitous success of service discovery techniques, curious clients are faced with an increasing overload of service instances and options listed when they browse for services. A typical domain may contain web servers, remote desktop servers, printers, file servers, video content servers, automatons, Points of Presence using artificial intelligence, etc., all advertising their presence. Unsurprisingly, it is expected that some protocols and services will choose the comfort of anonymity and avoid discovery.

This memo describes a new experimental protocol for this purpose utilizing the Domain Pseudonym System (DPS), and discusses strategies for its successful implementation and deployment.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

In today’s domains, there are services that, by choice, prefer to not be advertised and to cloak themselves with a shroud of anonymity. However, protocols do not address the needs of these services. To solve this, we propose a new paradigm of service hide-and-go-seek for services that do not want to be discovered. A client may be looking for a service, but an apathetic, playful, overwhelmed, or shy service might prefer a hide or hint engagement, instead of directly showing itself.

1.1. Scope

This document is unscoped, as the scoping service cannot be found.

2. Procedures Using the Domain Pseudonym System

Certain services conceal themselves with the intent of not being found, perhaps, by clients. The client trying to find the sneaky service is referred to as "seeker" or more precisely as "it". The concealed service is referred to as "hider". The process of Service Undiscovery using hide-and-go-seek is achieved using the Domain Pseudonym System (DPS), in which a service instance can hide behind a fictitious, fallacious, or facetious name. For example, a music streaming service may advertise itself as a tax collection agency’s web site.

2.1. Count to Live (CTL) for IPv4 and Count Limit (CL) for IPv6

The service hide-and-go-seek process begins with a services "ready or not" sequence whereby the "it" counts up to a default Count to Live (CTL) or Count Limit (CL) of 50. Services that are in hiding can change their hiding names while "it" is not looking, but when doing so their CTL (or CL) is decremented by one. It is imperative that "it" counts by one (count++) until reaching the CTL or CL. If "it" attempts to skip-count, and if this is discovered, its count is reset to zero.

If a client ("it") attempts to peek into a list of services before reaching the CTL, "it" will be placed into a "timeout" state in which "it" is denied access to all services until the hider feels "it" has learned its lesson. Other services may choose to mock "it" while "it" is in "timeout".

2.2. Implicit and Explicit Hiding

Various strategies can be used by service hiders, so that "it" (the go-seeker) does not find them. Implicit strategies are most common yet very effective, and employ Silence-as-a-Service (SiaaS). On the other hand, explicit strategies are best exemplified by an "I am not here" argument. Service names such as "empty", "no%20one", "gone-fishing", "/dev/ilinside", "/dev/ious", "out-to-lunch", "/opt/out", "/opt/ional", "/vol/atile", and "you're-not-much-of-a-bloodhound-are-you-Sherlock" are among the most commonly used for explicit hiding.

2.3. Timeout State and Finite State Machine for Misbehaving Clients

As discussed in Section 2.1, if "it" attempts to access a hiding service before the CTL (or CL) has expired, "it" will be placed into a "timeout" state and denied access to all services. When "it" attempts to contact any IPv4-based service during this period, the service will reply with an ICMPv4 Destination Unreachable message type (1) and a code of "Communication Administratively Prohibited" (13). An IPv6 service will also reply with an ICMPv6 Destination Unreachable message type (3) and a code of "communication with destination administratively prohibited" (1). Services will continue to reply with such messages until such time that they feel "it" has learned its lesson. During the "timeout" period, services may also choose to randomly send ICMP insults to "it". ICMPv4 type 253 (reserved for experimentation [RFC4727]) is used to specify an "Insult" class of messages, while ICMPv6 type 200 (reserved for experimentation [RFC4443]) is used for the same purpose. Within each type, there are three experimental codes.

```
LOSER              (code 0): The service wishes to convey that "it" is
                             incapable of winning

DORK               (code 1): The service wants to imply that "it" is
                             stupid or silly

TODAY IS SPECIAL   (code 2): The service intends to respond to the
                             question "are you always this stupid or
                             is today a special occasion?"
```

2.4. Echo

Echo, derived from [RFC0862], can also be an effective hiding technique. The hider simply repeats the service name that another service instance advertises, ensuring it is in UTF-27 lowercase to convey that it was fading out. The hider may also choose to echo the go-seeker's request back to the go-seeker as-is.

2.5. Service-as-a-Service (SaaS) Method

This method can be used recursively (i.e., this method can be used recursively (i.e., this method can be used recursively (i.e., this method can be used recursively))). (See Section 2.5).

