Архитектура на програмно приложение за мониторинг на система за видеонаблюдение

Делян Генков

Abstract: *Video surveillance systems are important part of modern security. When there is no live observation of the cameras image, it is important to have some alarm mechanisms for detection of physical impact against the cameras. Most simple video systems can detect motion and/or loss of video signal, but are vulnerable from covering or spraying the camera's lenses. Present study proposes an architecture of a software application for detecting anomalies in an IP based video surveillance system and raising alarms based on network traffic detection.*

Key words: *Software system, Video surveillance, Monitoring, Traffic, SNMP*

ВЪВЕДЕНИЕ

Системите за сигурност са важен компонент за съвременните организации. Системите за видеонаблюдение намират все по-широко разпространение. В някои организации има жива охрана и наблюдение на видеокамерите в реално време, но в други системата за видеонаблюдение се използва за преглед на записите при разследване на установено нарушение. Когато няма наблюдение на камерите в реално време атакуващият може да неутрализира камерата преди да извърши нарушението – например да покрие камерата с плат или дреха, да напръска обектива и със спрей или да среже кабела. Скъпите софтуери за видео наблюдение имат вградени аналитични функции, които им позволяват да откриват такива посегателства и да изпращат аларми по електронна поща, SMS или обаждане на телефон, но цените на тези софтуерни платформи са десетки хиляди лева. При евтините системи алармените механизми обикновено се ограничават до откриване на загуба на сигнал от камерата или до детекция на движение, така те са уязвими към атаки от гореописаните типове.

Голяма част от съвременните системи за видеонаблюдение са IP базирани – камерите имат интерфейс за компютърна мрежа и преобразуват сигнала във поток от пакети, които се предават през мрежата до компютърна система за наблюдение и запис. Така една и съща мрежова инфраструктура може да се използва както за предаване на данни, така и за видеонаблюдение. Такива системи могат да бъдат наблюдавани чрез механизми за наблюдение на компютърни мрежи. Най-популярният протокол за целта в съвременните компютърни мрежи е Simple Network Management Protocol (SNMP).[2]

Протоколът SNMP е разработен за наблюдение и управление на параметри на мрежови устройства. Той е част от стандартния набор протоколи TCP/IP на Интернет и е дефиниран от IETF. В типичните си приложения SNMP използва един или няколко компютъра с инсталиран специализиран софтуер, наречен мениджър, който наблюдава или управлява група мрежови устройства. На устройствата работи специализран софтуер, наречен агент, който отговаря на запитвания от мениджъра.

Агентите организират данните за наблюдение или управление в специални променливи. Променливите са организирани йерархично и тяхната организация, типове и описания са събрани в Management Information Base (MIB) – база данни за управление на устройството.

В момента съществуват три различни версии на протокола – версия 1, версия две с подверсии 2c и 2u и версия 3. В настоящата разработка се използва версия 2c. Дефинирани са седем типа съобщения:

- GetRequest: заявка от мениджъра към агента за получаване на стойност на променлива или списък стойности.

- SetRequest: заявка от мениджъра към агента за промяна на стойност на променлива или списък стойности.
- GetNextRequest: заявка от мениджъра към агента за откриване на достъпните променливи и стойностите им.
- GetBulkRequest: оптимизирана версия на GetNextRequest за много итерации.
- Response: отговор от агента, връщащ стойност или потвърждаващ заявка.
- Trap: асинхронно уведомяване от агента към мениджъра за настъпило събитие.
- InformRequest: потвърждение на Trap от мениджъра към агента.[4]

Йерархичната база данни (MIB) може да съдържа стандартна за всички устройства информация, както и специфична за даден потребител. Информацията се състои от множество идентификатори на обекти (Object identifiers, OID), всеки от които описва един параметър или група параметри на устройството. Всеки идентификатор е поредица от числа и/или думи, разделени с точки, например за да се получи името, назначено на дадена мрежова система, трябва да се прочете идентификаторът 1.3.6.1.2.1.1.5.0, като поредицата числа описва пътя от корена на дървото на базата данни до конкретната стойност.

