目次

10 周年記念 名前付きの脆弱性を振り返る

1　はじめに

需要があるんだかないんだか、どれだけ同じような本が出ているのかも全然知らないまま、なんか本を出してみようぜと urandom vol.1 を作って頒布したのがちょうど 10 年前、2015 年の冬コミ（C89）でした。

その頃は（快速じゃない）普通のセット、通常の締切で入稿してたのに……という思い出話もありますが、それはそれとして、10 年というのはキリが良いところなので、じゃあその間を何か振り返って書けることはなんだろうと考えてみました。しかしそもそもこの本、「セキュリティ関連のネタならオッケー」という方針で書いてるおかげで、せいぜい yyu の記事で技術的な連続性が見られるものがいくつかあるくらいで、毎号ほとんど脈絡がありません。どの号から買っても安心とは言えますが、この本は別にシリーズモノのゲームや小説じゃないので大したメリットではありません。困りました。

困ったので、世間一般に目を向けて、この 10 年でどんな脆弱性が世間を騒がせてきたのだろうか、というのを改めて見てみるのも面白いかな、と思い、今回の記事を書くことにしました。

なお、詳細な辞典のようなものを作りたいわけではなく、ざっと振り返る程度のものなので、各脆弱性がどんなもので、どんな製品・技術にあった問題かについては簡単な説明に留めています。ついでなので、その脆弱性の公表前後で話題になったことについても触れています。あれこれ詳細に述べて議論するというよりは、そんなこともあったなぁ、くらいの軽い気持ちで読んでもらえれば幸いです。

2　記載のルール

2015 年以降に公表された脆弱性であり、かつ、表題にもありますが、固有の名前が付けられたものからいくつか選んでいます。この「名前が付けられたもの」に

絞っている意図なんですが、名前が付いてるからには影響度が大きいだろう、という想定の一方で、「発見者が勝手に大事にしてるだけ、実影響は言うほど……」みたいなケースもあえて紹介しておきたいという気持ちがあります。

なお、日時に関しては別途明記しない限り全て日本時間（JST）とします。

3　2015 年

3.1　Stagefright

2015 年 7 月 27 日（現地時間）に公表された脆弱性で、`libstagefright` という Android に搭載されたメディア再生ライブラリにあった整数オーバーフローによる遠隔コード実行などを含む複数の脆弱性の総称です。名称は脆弱性のあったライブラリの名前がそのまま使われています。対象は Android 2.2（Froyo）から 5.1.1（Lollipop）[*1]と広範囲であり、曰く「全 Android デバイスの 95%、9 億 5000 万以上のデバイスが影響を受ける」とされていました。Zimperium[*2]という企業が公表したものです[1]。

メディアライブラリにある脆弱性ということで、何かしら再生したら発動するから気を付けようねー……と思いきや、OS が MMS に含まれるメディアを自動で読み込んで Stagefright で処理し始めてしまうため、細工された MMS メッセージを正常に受信した時点で攻撃が成立します。そのため、攻撃者は対象の電話番号さえ知っていれば、ユーザーの気付かないうちに攻撃することすら可能でした。当然ながらこの MMS を経由する以外にも、例えば Web ブラウザだとか、ファイルブラウザを通して特定のメディアファイルを処理させれば[*3]攻撃に至るわけで、その点でも影響が大きかったと言えます。一方で、実際のところはメーカーやキャリア毎にパッチ状況が異なるなど、Android 特有の事情によって本当にありとあらゆる人が影響を受けたかと言われると微妙なところもあるかもしれません。

---

*1　Froyo は 2010 年リリース。Lollipop は 2014 年にリリースされ、当時の最新版でした。なお、次の Android 6.0（Marshmallow）は 3 ヶ月後の 2015 年 10 月リリースです。

*2　`https://zimperium.com/`

*3　「処理」というのはユーザーが明示的にそのファイルを開く操作だけではなく、例えば一覧表示におけるサムネイル生成のために読み込むものも含みます。

量子紛失通信

イソップ寓話に“金の斧”という物語があります。きこりが斧を川に落としてしまい嘆いていると、女神が金の斧と普通の斧を拾ってくれ、きこりが普通の斧を指定して返してもらうといった内容です。きこりをボブ、女神をアリスと呼ぶことにすると、イソップ寓話のプロトロコルでは次の 2 つの情報がそれぞれに共有されます。

1. ボブは、アリスが 2 個の 斧_1 と 斧_2 を持っている
2. アリスは、ボブが 斧_1 か 斧_2 のどちらを選択したかを知る

この 2 つが共有されてしまうため、物語では不正直なきこりが登場し、ボブとは異なって金の斧を選択した結果、アリスは斧を一切渡さないという結末になります。

もし上記 2 つの情報が共有されなければ、不正直なきこりが生じることはありませんでした。つまり、アリスはボブの選択した 斧_i のインデックス $i \in \{1, 2\}$ を知ることはできず、かつボブは自分の選んだ 斧_i 以外の斧について一切の情報を得られないプロトコルです。

これを紛失通信（Oblivious Transfer）と言い、イソップ寓話のシチュエーションは斧の数が 2 個なので、これを紛失通信で行うとした場合は 1-out-of-2 の紛失通信プロトコルを用いることになります。実はこのようなシチュエーションは世の中に溢れており、たとえばトランプなどのカードゲームで山札からカードを引く場合も、他のプレイヤーは引いたカードがどれかが特定できませんし、かつ引いたプレイヤーは引いたカード以外については一切情報が得られません。

この記事ではまず量子コンピュータの基礎的な部分について説明し、量子コンピュータを用いた紛失通信—量子紛失通信（Quantum Oblivious Transfer）を紹介します。

1 量子計算の基礎

この章では、量子紛失通信の説明に入る前に、量子コンピュータで用いられる量子ビットとその計算について説明します。

1.1 量子ビットの行列表現

量子ビットは次の式（1）のような行列で表現されます。

$$|0\rangle \equiv \begin{pmatrix}1\\0\end{pmatrix}, |1\rangle \equiv \begin{pmatrix}0\\1\end{pmatrix} \tag{1}$$

$|0\rangle, |1\rangle$ が古典コンピュータ[*1]の 1 ビットの $0, 1$ に相当します。このままでは古典コンピュータ同様にビットあたり 2 通りしか表現できません。

そこで**確率振幅**（Probability Amplitude）という複素数 α, β を用いて次の式（2）の量子ビット $|\psi\rangle$ を考えていきます。

$$|\psi\rangle \equiv \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix} \tag{2}$$

確率振幅 α, β は $|0\rangle, |1\rangle$ が発生する確率の素となる概念となり、1 量子ビット $|\psi\rangle$ を測定したとき $|\alpha|^2$ の確率で $|0\rangle$ が観測され、$|\beta|^2$ の確率で $|1\rangle$ が観測されることを意味します。したがって確率の要請から式（3）が成り立ちます。

$$|\alpha|^2 + |\beta|^2 = 1 \tag{3}$$

複素数は実数 a, b を用いて $a + b\sqrt{-1}$ で表せます。そして複素数が α, β の 2 つ存在することから、ナイーブには 1 量子ビットは 4 つの実数変数の自由度を持つように考えられます。しかし、下記 2 つの条件により 1 量子ビットは図 1 に示した 2 つの角度 θ, φ によって表される**球の表面座標**と考えることができます。

1. 確率の満たす条件式（3）
2. α が実数になるように β を調整してもよい（同一とみなせる量子ビットが存在する）

*1 量子コンピュータと区別して従来のコンピュータをこのように呼びます。