

INTRO TO ETHICAL HACKING

MIS 5211.701
Week 8
Site:
<http://community.mis.temple.edu/mis5211sec701fall2018/>

Tonight's Plan

- Breaking Wireless News
- Social Engineering
- Encryption
- Encoding

MIS 5211.701 2

Social Engineering

- Definition
 - Getting people to do what you want
- Alternatively
 - Psychological manipulation of people into performing actions or divulging confidential information. - wikipedia.org
 - Or
 - Social engineering exploits people's emotions and their desire to help others - malware.wikia.com

MIS 5211.701 3

Attitude

- ☐ Confidence
 - Act like you belong there
- ☐ Friendliness
 - Make people want to help you
- ☐ Appearance
 - Dress for the part



MIS 5211.701

4

Categories

- ☐ Can take a number of forms
 - Pretexting
 - Phishing
 - Spear Phishing
 - Vishing
 - Tailgating
 - Quid Pro Quo
 - Baiting
 - Diversion Theft



MIS 5211.701

5

Pretexting

- ☐ Inventing a scenario
 - Do some recon
 - Speak the language
 - Impersonate someone who should be there
 - Give information outsider would not have
 - Legitimate name of supervisor or department
 - Reference correct office location
 - Project name or internal initiative
 - Pretend to be police, FBI, TSA, or Homeland Security
 - Note: this is a crime all by itself



MIS 5211.701

6

Phishing



- Email
 - Again, starts with Recon
 - Send legitimate looking email
 - Request verification of information and warn of consequences for non-compliance
 - Link to fraudulent web site
 - Note: Larger organizations pay for monitoring services to catch this

MIS 5211.701

7

Spear Phishing

- Similar to phishing, but much more targeted
 - Heavy recon
 - Identify just the right target or targets
 - Executive
 - IT Admins
 - Accounts payable
 - Create content very specific to Target(s)

MIS 5211.701

8

Phishing and Spear Phishing

- Often used to deliver malware
 - Tempting attachments:
 - New bonus plan
 - Layoff list
 - Memorial notice for recently passed employee
 - Web sites that deliver promised content
 - But infect browser

MIS 5211.701

9

Vishing

- Similar to phishing, but by phone or fraudulent IVR
- VOIP can be used to falsify source phone number (Caller ID Spoofing)
- Swatting - Initiating a police raid



MIS 5211.701

10

Tailgating

- May or May Not be Social Engineering
 - People feel a need to "Hold the door"
 - Especially problematic in the south eastern US
- Even man traps and roto-gates can be gotten around
 - Show up with large packages or boxes
 - Ask security for help



MIS 5211.701

11

Quid Pro Quo

- Call into company claiming to be Tech Support
 - May take a number of calls
 - Eventually you will hit someone that actually called for support
 - Help them (Sort of)
 - They'll follow your directions
 - Type commands
 - Download software
 - Provide data

MIS 5211.701

12

Baiting

- ❑ Spread USBs around parking lots
- ❑ Mail official looking CDs
- ❑ Send a token desk toy (with WiFi repeater installed)
- ❑ Replacement mouse (with malware preloaded)
- ❑ MP3 player



MIS 5211.701

13

Diversion Theft

- ❑ Fake ATM
- ❑ Intercept delivery man
- ❑ "Borrow" a FedEx or UPS truck and make a pickup

MIS 5211.701

14

Dumpster Diving

- ❑ More of a recon technique than actual Social Engineering
- ❑ Gold Standards of Dumpster Diving
 - Yellow Sticky
 - Hand written notes



MIS 5211.701

15

Questions

MIS 5211.701

16

Encryption (Short Version)

- Couple of points up front
 - Real "Standards based" encryption is hard to break 😞
 - Proprietary encryption is usually not as hard to break 😊
 - When encryption is broken, it is usually the implementation, not the cypher suite that is broken
 - Example: WEP and RC4
 - Regardless of encryption, the computer has to decrypt the data to act on it. Therefore, clear text data is in memory
 - Also true of browsers, browser must decrypt to act

MIS 5211.701

17

Encryption (Short Version)

- One exception to clear text in memory
- Homomorphic Encryption
 - Computations carried out on ciphertext
 - Result is also encrypted
- Problem:
 - Very resource intensive
 - Not fast enough for practical use (yet)

MIS 5211.701

18



Terms

- ❑ Algorithm - Mathematical rules used to encrypt and decrypt
- ❑ Ciphertext - The encrypted data
- ❑ Encipher - Encrypting
- ❑ Decipher - Decrypting
- ❑ Key - Sequence of bits and instruction that governs encryption and decryption
- ❑ Plaintext - Unencrypted data

