Modeling Security Threats: Attack Trees

Steve Chapin

Systems Assurance Institute
Syracuse University
Attack Trees

- Defined by Bruce Schneier
  - inventor of Twofish and Blowfish
  - Author of *Applied Cryptography* and *Secrets & Lies*

- (Quasi-)Formal methodology to model threats

- Source for this talk:
Attack Trees

![Attack Tree Diagram]

- Open Safe
  - Pick Lock
    - Find Written Combo
  - Learn Combo
  - Cut Open Safe
    - Get Combo From Target
      - Threaten
      - Blackmail
      - Eavesdrop
      - Bribe
  - Install Improperly

P = Possible
I = Impossible
Attack Trees

Open Safe

Pick Lock
Learn Combo
Cut Open Safe
Install Improperly

Find Written Combo
Get Combo From Target

Threaten
Blackmail
Eavesdrop
Bribe

Listen to Conversation
Get Target to State Combo

P = Possible
I = Impossible
Attack Trees

Open Safe

- Pick Lock SE
- Learn Combo
- Cut Open Safe SE
- Install Improperly NSE

Find Written Combo NSE
Get Combo From Target

Threaten NSE
Blackmail NSE
Eavesdrop
Bribe NSE

and

- Listen to Conversation SE
- Get Target to State Combo NSE

NSE = No special equipment
SE = Special equipment
Attack Trees

Open Safe $10K

Pick Lock $30K
Learn Combo $20K
Cut Open Safe $10K
Install Improperly $100K

Find Written Combo $75K
Get Combo From Target $20K

Threaten $60K
Blackmail $100K
Eavesdrop $60K
Bribe $20K

$ = Cost of attack

and

Listen to Conversation $20K
Get Target to State Combo $40K

Syracuse – p.6/3
Attack Trees

- Open Safe $10K
  - Pick Lock $30K
  - Learn Combo $20K
  - Cut Open Safe $10K
  - Install Improperly $100K

- Find Written Combo $75K
- Get Combo From Target $20K

- Threaten $60K
- Blackmail $100K
- Eavesdrop $60K
- Bribe $20K

$ = Cost of attack

- Listen to Conversation $20K
- Get Target to State Combo $40K
Attack Trees

- Open Safe
  - NSE/$20K
  - Pick Lock
    - SE/$30K
  - Learn Combo
    - NSE/$20K
  - Cut Open Safe
    - SE/$10K
  - Install Improperly
    - NSE/$100K

- Find Written Combo
  - NSE/$75K

- Get Combo From Target
  - NSE/$20K

- Threaten
  - NSE/$60K

- Blackmail
  - NSE/$100K

- Eavesdrop
  - SE/$60K

- Bribe
  - NSE/$20K

- Listen to Conversation
  - SE/$20K

- Get Target to State Combo
  - NSE/$40K

NSE = No special equipment required
SE = Special equipment required
$ = Cost of attack
Goal: Head a message encrypted with PGP. (OR)
1. Decrypt the message itself. (OR)
   1.1. Break asymmetric encryption. (OR)
       1.1.1. Brute-force break asymmetric encryption. (OR)
       1.1.2. Mathematically break asymmetric encryption. (OR)
           1.1.2.1 Break RSA. (OR)
           1.1.2.2 Factor RSA modulus/calculate EIGamal discrete log.
       1.1.3. Cryptanalyze asymmetric encryption.
           1.1.3.1. General cryptanalysis of RSA/EIGamal. (OR)
           1.1.3.2. Exploiting weaknesses in RSA/EIGamal. (OR)
           1.1.3.3. Timing attacks on RSA/EIGamal.
   1.2. Break symmetric-key encryption.
       1.2.1. Brute-force break symmetric-key encryption. (OR)
       1.2.2. Cryptanalyze symmetric-key encryption.
2. Determine symmetric key used to encrypt the message via other means.
   2.1. Fool sender into encrypting message using public key whose private key is known. (OR)
       2.1.1. Convince sender that a fake key (with known private key) is the key of the intended recipient.
       2.1.2. Convince sender to encrypt using more than one key—the real key of the recipient, and a key whose private key is known.
       2.1.3. Have the message encrypted with a different public key in the background, unknown to the sender.
Goal: Read a specific message that has been sent from one Windows 95 computer to another.
1. Convince sender to reveal message. (OR)
   1.1. Bribe user.
   1.2. Blackmail user.
   1.3. Threaten user.
   1.4. Fool user.
2. Read message when it is being entered into the computer. (OR)
   2.1. Monitor electromagnetic emanations from computer screen.
       (Countermeasure: use a TEMPEST computer.)
   2.2. Visually monitor computer screen.
3. Read message when it is being stored on sender's disk.
   (Countermeasure: use SFS to encrypt hard drive.) (AND)
   3.1. Get access to hard drive. (Countermeasure: put physical locks on all doors and windows.)
   3.2. Read a file protected with SFS.
4. Read message when it is being sent from sender to recipient.
   (Countermeasure: use PGP.) (AND)
   4.1. Intercept message in transit. (Countermeasure: use transport-layer encryption program.)
   4.2. Read message encrypted with PGP.
5. Convince recipient to reveal message. (OR)
   5.1. Bribe user.
   5.2. Blackmail user.
   5.3. Threaten user.