Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 41 (2012) 480 – 485

Engineering Procedia

www.elsevier.com/locate/procedia

International Symposium on Robotics and Intelligent Sensors 2012 (IRIS 2012)

Secure System Architecture for Wide Area Surveillance Using Security, Trust and Privacy (STP) Framework.

Mohd Anuar Mat Isa[a], Habibah Hashim[a], Jamalul-lail Ab Manan[b], Ramlan Mahmod[c], Mohd Saufy Rohmad[a], Abdul Hafiz Hamzah[a], Meor Mohd Azreen Meor Hamzah [a], Lucyantie Mazalan [a], Hanunah Othman [a], Lukman Adnan [a]

[a]*Faculty of Electrical Engineering, 40450 UiTM Shah Alam, Selangor, Malaysia.*
[b]*Advanced Analysis and Modeling Cluster, MIMOS Berhad, Technology Park Malaysia, 57000 Bukit Jalil, Kuala Lumpur, Malaysia.*
[c]*Faculty of Computer Science & Information Technology, 43400 UPM Serdang, Selangor, Malaysia.*

Abstract

Mobile computing emerged in the market for the past few years to provide solution for various platforms that range from smart phone, tablet, laptop, desktop computer, server to virtual computing systems such as cloud computing. The design approach and development of solutions for mobile computing continues to evolve in fulfilling the needs of diverse applications that run on various platforms. Recently, a new framework was introduced to provide a unified approach to resolve Security, Trust and Privacy (STP) enhancement on these platforms. This new framework emerged to enable a better way of dealing with security, trust and privacy conflicting aspects in pervasive environment such as mobile computing. This framework will be useful for system architects, engineers, designers and developers that are still struggling to create a secure, trustworthy, and privacy preserved environment to create confidence amongst users to do business transactions and collaborations especially in a more challenging environment such as cloud computing. In this paper, we discuss and propose new Secure System Architecture for strengthening surveillance activities in Wide Area using a combination of Trusted Computing (TC) via mutual attestation process to ensure integrity of components of the system, and Surveillance System. We further propose using Intel AMT chip that will generate a heartbeat pulse and transmit the signal through network interface to detect any possible physical intrusion. A failure to provide this pulse within a given time frame will trigger an action by the trusted security system for further analysis such as thievery detection.

Keywords: Trusted Computing; Surveillance; Heartbeat; Security; Trust; Privacy; STP; TPM; AMT; Attestation; Secure System; Sensor; Beacon; Energy; Power.

1. Introduction

This paper intends to propose new security system architecture using the concept of a unified security, trust and privacy (STP) framework for surveillance activities in cloud computing. In this proposal, we propose to merge Trusted Computing security model with a hardware based system such as Intel AMT, surveillance system. The strength of this paper is that it integrates the unified STP framework with existing cloud computing infrastructure which will hopefully help to reduce cost without compromising the security, trust and privacy elements.

1877-7058 © 2012 Published by Elsevier Ltd.
doi:10.1016/j.proeng.2012.07.201

2. Related Works

2.1. Trusted Computing

Trusted Computing Group (TCG) is a non-profit industry standard organization with the purpose of improving the trust aspect of the computing platforms [1]. Since 2003, the TCG has published specifications defining architectures, guidelines, functions and interfaces that provide a baseline for a wide variety of computing platform to implement the TC procedures [2]. TCG completed trusted computing specifications version 1.2 called Trusted Platform Modules (TPM). The TPM hardware along with its supporting software and firmware provides the main platform trust element, *root of trust* [3]. Since its inception, TCG had contributed tremendously to support the realization of many security solutions for enhancing platform or computing system based on the two trust elements, *root of trust* and *chain of trust* [4], [5]. Both are used in attestation process for integrity verification in networked environment such as client-server and cloud computing [6].

2.2. Intel Active Management Technology (AMT)

AMT is an embedded technology that is implemented in desktop and laptop mainboard with Intel VPro system. This mainboard is embedded with Intel Management Engine (ME) microcontroller used for low level system operations without the need for end-user's operating systems such as Linux Kernel or Windows NTOSKRNL. This Intel ME had its own Real-time Operating System (RTOS) which is housed in the mainboard flash memory (after BIOS segmentation). RTOS firmware provides the necessary independent and isolated system for networking and remote monitoring used in Intel VPro platform. These new functionalities would give more advantage to system the administrator for managing platform such as those discussed in references [5] and [6] as follows:

i. Hardware inventory management – to keep track hardware and software in the platform in concurrent mode without interfering a running OS of an end-user.

ii. Event logs and alerts management - to keep track of events that happen in hardware and software such as casing intrusion, system states and operations (on, off, reboot, crash and etc).

iii. Remote control management – to allow a legitimate system owner with proper authorization to remotely control the platform, such as, changing system boot sequences (e.g. network boot, USB boot and etc), accessing platform BIOS configuration through network, for example, to turn on, off or restart. This feature is available in passive mode of the Intel ME.

iv. Real-time agent watchdog – to monitor the platform states and actions, including software running in end-user's OS, detection of malicious rootkit in OS and etc. This feature is available in active mode of the Intel ME.

Platform recovery – remotely recover a platform such as installation of OS, repair OS and applications, or scanning and removing virus or malicious codes or mounting remote virtual CDROM drive for platform to boot.

2.3. Surveillance System

Yan, at el.[9] proposed a surveillance service for sensor networks based on an adaptable energy-efficient sensing coverage protocol, wherein each node is able to dynamically decide a schedule for itself, to guarantee a certain degree of coverage (DOC) with average energy consumption, which is inversely proportional to the node density. They presented an example; a node sends a heartbeat signal to nearest node within certain range, as flag that indicates the node is working properly. Each working node knows the schedules of its nearest neighbours and expects heartbeat signals from the working ones among known neighbours.

2.4. Security, Trust and Privacy (STP)

Security, Trust and Privacy framework can help reduce the many contradictions within an environment involving these three elements and tighten their relationship using a unified approach to improve security policy and security conduct in protecting user personal and working data [10]. Major concern in STP, which involve various stake holders such as systems architect, engineers, designers and developers who are still struggling to create a secure, trustworthy, and privacy preserved environment for us to do business transactions and collaborations. We also noted that currently, STP issues are addressed and alleviated in silos. With current and future cloud computing infrastructure being build, we are still facing a big challenge to protect user identity, data and platform, wherein all business transaction are being materialized virtually somewhere in the cloud [10].