Sun City Computer Club

Safer WEB Browsing

Part Two

- Audio Recording of this session
- Use the link above to access MP4 audio recording

- Audio Recording in Progress

- SIG attendees are required to be members of the chartered club sponsoring that SIG.
- Sun City Community Association By-law

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

- Safer not Safe
- E-postcard not e-mail
- Passphrases not passwords
- Radio not wireless
- ADMINISTRATOR
  Rights and Privilege

https://sccccyber.blogspot.com/2017/01/administrator.html
https://sccccyber.blogspot.com/2018/05/windows-administrator-account-revisit.html
https://sccccyber.blogspot.com/2020/02/windows-10-local-account-administrator.html

Vocabulary

Advantages to PowerPoint delivery

- Any length
- Any time
- Any schedule
- Timeliness
- Pause and continue
- Pause and look up for clarity
- Skip over
- Play again and again
- Adjust video size
- Adjust audio level
- Available to new users Months from now

Sun City Computer Club Resources

- Presentations
- SIGs
- Newsletters
- Wiki
- Help Center
- First Time
- Classes

Cyber Security SIG

- Bimonthly presentations Audio recorded
- Classes
  - Computer and Information Security
  - Cyber War
  - Safer Browsing
- Cyber Security News 196 Searchable
- News -> timely


More
Create Blog
SCCCCyber
Tuesday, June 2, 2020
Firefox version 77 released today 2-June-2020
https://www.mozilla.org/en-US/firefox/77.0/releasenotes/
Posted by John Jenkinson at 12:14 PM
No comments:
Sunday, May 31, 2020
eBay Chick-fil-A Citibank what are you doing?
A LOT of port scanning occurs on the Internet. A LOT.
The Internet accesses things via an IP address and the port at that IP address.
To get an HTTP web page you try to connect to the IP address on port 80. (A standard port number but it can be changed)
So port scanning tries all the IP addresses and all of the 65536 TCP ports and all 65536 UDP ports.
Blog Archive
2020 (35)
June (1)
Firefox version 77 released today 2-June-2020
May (5)
April (14)
March (8)
February (3)
January (4)
2019 (28)
2018 (57)
2017 (62)
2016 (16)

Fundamental Issues

- Trust
- Convenience

- FOMO
- Curiosity

- Now any/everyone can have a voice

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
- Interpreters/helpers
- ActiveX, Java, scripts, shells

- Name resolution
  Own name, Hosts file, NetBIOS, DNS
- Domain Name System
  Distributed, hierarchical, caching database
  No authentication
- BGP
  routing, No authentication

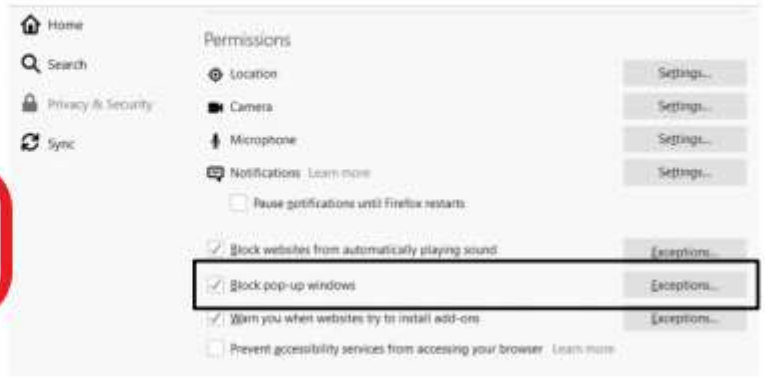
Journey to the Web site

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

cryptography

WEB BROWSER SAFETY TIPS

- Use pop-up blockers. Pop-up rules can be changed in a browser's "Settings" or "Options" menu
- Look for the "S" after http in the web address, indicating the website is secure
- Look for a padlock in the address bar. The padlock indicates secure mode.
- Make sure automatic updates are turned on and working efficiently.



- Beware of using the autofill and built-in password management feature in your browser. Autofill fills in the fields on a form automatically, according to the information that the user has previously used. 13

Semantics Government Safe

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

cryptography

- 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

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)
- HTTPS layered on SSL or TLS

More Detail

- Decide to visit WEB site
- Open Browser
- Type in URL (Universal Resource Locator)
- Name Lookup (IP address)
- System places information on *wire*
- Internet Service Provider (ISP) sends packet(s) to next router (BGP) Border Gate Protocol

More Detail

- TCP (Transmission Control Protocol) Handshake
- ClientHello TLS, random number, cypher suite list, compression method(s)
- ServerHello TLS version, random number, lowest common denominator for cypher and compression, perhaps session ID
- Server sends its Certificate message
  Certificate - binding Identity and public key
  Certificate chain of trust

