Sun City Computer Club

Computer and Information Security

August 29-30, 2018

Dixie Normous Credit Card Security ™

Is your credit card number in a hacker's database?

You can easily find out now! All you need to do is enter its information here and we will scan thousands of hacker databases to see if any they have match yours.

Credit Card Number:

Expiration Date:

Your Zip Code:

SCAN DATABASE

- Chicken Little
- Tortoise and hare
- Each of us safer, all of us safer
- Age does NOT diminish cognitive ability
- Life, Liberty, Pursuit of Happiness

  Cyber Security SIG

  Cyber Security Blog

  Internet

- Do nothing no problem
  <most of us>
- Do everything - catastrophic

Vocabulary

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless
- Internet is vital Internet is vulnerable

- First job computing 1962
- 9 years semi-conductor manufacturer
- 30 years Cyber engineer Major Oil Co.
- Very early WEB experience
- 3 years Alyeska Pipeline DHS
- Major Cyber Security Certifications
- Network of cyber professionals
- Computer Club presentations
- Cyber Security SIG
- Windows SIG
- Senior University

What does John know

you

Biggest cyber security threat

you

Best cyber security defense

Fundamental Issues

- Trust
- Convenience

- FOMO
- Curiosity

- Use cellular
  Wi-Fi & Bluetooth off unless required
- Use Linux
  bootable CD/DVD write protected USB
  Virtual machine
  tethered to Cellular hotspot
- Old devices
  smart phone for IoT command & control
  old laptop/desktop for Linux
- Hard wire ethernet connection
  Unplugged when not in use

The chase

Multiple

- Identity
- Machines
- Browsers
- Security suites
- HOME NETWORKS
  segmentation
  VLANs Guest wireless
  email addresses
  Phone numbers

How Internet gets into your home

- Dial-up modem
- Digital Subscriber Line DSL
- Satellite down link
- Wi-Fi metro mesh
- Fixed Wireless
- Cellular
- Cable modem

Cable modem

- Uses portion of bandwidth to home
  TCP/IP
- Shared with neighbors
- NAT
  Network Address Translation
- DHCP
  Dynamic Host Configuration Protocol
  DNS, host name, subnet, etc.

Router, Wireless Access Point

- Default route to Internet
- Firewall
- Security Appliance
- QOS
  Quality of Service
- VPN
- Speed bottleneck

Router WAP settings

- Wi-Fi protected setup OFF
- Remote Access OFF enable only when needed
- STRONG Admin passphrase
- Firewall ON
- UPnP Universal Plug and Play OFF
- MAC filtering
- Parental Controls
- Band control 2.4GHz 5GHz
- WPA2 Personal Shared Secret
- Broadcast SSID
- DHCP on and configured
- Firmware update

