

A1



Vulnerability and Threat Management and Prevention



Weston Hecker Security Expert With KLJ

Systems Network
Analyst/Penetration
Tester/President Of Computer
Security Association Of
North Dakota

Slide 1

A1

Author, 9/16/2013

About Me

- About Me: CISSP, CEH, CCNP Security, Certified Microsoft Professional, Security + Licensed Penetration Tester, Computer Science/Geophysics, and spoke at Defcon 22
- About 10 years pen-testing, disaster recovery, security design, and security research experience
- Research including DHS contract to attack 911 systems in the USA. Skim Bad software project.
- NERC, FFIEC, FISMA/NIST, ISO, GLBA and FDIC, Compliance audits HIPAA, Omnibus, HI-TECH

What is being covered

- How is it different in The Midwest? What are hackers using to compromise networks?
- How has it changed, Why is hacking in the news so much.
- Tools of the trade “Fleet of Fake I phones”.
- Key loggers and Raspberry Pi hacking machines.
- RFID “Radio Badges” and physical security portion of Pentesting.
- Distributed Denial of Service Phone Systems “What it is how its used” “How it affects businesses”
- Credit card skimming methods, POS memory scraping malware, and phone DDOS.

Methods Blackhat Hackers Use to Get Into Networks/Methods Found In ND

- Findings from Pentests in ND and the Midwest
- How does it differ from rest of USA
- Why would people target ND we are too small to be noticed ...
- Types of audits
- Need for Security Framework
- Forced compliance
- What can IT staff do to secure their networks
- When does a 3rd party pay? Everyone thinks North Dakota has oil money why are companies still paying 90s prices for security services

Fleet of Fake iPhones With Teensy 3.0



Key Stroke Catchers Rouge USB Drives



Computers Used Specifically for Password Cracking, USB Plugged into USB Monitor

GPU Farm Built for \$2400, 13 Billion Password attempts a second



Raspberry Pi Hacking Boxes, Alfa Card with promiscuous mode chip set, RP Recording calls from VOIP phone.

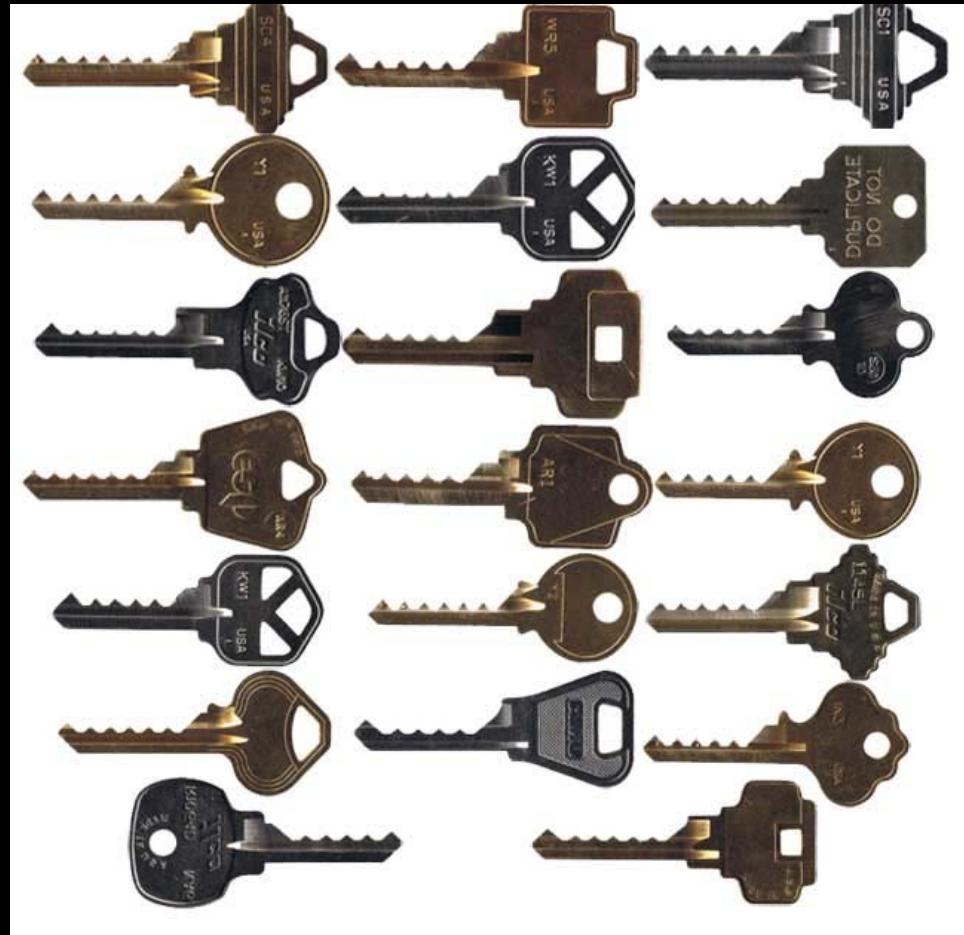


Bump Keys

80% of Locks Can
Be “Bumped”