Връзката между мениджъра и агента се осъществява чрез въвеждане на Community string – дума, играеща роля на парола. Обикновено на устройствата могат да се задават две нива на пароли – RO, която се използва само за четене на параметрите и RW, която може да се използва и за запис на стойности. За реализация на Set заявки е необходимо да се разполага със стринга за четене и запис.

Протоколът SNMP се поддържа от много устройства на различни производители и е стандарт за мрежово наблюдение и управление.

ИЗЛОЖЕНИЕ

В настоящата разработка се предлага архитектура на програмно приложение за наблюдение на IP базирана видеосистема чрез протокол SNMP. Предложеният подход изисква комутаторите, към които са свързани IP камерите да поддържат протокола и на тях да бъде конфигуриран Community string за четене на информация.

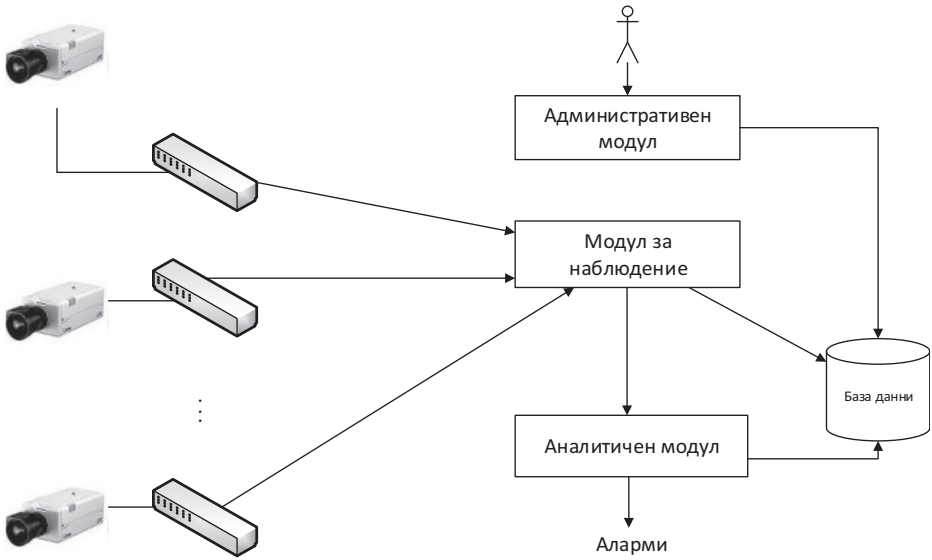
При предишна разработка опитно е установено, че при нормални условия трафикът генериран от една камера има видима повтаряемост в рамките на едно денонощие. През деня обикновено нивото на трафик е еднакво, като при нормални изменения на околната среда – промяна на слънчевата светлина, облаци и други подобни явления обикновено промяната е в рамките на 10 – 15%. Закриване на обектива на камерата води до драстично намаляване на трафика, генериран от нея до нива съизмерими с нощно наблюдение при липса на видимо или инфрачервено осветление. При покриване на камерата с полупрозрачен текстилен материал също се наблюдава спад в мрежовия трафик с около 20 - 25%, което предполага че разликата е достатъчна, за да се открие такъв вид атака [1]. При изключване на захранването на камерата, изключване или прерязване на мрежовия кабел свързващ камерата към мрежовия комутатор портът на устройството променя своето състояние на изключен, което също може лесно да се установи чрез протокола SNMP.

Приложението за откриване на аномалии в IP базирана система за видеонаблюдение ще наблюдава състоянието на три параметъра за всяка от камерите:

- Наличие на връзка до IP адреса на камерата чрез ICMP протокол;

- Състояние на порта на комутатора, където е свързана камерата;
- Входящ трафик на порта, където е свързана камерата.

