Credit Card Networks Revisted: Penitration in Real-Time

By Robert Imhoff-Dousharm

About Talk

This talk is designed to show first hand, with audience partisapation, how to search out and understand credit card traffic on TCP/IP Network. It will also demonstrate credit card packet de-constructing, along with rebuilding and sending rouge packets. As an added bonus, prizes will be handed out to those who can craft, and transmit rouge packets by end of speech. This insentive togeather with my guidence will prove how vulnerable credit card data is on merchant networks.

Speech Flow

-Background

We will touch up on a (very)brief overview of credit card traffic in merchant networks
Definitions will be presented for different technologies used
Charts (on ppt) will show flow in networks

-Credit Card Data

We'll go over basic's of TCP/IP packet standards in the credit card world (not different by much from normal packet structure, but this allows the novice to catch up, and give others the right mind set).

What's in a packet? We'll cover the standard data found in 100% of credit card packets, and how to logicly identify it.

-Finding packets

This is where it get's fun. Wi-Fi AP's (approx 3) will be turned on, and the credit card simulator is started

Simulator will begain transmitting credit card packets across network to authorization host

Audience will turn on packet sniffers, and start hunting traffic down. It is not determined yet if fake non-credit card traffic will be mixed in (http, pop, snmp traffic for example) to make discrimination of packets harder.

-Identifying Packet

I will have packet sniffer on LCD, and will provide "hints" to audience. It is their job to tell ME what looks like credit card traffic.

Once packet is identifyed will will isolate it, and begain breaking it down.

-Analysis of Packet

Once again, I will turn to audience, with multiple packets the appear to be credit card data. I will ask them to find trends in packets, and help determin what offsets coorespond to what data. Example:

Offset 4-8 is merchant id
Offset 9-25 is Credit Card number, etc and soforth

-Crafting new packet

Once will have isolated fields, we can then design our own packets. We turn to the audience once again for assistants.

-Transmitting packets

Here's were the prizes come into play. Not everyone will follow along step by step. Some might not have the fastest typing skills. Some might just be dumb! So it turns to a free for all. First to get a credit packet accepted by host wins the grand prized (TBD), and subsequent audience members get lower level prizes (like shirts, hats, stickers, etc).

-Q/A

Questions will be accepted last 10min of demonstration

Audience Requirement

That's a tall order! Sound like a lot of equipement may be involved. Let's break down the equipment check list:

- Computing device capible of accepting a Wireless NIC.
- Wireless NIC
- Text editor or IDE
- Packet Sniffing software
- Web Browser
- Coding language that supports sockets (recommended, but not required)

See not too shabby, oh, some coding experience may be nessarcy to open a port and transmit data. I will have some PHP examples avalible on web site prior to conference for those who are not coders

Tracking Progress

All those that would like to partisapate should sign-up for fake credit card account at web site http://www.hackajar.com/credit (will be created if CFP is approved). If they don't sign-up pre-con, they will have oppertunity to sign-up during speech. Site will provide background on credit card industry, and preparing audience for live demonstration.

File List

Files to be provided for CD will include design of my credit card dB (making Virgin dB so not to step on my employeers toes), php files used during demonstration, Full text of speech, external references for further research, ppt files and personal bio.

EOF