2.6. Foobar, Mononymous, and other Disguises

A common practice is for services to employ the use of mononyms. In fact, there are documented use cases of using mononyms such as great Brazilian athletes or famous musicians, such as Prince (or "the-service-formally-known-as-Prince") as a service. These are techniques allowed by the protocol definition to hide a service. Similarly, metasyntactic service names (e.g., foo, bar, foobar, baz, and other aliases) are among the most evolved hiding techniques. Conversely, hypocorisms do not hide the service and typically lead to confusion. Hiders requiring government-level security may simply respond with "service-name-redacted", essentially presenting the go-seeker with a black bar where the service name would be.

2.7. Hinting

If a go-seeker requests a service list from a hider, the hider can optionally respond with a GUESS reply instead of the service list. The go-seeker will then request specific services from the hider using HINT-REQUEST PDUs, and the hider will respond with temperature-based HINT-REPLY PDUs to indicate whether or not the go-seeker is close to identifying an available service. For example, the go-seeker may request a web service, and the hider can respond with WARM or COLD HINT types to indicate if a related service might be available. A go-seeker may only guess up to 20 times. After which, the go-seeker must reset the CTL/CL before guessing again. This is depicted in Figure 1.

```
                  "It"                             Hider
                    |                                 |
                    |....."Ready or Not" Sequence.....|
                    |                                 |
                    |-------Service List Request----->|
                    |                                 |
                    |<-------------GUESS--------------|
                    |                                 |
                    |----------HINT-REQUEST---------->|
                    |         [web service]           |
                    |                                 |
                    |<----------HINT-REPLY------------|
                    |              [COLD]             |
                    |                                 |
                    |----------HINT-REQUEST---------->|
                    |        [print service]          |
                    |                                 |
                    |<----------HINT-REPLY------------|
                    |            [FREEZING]           |
                    |                                 |
```

Figure 1: Hinting

This document defines the following HINT types. HINTs are mutually exclusive.

ABSOLUTE-ZERO : The seeker is not even close to identifying an available service

FREEZING : The seeker is remotely close to identifying an available service

COLD : The seeker is somewhat close to identifying an available service

WARM : The seeker is fairly close to identifying an available service

HOT : The seeker is very close to identifying an available service

BURNING-UP : The seeker is extremely close and is on the verge of identifying an available service

To allow for the variability in geographic weather, extensibility through vendor-specified HINT types is possible. These might includes HINTs such as "COLDER THAN A FREEZER IN ANTARCTICA". New HINT types do not need registration.

2.8. Truth or Dare as Disambiguation

Hinting, unlike truth or dare, does not require "it" to complete any challenges other than making guesses to obtain a service list. "It" is also forbidden from asking the hider any personal questions.

3. Protocol Definition

DPS, needing a reliable transport, uses TCP. However, DPS packets (both unicast and omnicast) need to signal their mood as Sneaky ;) [RFC5841].

4. Security Considerations

Inherently, services not discovered are more secure than those discovered, due to their obscurity. However, the discoverability or undiscoverability of a given service is largely independent of its security characteristics. Instead, an implementor is guided to [RFC3514] to denote evilness (and associated security) status. Since [RFC3514] only defines evil and non-evil intent of packets, this document suggests assigning an "I am not sure" additional value for the evil bit. The intentional ambiguity of this additional state makes it a perfect third value for a binary bit.

5. IANA Considerations

IANA is strongly encouraged to look the other way and pretend they know nothing of this. This document uses values reserved by IANA for experimentation. It uses ICMPv4 type 253 and ICMPv6 type 200 for "Insult" with three experimental codes in each, "LOSER" (0), "DORK" (1), and "TODAY IS SPECIAL" (2). After the experimental phase, well-known hiding names, including "gone-fishing", "foobar", "service-name-redacted", and all others listed throughout this document could be reserved. Famous stage names and Three-Letter Acronyms (TLAs) [RFC5513] could also be reserved. Lastly, IANA is begged to reserve the "I am not sure" value for the evil bit.

6. Acknowledgments

The authors of this memo and all their pseudonyms do not make any claims on the originality of the ideas herein described.

7. Informative References

[RFC0862] Postel, J., "Echo Protocol", STD 20, RFC 862, May 1983.

[RFC3514] Bellovin, S., "The Security Flag in the IPv4 Header", RFC 3514, April 1 2003.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC4727] Fenner, B., "Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers", RFC 4727, November 2006.

[RFC5513] Farrel, A., "IANA Considerations for Three Letter Acronyms", RFC 5513, April 1 2009.

[RFC5841] Hay, R. and W. Turkal, "TCP Option to Denote Packet Mood", RFC 5841, April 1 2010.

Authors’ Addresses

Carlos Pignataro
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

EMail: cpignata@cisco.com

Joe Clarke
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

EMail: jclarke@cisco.com

Gonzalo Salgueiro
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

EMail: gsalguei@cisco.com