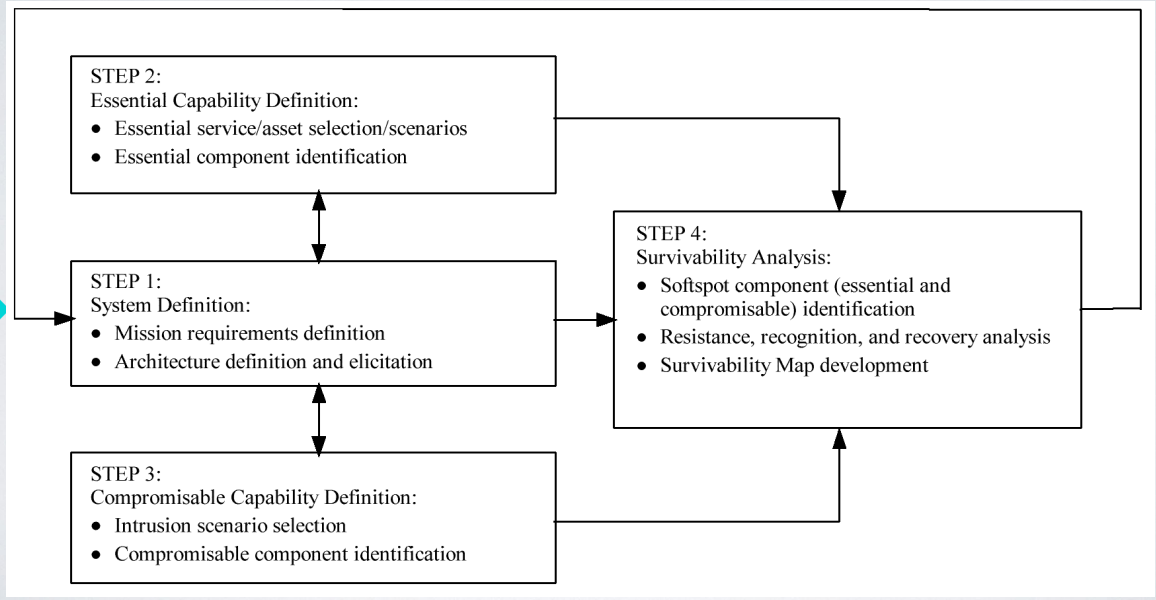
SURVIVABLE NETWORK ANALYSIS

- This discussion is based on
  - A Case Study in Survivable Network System Analysis, R. J. Ellison, R. C. Linger, T. Longstaff, N. R. Mead, TECHNICAL REPORT CMU/SEI-98-TR-014 ESC-TR-98-014, September 1998
  - and
  - Survivable Network Analysis Method, Nancy R. Mead, Robert J. Ellison, Richard C. Linger, Thomas Longstaff, John McHugh, CMU/SEI-2000-TR-013, ESC-TR-2000-013, September 2000.

SURVIVABLE NETWORK ANALYSIS (SNA)



SURVIVABLE NETWORK ANALYSIS (SNA)

- SNA Model builds on
  - Multi-step approach
  - Information Security Evaluation method
  - Evaluation of a distributed architecture rather than focussing on site-level security
  - Small team of trained evaluators
  - Several meetings and working sessions

SNA

- Compromisable Components
  - components that could be penetrated and damaged by intrusion
- Softspot Components
  - components that are both, essential and compromisable
- Strategy uses "three R's:

Intrusion Scenario	Resistance Strategy	Recognition Strategy	Recovery Strategy
(Scenario 1) …	Current:	Current:	Current:
	Recommended:	Recommended	Recommended:
(Scenario n)	Current:	Current:	Current:
	Recommended:	Recommended:	Recommended:

Figure 2. Survivability Map Template

SNA

- Case Study Subsystem
  - Application: management of mental health treatment
  - Carnegie Works, Inc (CWI) is developing a large-scale management system to:
    - automate, systematize, integrate multiple aspects of regional mental health care
  - System named Vigilant
    - 22 subsystems
    - distributed client/server networked environment
    - Vigilant vital part
      - development and management of treatment plans for patient and provider
    - problem of each patient, goals, actions, medication, therapy
    - treatment plan is carried out by action team composed of providers

