Survivable Network Analysis (SNA)

- Continuation of discussion which was based on


  and

## What is the threat?

[Source: CMU/SEI-2000-TR-013]

<table>
<thead>
<tr>
<th>Attacker</th>
<th>Resources</th>
<th>Time</th>
<th>Tools</th>
<th>Risk</th>
<th>Access</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recreational Hacker</td>
<td>Range of skills</td>
<td>Can be patient, but usually looks for opportunity</td>
<td>Uses readily available tool sets</td>
<td>May not understand or appreciate the risk</td>
<td>External</td>
<td>Personal recognition, Develop hacking skills</td>
</tr>
<tr>
<td></td>
<td>Many have limited ability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>May operate as part of a team</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disgruntled Employee</td>
<td>Depends on personal skills</td>
<td>Could be very patient and wait for opportunity</td>
<td>Uses readily available tool sets</td>
<td>Risk averse particularly if still employed</td>
<td>Internal or external or Internet or LAN</td>
<td>Personal gain, Embarrass organization</td>
</tr>
<tr>
<td></td>
<td>May have knowledge of process</td>
<td></td>
<td>Former system admin could develop tools</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unlikely to use external resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© A.K. Krings 2011  
Sequence 6
What is the threat?

<table>
<thead>
<tr>
<th>Activist who targets organization for ethical or political reasons</th>
<th>Limited means to hire external expertise, but could have talented members</th>
<th>Likely very patient, but specific events may force quicker action</th>
<th>Uses readily available tool sets</th>
<th>Not risk averse</th>
<th>External Internet</th>
<th>Embarrass organization, Impact public or customer opinions, Impact government or corporate partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial Spy</td>
<td>Expert knowledge</td>
<td>Desired information has limited shelf life</td>
<td>Can customize tools</td>
<td>Somewhat risk averse</td>
<td>Capture could impact corporate sponsors</td>
<td>External Internet</td>
</tr>
</tbody>
</table>

[source CMU/SEI-2000-TR-013]
## What is the threat?

[source CMU/SEI-2000-TR-013]

<table>
<thead>
<tr>
<th>Nation-State</th>
<th>Could hire external resources for high-payoff attack</th>
<th>Patient, but desired information may be needed quickly</th>
<th>Could develop tools if payoff is high</th>
<th>Moderately risk averse and may be able to operate outside of U.S.</th>
<th>External and Internet</th>
<th>Could be organizational visitor</th>
<th>Access government information or corporate proprietary information</th>
</tr>
</thead>
</table>

© A.K. Krings 2011
Survivable Network Analysis (SNA)

Step 3: Compromisable Capability Definition
- Intrusion Scenario Selection: Intrusion Usage Scenarios (IUS)

  » IUS1 (Data Integrity and Spoofing Attack): An intruder swaps the patient identification of two validated treatment plans.
    - Sentinel performs validation of treatment plans before entering them into the database. In this scenario, an intruder accesses the database server to corrupt treatment plans without using the Sentinel client, but rather by spoofing a legitimate client.

  » IUS2 (Data Integrity and Insider Attack): An insider uses other legitimate database clients to modify or view treatment plans controlled by Sentinel.
    - The database security assumes that clients have exclusive write access to specific database tables. While the IUS1 scenario attempts to access the database directly, this scenario examines inappropriate access through other database clients.
Survivable Network Analysis (SNA)

» IUS3 (*Spoofing Attack*): An unauthorized user employs Sentinel to modify or view treatment plans by spoofing a legitimate user.
  - Some terminal access points for Sentinel are located in public areas, and hence are not as physically secure as those in private offices. This scenario illustrates opportunistic use of an unoccupied but logged-in terminal by an illegitimate user who spoofs the legitimate logged-in user.

» IUS4 (*Data Integrity and Recovery Attack*): An intruder corrupts major portions of the database, leading to loss of trust in validated treatment plans.
  - Scenarios IUS1 and IUS2 assume a sophisticated attacker who targets and recognizes specific treatment plans, and modifies only a few fields. This scenario assumes a brute-force corruption of the database, leading to large-scale loss of trust and potential denial of service during massive recovery operations.

» IUS5 (*Insider and Availability Attack*): An intruder destroys or limits access to the Sentinel software so it cannot be used to retrieve treatment plans.
  - This scenario could be as simple as removing the Sentinel software, or could involve attacks on the network or application ports to limit application access.
− Compromisable Component Identification
  » IUS1 (*Data Integrity and Spoofing Attack*): An intruder swaps the patient identification of two validated treatment plans.
    ■ Sentinel performs validation of treatment plans before entering them into the database. In this scenario, an intruder accesses the database server to corrupt treatment plans without using the Sentinel client, but rather by spoofing a legitimate client.

