

“Revisiting the Survivability Design Process (SDP) to Retrofit Commercial Mobile Platforms in support of Survivable Tele-client Remote Access Services (ST-RAS)”

Information Survivability Workshop (ISW) 2000: October 24-26, 2000 (Boston, MA)

Stephen F. Fiore - principal consultant: PrioriTech, State College, PA 16803

Internet e-mail: prioritech@ibm.net

Abstract

At ISW '98 (ref [1]), this author presented the algorithm for Survivability Design Process (SDP) during the session on "How to Evaluate System Survivability". The original SDP addressed the need to design or retrofit a generic inter-network consisting of one or more corporate intranets/ LANs with one or more Internet access gateways.

For this presentation, we will address a much more specific application: the retrofit of commercial mobile elements, including PC-based client platform (O/S plus processor/ memory/ disk), as a *Survivable Tele-Client for Remote Access Services* (or "ST-RAS").

The purpose of our presentation will be two-fold. First, we will define the attributes related to the ST-RAS end environment and tradeoff parameters for this retrofit application. Secondly, we revisit our original SDP algorithm and address how it can be enhanced to support an efficient, yet thorough process, for methodically determining the necessary and sufficient:

- Tele-client elements and RAS configuration(s)
- Access services and Tele-client processes to retain during *stress states*
- Add-on mechanisms for enhancing survivability features including reliability, fault tolerance, security, etc.

The goal is to aid the designer by providing insight to ST-RAS solutions and evolve the SDP algorithm by adding improvements to address a highly constrained retrofit application such as the ST-RAS application presents.

Introduction

Service Providers (SPs) of various types have recently expressed high interest in pushing the commercial, open system PC client to be **the** user's information data platform which stores contact information, schedules and critical notes often of a sensitive nature. It is also the trend to support this client platform as a "mobile" (to include "highly transportable") connected device. These two trends have created a need, as well as, possibly the most significant challenge in applying concepts of survivability.

Survivable systems are said to embody two essential characteristics (ref [2,3]):

- Preserve essential services given failure or attack
- Function in unbounded and dynamic network environments.

In the context of the ST-RAS application, dynamic network environments are inherent in that it is desired to support multiple access points to the end (corporate/LAN) environment through a variety of one or more Internet gateway access types including:

- Wireless LANs (e.g., IEEE 802.11/12)
- Wireless local loop and PCS data access (e.g., WAP)
- Dial-up via the PSTN (PPTP via V.90 modems)
- Broadband remote access (via the various x-DSL and cable modems).

In these Tele-client applications, Remote Access Services (RAS) are implemented using a variety of interoperable IP service layer *gateways* for accessing the Internet (and corporate intranets via the Internet and VPN technology).

ST-RAS clients and gateways are based on industry standardized session, transport and security protocols as the mechanisms for user authentication (e.g., RADIUS), firewall (IP packet filtering and TCP/UDP service permit/deny blocking using stateful stack inspection rules) and VPN (where supported). If VPNs are deployed, implementations likely employ at least basic layer 2/3 tunneling (e.g., PPTP, L2TP, IP-Sec/ ESP tunnel).

If secure (encrypted) VPNs are to be employed a worthwhile integrated tunneling and IP packet encryption scheme should be employed using a version of the IETF standard IP-Sec/ IKE (e.g., packet authenticated ESP tunneling with triple DES encryption).

Obviously, we must maintain the desire to keep the client platform "thin" to retain attributes needed in ST-RAS applications. The SDP retrofit effort is thus additionally burdened by the mobile RAS requirement to support interoperability with multiple gateways and managing the client design to Size, Weight And Power consumption (SWAP) constraints. In other words, we must assist the designer's task to select the appropriate mix of survivability techniques and mechanisms by avoiding a Tele-client that is undesirably large or a heavy power consumer or an ST-RAS solution that is either an unreliable or insecure service.

Requirements Areas

Survivability requirements encompass areas beyond security (ref [3]). The following requirement areas must be included in a comprehensive approach:

- Overall system availability (to include wireless outages caused by blocking & fades, connection establishment failures due to a variety of possible causes)
- Fault tolerance (to include hung processes within the PC-based mobile client and hung connections at foreign Gateways being accessed by roaming clients)
- (Network) reconstitution and restoration (via multi-gateway, -connection, -service diversity methods)
- Security & integrity (user authentication, session control, packet integrity, information (IP packet payload) confidentiality, traffic (IP packet header) confidentiality).
- Intrusion & attack mitigation (against virus, Trojan horse or DDoS/ flooding threats).

State of commercial practice is to select techniques and tools to satisfy a specific point vulnerability based on either what is the "latest" or "available" for a specific platform (i.e., O/S and/or application-driven environment). Such "ad-hoc" approaches often result in significantly less than optimal solutions as related to jointly satisfying the above requirements areas. In addition, retrofits are often implemented as a series of successive incremental changes which can produce solutions that are non-scalable, and non- extensible with respect to inter-networking, become too costly to manage and maintain and/or evolves to a solution which is service constrained due to performance limitations.

The original goal of the SDP algorithm was to provide a survivable system design method that supports survivability goals by considering the interdependencies of the above five requirements areas while converging to effective, yet practical, *system* solutions.

SDP Description

For the ST-RAS application, we only consider the retrofit mode of the original SDP algorithm.

Algorithm Overview

The following describes the highest level of PrioTech's original SDP algorithm for survivability retrofit.