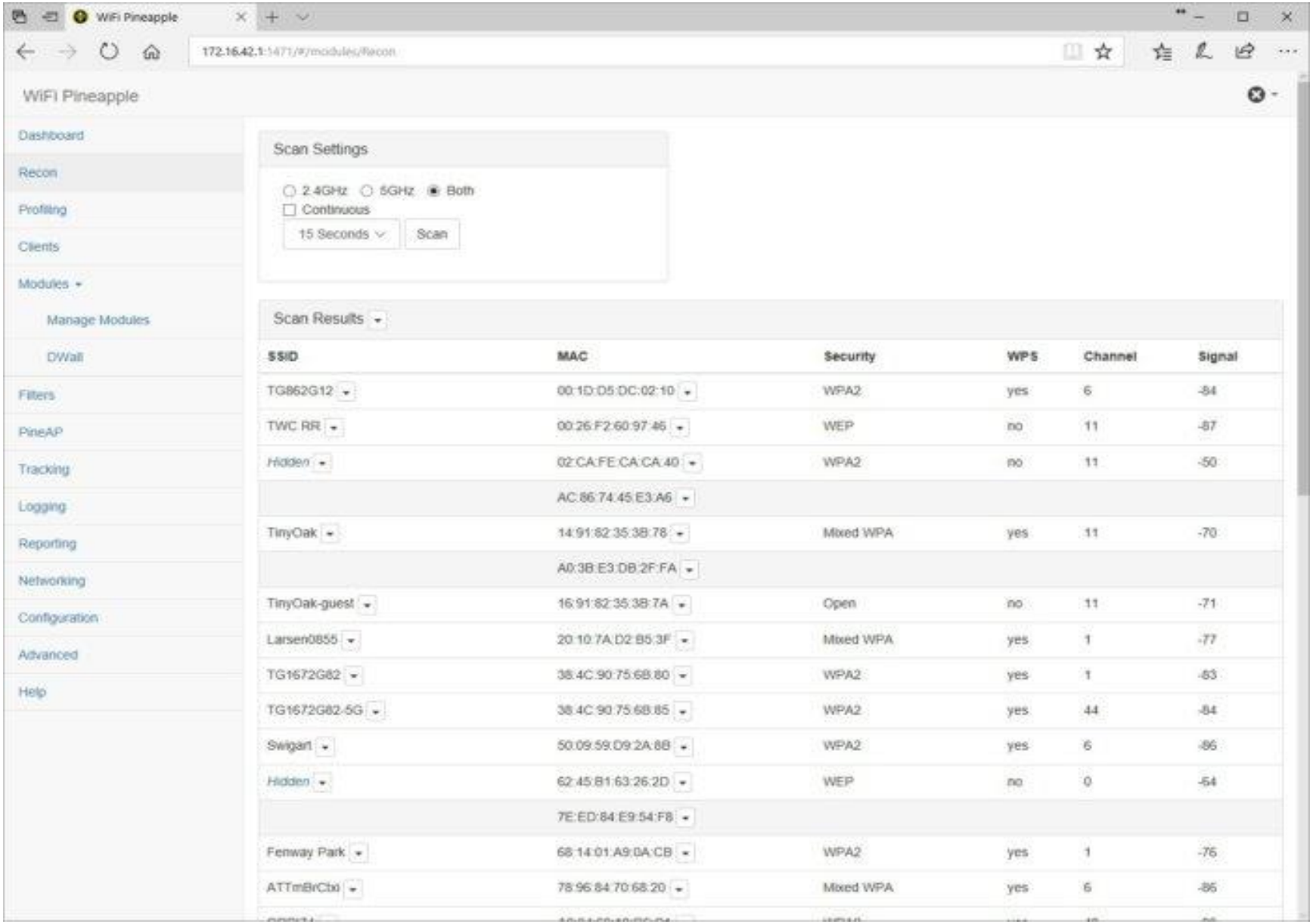
Wireless Access Point

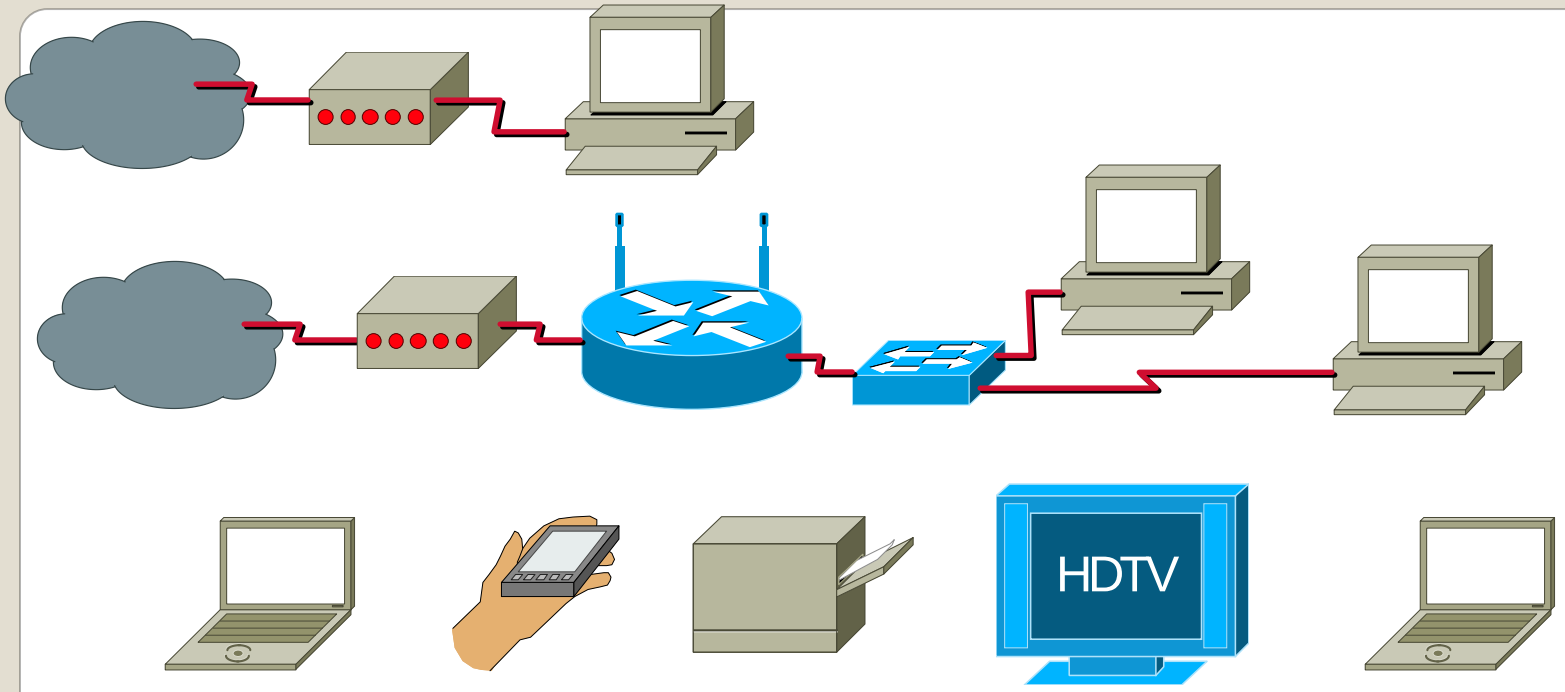
- SSID - Network name
- ADMINISTRATOR passphrase
- Disable Remote Access
- Use Guest Access
- Use VLans
- MAC filtering
- Network Map