Предложената структура на приложението е показана на фигура 1.



Фиг. 1 - Структура на системата

Административният модул ще служи за настройка на системата. Там потребителят трябва да въведе IP адресите на камерите и комутаторите, портовете в които са включени камерите и SNMP настройките на комутаторите. Тези параметри се записват в базата данни и се използват от другите модули за работата на системата.

Модулът за наблюдение ще реализира трите функции за мониторинг на състоянието на камерите, описани по-горе. За определянето на достъпността на дадената камера модулът ще изпраща периодично ICMP exo заявка до зададения IP адрес на камерата и ще очаква отговор. При неполучен отговор на няколко последователни заявки ще се счита, че камерата е загубила функционалност и ще се изпраща сигнал към аналитичния модул за изпращане на аларма. Събитието също така ще се записва в базата данни с цел отчетност.

Модулът ще осъществява и SNMP сесии с комутаторите, към които са включени камерите. Той ще следи следните стандартни идентификатори:

- 1.3.6.1.2.1.2.2.1.8.x (ifOperStatus) показва състоянието на интерфейса. Ако стойността е 1, то интрефейсът е работоспособен. При всички други състояния интерфейсът е неработоспособен и следва да се подаде сигнал към аналитичния модул. X е номерът на съответния интерфейс.
- 1.3.6.1.2.1.31.1.1.1.6.x (ifHCInOctets) показва броя байтове входящи за интерфейса X, т.е. изходящи от камерата в 64 битов брояч. Понеже стойността е с натрупване, за да се изчисли средната скорост, трябва да се записва времето на всяка проба и да се изчислява разликата на броя байтове от предишното измерване върху разликата от времената.

Основната роля на системата ще се изпълнява от аналитичния модул. Той трябва да следи нивата на трафика, записани в базата данни, да ги сравнява с

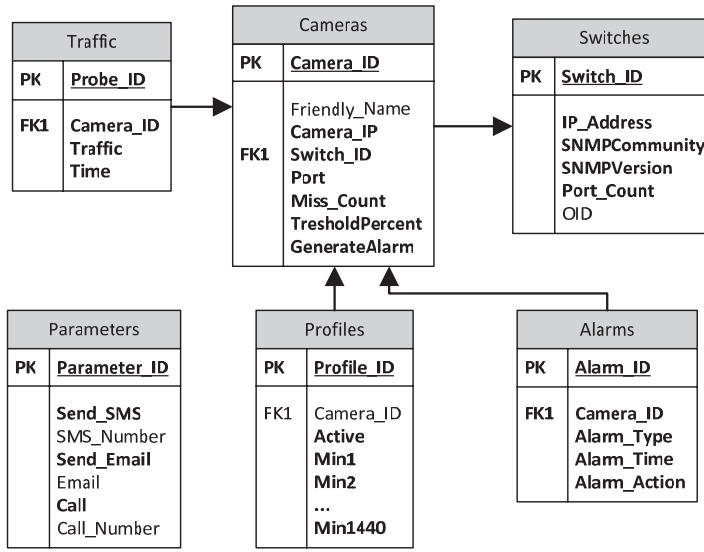
предишни стойности, да следи за отклонения и да взима решения за извикване на аларми. За целта е предвидено да се използва статистически метод, като предварително се изчислява профил на камерата от предишни дни, записани в базата данни и сравнението на текущия трафик с профила. За да се намали възможността за фалшиви задействания на аларми трябва опитно да се дефинират праг на задействие (например 20% отклонение от стойността на профила) и време на отклонение. Тези стойности могат да бъдат различни за всяка камера и следва да бъдат настройвани опитно по време на първоначалната работа на системата.