Physical Security
RFID Badge Hacking

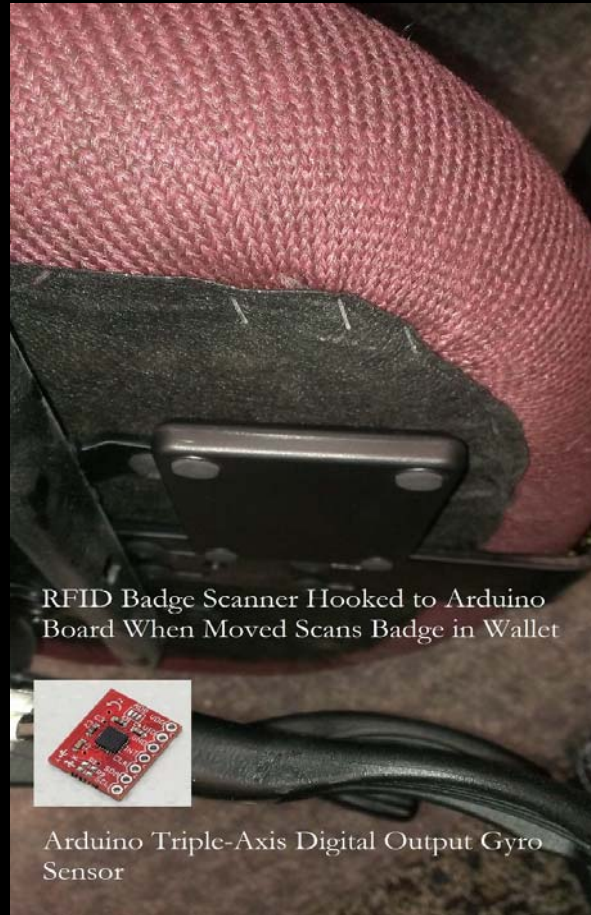
Tailgating Doors Left Open



RFID Badge Cloning Hardware, Front door Cards Read up to 10ft Away



RFID Badge Reader Scans Through Seat Where Customers Wallet Would Be.



