分散システム特論レポート RFC1288のまとめ

情報工学専攻修士1年 石本 林

2/8

1 RFC1288の概要

Fingerはremote user information program(RUIP)にインターフェースを提供するプロトコルである。RFC742においてオリジナルのFingerが記述されている。

このRFCでは

- コネクションの両端において、予期される通信を明らかにする
- 現在ある実装を無効にしたり、オリジナルのプロトコルに不必要な制限をかけたりしない
- いくつかの重要なセキュリティに関するコメントや勧告を行なう

ことを目的にしている。なお、このRFCはBSD版を基盤としている。

2 イベントの流れ

FingerはTCPを基盤とし、TCPの79番ポートを使用する。そのイベントの流れは図1のようになる。

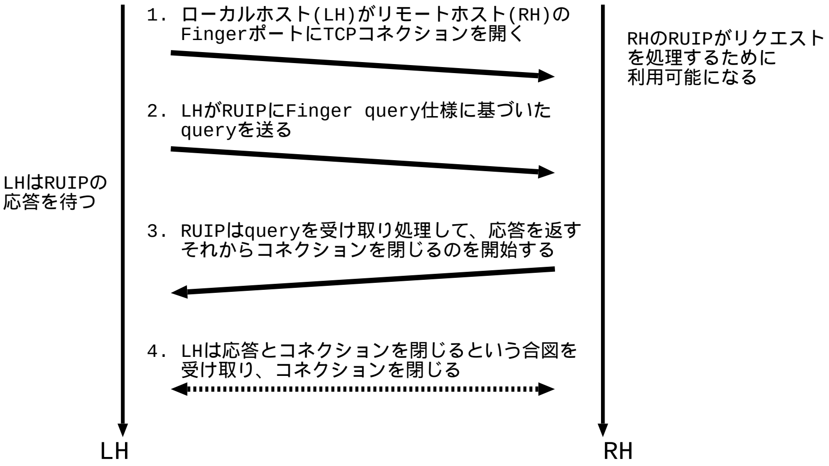

図1: イベントの流れ

また、Fingerで転送されるデータはASCIIフォーマット、パリティなし、CRLFで終わる行でなければならない。このことは他のキャラクタフォーマットを除外するだけでなく、ASCII 128からASCII 255のキャラクタが、パリティビットを持った7ビットASCIIではなく真に国際データであるべきであるということも意味している。

3 query 仕様

Finger の query 仕様は以下のように定義される。

{Q1} ::= [{W}|{W}{S}{U}]{C}

{Q2} ::= [{W}{S}][{U}]{H}{C}

{U} ::= username

{H} ::= @hostname | @hostname{H}

{W} ::= /W

{S} ::= <SP> | <SP>{S}

{C} ::= <CRLF>

{Q1} は現在使用しているホストの RUIP へのリクエストである。これに対し、{Q2} は別の RUIP へ query を転送するリクエストである。RUIP は転送されたこのサービスを提供するか、拒否するかしなければならない。もし、このサービスを提供するのであれば図 2のような振る舞いをする。
(例　FOO@HOST1@HOST2)

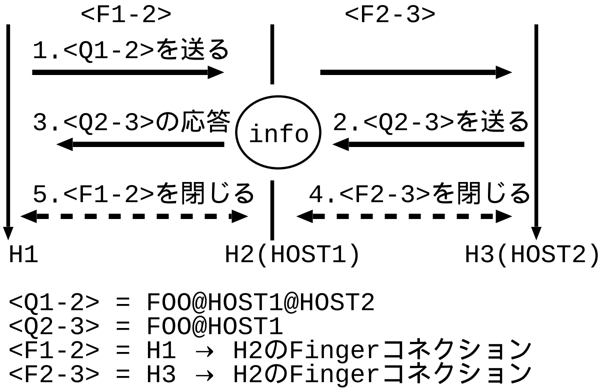

図 2: {Q2} の振る舞い

また、RUIP の応答としては以下のようなことが予期される。

- {C} query
  すべてのオンラインユーザのリストを知るためのリクエストである。もし応答するのならば、少なくともユーザのフルネームは提供しなければならない。また、他にも提供する情報 (端末、オフィスとその電話番号、アイドル時間など) の決定権をシステム管理者が与えられるべきである。

- {U}{C} query
  ユーザ {U} の詳細な状態を知るリクエストである。応答には少なくともユーザのフルネームは含まなければならない。もしそのユーザがログインしているならば、少なくとも {C}query で返されるのと同じ程度の情報を返さなければならない。

  {U}{C}query では user information file という情報を返すことができる。user information file とは、ユーザが Finger の request に対する応答にメッセージを残すことができるという特徴である。これ

