Lehrkraft

Hr. Mühlenhoff

Klausurtermine

1. Klausur
   - 16.10
   - 2.Block, 2.Woche

Themen

- Computercrimes and Security
  - Sicherer Datentransfer
  - (bei Interesse Internetrecherche)
- Projectmanagement
  - vielleicht auch in anderen Fächern? eher weniger
  - grundbegriffe: Task, Scope, Milestone, Schedule, Implementation
  - Project Team Kickoff Meeting zum Abschluss :rolleyes:
  - vorbereitung über mehrere Unterrichtsstunden, kann über mehrere Blöcke gehen

Task 8

- Salami Shaving
  - f
  - Manipulating programs or data so that small amounts of money are deducted from large a number of transactions.
- Denial of Service Attack
  - h
  - swamping a server with large numbers of requests
- Trojan Horse
  - c
  - Concealed instructions to a program, so that it will still work, but also perform other malicious duties
- Trapdoors
  - a
  - leaving an illicit program within a completed program, allowing unauthorised entry
- Mail Bombing
  - e
  - Innundating an email address
- Software Piracy
  - g
  - unauthorised copying of software
- Piggybacking
  - b
  - using another persons identification code before they logged off
- Phishing
  - d
  - tricking users to reveal confidential information
- Defacing
  - j

    - changing information shown on another persons website
- Hijacking
    - i
    - redirecting anyone trying to visit a certain site elsewhere

What other computer crimes are there?

- "Gemcutting" Runscape Scam
- gambling scams
- shipping scam
- social engineering
    - attack from the inside
- phone phreaking
- file sharing
- man in the middle attack
- exploitation of bugs or glitches
- (jailbreaking?)
- overflow based attacks
- spreading malware
    - ransomware
    - spyware
    - adware
    - hardware manipulation software
    - keylogger
- spoofing
- vishing (phishing over VoIP)
- spam
- cracking
- Identity Theft
- Data Traficking

Research

Man in the middle Attacks

- attacker relays and/or alters communication between two parties
- they believe to be directly communicating
- active eavesdropping
    - M receives Message from BOB
    - M reads Message and/or alters it
    - M transmits Message to ALICE, pretending to be BOB
    - both parties see M as the respective other dialog partner
- easy to do in unencrypted WiFi networks, as all packets are sent in the clear
- mutual authentication makes it harder for the MitM
- if the establishing of a key based authentication happens unencrypted the attacker can insert their own key.

```
Alice -> Hi Bob, give me your Key -> M -> Bob
```

```
Alice -> M -> Hi Bob, its Alice give me your key -> Bob
```

```
Alice <- M <- Bobs key <- Bob
```

```
Alice <- Ms Key <- M <- Bob
```

```
Alice -> Meet me at A(Ms Key) -> M -> Bob

Alice -> M -> Meet me at b(Bobs Key) -> Bob
```

- Defense
- Authentication
  - not over insecure channels (see above)
  - public private key infrastructure is the best option right now
  - encrypt message with recipients public key
  - decrpyt message with recipients private key
  - exchange keys in person for best security
- Tamper Detection
  - does a transaction take a lot longer than usual? -> it might be tampered with!
- notable instances of MitM Attacks
- Belkin wireless routers hijacked unsecured HTTP connections and pretended to be the desired destination server. in this malicious response they presented ads for different belkin products. ### Cracking

Vocabulary

phishing - “”“Password harvesting”“” nope neologismus basierend auf Phone Phreaking