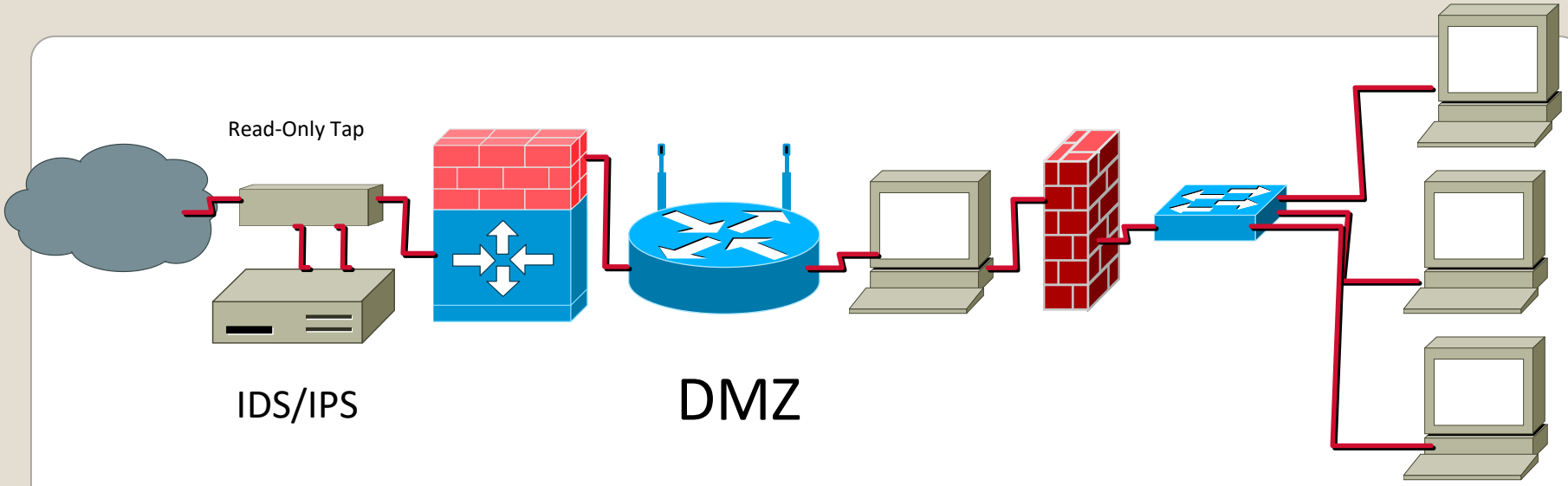
- Radio
- Disassociate

DNS & Name Lookup

- Hierarchical Distributed
- Each device
- Quad 9 Quad 1
- Local hosts file
- Keep trusted record of IP addresses


WiFi Pineapple
172.16.42.1:1471/#/modules/Recon
WiFi Pineapple
Dashboard
Recon
Profiling
Clients
Modules
Manage Modules
DWall
Filters
PineAP
Tracking
Logging
Reporting
Networking
Configuration
Advanced
Help
Scan Settings
2.4GHz
5GHz
Both
Continuous
15 Seconds
Scan
Scan Results
SSID
MAC
Security
WPS
Channel
Signal
TG862G12 00:1D:D5:DC:02:10 WPA2 yes 6 -84
TWC RR 00:26:F2:60:97:46 WEP no 11 -87
Hidden 02:CA:FE:CA:CA:40 WPA2 no 11 -50
AC:86:74:45:E3:A6
TinyOak 14:91:82:35:3B:78 Mixed WPA yes 11 -70
A0:3B:E3:DB:2F:FA
TinyOak-guest 16:91:82:35:3B:7A Open no 11 -71
Larsen0855 20:10:7A:D2:B5:3F Mixed WPA yes 1 -77
TG1672G82 38:4C:90:75:6B:80 WPA2 yes 1 -83
TG1672G82-5G 38:4C:90:75:6B:85 WPA2 yes 44 -84
Swigart 50:09:59:D9:2A:8B WPA2 yes 6 -86
Hidden 62:45:B1:63:26:2D WEP no 0 -64
7E:ED:84:E9:54:F8
Fenway Park 68:14:01:A9:0A:CB WPA2 yes 1 -76
ATTmBrCbt 78:96:84:70:68:20 Mixed WPA yes 6 -86


HDTV



Wireless

NotPetya

- Stuxnet, Haiti invasion, Sony & response
- June, 2017 A.P. Møller-Maersk
- Kiev, Ukraine Linkos Group M.E.Doc
- Update -> backdoor -> EternalBlue (NSA)
- Island hopping unpatched -> patched
- Encryption with random key
- $10Billion
- Infection world wide including Russia
- Nation-state weapon of cyber war

WEB issues

- Connectionless
- Not intended for current use
- Query & Response
- Client Server
  either can run code on the other
- Any/everything apps, attachments, audio, video

WEB Issues

- connectionless
- Interpreters/helpers
- ActiveX, Java, scripts, shells
- HTTP
- HTML
- Akamai, cloud
- Increased use of third party services
- What, me worry?
- Information gives no indication of being stolen
- Information is cumulative
- connectionless

Multi Factor Authentication

- SMS or text message
  Telecom companies not IDentity issuers
- Authenticator App
  Stolen phone or backup
- Physical FOB
  Long time to replace
- Biometrics
  impossible to replace