SNA

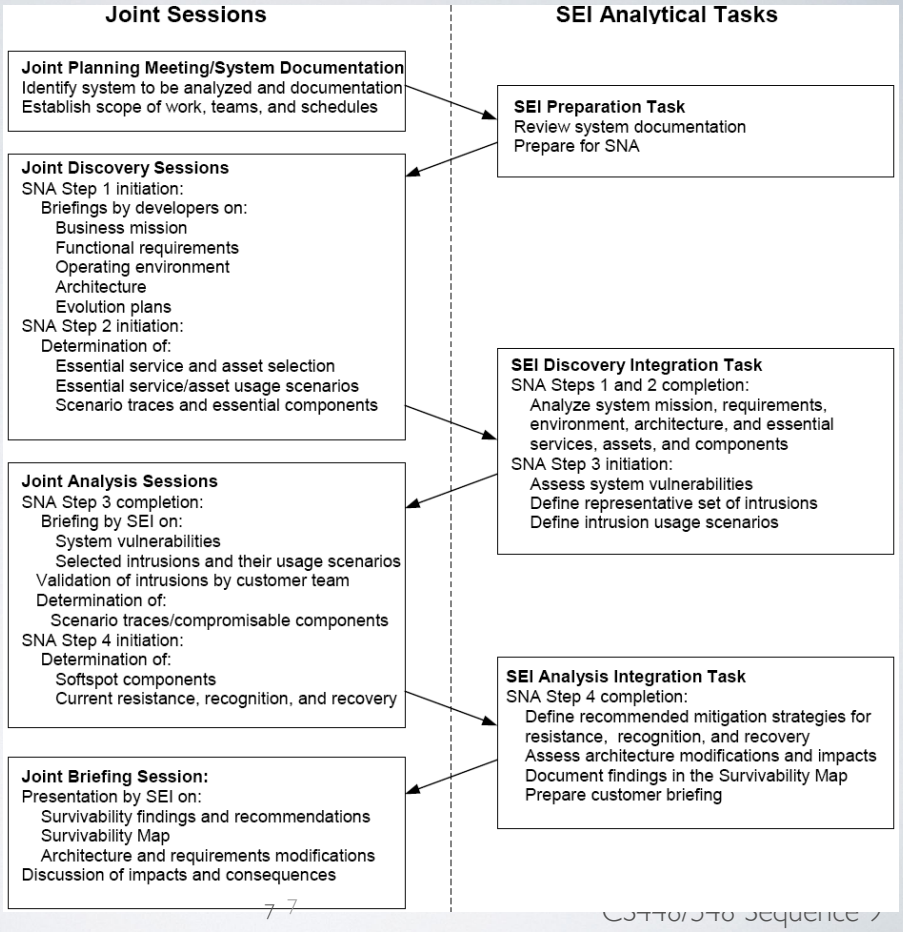
- Case Study Subsystem (cont.)
  - Sentinel Subsystem
    - subsystem of Vigilant
    - interacts with providers, affiliations and other subsystems
    - maintains action teams and treatment plans as part of Vigilant database
    - severe consequences of system failure
    - survivability of key Sentinel capabilities viewed by CWI as extremely important

CMU/SEI-2000-TR-013
Fig.5

SNA

Method

Application



SNA

- 1) Joint Planning Meeting
  - Analysis team responsibilities:
    - establish team (typically 3 members) and single point of contact (POC)
  - Customer responsibilities
    - establish team
      - should have the expertise required: e.g. system mission, requirements, operating environment, usage and architecture.
      - e.g. system architect, a lead designer, several stakeholders like system owners and system users
      - establish POC (should have authority to call on members)
    - identify system to be analyzed
      - should be appropriate size (realistic w.r.t. team size and time constraints)
      - establish clear boundaries, (e.g. should know every network connection)
  - Joint responsibilities
    - Scope the system to be analyzed and establish bound for the SNA
    - Establish work schedules and venues for joint sessions

SNA

- System Documentation
  - Customer Responsibilities
    - provide system documentation that describes:
      - Business mission
      - Functional requirements
      - Operating environment and users
      - Architecture: define system configuration in terms of
        - hardware & connections. e.g. in block diagram form
        - software in every hardware, protocols used, operating systems, application programs, databases, security, maintenance, backup, recovery facilities
        - administrators, developers, maintainers, operators