Предвидените аларми са следните:

- Аларма при недостижимост на камера: при неполучени няколко поредни отговора на ICMP съобщения;
- Аларма при отпадане на порт, на който е свързана камера: веднага при промяна на състоянието на порта;
- Аларма при отклонение от профила.
- Ако компютърната система за запис на камерите поддържа SNMP, могат да се генерират аларми за запълване на твърдия диск, натоварване на RAM памет или процесор, както и за отпадане на компютърната система, въпреки че това ще бъде разпознато и от алармата на профила на камерите.

Алармите се генерират на екран, могат да се изпращат по електронна поща, по SMS или чрез набиране на мобилен телефон и възпроизвеждане на предварително записано аудио съобщение.

Базата данни на приложението е показана на фигура 2.



Фиг. 2 - Структура на базата данни

Избран е релационен модел на базата, състоящ се от шест таблици. В таблицата Cameras се записва информацията за всяка от наблюдаваните камери – име, IP адрес, комутатор и порт, където е свързана камерата, брой пропуснати отговори и процентна промяна на трафика за генериране на аларма и дали да се генерира аларма. В таблицата Switches се пази информация за комутаторите – IP адрес, SNMP параметри и брой портове. В полето OID за съвместимост може да се

запише различен от стандартния SNMP идентификатор. В таблицата Profiles се записва информация за изчислените профили на трафика на камерите от аналитичния модул. Предвидено е да се поддържат няколко профила за камера, като само един от тях може да бъде активен за единица време. В таблицата Traffic се записват измерените нива на трафика, а в таблицата Alarms се пази информация за генерираните аларми. В последната таблица Parameters се пази допълнителна информация какви аларми да се генерират от системата, както и адрес на електронна поща и телефонни номера за получаване на тези аларми. Вероятно при бъдещи разширения там ще се добавят още параметри.

За реализацията на системата е предвидено да се използва Microsoft Visual Studio 2010 и езикът за програмиране C#. За система за управление на базата данни ще се използва Microsoft SQL Server 2010, а за реализацията на комуникацията по SNMP ще се използва безплатната библиотека SNMP#Net [3].

ЗАКЛЮЧЕНИЕ

В настоящата разработка е проектирана архитектура и база от данни на програмно приложение за наблюдение на IP базирана видеосистема. Разработката е предназначена за изграждащата се система за видеонаблюдение в Технически университет – Габрово, но може да намери приложение във всяка подобна система с описаната структура и възможности. Предложеният подход не изисква скъпо софтуерно решение за аналитични функции. В момента е реализирана част от потребителския интерфейс и базата данни, както и частта от модула за наблюдение, определяща състоянието на портовете и записваща текущите нива на трафик в базата. За в бъдеще се предвижда реализация на останалите модули, асемблиране и тестване на приложението, както и пускането му в реална среда.

БЛАГОДАРНОСТИ

Настоящата статия е изготвена с финансовата помощ на Европейския социален фонд. Русенският университет „Ангел Кънчев” носи цялата отговорност за съдържанието на настоящия документ, и при никакви обстоятелства не може да се приеме като официална позиция на Европейския съюз или Министерството на образованието и науката.

Проект: № BG051PO001-3.3.06-0008 „Подпомагане израстването на научните кадри в инженерните науки и информационните технологии”

ЛИТЕРАТУРА

[1] Genkov, D., Using Network Monitoring Application for Detection of Anomalies in Surveillance Video Traffic, Telfor’11, Belgrade, 2011, стр. .

[2] Harrington, D., R. Presuhn, B. Wijnen. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. IETF, RFC 3411, 2002.

[3] SNMP#Net Library, http://www.snmpsharpnet.com/, дата на използване 10.08.2013.

[4] Wikipedia. Simple Network Management Protocol. http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol, дата на използване 07.07.2013.

За контакти:

гл. ас. д-р Делян Генков, катедра “Компютърни системи и технологии”, Технически университет - Габрово, тел.: 066-827 419, e-mail: dgenkov@tugab.bg

Докладът е рецензиран.