



# Practical Threat Analysis

## A Practical Threat Analysis Case Study: Next Generation Call Accounting

### Abstract

This paper describes a customer case study of a threat analysis for a next generation call accounting solution. Campton College, a private medical school, needed to replace an aging call accounting system, which frequently lost call records and lacked the capability to provide unified campus-wide telephony billing features. Campton wanted to create an integrated Web based call accounting system that would service student dorms and administrative departments. The institution contracted with TACS, a call accounting solution provider, to replace the old software and provide a modern, Web-based solution that would be cheaper to own and easier to use. Faced with a steep bill for information security, Campton contracted with Software Associates in order to find a way to reduce liability at the lowest possible cost. By using the PTA tools, Software Associates was able to demonstrate to Campton how to reduce risk from 250% to 50% at less than half the original InfoSec budget proposed by the vendor.

### The TACS managed call accounting service in a nutshell

TACS offers small to mid-sized clients a managed service for call accounting that includes basic billing functionality and is capable of collecting and processing call detail records from variety of sources. The user interface is Web-based and caters to four different types of users: PBX technicians, administrators, phone users and organization managers.

**Technicians** - TACS technicians are responsible for installing the CDR (call detail records) buffer devices connected to the PBXs for accumulating the calls. A technician defines the parameters of the protocols used by the buffer, data collection schedule, format of call records and performs initial testing of data collection in order to validate that the calls are collected and parsed successfully by TACS data back-end data processing systems.

**Administrators** - Customer administrators handle ongoing management of the telephone switch resources and subscribers as follows:

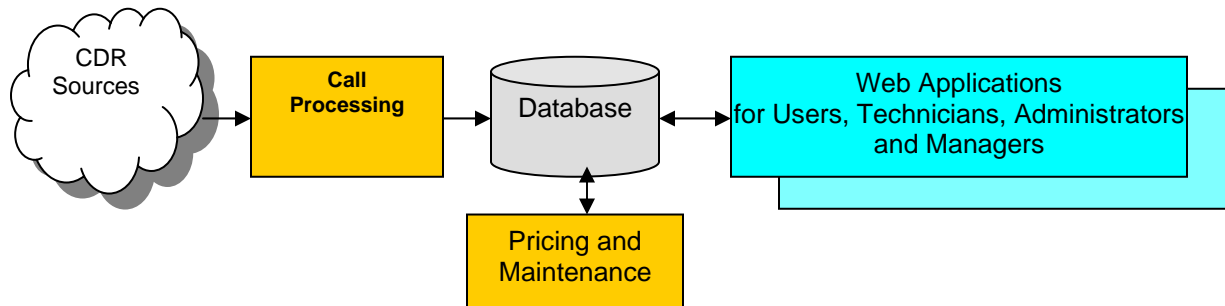
- Allocate phone-extensions and other telephony resources, such as cellular phones etc.
- Set the pricing programs that calculates and attaches a price tag to each call
- Define phone users and system users
- Associate users with telephony resources and pricing programs
- Manage system access permissions

**Subscribers** (phone users) - Subscribers can view and print the detailed listings of their private calls and their monthly bills.

**Managers** - User department Managers can produce reports that summarize calls traffic and the usage of telephony resources in the organization. They also monitor the billing and payments of phone users.

## System Architecture

The TACS system ASP architecture is based on Microsoft Windows Server 2003 that runs several .Net applications responsible for the call accounting processing, and a suite of web applications that interact with users via browsers (IE 5.5 and higher). The system's database is managed by a stand alone MS SQL 2000 machine connected to the application server via LAN.



### Database

The TACS MS SQL Server 2000 stores all types of system data, including call records, pricing programs, users, organizational structure and system configuration. The CDR tables can handle several million records per month and are indexed by a multiple fields to support rich reporting.

The SQL Server scheduler mechanism is used to schedule and dispatch the data collection activities.