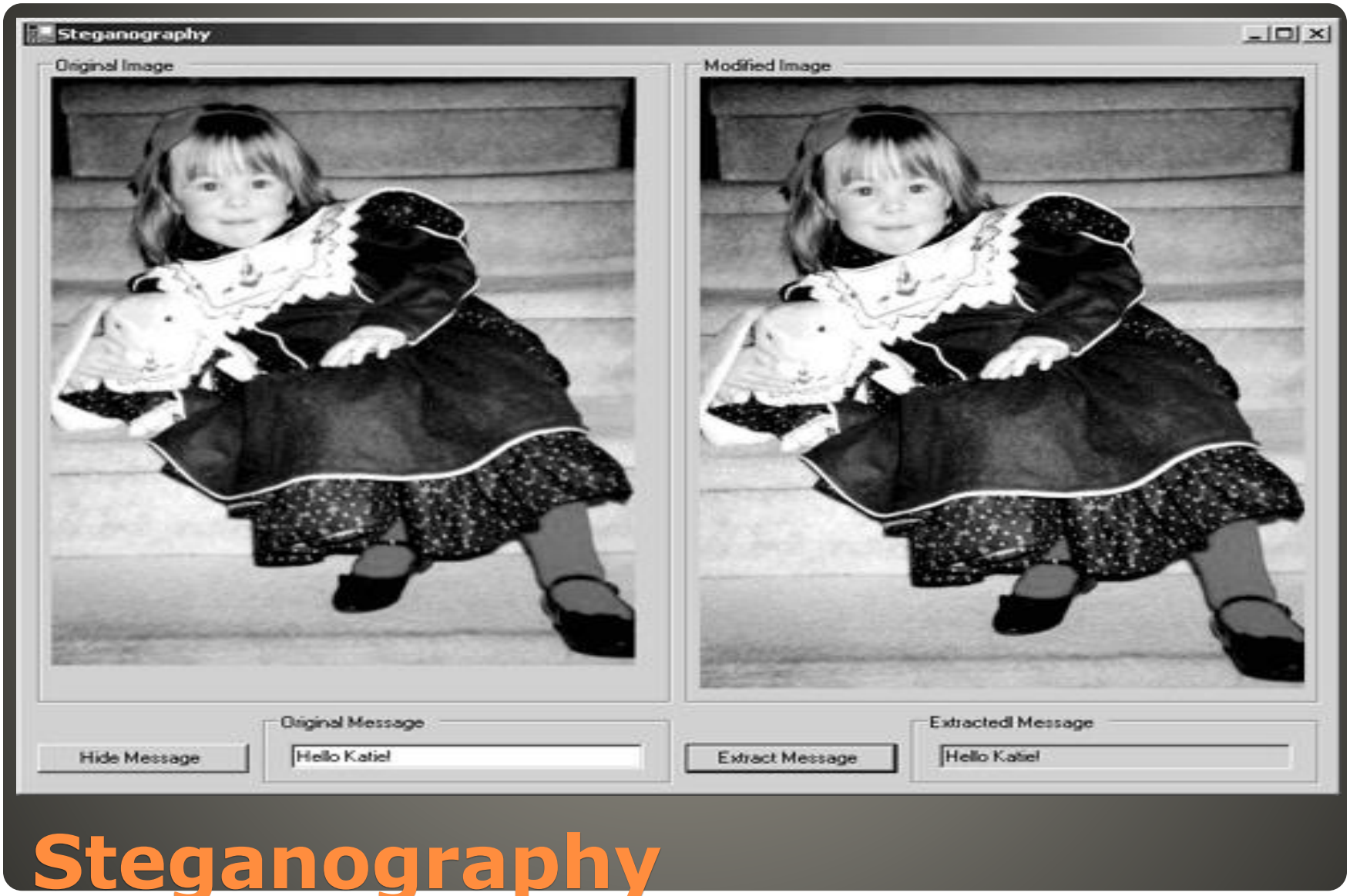
- Exactis
- Best tracking and surveillance ever conceived
- Cloud
- Crypto mining

- 1-2-3-4
- Steganography
- Hash
- Symmetric
- Asymmetric

cryptography

- 1-2-3-4
- Algorithm
- Key
- Plain text
- Cypher text

cryptography



Steganography

- One way
- Fixed length output
- Any length input
- Message digests
- E.g. MD2,MD4,MD5,SHA-1,SHA-2
- Used for integrity, digital signing & passphrases

hash

symmetric

- Plain text, algorithm, key, cypher text
- Algorithm usually public
- Key space is important
- Reversible with the one key
- Does not scale
- E.g. RC4,SEAL DES,3DES,RC5,Rijndael
- One-time pad
- Cryptanalysis
- Control

- Confidentiality
- Integrity
- Authentication
- Non-Repudiation

CIA

Asymmetric

- Public & private key
- Intractable problem
- Symmetric key exchange in presence of advisory
- Thousands of times slower
- E.g. RSA, El Gamal, ECC
- Public key distributed and verified via Digital Certificate
- Signing via digital signature