SNA

- Exit criteria
  - both teams and team leaders are assigned
  - system to be analyzed is identified
  - schedules are set
  - documentation is identified

SNA

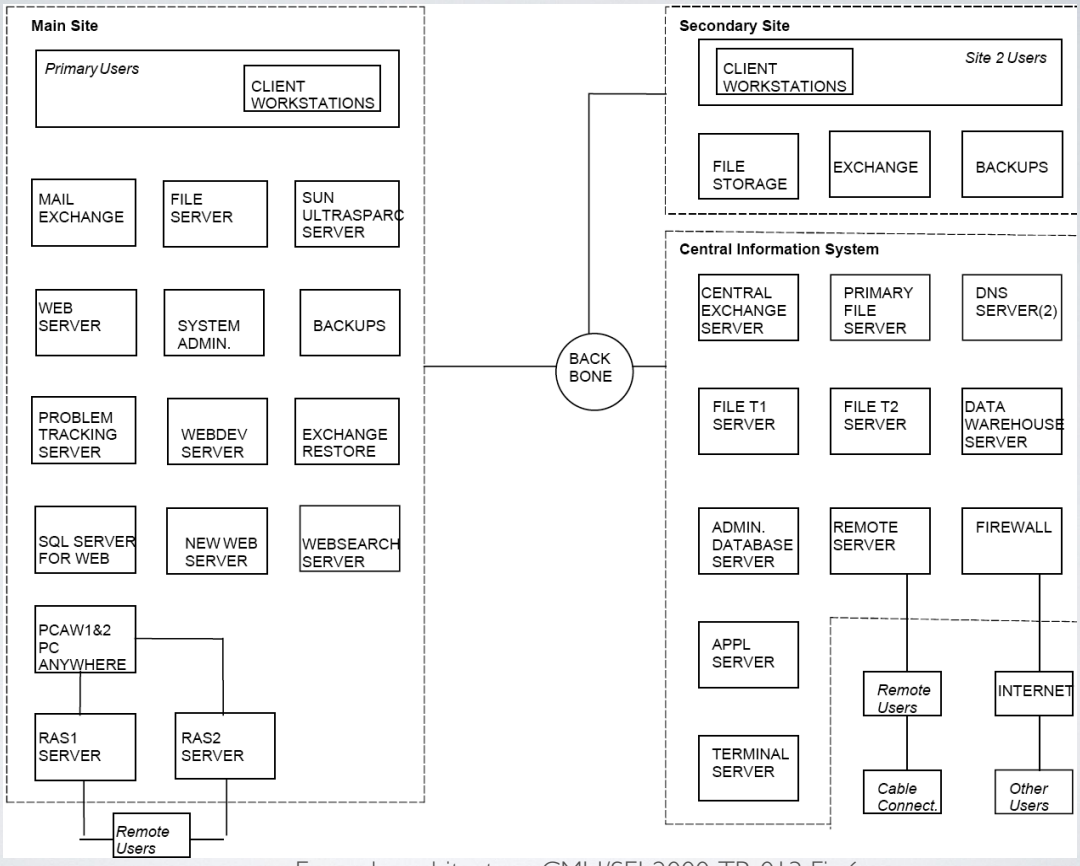
- 2) Analysis Team Preparation Task
  - review documentation
  - prepare for joint discovery sessions