### Processing

The processing of CDRs has 3 stages:

- **Data Collection** – collecting the calls from the CDR buffers. The output is blocks of raw CDR data.
- **Parsing and reformatting** - the output is structured call records in a uniform format invariant to origin of the calls.
- **Load to database** - call record are associated with the corresponding end point device, subscriber id and telecom provider and then inserted to the database.

The implementation is based on a several Windows services that use worker components to implement the required functionality. For example, the data collection service operates several different 'collector' components to collect the call records from different data sources via the appropriate protocols. Campton College operates 3 PBXs from different vendors: Avaya, Siemens and a small Cisco VoIP switch. The operating parameters of the components are kept in the database.

The data is transferred between the 3 processing stages via MSMQ private queues that serve as non-volatile buffers for data in process.

The service processes and some of the worker components were developed using .NET technology. Other worker components are legacy Win32 components wrapped with .NET Interop layer.

## Web applications

The Web Applications are implemented in ASP.NET combined with Microsoft reporting engine. Some of the applications are capable of directly viewing and editing data tables in the database via ASP.NET server side controls.

In the TACS system, all Web applications share the same infrastructure for user login and secure access to the database.

## Pricing, database maintenance and data exchange

The pricing, database maintenance and data exchange tasks are implemented with a Windows service that uses worker components to perform the actual tasks, similar to the call records processing architecture. The tasks are executed in a periodical manner according to the system's schedule.

## Why conduct a threat analysis?

"By retiring an aging 80's in-house system and outsourcing to TACS we will move into the 21st Century in less than nine months; and get an easy to use service that's available to all students and generates a revenue stream," said Steve Walz, Campton campus operations manager, "but we had security concerns about using an outsourced service."

"We knew that TACS is an experienced call accounting solution provider but we were unsure that their software and operations team had adopted a best-practices approach to information security and we asked TACS to submit to an external assessment of their systems..." said Walz.

## What is Practical Threat Analysis?

A **PTA**® study focuses on protecting valuable assets, is sponsored by a senior manager, has 2-5 participants with relevant knowledge, is guided by an experienced security consultant, lasts 5 days and is facilitated by an advanced software tool.

In a pre-kickoff planning meeting, the consultant works with the sponsor to set clearly defined goals and outcomes for the session. Since much of the work is done in small breakout groups, all stakeholders take an active part. The consultant guides the group through a fast-paced process to:

- 1-Identify assets
- 2-Identify vulnerabilities
- 3-Define countermeasures
- 4-Compose threat scenarios
- 5-Understand calculated risk
- 6-Optimize countermeasures

A PTA study is particularly effective because it is facilitated and accelerated with the accompanying PTA Professional Edition software tool that ensures that all the information is captured in a structured database and automates the economic risk what-if calculation process. Analysts and stakeholders don't need to maintain unstructured Word or Excel documents and can quickly create new threat scenarios and countermeasures. All issues are captured and nothing is lost. Management can ask for and quickly receive any reports they want.

## PTA kickoff

At the first day kickoff session, the functional and architectural descriptions of TACS's system were presented to the Software Associates lead analyst, by Dympna O'Connell, TACS product manager. "We're already documenting and revising our customer provisioning and configuration procedures", said O'Connell. "We realize that these process steps are crucial to our customer's information security and we want to make sure there are no security holes and opportunities for data manipulation".

### Step 1 of the study – Identify Assets

In the first step of the study the group mapped the system's major assets, their financial values and the losses that may be caused when assets are damaged. The following major system assets were identified:

Asset Name	Asset Value (annual)
The accuracy and integrity of the data in system database	<b>\$2,000,000</b> or 90.5% of total assets
Private call details information	<b>\$150,000</b> or 6.8% of total assets
The availability of the system's web application and service	<b>\$50,000</b> or 2.2% of total assets
The integrity of system passwords	<b>\$10,000</b> 0.5 % of total assets

The total value of all system assets was \$2,210,000 - a detailed list of identified assets is part of the full threat-model database available for download from [call accounting case study threat model](#). To view the detailed entities lists you should have [PTA software](#) installed on your computer.

