Credit Card Networks Revisited: Penetration in Real-Time

By Robert Imhoff-Dousharm

About the Presentation

This interacitve demonstration will give first hand experience in understanding and searching out credit card traffic on TCP/IP networks. It will also demonstrate how to deconstruct, rebuild and transmit rouge credit card packets. As an added bonus, prizes will be handed out to those who can craft and transmit rouge packets by end of speech. My incentives and guidance will illustrate how vulnerable credit card data is on merchant networks.

Background Information

- History of the Credit Card
  - 1961 – Diners Club
  - 1971 Bankamericard
  - 1971 Master Card
  - 1987 Discover Card

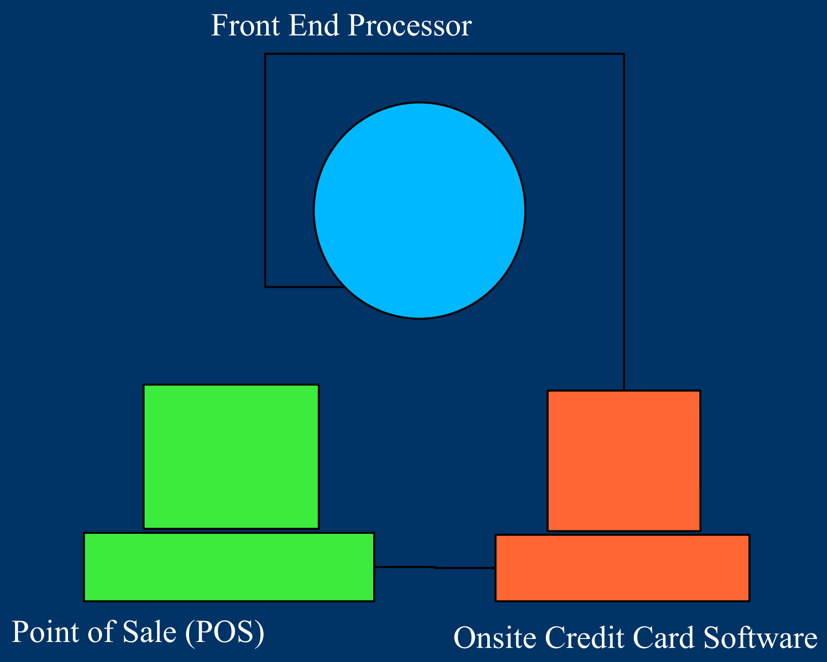
History (cont)

- F.E.P
  - Bankamericacards's problem
  - The first F.E.P. - VisaNet
  - Methods of connections
  - Current F.E.P's role
  - Industry Leaders

History (cont)

- Credit Card Networks
  - General Flow of Credit Card Traffic
  - Connection Methods
  - Discriminating Traffic

Credit Card Network Topology



- Simple Network Design
- Flows Seamlessly
- Easy to Troubleshoot

Definitions

- F.E.P – Front End Processor
- LuhnMod – Credit Card Checksum Algorythm
- Back End – Merchant Aquirerer's Network
- Issuer – Merchant Clients Bank
- Authorization Code – 6 digit code ; pre-authorization confirmation number
- Merchant ID – Unique ID issued to any merchant that accepts credit cards
- Terminal ID – Unique ID issued to merchant for each terminal in use at site

Credit Card Packets

- Offset Based
- Packet Type Indicators
- Field Separators
- STX/ETX/LRC
- Credit Card Data

Finding Packets

- What's required:
  - Packet Sniffer (ethereal, libpcap, etc)
  - Wi-Fi Card that supports sniffing
  - Programing language (we will use php)

Rules of Engagement

- Connecting to our AP
  - We reserve the right to capture and save YOUR traffic
  - No network flooding
- Prizes
  - Grand Prize - $50 Bar Tab (TBD location), Credit Card Network T-Shirt
  - Runner up's – Credit Card Network T-Shirts, bumper stickers

Finding Packets (cont)

1) Activating AP's

2) Turning On Authorization Host

3) Turning on Packet Generator

4) Turning on Accounting Software

Initial Packet Analysis

- Reviewing Packets
- Writing program to hunt though packets for unique data (like exp dates and credit cards)
- Q/A on current packets seen in capture

Generating Rouge Packet

- Q/A for people not attacking network
- Assistance for attcking group (helpers will walk around to assist any of your questions about network and credit card traffic)

Credit Card Newbies Guide

- How do we look for a packet
- What's in a packet
- How do we craft a rouge packet
- What do we send it this packet

- Understanding fundamentals of packets
- Writing code to disect packets

Hints and Tips

- Hints on trapping and understanding credit card packets
- Hints on crafting a packet at the programming level (using array's and string buffers)
- Hints (and example PHP code) on transmitting packets from programming code across TCP/IP network

Logical Packet Analysis

Theory – If you are looking for credit card data in a packet, you should parse and search the packet for a credit card number and expiration date.

Application – Use common logic and standard utilities to find static data in packet: merchant id, card number, expiration date, dollar amount

Example Application – If an expiration date is in fixed range – 4 digits, two digit month, two digit year – look for numbers only in packet where they extend into 4 offsets of string. Use basic logic. If a expiration date will always begain with 01 through 12 (numeric month values), the first two digits you are looking for should be in this range. Next, expiration dates year is usually NOT BEFORE the current year, nor past 10 years from now.

PHP Example – Expiration Date

```
<?php $range = array(“01”, “02”, “03”, “04”, “05”, “06”, “07”, “08”,
                                                        “09”, “10”, “11”, “12”);
$string = data;
$count = strlen($string);
for($i=0; $i<$count; $i++) {
    foreach($range as $month) {
                if(substr(string, $i, 2)==$month) {
                        foreach($range as $year) {
                                if(substr($string, $i+2, 2)==$year) {
                                        echo “<br>Possible Exp date: “.substr($string, $i, 2)
                                        substr($string, $i+2, 2);
                                }
                        }
                }
        }
}
?>
```

Credit Card Packet Analysis

Questions
and
Answers

Conclusion

- Inseption of credit cards
- Initial shortfalls of F.E.P's
- New problems with inseption of credit card networks
- What the future hold for the industry