SNA

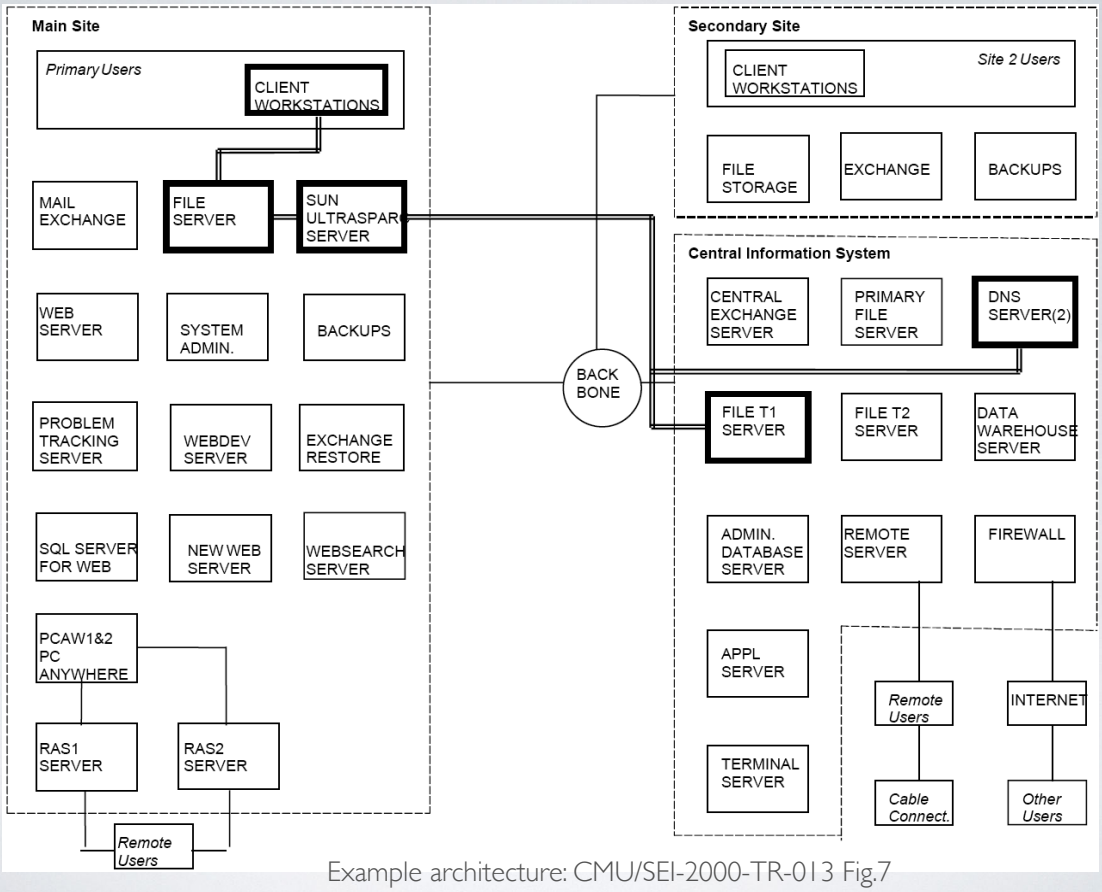
- 3) Joint Discovery Sessions
  - Customer initiates SNA Step 1 (System Definition)
    - Briefing on
      - business mission
      - principle functional requirements
      - system architecture
      - operating environment
      - typical usage scenarios (NUS)
      - evolution plans
  - Joint Responsibilities
    - Both teams initiate SNA Step 2 (Essential capability definition)
      - customer identifies set of essential services & assets and usage scenarios that invoke and access them
      - both teams trace them through the architecture to identify essential components
      - the highest priority services and assets are identified

SNA

- Exit criteria
  - Both teams share common level of understanding of
    - system
    - essential services
    - essential assets
    - scenarios have been traced though the architecture =>
    - essential components are revealed



Example architecture: CMU/SEI-2000-TR-013 Fig.6



Example architecture: CMU/SEI-2000-TR-013 Fig.7

SNA

- 4) Analysis Team Discovery Integration Task
  - Complete SNA Step 1 & 2 (sys.def. & essential cap. def.)
    - analyze and summarize
      - system mission
      - functional requirements
      - operational environment
      - essential services and assets
      - scenarios traces
      - essential components
  - Initiate SNA Step 3 (Compromisable Capability Definition)
      - assess system vulnerabilities
      - identify representative intrusion scenarios
      - define corresponding usage scenarios
  - Exit criteria
    - system vulnerabilities and representative intrusions have been identified

SNA

- 5) Joint Analysis Session
  - Customer team
    - validates selected intrusion scenarios
    - proposes modifications and extensions
  - Joint responsibilities
    - complete SNA Step 3 (Compromisable Capability Definition)
      - trace intrusion scenarios through architecture to reveal compromisable components
    - initiate SNA Step 4 (Survivability Analysis)
      - identification of softspot components
      - propose/discuss potential strategies for 3Rs
  - Exit Criteria

