Security in UTMC systems

A UTMC Technical Guide
Library reference ***UTMC-TR005.001***

10 December 2009

Cover + 7 pages

List of contents

1 Introduction

1.1 About this document

1.1.1 UTMC is a UK-led initiative which provides and maintains a technical framework for traffic management and related systems. It is geared to producing open specifications geared to the needs of real world projects, delivered through an efficient and innovative supply market. UTMC specifications are endorsed by the UK Department for Transport and are published on the UTMC website at: http://www.utmc.uk.com.

1.1.2 To help users get the best out of the UTMC Technical Specification, we provide a set of guidance documents addressing some of the associated issues, ranging from non technical aspects such as procurement policy and operations, to technical aspects such as database design and communications network configuration.

1.1.3 This document is a guidance document for both developers and users, and is concerned with ensuring that UTMC systems and operations are kept secure.

1.2 Status of this document

1.2.1 This document is based on guidance developed during the early 2000s and published as Annex G to the Technical Specification TS003:2005. It is current undergoing revision.

1.3 Security in UTMC

1.3.1 Security is a complex mix of the way systems are built and the way in which their users/managers understand and operate them.

1.3.2 Security needs to be addressed at a system level, by means of appropriate (process and technical) measures. This annex outlines the general security framework for UTMC and provides assistance in how this applies to communications.

1.3.3 Implementing security in any system leads to an increase in both capital and operating expenditure costs. This should be seen as the costs of an 'insurance policy' against failures of particular types.

1.3.4 The UTMC Technical Specification says that "all UTMC projects should prepare a security policy, based on BS/ISO/IEC 27000. The detail of the security policy should be decided by each project individually." A small number of areas are highlighted for specific consideration, including access control/authentication, physical robustness, and firewalls.

1.3.5 As systems vary in their complexity, it is difficult to be more definitive in the Technical Specification without introducing unnecessary complexities for some systems. This document helps to fill this gap by providing non-normative advice which will be relevant for some systems.

2 UTMC security requirements

2.1 UTMC networks must be engineered to avoid ‘flooding’ attacks, through appropriate network topology, instation router sizing and attack detection/rejection.

2.2 Appropriate provision should be made for system sizing, software quality testing, and system resilience/redundancy.

2.3 Commercial use of UTMC networks and systems needs to include end-to-end protection of transactions. This includes design of in-vehicle units, communications protocols, applications, transaction control and commitment, transaction auditing facilities etc.

2.4 UTMC systems managers must ensure that the communications services they provide to financial systems, commercial services etc enable the latter to operate securely.

2.5 Systems which identify and track individual vehicles need to have the highest level of security provision. This includes the need for well-protected special access for law enforcement agencies – not just the Police but other Government agencies as well.

2.6 Enforcement devices will continue to be type-approved to Home Office/ACPO requirements.

2.7 Communications links with vehicles should not be susceptible to tapping or jamming.

2.8 Partners should be given limited and managed access only to their information, unless there are good reasons to the contrary (eg the trustworthiness and legal requirements surrounding police activity).

3 UTMC security solutions

3.1 Structural security

Architecture principles

3.1.1 Security should focus on the following boundaries within the UTMC architecture:

3.1.2 From the Logical Reference Model:

a) interceptable or interruptible wide area communications links (achieved by protocol handshaking, encryption and/or link redundancy);

b) the interface from Node B (instation) to communications links (achieved by firewalls);

c) Node C, D and E (street and in-vehicle device) hardware (achieved by physical means);

3.1.3 From the Functional Reference Model:

a) the user interface (achieved by physical protection and authentication);

b) the applications to data service (common database) interface (achieved by authentication and redundancy);

c) the interface with management applications and services (achieved by audit logs).

3.1.4 Figure 1 indicates the points at which particular security measures apply to the UTMC Logical Reference Model. Figure 2 does the same for the UTMC Functional Reference Model.