  » IUS1: This scenario compromises the treatment plan component. There were no validity checks made on treatment plans after the initial entry.
Compromisable Component Identification

IUS2 (*Data Integrity and Insider Attack*): An insider uses other legitimate database clients to modify or view treatment plans controlled by Sentinel.

- The database security assumes that clients have exclusive write access to specific database tables. While the IUS1 scenario attempts to access the database directly, this scenario examines inappropriate access through other database clients.

IUS2: This scenario compromises the treatment plan component. The treatment plan changes might be consistent but made by an improper agent.
Survivable Network Analysis (SNA)

- Compromisable Component Identification
  » IUS3 (Spoofing Attack): An unauthorized user employs Sentinel to modify or view treatment plans by spoofing a legitimate user.
    ■ Some terminal access points for Sentinel are located in public areas, and hence are not as physically secure as those in private offices. This scenario illustrates opportunistic use of an unoccupied but logged-in terminal by an illegitimate user who spoofs the legitimate logged-in user.

  » IUS3: This scenario compromises the treatment plan component. The majority of system users would object to logging into the system repeatedly as a way to continually monitor the validity of the user. The system had not considered those terminals which were in open areas easily accessible by unauthorized users.
Survivable Network Analysis (SNA)

- Compromisable Component Identification
  
  » IUS4 (*Data Integrity and Recovery Attack*): An intruder corrupts major portions of the database, leading to loss of trust in validated treatment plans.
    
    ▪ Scenarios IUS1 and IUS2 assume a sophisticated attacker who targets and recognizes specific treatment plans, and modifies only a few fields. This scenario assumes a *brute-force corruption* of the database, leading to large-scale loss of trust and potential denial of service during massive recovery operations.

  » IUS4: This scenario compromises the treatment plan component. Database recovery required higher priority with respect to operations.
Compromisable Component Identification

» IUS5 (Insider and Availability Attack): An intruder destroys or limits access to the Sentinel software so it cannot be used to retrieve treatment plans.
  ■ This scenario could be as simple as removing the Sentinel software, or could involve attacks on the network or application ports to limit application access.

» IUS5: All software components of the Sentinel subsystem are affected by this scenario. While there were implicit user requirements on availability, it had not been considered in the architecture.
Survivable Network Analysis (SNA)

- **Step 4: Survivability Analysis**
  - Softspot Component Identification
    » What is a Softspot component?
      ▪ a component that are both essential and compromisable
  - 3R’s Analysis
    » result: Survivability Map
      ▪ ID = identification
      ▪ TP = treatment plan
      ▪ UI = user interface
      ▪ DB = database
# Survivable Network Analysis (SNA)

- Survivability Map

<table>
<thead>
<tr>
<th>Intrusion Scenario</th>
<th>Resistance Strategy</th>
<th>Recognition Strategy</th>
<th>Recovery Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>IUS1:</td>
<td><strong>Current:</strong> Two passwords are required for TP access.</td>
<td><strong>Current:</strong> Logging of changes made to DB. Provider may recognize an incorrect TP.</td>
<td><strong>Current:</strong> Built-in recovery in commercial DB. Backup and recovery scheme defined.</td>
</tr>
<tr>
<td></td>
<td><strong>Recommended:</strong> Implement strong authentication supported in a security API layer. {1}</td>
<td><strong>Recommended:</strong> Add crypto-checksum when TP is validated. {3} Verify crypto-checksum when TP is retrieved. {4}</td>
<td><strong>Recommended:</strong> Implement a recovery mode in the user interface to support searching for and recovering incorrect TPs. {1}</td>
</tr>
<tr>
<td>IUS2:</td>
<td><strong>Current:</strong> Security model for DB field access.</td>
<td><strong>Current:</strong> None.</td>
<td><strong>Current:</strong> Scrap data and start over, or find an early backup and verify each entry.</td>
</tr>
<tr>
<td></td>
<td><strong>Recommended:</strong> Need to verify the security model in light of module addition and integration.</td>
<td><strong>Recommended:</strong> Perform a validation on access of a TP for verification. {2} Add crypto-checksum when TP is validated. {3} Verify this checksum when TP is retrieved. {4}</td>
<td><strong>Recommended:</strong> Scan DB for invalid crypto-checksums and/or invalid TPs and recover to last known correct TP. {4}</td>
</tr>
</tbody>
</table>
### Survivable Network Analysis (SNA)