### Step 2 – Identify Vulnerabilities

In order to identify vulnerabilities and flaws, Software Associates analysts studied the functional and architecture documents supplied by Ms. O'Connell. "Since TACS bases its architecture on Microsoft infrastructure, we used the PTA MS-Telecom entity library as a base line checklist for picking up system common vulnerabilities" said Yuval, Software Associates lead risk analyst. "More then 70% of the stuff was already there. We have just had to complement the picture by diving into the CDR collection equipment and by studying Campton specific business procedures with the help of Mr. Walz.

"Identifying the relevant vulnerabilities is an iterative process bundled with the understanding of the actual threats. All in all, we came up with 15 focused vulnerabilities relevant to the specific architecture, the specific telephony infrastructure and the ASP mode of operation" said Yuval.

### Step 3 – Define Countermeasures

During this step the team defined the countermeasures relevant for mitigating the identified vulnerabilities. Some of the countermeasures were well known safeguards picked up from the predefined PTA entity library such as enforcing OS patches deployment and strong passwords policy. Others were more unique e.g. the development of mechanism for managing data collection buffer passwords in an encrypted repository.

“We worked directly with Ms. O’Connell and her developers on estimating countermeasures’ implementation costs needed by PTA for calculating countermeasures cost-effectiveness” said Yuval.

The lists of the 22 countermeasures that were defined and the identified vulnerabilities are included in the case study database available for download from [call accounting case study threat model](#).

## Step 4 – Build Threat Scenarios

“Building the threats is the peak of the process” said Software Associates founder and CTO Mr. Danny Lieberman, “this is the point where we use our experience to compose the threat scenarios, evaluate their feasibility and estimate the probability they’ll actually happen”.

“The flexibility of the PTA database driven model enables us ‘what-if’ experiments and the calculative capabilities gives us immediate feedback on the severity of threats” , said Yuval.

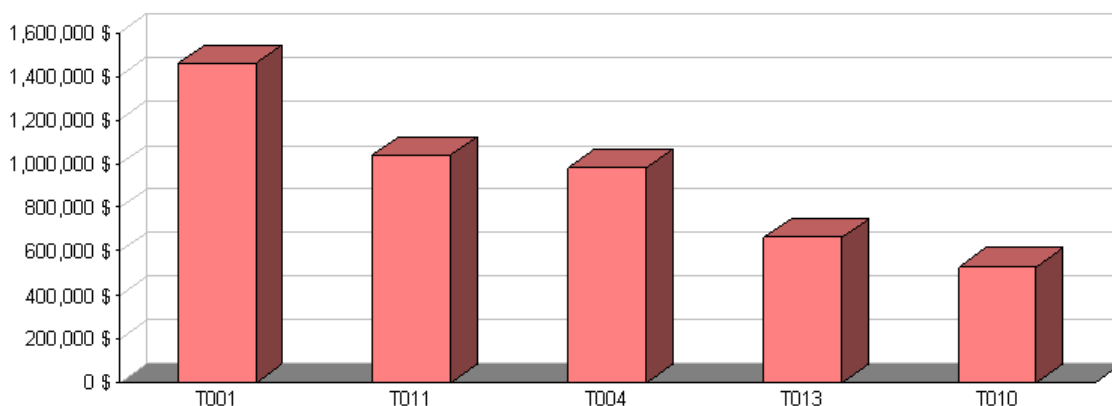
## Step 5 - Understand the calculated Risk

After refining threat probabilities, the PTA software calculated the following bottom-line:

- The total yearly value of assets that might be damaged if threats materialize is \$2.21M
- The risk level (the value of the financial losses that may be caused to the system due to the identified threats) is 249% of the total assets (~\$5.5M). Although it is clear that the actual damage to the system’s assets cannot exceed their total value, the risk level does not express the actual damage. It reflects the amount of effort that has to be invested in order to mitigate the threats to the system, and since in this specific system several threats threaten the same assets, the risk level exceeds 100%.