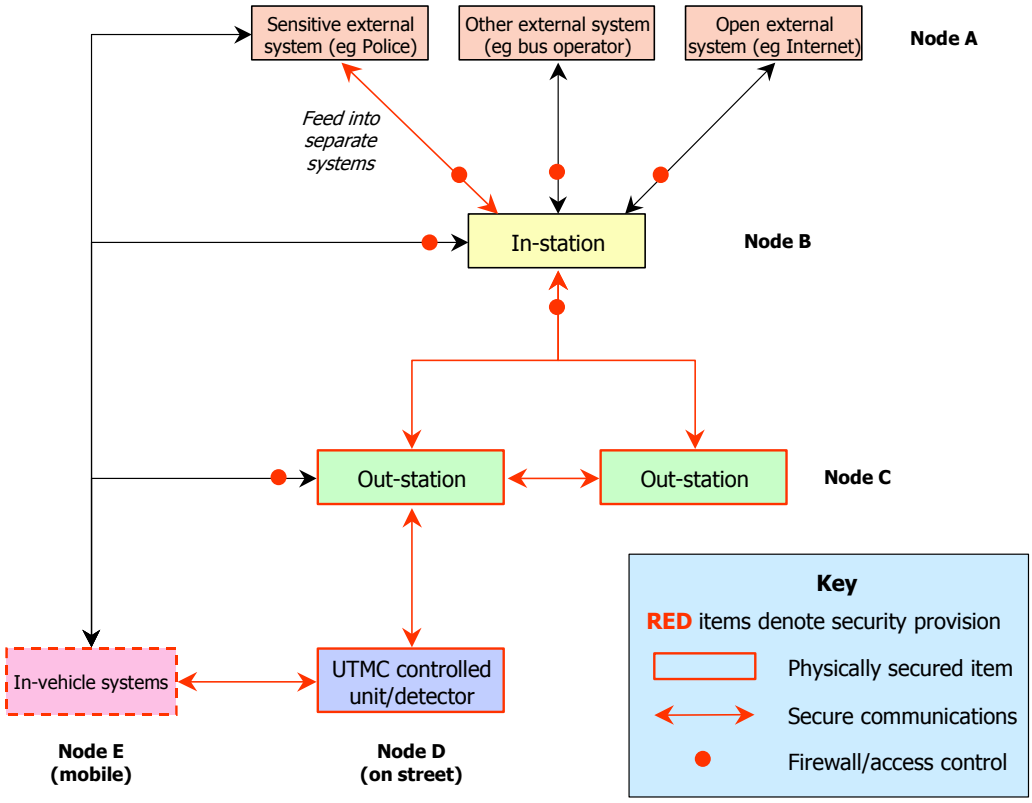

Figure 1: Diagram indicating security points on UTMC Logical Reference Model

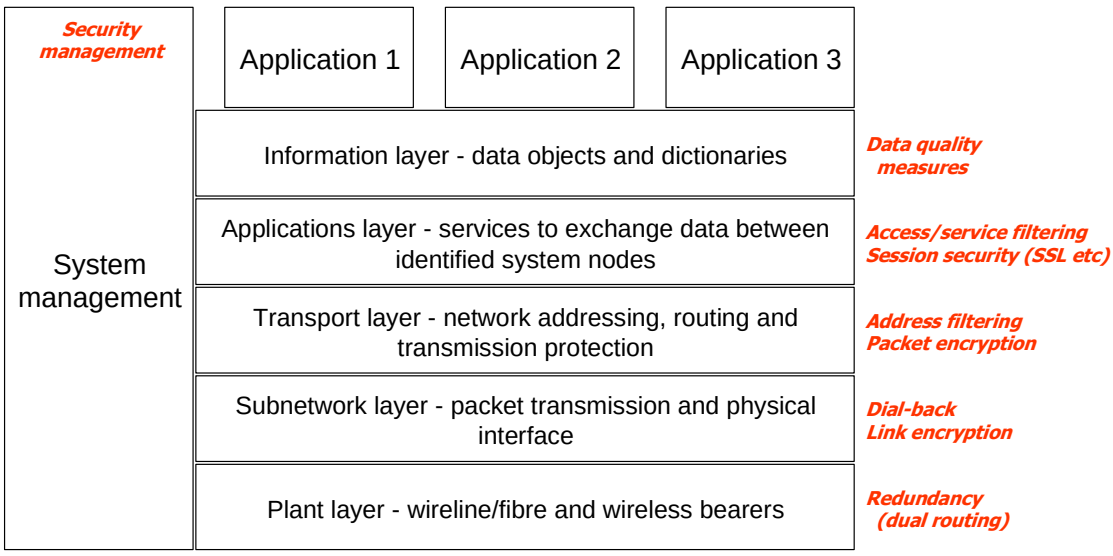

Figure 2: Diagram indicating security options on UTMC Functional Reference Model

3.1.5 There is a primary security barrier at the external boundary of the instation, of the 'firewall' kind. This needs to prevent unauthorised entry into the main system from roadside and from partners.

This needs to incorporate access control, audit log, and virus protection in addition to the standard firewall functions (address filtering etc).

3.1.6 There is a similar primary security barrier at the instation desktops, particularly for applications host machines carrying sensitive information (traffic control, enforcement or financial). This also needs to incorporate access control, audit log, and virus protection.

3.1.7 There are various secure options for access control by users to applications and data. Specifically:

a) Direct dial-in may be appropriate for own staff conducting external maintenance on the UTMC system, or occasionally access to systems contractors for support and maintenance; while proxy access is technically preferable for business partners, police access, etc.

b) For internal users, either an applications-specific access control or a 'single sign-on' approach could be taken. As a UTMC system gains more separately-controlled applications, it may be worth considering a single sign-on architecture.

3.2 Technology: security layers

3.2.1 The general focus of security-conscious industries – on access control/authentication as the primary means of assurance at the user level, supported by encryption at the data level and connectivity at the system level – should be adopted by UTMC.

3.2.2 Common database implementations may consider use of CORBA security tools, though control at the network layer (though address filtering etc) may be sufficient.

3.2.3 UTMC Objects should include parameters, where relevant, to cover security needs.

3.2.4 Address filtering and user filtering (through commercial firewalls) will provide protection at specific points (eg external interfaces), and should be a mainstay of all UTMC networks with external connectivity. HTTPS connections (HTTP over TLS) should be considered for all non-public Web-enabled access.

3.2.5 Electronic financial exchange (eg using the SET standard) is unlikely to be an internal UTMC matter.