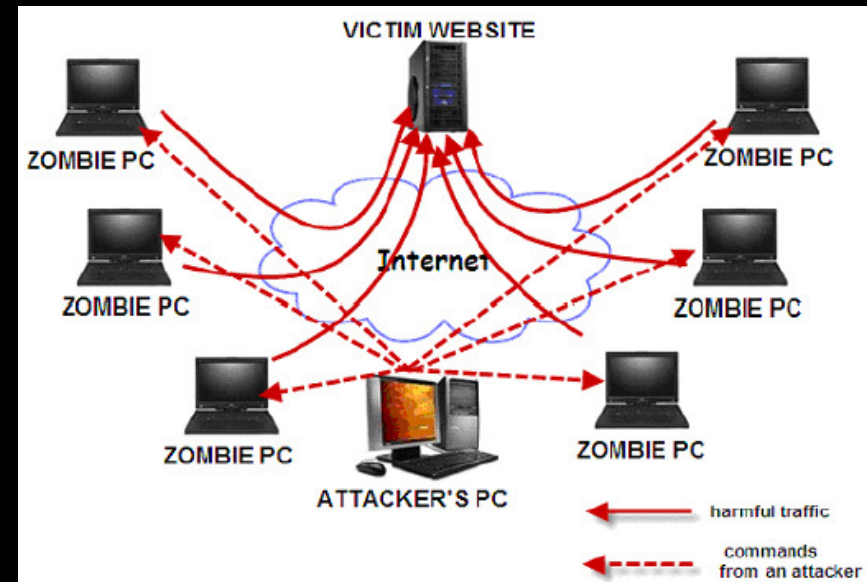
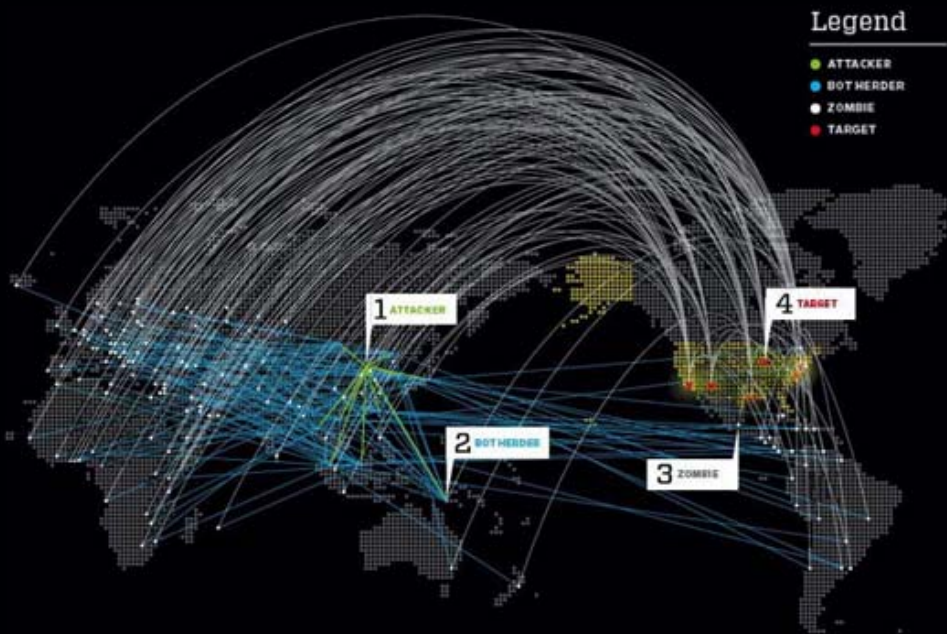
RFID Badge Scanner Hooked to Arduino Board When Moved Scans Badge in Wallet

Arduino Triple-Axis Digital Output Gyro Sensor

Everyone is familiar with DDOS it has been a problem for more than 15 years

Computers are asked to respond to more requests than it can handle

Think of it as 30 people driving thru a drive thru at lunch hour and ordering food then driving off.



This Prepaid Cell Phone Can Deny Legitimate Phone Calls for 5 Days Strait

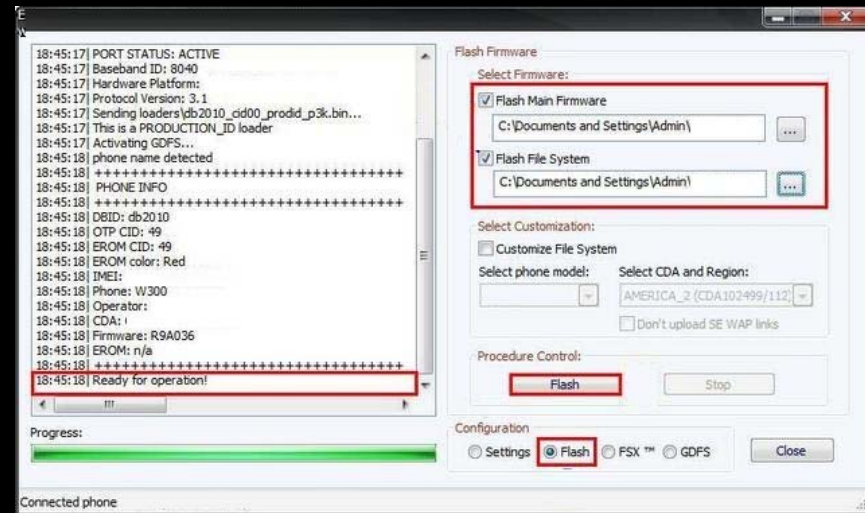
- Anonymous Purchase
- 2 Dollars Days That it is Used
- Untraceable Can be Charged With Solar USB Charger PRL List Hopping.
- GPS Not Recoverable Unless in 911 Mode.



Cell Phone DDOS call Some one non stop two times a second for 5 days for \$14.00

\$14 Dollar Prepaid Phone

Firmware Flashed To Become Anonymous DDOS Attack



Malware, DDOS, Ransomware, Web Application Injection, Spearfishing.

What is a SQL Injection

Why Scanning tools don't always catch these methods?

SQL Injection.

