GSi Compliant RAS for Public Private Sector Partnership

F. Fawzi [1,2], R. Bashroush[2], H. Jahankhani[2]

[1] Head of IT Developments and Technical Innovations, London Probation Trust, London, UK
[2] School of Computing IT and Engineering, University of East London, London, UK
{fawzi, rabih, hamid2}@uel.ac.uk

Abstract. With the current trend of moving intelligent services and administration towards the public private partnership, and the security controls that are currently in place, the shareable data modeling initiative has become a controversial issue. Existing applications often rely on isolation or trusted networks for their access control or security, whereas untrusted wide area networks pay little attention to the authenticity, integrity or confidentiality of the data they transport. In this paper, we examine the issues that must be considered when providing network access to an existing probation service environment. We describe how we intend to implement the proposed solution in one probation service application. We describe the architecture that allows remote access to the legacy application, providing it with encrypted communications and strongly authenticated access control but without requiring any modifications to the underlying application.

Keywords: RAS, Secure Mobile Working, Security Standards.

1 Introduction

The public sector model has evolved over the years but it continues to be a reactive model to new legislations and policies. The arching factor of cost versus scalability and robustness has become very visible, and it has established itself as the most significant consideration in any technical design. The traditional Virtual Private Network (VPN) structure has not evolved as fast as technology and the offering of new tools on traditional infrastructures where the essence of these is to protect data and uphold confidentiality. However, the limitation and the disparity between what the private and public sector can offer has exaggerated the need for bridging connectivity over legacy boundaries that are no longer flexible enough to accommodate new advances and developments. This is very much a systematic problem for the public sector in particular where the requirements for personnel to have remote and mobile access to classified data (e.g. at Restricted or IL3 level or higher). The modeling of true, secure mobile working shouldn't be a generic implementation of technology. It needs to ensure acceptance of various managements within a complex structure of partnership adhering to different affiliations' of security standards. To mitigate the risks, the implementation needs to address both technical controls and potential human intervention or malicious intent.

The next section discusses the RAS modeling guidelines. Section 3 then provides an overview of the potential design of the solution. Finally, conclusion and future work is presented in section 4.

2 RAS Modeling Guidelines

In its logical interpretation, the conceptual design of the solution and how it manages security accreditation (certification) [1] is based on the below guidelines:

1. **Protection and Confidentiality:** each traffic flow is protected in accordance with the established requirements. This includes flows between the remote client device and the remote access server, and between the remote access server and internal resources. Protection should be verified by means such as monitoring network traffic or checking traffic logs.

2. **Authentication:** is required and cannot be readily compromised or circumvented. All authentication policies are enforced. Performing robust testing of authentication is important to reduce the risk of attackers accessing protected internal resources.

3. **Applications:** the remote access solution does not interfere with the use of software applications that are permitted to be used through remote access, nor does it disrupt the operation of the remote client devices (for example, a VPN client conflicting with a host-based firewall).

4. **Management:** Administrators can configure and manage the solution effectively and securely. This includes all components, including remote access servers, authentication services, and client software. The ease of deployment and configuration is particularly important, such as having fully automated client configuration versus administrators manually configuring each client. Another concern is the ability of users to alter remote access client settings, which could weaken remote access security. Automating configurations for devices can greatly reduce unintentional errors from users incorrectly configuring settings.

5. **Logging:** the remote access solution logs security events in accordance with the organisation's policies. Some remote access solutions provide more granular logging capabilities than others. An example is logging usage of individual applications versus only connections to particular hosts. So in some cases it may be necessary to rely on the resources used through remote access to perform portions of the logging that the remote access server cannot perform.

6. **Performance:** the solution provides adequate performance during normal and peak usage. It is important to consider not only the performance of the primary remote access components, but also that of intermediate devices,

such as routers and firewalls. Performance is particularly important when large software updates are being provided through the remote access solution to the remote client devices. Encrypted traffic often consumes more processing power than unencrypted traffic, so it may cause bottlenecks. In many cases, the best way to test the performance under load of a prototype is to use simulated traffic generators on a live test network to mimic the actual characteristics of expected traffic as closely as possible. Testing should incorporate a variety of applications that will be used with remote access.

7. **Security:** the remote access implementation itself may contain vulnerabilities and weaknesses that attackers could exploit. High security needs may choose to perform extensive vulnerability assessments against the remote access components. At a minimum, all components should be updated with the latest patches and configured following sound security practices.

8. **Default Settings:** The default values for each remote access setting and alter the settings are reviewed as necessary o support security requirements. The remote access device should be assured to ensure that it does not unexpectedly "fall back" to default settings for interoperability or other reasons.

9. **Acceptance:** the CA "certification authority" will depend on a holistic approach necessary to develop an effective security infrastructure. This is in addition to discussing the individual components and the role they play [2][3].