3.2.6 There are a number of low-level Internet protocol standards that are applicable to UTMC. Many off-the-shelf products incorporate these and no specific standards need normally be called up.

3.2.7 The choice of IP, as the communications network protocol for UTMC, is a good one from the security point of view. Because of the (justified) public concerns about internet security, there is a great deal of development on security devices, add-ons and plug-ins for IP that should make communications security for UTMC entirely sound, at the three main points (Node B to Node A, within Node B, and Node B to Nodes C/D/E).

3.2.8 Encryption and segregated networks will provide bearer-level security. For the immediate future, private networks will still need to be used for any link that requires reliable high-timeliness communications.

3.3 Operations

3.3.1 Security needs to be tailored to local commercial, legal and institutional requirements. UTMC security should not be solely at the request of commercial third parties (eg travel information services), although clearly this is an important aspect of it.

3.3.2 As UTMC systems become more complex, all systems-level concerns will become more significant. As with safety, type approval will feed into this but will not by itself be sufficient, because of all the architecture issues discussed.

3.3.3 The Code of Practice BS/ISO/IEC 27000:2005 (previously the national standard BS7799) is fully relevant to UTMC systems, it is recommended that local authorities to adopt it as a framework standard. It addresses the management issues associated with access control of all sorts.

3.3.4 Security needs to be maintained through the implementation and migration processes, which means ensuring that:

a) partially-implemented systems do not have unacceptable functional security 'holes' (eg communications access to traffic signals before they are linked to the UTMC centre);

b) maintenance and repair do not expose security flaws (eg opportunity for access into network from a 'down' device);

c) the process of integration with legacy systems does not expose sensitive data to unacceptable risk;

d) security management procedures are in place and tested before the system goes live.

3.3.5 Tools are widely available to support the security management of networks and systems, and these should be considered in any UTMC system. Some aspects of this (eg privilege management) are naturally implied by the needs for access control.