User-Id:

Password:

```
select * from Users where user_id= 'srinivas'
and password = 'mypassword'
```

User-Id:

Password:

```
select * from Users where user_id= '^ OR 1 = 1; /*'
and password = '*/--'
```

-: Administrator Login :-

Username :

Password :

Sanitize your inputs

- Most application exploits come from not sanitizing inputs.
- Assume that any data you do not have control over is malicious.
- Have web applications made by third parties undergo an audit.
- Scanning tools are ineffective at finding any more than the most basic vulnerabilities.

Malware, DDOS, Ransomware, Spearfishing. Targeted Malware In ND

Spoofted Emails, J:// Encrypted over the weekend Ooooo no.

Malware custom made for customers in ND

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through

To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



```
// If we can read from the TCP socket, send
// data to process's North Dakota
if (in_array($sock, $read_a)) {
    if ($debug) printit("SOCK READ");
    $input = fread($sock, $chunk_size);
    if ($debug) printit("SOCK: $input");
    fwrite($pipes[0], $input);
}
```

What Are The Hackers After?

- Personally identifiable information
- Financial information ex. Credit card number, Bank account numbers
- Trade secrets ex. Customer data, Bid information, Volume license information
- Network Resources ex. Servers, email accounts, desktops used to attack and infect other systems

Credit Card Skimmer Used to Steal Magnetic Data on Cards.



WITHOUT

WITH

Where Do they Sell Credit card Data and SSN#



Welcome **admin**
Balance **\$0.00**
[My Products](#)
User-Type: **non**

Filter:
Card Type: Contry:

Total: 10200

ID	Type	BIN	Expire	Name	Coutry	State	ZIP	Price	Buy Now
1	VISA	456785	9/15	*****	Nauru	*****	111122	\$1.00	Buy CC
2	VISA	455843	6/14	*****	Dominican Republic	*****	222244	\$1.00	Buy CC
3	VISA	457413	3/15	*****	Tanzania	*****	333366	\$1.00	Buy CC
4	VISA	455215	11/14	*****	Libya	*****	444488	\$1.00	Buy CC
5	Mastercard	547104	8/15	*****	Burkina Faso	*****	555610	\$1.00	Buy CC
6	VISA	454587	5/14	*****	San Marino	*****	666732	\$1.00	Buy CC
7	VISA	456669	2/15	*****	Iceland	*****	777854	\$1.00	Buy CC
8	AMEX	371247	10/14	*****	Andorra	*****	888976	\$1.00	Buy CC
9	VISA	457297	7/15	*****	New Zealand	*****	99	\$1.00	Buy CC
10	Dicover	600009	4/14	*****	Egypt	*****	111221	\$1.00	Buy CC
11	VISA	457925	1/15	*****	Tonga	*****	222343	\$1.00	Buy CC
12	VISA	454703	9/14	*****	Luxembourg	*****	333465	\$1.00	Buy CC
13	VISA	456553	6/15	*****	Cameroon	*****	444587	\$1.00	Buy CC
14	VISA	456075	3/14	*****	Senegal	*****	555709	\$1.00	Buy CC
15	Mastercard	546244	11/15	*****	Iran	*****	666831	\$1.00	Buy CC
16	AMEX	370735	8/14	*****	Argentina	*****	777953	\$1.00	Buy CC
17	VISA	457809	5/15	*****	Nigeria	*****	889075	\$1.00	Buy CC
18	VISA	454819	2/14	*****	Eritrea	*****	198	\$1.00	Buy CC
19	VISA	458437	10/15	*****	Turkey	*****	111320	\$1.00	Buy CC
20	Dicover	600869	7/14	*****	Malawi	*****	222442	\$1.00	Buy CC

Page: [Back](#) | [Next](#)

LIMITED LISTING: Your account must be VIP to view all the products! Click [here](#) to purchase VIP status!

About 150,000 results (0.54 seconds)

Carding Forum | Carders Forum | Review

[www.blackstuff.net/](#)

carding forums, Blackstuff.net Review , WU transfer, Hacked cc, dumps, pin, legit carders, hacked ... Most Popular Forums, Latest Posts ... VIP Credit Cards. Free CVW - Free Bank and PayPal Accounts - Verified Sellers/dealers - First

Carding Forum - Carding - Credit Cards - Dumps - Tracks ...

[cardingmafia.ws/](#)

carding forum, carding, carders, western union transfer, illegal credit cards, credit card, cc, tracks, dumps, pin, dell alienware, hacking, botnet, security, paypal, ...