SNA

- 6) Analysis Team Analysis Integration Task
  - complete Step 4 (**Survivability Analysis**)
  - **generate Survivability Map**
  - **prepare for review of SNA findings and recommendations**

SNA

- 7) Joint Briefing Session
  - Attended by customer team and customer management
  - Analysis team presents findings and recommendations covering:
    - principle business mission, requirements, operating environment
    - current system architecture
    - selected essential services and assets and their usage scenarios
    - essential system components
    - selected intrusions and their usage scenarios
    - compromisable system components
    - resistance, recognition and recovery analysis
    - recommended architecture modifications and Survivability Map

SNA

- Final Report
  - Executive Summary
  - Sections
    - 1. Overview
    - 2. The Survivable Network Analysis Method
    - 3. Architecture
    - 4. Essential Services
    - 5. Intrusion Scenarios
    - 6. Recommendations
    - 7. Implementation
  - Appendices, and References

SNA

- Let's take a look at the case study
  - *A Case Study in Survivable Network System Analysis,* R. J. Ellison, R. C. Linger, T. Longstaff, N. R. Mead, TECHNICAL REPORT CMU/SEI-98-TR-014 ESC-TR-98-014, September 1998

SNA

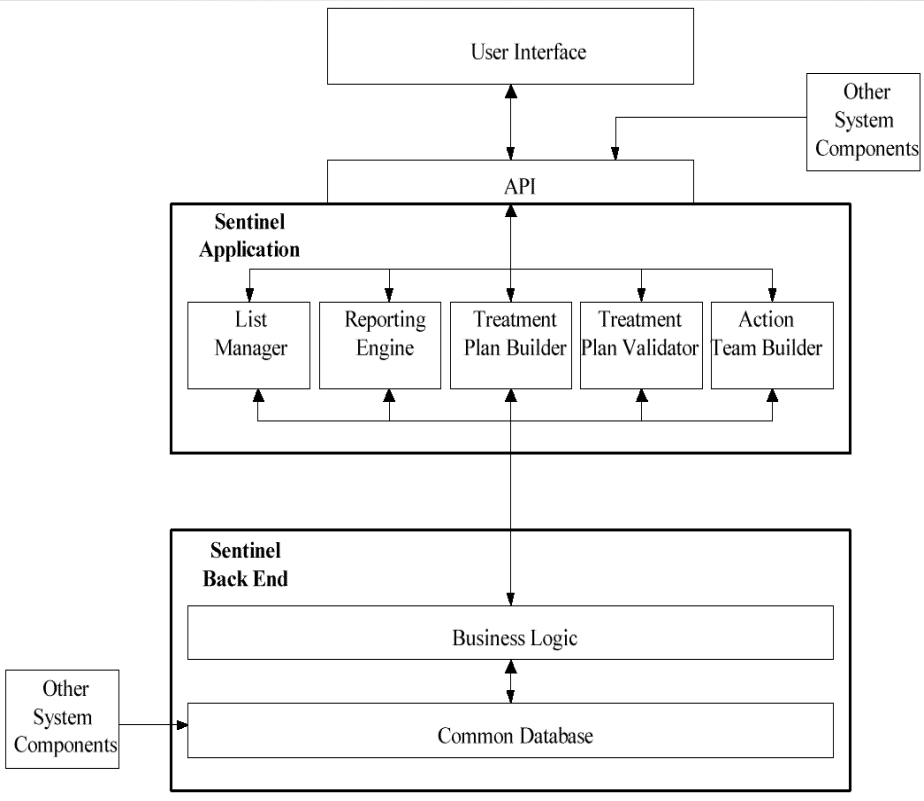
- Step 1: System Definition
  - Mission Requirements Definition
  - Normal Usage Scenarios (NUS)
    - NUS1: **Enter a new treatment plan**. A provider assigned to a patient admitted into an affiliation performs an initial assessment and defines a treatment plan, specifying problems, goals, and actions. Sentinel must apply business rules to treatment plan definition and validation.
    - NUS2: **Update a treatment plan**. A provider reviews a treatment plan, possibly adding or changing problems, goals, or actions, and possibly updating the status of these items. Sentinel must apply business rules to treatment plan update and validation.
    - NUS3: **View a treatment plan**. A provider treating a patient views a treatment plan to learn the status of problems, goals, and actions. Sentinel must ensure that the plan displayed is current and valid.