The following bar chart presents the 5 most dangerous threats calculated and displayed by PTA (the value of risk is presented in real \$):

### Top Threats by Risk



ID	Name	Risk (\$)
T001	Intruder accesses system application and database servers directly from the Internet	1,458,600
T011	Intruder sniffs CDR buffers passwords and then steals or corrupts calls data	1,040,247
T004	Intruder corrupts database by injecting malicious SQLs in input fields of Web pages	979,914
T013	Intruder gets control of call processing engine after hacking the Web server machine	663,000
T010	A malicious user with managerial rights manipulates calls data	528,632

Not surprising, it was found that the most dangerous threats are the ones that threaten the calls data either in the system's database on the various collecting stages.

"The ranking of the threats reflects a typical heterogeneous software system. The ability to take into account non-standard threats specific to the analyzed system is one of the great strengths of PTA " said Lieberman, "We weren't limited to generic info security standards, such as ISO17799 and indeed you can see some interesting threats that indigenous to this particular system e.g. the CDR buffers vulnerabilities. Complex systems like this often have huge risks that are hidden in the cracks of generic standards..."

## Step 6 – Optimize Countermeasures

It was clear that a level of 249% of risk is dangerous and that countermeasures should be applied to reduce the system's risk before going into heavy-duty production operation.

"We asked Software Associates to show us how to reduce the risk to an acceptable level of 60% at lowest cost" said Steve Walz. "Since our budget was constrained, we considered canceling the whole info-sec project and taking our risks by doing nothing".

"At that step we ran PTA 'Optimized Risk Reduction Plan' with the target risk level of ~ 50%" said Yuval "and we received an optimized plan with the following countermeasures that should be applied:

1. Install content leakage prevention system
2. Install firewall
3. Enforce deployment of latest security patches for OS, database and Web server
4. Develop mechanism for secure managing of CDR buffers passwords
5. Use CDR buffers with secure transfer and login authentication protocols
6. Enforce security code review
7. Enforce data access via stored procedures with formal parameters content validation
8. Implement validation of input fields in web pages
9. Develop secured passwords and role-based mechanism for web users
10. Develop monitoring mechanism for back-end processing (system health)
11. Limit access of ASP employees and technicians to system resources
12. Enforce quality passwords policy for protecting each of the machines on the network
13. Use Windows integrated authentication policy
14. Database login accounts should be given the minimal rights that are necessary for their functionality

Implementing the recommended set of countermeasures reduces the system's risk to 54.3% at a cost of \$127,000. Only 14 countermeasures out of the 22 were selected - the proposed order of countermeasures also ensures a quickest reduction of risk per \$ spent throughout the system modification process. The implementation of the following countermeasures was suspended to later stages in system life cycle:

- Create acceptable use policy for email and Internet access
- Install anti-DoS appliance
- Develop fraud detection mechanism
- Security officer should assure the personal integrity of employees
- Develop module for logging changes in data initiated by users
- Enforce employees' liability for disclosing private calls information
- Restrict display of phone numbers and sensitive information in detailed reports

“All-in-all, we were pleased with the speed and quality of results of the PTA methodology that Software Associates uses and with the fact that it created consensus among the stakeholders with effective use of senior manager time and above all got us the best risk reduction at the lowest cost...” summarized both Steve Walz of Campton College and Ms. O’Connell of TACS.

## Appendix 1. Abbreviations and terminology

**PBX** – Private Exchange telephony device; interchangeable with the term **Switch**

**MSMQ** - Microsoft Middleware Queue system

**CDR** – Telephony Call Detail Record

**CDR buffer** – Intermediate buffer device for storing CDRs collected from PBX

**Data Source** – Origin of telephony calls data e.g. PBXs, IP Switches etc.

**Users** – Individuals that have access to the university telephony resources and to TACS system  
e.g. students, academic staff, administration and personnel

© PTA Technologies 2005

[www.ptatechnologies.com](http://www.ptatechnologies.com)

+972 3 5443085