はユーザのホームディレクトリや共通のエリアに特別に名付けられたファイルを探すようにすることで、簡単に実装できる。

- {U} ambiguity
  コマンドラインで許される名前は"ユーザネーム"か"ログインネーム"を含まなければならない。もし名前があいまいな場合、いくつかの方法で可能性のあるユーザすべてを返すかどうかという決定権をシステム管理者が与えられるべきである。
- /W query token
  せいぜい最後の RUIP でユーザ情報の出力の冗長を意味していると解釈されるべきで、最悪無視されるべきである。
- Vending machines
  自動販売機は {C}request に対して現在利用可能なすべての項目を応答する。{U}{C}request に対して詳細な数または特定の製品か製品のスロットを応答する

4 セキュリティ

この RFC では Finger における実装上のセキュリティ、RUIP のセキュリティ、クライアントのセキュリティについて述べている。

- 実装のセキュリティ
  Finger の健全な実装は最も重要である。実装は様々な攻撃に対してテストされるべきである。特に、通常とは異なる入力に対して RUIP は自分自身を守るべきである。Finger は Telnet や FTP や SMTP と同様に、ホストのセキュリティの境界にあるプロトコルである。設計・実装・テストの間、十分なセキュリティ検査を受けるべきである。
- RUIP のセキュリティ
  Finger はユーザに関する情報、それも慎重を要する情報を露出する恐れがある。管理者は Finger を実行するのか、応答としてどんな情報を提供するのか、はっきりと決定すべきである。どのくらいの情報を明らかにしているのかはっきりとした理解なしに、Finger を実行すべきではない。

  また、RUIP のセキュリティに関しては以下のようなことが考えられる。

  - {Q2} refusal
    RUIP が {Q2} の処理を行うか行わないかをシステム管理者が個別に選択できるようにすべきである。処理を行わないのならば、RUIP は拒否のメッセージを返さなければならない。この目的は query の転送しないことを選択できることであるが、もし選択したなら、首尾一貫すべきである。

    もしマシンがセキュリティの境界部分 (すなわち、外部と内部を接続するゲートウェイ) にあれば、query の転送はセキュリティの境界への通り道を提供してしまうことになる。したがって、デフォルトでは query の転送は拒否することが推奨されている。
  - {C} refusal
    {Q2} refusal と同様、RUIP が {C} の処理を行うかどうかをシステム管理者が個別に選択し、行わないのならば拒否のメッセージを返さなければならない。この目的は、個々のホストが現在のオンラインユーザのリストを返さないようにできることである。

  - Atomic dischrge
    Finger の実装では、システム管理者が query に対して返す情報を調整できるようにすべきである。
  - user information file
    ユーザが修正可能なファイルからの情報を RUIP が返すことができることはシステムに関する情報を自由に外部に配布のと同等に見られるべきである。すなわち、潜在的にすべてのオプションを行えるようにしているのと同じである。この情報セキュリティの侵害は、巧妙なものや単純なものなどたくさんの方法で行うことができる。
  - ユーザプログラムの実行
    応答でユーザプログラムを実行させせることを RUIP ができることは潜在的に危険である。RUIP はそのプログラムによってシステムのセキュリティが傷つけられるのを許してはならない。この種のメカニズムによって開発された OS には常にバグがあるので、この特徴を実装することは価値よりも危険の方が多いかもしれない。
  - {U} ambiguity
    悪意のあるユーザによる巧妙または執拗なこの特徴の利用は、システムにおけるほとんどのユーザネームに帰着する。{U} ambiguity refusal は {C} refusal と同様の気持ちで考えられるべきである。
  - 検査
    実装は、システム管理者が Finger query のログ取りができるようにすべきである。

- クライアントのセキュリティ
  最初の RUIP に質問するために、ユーザが実行しているクライアントプログラムが通常はあると予期される。デフォルトで、このプログラムは printable な 7 ビットキャラクタ、tab、CRLF を除いて、unprintable なデータをフィルタすべきである。これはエスケープシーケンスを使ったり、他人の X window 名を変えたり、他の卑怯なまたは混乱を招く行為をしたりする人から守るためである。この振る舞いを修正するユーザの選択は 2 つに分けられて考えられるべきで、そのためユーザは国際キャラクタを見るのか、それとも制御キャラクタを見るのかを選ぶことになるかもしれない。

  1 つは ASCII 32 より小さいすべてのキャラクタを許す。

  もう 1 つは ASCII 126 より大きいすべてのキャラクタを許す。

  国際データのある環境では、すべてのユーザがデフォルトで後者を選択できるようなメカニズムをシステム管理者は与えられるべきである。これはグローバル環境変数または同様のメカニズムによって行なうことができる。