SNA

- Normal Usage Scenarios (NUS) (cont.)
  - NUS4: **Create or modify an action team**. A provider defines or changes the membership of a treatment team in an affiliation for a patient. Sentinel must ensure that the treatment team definition is current and correct.
  - NUS5: **Report the current treatment plans in an affiliation**. An administrator views the current state of her affiliation's treatment of a patient or set of patients. Sentinel must ensure that the treatment plan summaries are current and correct.
  - NUS6: **Change patient medication**. A provider changes the medication protocol in a treatment plan for a patient, possibly in response to unforeseen complications or side effects. Sentinel must ensure that the treatment plan is current and valid.

– Architecture Definition and Elicitation

Original Sentinel Architecture



SNA

- User Interface
  - resides outside of Sentinel
- API
  - synchronous RPC, asynchronous messaging
- List Manager
  - maintains lists: patients, affiliations, providers, action teams,...
- Reporting Engine
  - provides read-only viewing and reporting of treatment plans and history
- Treatment Plan Builder
  - creates treatment plans (problems, goals, actions)

SNA

- Treatment Plan Validator
  - checks completeness and consistency of treatment plan
- Action Team Builder
  - define/modify action team membership
- Business Logic
  - contains enterprise-defined business rules, validation checks for treatment plan development,
  - logging triggers that manage change control of sensitive data
- Database
  - shared access to common database with other subsystems and components

SNA

- Step 2: Essential Capability Definition
  - essential services and assets
    - critical system capabilities that must survive
    - be available during intrusions
  - criticality is based on
    - analysis of mission objectives,
    - risks
    - consequences of failure
    - availability of alternatives
  - result may be survivability classes of varying criticality

SNA

- Step 2: (cont.)
  - Single essential service: NUS3
    - providers depend on real-time, on-demand access to treatment plans in clinical situations
    - especially in cases of medication or therapeutic problems of an emergency or life-critical nature
    - other normal usage scenarios could be postponed for hours or days
  - Single essential asset: treatment plans
    - treatment plan integrity and confidentiality was deemed essential
    - other artifacts like action team, affiliations, providers etc. could be reconstructed/updated hours or days after intrusion with no irreversible consequences
  - Essential Component Identification
    - execution trace revealed that reporting engine and database components (including their supporting components and artifacts) are essential
      - integrity and confidentiality of treatment plans depend on database components for security and validation

SNA

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

But, what is the threat?

WHAT IS THE THREAT?

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

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

WHAT IS THE THREAT?

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

Activist who targets organization for ethical or political reasons	Limited means to hire external expertise, but could have talented members	Likely very patient, but specific events may force quicker action	Uses readily available tool sets	Not risk averse	External Internet	Embarrass organization Impact public or customer opinions Impact government or corporate partners
Industrial Spy	Expert knowledge	Desired information has limited shelf life	Can customize tools	Somewhat risk averse Capture could impact corporate sponsors	External Internet	Sell proprietary information Gain knowledge of competitor's research, learn of corporate strategies

WHAT IS THE THREAT?

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

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

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.

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.

SNA

- 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.

SNA

- 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.

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.

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.

SNA

- 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.

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

SNA

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

Intrusion Scenario	Resistance Strategy	Recognition Strategy	Recovery Strategy
IUS1: Intruder swaps the ID of two validated TPs.	**Current:** Two passwords are required for TP access.	**Current:** Logging of changes made to DB. Provider may recognize an incorrect TP.	**Current:** Built-in recovery in commercial DB. Backup and recovery scheme defined.
	Recommended: Implement strong authentication supported in a security API layer. {1}	**Recommended:** Add crypto-checksum when TP is validated.{3} Verify crypto-checksum when TP is retrieved. {4}	**Recommended:** Implement a recovery mode in the user interface to support searching for and recovering incorrect TPs. {1}
IUS2: Outside agents exercise (legitimate) access to DB fields controlled by Sentinel.	**Current**: Security model for DB field access.	**Current**: None.	**Current**: Scrap data and start over, or find an early backup and verify each entry.
	Recommended: Need to verify the security model in light of module addition and integration.	**Recommended**: 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}	**Recommended**: Scan DB for invalid crypto-checksums and/or invalid TPs and recover to last known correct TP. {4}