Yet more detail

- Server sends ServerKeyExchange message
- Server sends ServerHelloDone
- Client sends ClientKeyExchange message
  PreMasterSecret, {client public key}
  Encrypted with server's public key
- Compute Master Secret (symmetric key)
  Using PreMasterSecret, random numbers
- Client sends ChangeCipherSpec message
  Encrypted tunnel established

- Client sends Finished message
  hash & MAC of previous handshake msgs.
- Server rejects or accepts
- Connection torn down –or-
- Server sends ChangeCipherSpec then
- Server sends Finished

- Connection established and uses negotiated encryption and compression

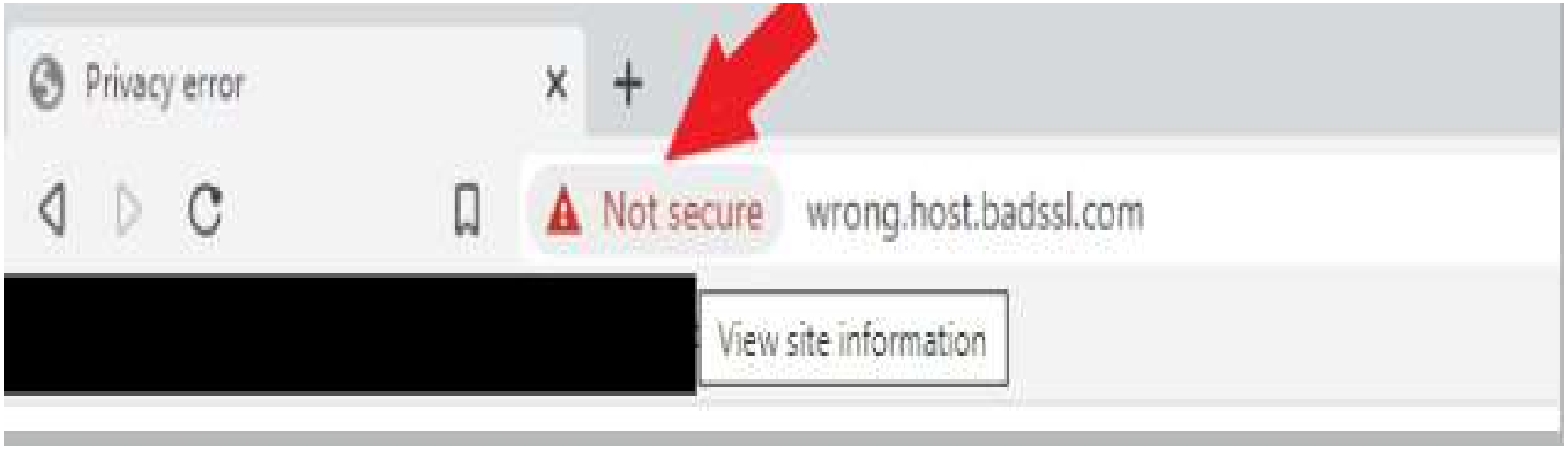
More than enough detail

- Encrypted (symmetric) tunnel atop network
- Session-less HTTP
- HTML HTML5
- Request Response
- Request Response
- Request Response
- Encoding in URL
- Hidden Form Fields in HTML
- Cookies

Now what?

- HTML interpreted language
- Some sites revert to HTTP from HTTPS
- Thousands times slower
- Getting to be very rare and defended
- Not a WEB page Million dollar page
- Past resources could not keep up with demand

Busy Busy Busy Busy Busy


Privacy error
Not secure
wrong.host.badssl.com
View site information

Safer Browsing

- Tails
- Linux
- 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

Gotchas

- Overlay Lock Icon
- Overlay https://
- Sites can and do revert to http
- Browser extension to force https
- Complete Window overlay

Certificate & Encryption

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

Scripts

- Like a movie or play detailed instructions
- HEAVILY used for dynamic content
- WEB page -> WEB pages
- Million Dollar home page
- Root page has carved out many *other* pages - each yet another connection, request, reply
- JavaScript
- iframe

Scripts

- Cross Site Scripting
- Cross Site Request Forgery
- Browsers and/or extensions can block
- Most sites use Scripts
- Can white list (allow list) trusted sites
- Drive-By download
- Scripts query and Modify DOM
  Document Object Model
- Hosting sites hacked to host drive-by
- Most browsers vulnerable
- OS vs browser notifications

Safer

- VMs
- Live CD/DVD/USB
- Sandbox
- 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, Preparedness, Understanding

- Questions, suggestions, comments?

SCCCCyber@gmail.com