<table>
<thead>
<tr>
<th>IUS3: An unauthorized user employs Sentinel to modify or view TPs by spoofing a legitimate user.</th>
<th><strong>Current:</strong> None. No timeout is specified so that anyone can use a logged in but vacated terminal. However, intruder only has access to logged in user’s TPs</th>
<th><strong>Current:</strong> None, except for unusual number of denied accesses to TPs as an intruder attempts to locate particular TPs.</th>
<th><strong>Current:</strong> Can get list of modified TPs through the spoofed users transaction history. Manually recover each modified record.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommended:</strong> Add a short logout timeout for any terminals in uncontrolled areas (not physician’s offices). [1]</td>
<td><strong>Recommended:</strong> Add logging, access control, and illegal access thresholds to the security API. [1]</td>
<td></td>
<td><strong>Recommended:</strong> Develop a recovery procedure and support it in the UI. [1]</td>
</tr>
<tr>
<td>IUS4: Intruder corrupts DB leading to loss of trust in validated TPs.</td>
<td><strong>Current:</strong> Security model in the DB protects data against corruption.</td>
<td><strong>Current:</strong> None, except when provider happens to recognize a corrupted TP.</td>
<td><strong>Current:</strong> Locate an uncorrupted backup or reconstruct TPs from scratch.</td>
</tr>
<tr>
<td><strong>Recommended:</strong> Implement live replicated DB systems that cross check for validity (supported in many commercial DB systems). [5]</td>
<td><strong>Recommended:</strong> Add and check crypto-checksums on records in the DB. [3] [4]</td>
<td><strong>Recommended:</strong> Reduce the backup cycle to quickly rebuild once a corrupted DB is detected. [5]</td>
<td></td>
</tr>
<tr>
<td>IUS5: Intruder destroys the Sentinel software so it cannot be used to retrieve TPs</td>
<td><strong>Current:</strong> Keep originals available.</td>
<td><strong>Current:</strong> System doesn’t work.</td>
<td><strong>Current:</strong> Reload the system from originals.</td>
</tr>
<tr>
<td><strong>Recommended:</strong> Keep a spare CD available for quick recovery</td>
<td><strong>Recommended:</strong> None. Easy to detect this one.</td>
<td></td>
<td><strong>Recommended:</strong> Fast recovery from CD. Create a small sub-system that can retrieve TPs while Sentinel is down or being upgraded. [6]</td>
</tr>
</tbody>
</table>
Survivable Network Analysis (SNA)

- Sentinel Architecture with Survivability Modifications

- Sentinel Application
  - Security Layer
    - List Manager
    - TP Builder - crypto-chk
    - TP Validator - crypto-chk
    - Action Team Builder

- Sentinel Back End
  - Business Logic
  - Security
    - Common Database - Replicated and Daily Backups
Examples (with respect to Survivability Map)

» IUS2
  - recommendation that all data retrieved from DB should pass through validation module to verify correctness of crypto-checksums

» IUS3
  - documented assumption that provider will become suspicious if large number of denied accesses to treatment plans
  - security layer {1} should be added
  - provide monitoring and logging capability
    - specifically important if recommendations on user interface in IUS1, 3 and 4 were not implemented

» IUS5
  - isolated reporting system was added outside of the original architecture
  - allows retrieving of treatment plan if primary system should fail
    - could be used as simple DB retrieval program
Survivable Network Analysis (SNA)

- Additional software, procedural and hardware requirements
  » software requirements might be:
    - emergency reporting system shall allow treatment plans to be viewed during recovery.
    - treatment plans shall be validated when they are read and written.
      - If a treatment plan is invalid, the last valid version of the treatment plan shall be recovered.
    - encrypted checksums shall be used to protect the integrity of the treatment plans.
    - database software shall support replication.
  » procedural requirements might be:
    - Sentinel software shall be backed up on CD.
    - daily backups of the database shall be performed.
  » hardware/operating system requirement might be:
    - workstations located in public areas shall have a short timeout based on inactivity.
    - there shall be login access thresholds for incorrect logins.
Final Observations

- Survivability strategy can be organized in terms of 3R’s
  » resistance, recognition, recovery
- Analysis should focus on early phases of life cycle
  » the study was done when Sentinel was just entering its implementation phase
- Application logic should bear significant responsibilities for implementing of survivability strategies
  » rather than the system infrastructure
- Can customer incorporate the recommendations?
  » here recommendations refined existing architecture rather than requiring redesign
- Study did not involve extensive distributed system requirements
Survivable Network Analysis (SNA)

Lessons learned from

- Survivability assessments of 11 control applications
- SSA in the context of CS448/548 Survivable Systems & Networks course with university internal and private entities

- Trust, Concerns and Fears
  - Great need for protection of client and team
  - Client expected to open up and show vulnerabilities
    - Why should they drop all shields? Is there a basis for trust?
  - Great fear of client personnel of being held accountable
    - IRS audit fear -- people felt on the defensive
  - Fear of consequences, e.g. individual or corporate
    - What if someone finds out the corporation is conducting an analysis?
    - Immediate response: Was there grounds for this?
  - Absolute need for confidentiality and non-tractability of findings and results

- The art is to ensure (1) client protection and (2) that we are trying to help
  - We are trying to understand
  - We need their help
  - We will guarantee to protect individuals, no names, no finger pointing, just finding better ways…