Uses of cryptography

- Code signing
- VPN
- Confidentiality
- Integrity
- Authentication
- Non-Repudiation
- Disk and file encryption
- IPSec
- PKI
- blockchain

Some detail

- Client hello
- Server hello
- Client validation and pre-master secret
- Both sides use secret to generate session key(s)
- Web session proceeds with data in transit encrypted with symmetric key(s)

Digital Certificates

- Part of PKI
- Binding of public key to entity
- Verified and signed by certificate authority
- Chain of trust
- X.509

Safer Browsing

- Virtual machines Linux
- Live CD/DVD
- Check for updates before each sensitive session
- New browser for each sensitive session
- Clickjacking
- Cross Site Scripting
- Cross Site Request Forgery
- “Private” sessions

Safer Browsing

- Browser wars
- Brave, Lynx
- Add-ons and extensions

  uBlock Origin, NoScript, uMatrix, AdBlocker
- MultiFactor Authentication
- Maintain state

  URL, Hidden form fields, cookies
- Proxy
- TOR
- Business Practices IRS – Phone Bank - PIN

Tracking

- Cookies
- IP Address
- History
- Local logs
- Browser User Agent string
- Fingerprinting
- Referrer
- “I am not a robot”
- Anything coders can think of …

Maintaining State

- URL

https://mg.mail.yahoo.com/neo/b/launch?&filterBy=&fid=Inbox&fidx=1&ac=gfVcFbP06soZ0XxbtXJq5aW8I1M-&mailboxId=VjJ-C_UFXi_-EVMadxLtWRtp9zjHo-i8cY1FYym0mI8b9spZcwe1Zg2b-H0cYx2fOJ3OGH4nkLovJSeSm65J6U1w&.rand=1655841https://mg.mail.yahoo.com/neo/b/launch?&filterBy=&fid=Inbox&fidx=1&ac=gfVcFbP06soZ0XxbtXJq5aW8I1M-&mailboxId=VjJ-C_UFXi_-EVMadxLtWRtp9zjHo-i8cY1FYym0mI8b9spZcwe1Zg2b-H0cYx2fOJ3OGH4nkLovJSeSm65J69qU1w&.rand=165584188&nsc88&nsc

- Hidden Form Fields

```
<form action="myform.cgi">
<input type="file" name="fileupload" value="fileupload" id="fileupload">
<label for="fileupload"> Select a file to upload</label>
<input type="hidden" id="ipaddr" name="ipaddr" value="<?php echo $_SERVER['REMOTE_ADDR']; ?>">
<input type="hidden" id="referer" name="referer" value="<?php echo $_SERVER['HTTP_REFERER']; ?>">
<input type="submit" value="submit">
</form>
```

- Cookies

Safer

- VMs
- Live CD/DVD/USB
- Google Search Engine
- Hover Over
- Multiple Browsers
- Multiple security configurations
- VPN
- Tiny URL expansion
- Popups
- Certificate warnings
- Drive By
- Sites with user supplied WEB content
- EULA
- Deliberate mistakes
- Become informed, aware, suspicious

- Search engines
- Browser indicators
- Hover Over
- URL inspection
- Professionalism
- Surveys & Account creation
- Google Transparency Report
- Lynx
- F12
- BBB
- Intent & AutoFill
- Security Images
- Multi Factor Authentication

Safer

Safer

- Update Update Update Update
- 3-2-1 Backup
- Security Suites Defense in Depth
- MultiFactor authentication
- https
- VPN
- Deliberate mistakes on Data Entry
- Awareness

- DuckDuckGo
- WolframAlpha
- Startpage
- Privatelee
- Yippy
- Hulbee
- Gibiru
- Disconnect Search
- Lukol
- MetaGer

Search Engines without tracking

- Questions, suggestions, comments?

SCCCCyber@gmail.com

Useful Links

- https://heimdalsecurity.com/blog/ultimate-guide-secure-online-browsing/
- https://www.google.com/transparencyreport/
- https://myaccount.google.com/activitycontrols