

電子工作愛好者向けセキュリティゲートウェイの実装と 運用体制の構築

大野 浩之[†] 鈴木 裕信^{††} 北口 善明[†]

[†] 金沢大学 ^{††} 専修大学

An Implementation of Security Gateway for Electronics Hobbyists

And Development of Its Operation Environment

Hiroyuki OHNO[†], Hironobu SUZUKI^{††}, and Yoshiaki KITAGUCHI[†]

[†] Kanazawa University ^{††} Senshu University

1. はじめに

近年、電子回路を活用したものづくりを趣味として楽しむ人々が増えている。

ボードコンピュータ “Raspberry Pi” [1] は、手のひらサイズでありながら GNU/Linux を始めとする UNIX 系 OS が動き、価格も 35 ドル程度と安価だったため、2012 年の発売開始から 1 年半で全世界に 200 万台以上出荷するベストセラーとなった [2]。しかし、センサやアクチュエータを接続した CPU ボードが無防備のままインターネットにさらされれば、望まぬ事件や事故を起こしかねない。

筆者らは Raspberry Pi の利用や開発のモデルは今後訪れる IoT (Internet of Things) 時代の先行と捉え、Raspberry Gate [3] や Raspberry Guardian [4] を提案し開発者や利用者の負担を極力かけない形で情報セキュリティを維持する体制の構築を進めている。Raspberry Gate は Raspberry Pi のために Raspberry Pi で作ったセキュリティゲートウェイであり、Raspberry Gate に施す「セキュリティアップデート」をソーシャルネットワークの考えに基づいて有志が作り「みんなで」共有しようという試みが Raspberry Guardian である。

2. Raspberry Guardian

インターネットへの接続性を有する Raspberry Pi とその周辺環境のセキュリティ確保を検討するにあたり、「ラズベリー」がいちごの一種であることから、いちご畑、いちご農場、いちご農家などに見立て、以下の用語を定義した。なお、以下においてのみ Raspberry Pi を R.Pi と記すなど、Raspberry を R. と略記している。

- R.Field – 多数の R.Pi が散在している環境
- R.Garden – 所有者に管理運用されている R.Pi の集合体
- R.House – R.Garden を管理運用する者の拠点
- R.Farm – R.House と R.Garden からなる、一まとまりの実体

- R.Gate – R.Farm を外部と区切る門。この門以外は塀で囲まれていて出入りできない

- R.Guardian – R.House を拠点に行動し R.Garden に安全安心をもたらす者および組織

Raspberry Guardian は、図 1 のような異なる役割をもったユーザから構成される。彼らの多くは一つあるいはそれ以上の Raspberry Farm の所有者である。所有者が違う Raspberry Farm は設置場所も運用規模も異なるし、運用方針も厳密には同一ではない。しかし、Raspberry Guardian においては、ソーシャルネットワークのしくみを活用して意見交換を行い、多少の意見の違いは受容しつつ Raspberry Gate の運用方針やそれに基づく諸機能の諸設定を共有し、ひとりではなし得ない Raspberry Farm の安全と安心を継続的に享受することを目指す。

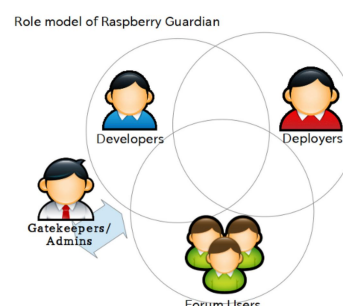


図 1 Raspberry Guardian の概念

上述のように、Raspberry Gate に設定する内容を合議で決めるしくみ (コミュニティ・サイト) と、そのしくみを利用する Raspberry Gate ユーザが Raspberry Guardian であり、Raspberry Guardian で合意した結果は更新スクリプトにまとめられ、github を介して個々の Raspberry Gate にインストールされる。

Redmine ベースで作成されている Raspberry Guardian サイトは、開発者 (Developer)・利用促進者 (Deployer)・利用者 (User) からなるコミュニティ・サイトとして機能するが、独自にユーザ管理するのではなく、OAuth [5] を使い、Google などの既存の SNS サイトやコミュニティサイトと連動させる。

OAuth2 ライブラリである intridea の OAuth2 を使い実装を進めている。

3. Raspberry Gate

Raspberry Gate は、Raspberry Pi が 1 つまたは複数 LAN に接続されている Raspberry Farm 環境と外部であるインターネット側の WAN を区切るセキュリティ機能を持ったゲートウェイの役目を果たす (図 2)。