Dark Stuff - #1 carding forum, Credit Cards, Hacking Forum

[www.darkstuff.net/](#)

carding forum, Cardingforum , carders , Crackingforum , crackers , exploit, hacking , cv, vcc , Wu , Westernunion , paypal , bank , credit cards , transfer , dork...

Tuxedo Crew - #1 Carding Forum - Credit Cards - Cvv ...

[www.tuxedocrew.biz/](#)

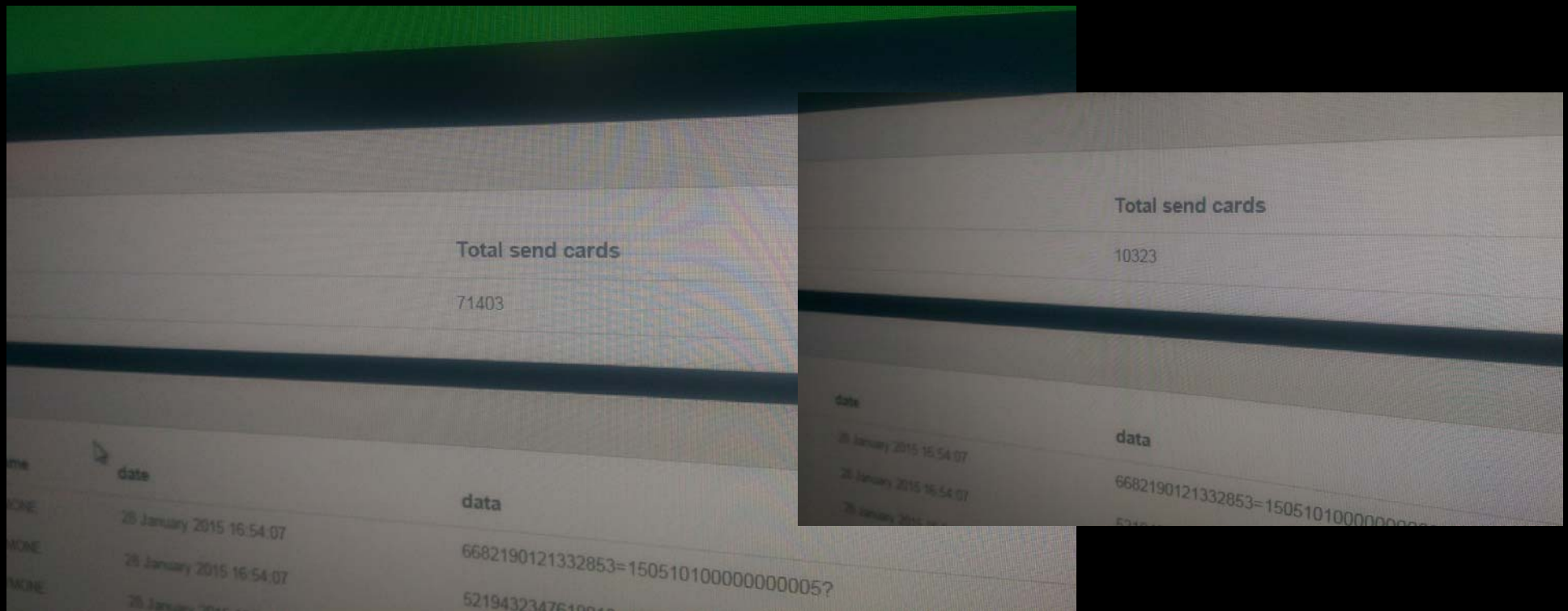
Welcome to the Tuxedo Crew - #1 Carding Forum - Credit Cards - Cw - Fullz - Code 10 - Dumps - Track 1 - Track 2 - Bank Logins - Bank Transfers - Western ...

DRK.bz - Carding forum | Кардинг форум

[www.drk.bz/](#)

One of the best carding forums - Dark Street. Russian hackers forum with ... Credit Card selling, Fulls, SSN, MMN, DOB Reserch. Threads: 13. Posts: 1496.

POS Skimming Malware How It Works How It Can Be Defeated.



Thank You For Inviting Me and For Your
Time Any Questions, Please Contact Me.



Weston.Hecker@kljeng.com
[westonhecker@twitter](https://twitter.com/westonhecker)
WWW.KLJNETWORKSOLUTIONS.COM
Phone Number 701-934-1292