3 Technical Foundation

The implementation enables the Public/Private partnership to build a RAS offering that meets the requirements for CESG "National Technical Authority for Information Assurance" [8]. The RAS solution will need to meet CESG guidelines for data handling and as such the data classification for the RAS compliance with IL3 level [4][5].

An application database that is hosted within the GSI cloud would be built around application guidelines and would adhere to CESG policy. The database would be migrated into a previously accredited environment and therefore would not be required to follow an additional accreditation submission. The model proposes that the desired solution for Users within the field recording and updating national and protected records would be a 3G enabled device.

This remote device solution will be designed within the following recommendations:

- Hardware must support TPM "Trusted Platform Module" chip technology.
- The Operating System will be Microsoft based.

- The hardware will be encrypted using Windows Bitlocker.
- The Bitlocker entropy will be supplied by Becrypt.
- Backup Entropy will be stored on a secure server within the previously accredited environment.
- USB bitlocker token authentication will be required to log on to the laptop.
- The hardware build will include Cisco VPN client and require client certificates.
- Internet browsing will be by proxy via the secure internet [6].
- 3G dongle for internet connectivity for hardware devices

The figure below shows a user connecting to the complimentary environment via a client/server VPN connection and then being forwarded to the application VLAN within the same environment.

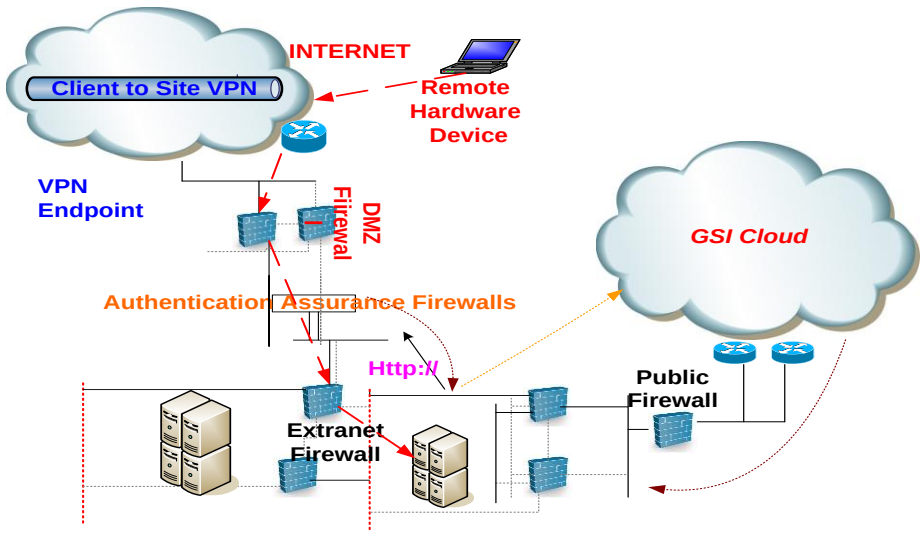

Fig. 1. Proposed solution architecture overview

4 Conclusion

Internet is changing the way public sector activities are conducted. Security compliance of mobile working solutions is the enabling technologies that simplify the management and security of such activities. With the right approach to an accredited implementation, public sector organizations with obligatory responsibility to protect confidentiality can spend less time worrying about security, while focusing on their

main activities. For example, confidential documents no longer need to wait for days to be physically shipped. Instead, they can be securely sent through e-mail. Web servers can allow secure access for only designated users, eliminating the need for human intervention. Public sector organization networks including military can securely extend over the Internet, eliminating expensive leased data lines. Future work is geared towards further integration and consolidation of platforms to deliver further efficiencies. In practical terms certifying authorities will be encouraged to come together in a cooperative intervention to deliver an agreed upon security baseline.

References

1. E. Gerk "Overview of Certification Systems – X.509, CA, PGP and SKIP", Meta-Certificate Group, 1998.
2. Andress "Surviving Security" How to Integrate People, Process, and Technology Second Edition AUERBACH PUBLICATIONS A CRC Press Company Boca Raton London New York Washington, D.C.
3. J. Scambray "Hacking Exposed", April 2, 2001
4. W. E. Burr "Public Key Infrastructure Technical Specification", NIST, 1997.
5. C. King "Building a Corporate PKI", INFOSEC Engineering, 1999.
6. F. Warwick, and M. Baum "Secure Electronic Commerce – Building Infrastructure for Digital Signatures and Encryption", Prentice Hall, 1997.
7. R Fraser, "Information Governance & Technology Policies - Remote Access Procedure", Oct, 2009
8. CESG: National Technical Authority for Information Assurance. URL: http://www.cesg.gov.uk/index.shtml