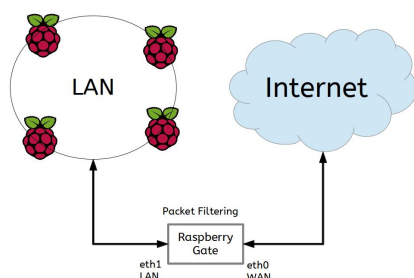


図 2 Raspberry Gate の位置づけ

既報で述べたように Raspberry Pi はセキュリティ機能を持ったゲートウェイとして構成可能であり [6] [7]、現在の実装では「初期化」「アップデート」「ブリッジ動作」「ルータ動作」の 4 つのモードを用意している。

Raspberry Pi はハードウェアとして 100Mbps の Ethernet 接続の機能を有しているが、実用的に利用するためにはブリッジ動作モードとルータ動作モードのスループットが重要であるため性能評価を実施し、何も設定しないブリッジ動作モードの場合、そのスループットは 90Mbps 以上であり性能的に問題はないことが明らかになった。

次に、iptables を設定した際のスループット変化を計測した

ところ、フィルタの有無やフィルタールールの数の多少 (ルールが 1 個の場合と 202 個の場合を比較した) によらず、いずれも約 92Mbps となった。

ルータ動作モードは、NAT を用いて LAN 環境を WAN 環境 (上位 LAN 環境) に接続するための機能である。NAT 機能を使うためには、カーネルに iptables_nat モジュールをロードする。

NAT は接続数に応じて内部でテーブルを作る。そのため内部ではメモリを消費し、その利用できるメモリ上限が接続数上限となる。今回テストで利用している iperf のサーバ及びクライアントの性能の制限で Raspberry Pi の接続限界のテストは行えなかった。そこで、ここでは接続の目安となる数値を示すに留まるが、Raspberry Gate では、同時接続 (同時 NAT 数) に関しては同時接続数 256 で問題は発生しなかった。よって、同時接続数 256 であれば安定して接続可能であることが示せた。この時、各接続スレッドのスループットを合算すると約 65Mbps となり予想の範囲内の値となった。

4. おわりに

Raspberry Gate の実装は IPv6 対応を含めて進んでおり、今後 Raspberry Guardian の運用が始まれば、Raspberry Pi に限らず IoT デバイスの開発者や利用者に極力負担をかけない形で Raspberry Gate の内側の情報セキュリティを維持することが可能になる。今回のポスターセッションでは、Raspberry Gate の実機を展示してその動作をデモするとともに、Raspberry Guardian による情報セキュリティ確保の流れを解説する。

参考文献

- [1] Raspberry Pi Foundation. Raspberry Pi. <http://www.raspberrypi.org/> 2014 年 7 月 1 日閲覧。
- [2] kanai. Raspberry Pi が 200 万台を突破. <http://makezine.jp/blog/2013/11/two-million-raspberry-pis-in-the-wild.html> 2014 年 5 月 16 日閲覧。
- [3] 大野浩之, 鈴木裕信. 6D-4 電子工作愛好者向けセキュリティゲートウェイの構築 (第一報: 設計と実装). 情報処理学会全国大会講演論文集, Vol. 2014, No. 3, pp. 47-48, mar 2014.
- [4] 大野浩之, 鈴木裕信. 6D-5 電子工作愛好者向けセキュリティゲートウェイの構築 (第二報: 運用と管理). 情報処理学会全国大会講演論文集, Vol. 2014, No. 3, pp. 49-50, mar 2014.
- [5] specs@openid.net. OpenID Authentication 2.0 - Final. Technical report, OpenID Foundation, December 2007. <http://openid.net/specs/openid-authentication-2.0.txt>.
- [6] 大野浩之, 鈴木裕信. 電子工作愛好者向けセキュリティゲートウェイの構築 (第三報: 構成要素の検討と性能評価). 情報処理学会第 160 回マルチメディア通信と分散処理研究会予稿集, Jul 2014.
- [7] 大野浩之, 鈴木裕信. 電子工作愛好者向けセキュリティゲートウェイの構築 (第四報: Raspberry Guardian の実証実験に向けて). マルチメディア, 分散, 協調とモバイル (DICOMO2014) シンポジウム講演論文集, Jul 2014.