MIS 5211.701

19

Symmetric vs Asymmetric

- ❑ **Symmetric - Both parties use the same key** 
 - Anyone with a key can encrypt and decrypt
 - Relatively fast, less intensive to use
- ❑ **Asymmetric - Keys linked mathematically, but cannot be derived from each other** 
 - What one key encrypts, the other key decrypts
 - Works both ways
 - Also known as a key pair and associated with PKI or public key encryption
 - Relatively slow, resource intensive

MIS 5211.701

20

Stream and Block Ciphers

- ❑ Block Ciphers
 - Data is broken in to blocks
 - Blocks are encrypted/decrypted individually
- ❑ Stream Cipher
 - Message is not broken up
 - Encrypted/decrypted one bit at a time

MIS 5211.701

21

Types of Symmetric Systems

- ❑ DES
- ❑ 3DES
- ❑ AES or Advanced Encryption Standard
- ❑ Blowfish

MIS 5211.701

22

Types of Asymmetric Ciphers

- ❑ RC4
- ❑ RSA
- ❑ El Gamal
- ❑ ECC or Elliptic Curve Cryptosystems

MIS 5211.701

23

Public Key Encryption

- ❑ A "Hybrid" encryption method
- ❑ Symmetric key is used to perform bulk encryption/decryption of data
- ❑ Asymmetric keys are used to pass the symmetric key securely

MIS 5211.701

24

Session Keys

- Basically just a secret key that is only used for one session between users (or systems) and is then disposed of.

MIS 5211.701

25

Public Key Infrastructure (PKI)

- Comprehensive process including:
 - Programs
 - Data formats
 - Procedures
 - Protocols
 - Policies
 - Mechanisms
- All working together to secure communications

MIS 5211.701

26

Certificate Authority

- Certificate Authority (CA)
 - Issues public keys
 - Verifies you are who you say you are and provides certificate to prove it that can only come from a secret key you possess
- Registration Authority (RA)
 - Performs registration activities for a CA

MIS 5211.701

27

One Way Function or Hashing

- Provides for message integrity
- Mathematical value calculated from data that cannot be reversed
 - Sender and receiver can both calculate the value and verify that the data sent is the data received



MIS 5211.701

28

Digital Signature

- Encrypted hash value
 - Data sent is data received
 - Data can only have come from someone with the appropriate key(s)

| | |
|--------------------------------|--|
| Encrypted | Confidentiality |
| Hashed | Integrity |
| Digitally signed | Authentication and integrity |
| Encrypted and Digitally Signed | Confidentiality, Authentication, and integrity |

- Reference: CISSP Certification, Shon Harris

MIS 5211.701

29

The Unbreakable Code

- Only one cipher is truly unbreakable
- One-Time Pad
 - Each pad is only used once
 - Pad is XORd against cleartext data
 - Ciphertext is XORd against pad at receiver
- Generally not used due to difficulty in distributing non-recurring pads

MIS 5211.701

30

Rules for Key Management

- ❑ Longer keys are better
- ❑ Keys need to be protected
- ❑ Keys should be extremely random and use full spectrum of keyspace

MIS 5211.701

31

Encoding

- ❑ Encoding is NOT encrypting
- ❑ Perfect example: Base64 encoding
 - Well known
 - Reversible
 - Provide limited obfuscation
- ❑ Other examples
 - Morse code
 - ASCII
 - UTF-8, 16, 32
 - EBCDIC
 - Unicode

MIS 5211.701

32

Why we care about Encoding

- ❑ Often used incorrectly as a substitute for encryption
- ❑ Some “proprietary” encryption systems were nothing more than Base64 or Base64 with character substitution
 - Even if you don’t recognize the encoding it is easily “cracked” with frequency analysis

MIS 5211.701

33

Encoding and Web Attacks

- We will see this again when we cover Web applications and intercepting proxies
 - Base64 encoding is often used as an obfuscation technique

MIS 5211.701

34

Blockchain



- Distributed Ledger
 - All parties have a copy
 - Data can be added and is replicated across all copies
 - Data cannot be modified or deleted
- Benefits
 - Distributed
 - Lower transaction costs
 - Faster transaction times
 - Transparency & accountability & integrity
 - Usage information and traceability
 - Data security through encryption

MIS 5211.701

35

Ruby

- Link to Language
 - <https://www.ruby-lang.org/en/>
- Link to Interactive Ruby Website
 - <https://ruby.github.io/TryRuby/>
- Work through exercise section labeled "Summary #6 Which Means You've Come So Far" down to "You've Taught Your App to Reject Worthless Things"

36

Next Week

- ▣ Malware

MIS 5211.701

37

Questions

?

MIS 5211.701

38