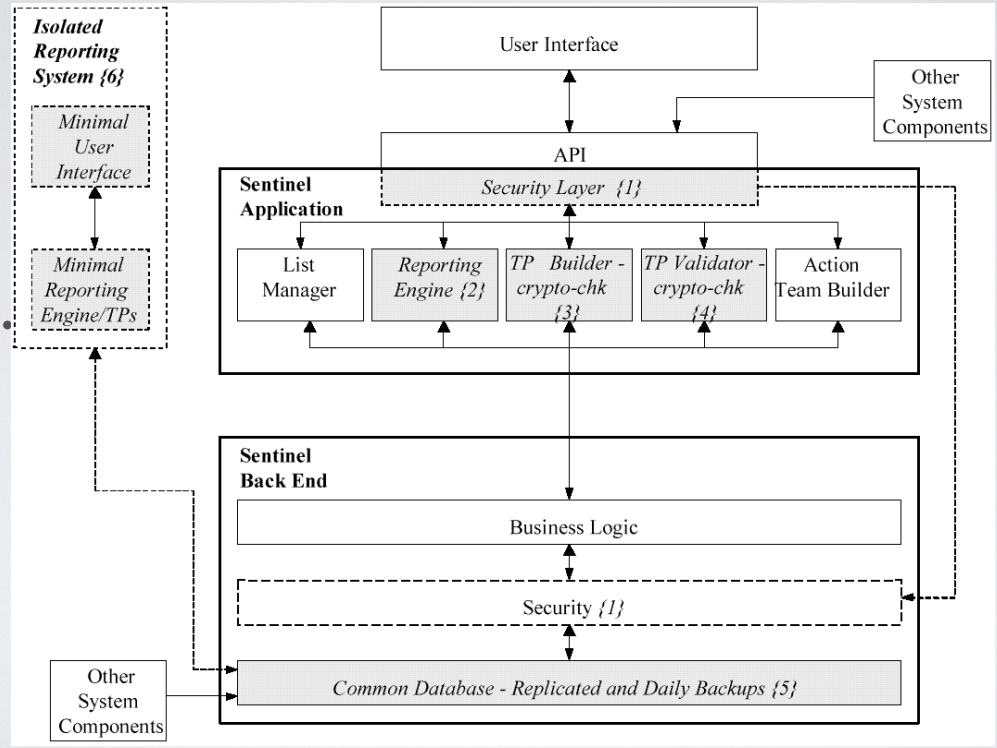
SNA

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

IUS3: An unauthorized user employs Sentinel to modify or view TPs by spoofing a legitimate user.	**Current**: 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	**Current**: None, except for unusual number of denied accesses to TPs as an intruder attempts to locate particular TPs.	**Current**: Can get list of modified TPs through the spoofed users transaction history. Manually recover each modified record.
	Recommended: Add a short logout timeout for any terminals in uncontrolled areas (not physician's offices). {1}	**Recommended**: Add logging, access control, and illegal access thresholds to the security API. {1}	**Recommended**: Develop a recovery procedure and support it in the UI. {1}
IUS4: Intruder corrupts DB leading to loss of trust in validated TPs.	**Current**: Security model in the DB protects data against corruption.	**Current**: None, except when provider happens to recognize a corrupted TP.	**Current**: Locate an uncorrupted backup or reconstruct TPs from scratch.
	Recommended: Implement live replicated DB systems that cross check for validity (supported in many commercial DB systems). {5}	**Recommended**: Add and check crypto-checksums on records in the DB. {3} {4}	**Recommended**: Reduce the backup cycle to quickly rebuild once a corrupted DB is detected. {5}
IUS5: Intruder destroys the Sentinel software so it cannot be used to retrieve TPs	**Current**: Keep originals available.	**Current**: System doesn't work.	**Current**: Reload the system from originals.
	Recommended: Keep a spare CD available for quick recovery	**Recommended**: None. Easy to detect this one.	**Recommended**: Fast recovery from CD. Create a small sub-system that can retrieve TPs while Sentinel is down or being upgraded. {6}

SNA

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



SNA

- 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

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.

SNA

- 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

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

SNA

- Lessons learned cont.
  - 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…