1. SPECIFY *essential* (or fallback) services which are necessary and sufficient for continuing operations during *crisis* conditions. These are considered **PRIORITY 1** survivable services. (NOTE: Some essential service types may be new to the suite of legacy system services defined under full-up legacy service conditions.)
2. SPECIFY all *requirements* relevant to the essential services that are necessary and sufficient for successful operation under the crisis condition. These are considered PRIORITY 1 survivability requirements.
3. DEFINE all services from the legacy system as being full-up *normal*.
4. DEFINE a number of discrete states, *N*, as the *stress states*, where stress state #1 is at the highest PRIORITY level. (Practical constraints of the application are used to determine the appropriate value for N).
5. From the set of (all) normal services, incrementally DEplete according to specified level of need for survivability and required support for transmission services.

6. ALLOCATE services via an iterative assignment to stress states from stress state (or **PRIORITY**) *N* -1 to that for the next highest level (or **PRIORITY 2**).
7. DEFINE acceptable performance levels for the supporting the transmission layers of all corresponding services within each stress state by a depletion method in an orderly manner from Nth PRIORITY (or normal state) to the 1st PRIORITY (or highest stress state).

The next five steps are performed for each PRIORITY level by iteration from the highest stress state (PRIORITY 1) to the lowest (PRIORITY N-1).

8. DEFINE subscriber use cases within the context of the specific Stress State and corresponding performance levels set for support the transmission layer.
9. For each use case within each stress state, MAP the functional requirements to an existing (or specify a new) set of processes and corresponding objects (if OOD).
10. DEVELOP transaction flows for each new process/object relevant to legacy process/ objects. Reuse existing APIs, as appropriate, or define new APIs and/or reuse/ add new physical (I/O or link) interfaces.
11. For each specific stress state, STRIP the O/S kernel of all unnecessary services and objects considered all subscriber usage cases for that state.
12. SELECT supplementary survivability mechanisms (i.e., software, hardware or firmware plug-ins) as necessary for each stress state considering all usage cases.
13. EVALUATE (via customer review) services and performance levels supported for each specific stress state per each use case (specified in steps 5, 6 and 7).
14. If service or performance levels are not satisfactory, ITERATE by looping back to repeat steps 8 through 13.

Transmission performance restrictions are planned for adaptation from *normal* to *stress* states to support *essential* services. As a result of the SDP, a set of discrete stress states is determined along with the degree of restriction of normal services. Also for each stress state, adaptable transmission parameters are determined. These can include flow throughput efficiency per connection and data rate or bandwidth per link. Within an SDP solution, performance impacts for a given state can be offset by the addition of more concurrent gateway access points and/ or more concurrent connections per gateway.

ST-RAS Application Issues

Subscriber perceptions of need are often the only source of real requirements, however his inputs will require interpretation to derive useful specifications for survivability. To the service provider customer, the justification for applying any mechanism to enhance survivability for a ST-RAS application will depend on past negative experiences of the customer and projecting possible compound detriments to the intended service.

Outages, downtime or delays due to radio signal fading and blockage, low battery charge conditions or non-interoperable foreignGateway protocols at the link connection or session layer (e.g., username/ account authentication) are noted as the frequent sources of subscriber frustration with wireless Internet access clients at this time and are somewhat discounted by the subscriber as "expected" with the immature nature of such a new technology.

However, the designer must anticipate potential compound detrimental impacts with of these acceptable availability risks with new issues such as:

- Inability to sync-up secure connections due to non-interoperable key distribution with foreign Gateways
- Hanging of connection establishment attempts due to asymmetric tunneling from nesting/ chaining of VPN tunnels
- Poor or disparate service-layer management schemes at foreign RAS Gateways accessed by roaming clients.

At some point, the potential exists for the subscriber to be overwhelmed by too many availability and/ or performance issue to continue to accept the service as a satisfactory. Once the customer experiences significant impacts such as performance degradation, disruption of service, inability to complete critical tasks, loss of data, loss of income, etc., the customer will substantiate the need in a non-articulate manner ... by canceling his subscription.

Once the Service Provider determines that "something must be done", the following questions are usually asked:

1. "How *much* needs to be done?"
2. Do the *costs of implementing* and *maintaining* these measures out-weigh the lost business incurred due to the known detrimental impacts *of doing without*?
3. How do I perform a valuation of the worth of one individual measure over another?"

Summary

These issues will be discussed at the workshop with the intended objective to provide insight into potential solutions and methods to achieving acceptable and even superior solutions. From the service provider's perspective, what is sought are solutions in which practical retrofits can be made to deploy survivable Tele-clients. This will enable more rapid future deployment of ST-RAS for commercial business and consumer applications need to be addressed. The revised SDP retrofit algorithm is successfully employed as a means to derive such solutions for ST-RAS may be also useful for other complex inter-network service implementations and deployment rollouts.

References

1. " Issues and Insights Regarding Survivable Inter-Network Design and Retrofit", S. Fiore, Priority Technology, position paper for ISW '98, October 1998.
2. "Survivable Network Systems: An Emerging Discipline", CMU/SEI-97-TR-013, R.J. Elision, DA Fisher, R.C. Linger, H.F. Lipton, T. Longstaff, N.R. Mead; Carnegie Mellon University (CMU) Software Engineering Institute (SEI), November 1997.
3. "Requirements Definition for Survivable Network Systems", R.C. Linger, N. R. Mead and H. F. Lipson.