Enabling Civil/Military Cooperation in Crisis Management

Chera Bekker Maurits de Graaf Gerard Hoekstra
Thomas Quillinan[*]
[firstname.lastname]@nl.thalesgroup.com
Thales Nederlands B.V.,
Postbus 90,
2600 AB Delft,
The Netherlands.

June 21, 2018

Keywords: Application of novel and existing information flow models/policies; Use-cases for compositional design/assurance; MILS components and eco-system

Abstract

Civil/Military cooperation is vital when addressing civil emergencies. In order to most efficiently enable such cooperations, it is important to ensure easy and secure information exchange. This paper describes an approach to enable such information exchange using a robust MILS kernel, using a content-based security approach to allow each organisation to remain in control of their own data. Furthermore, we demonstrate the approach by combining a military standard Command and Control (C2) system with a civilian system, where specific information can be securely and easily transmitted between the parties.

1 Introduction

There are several challenges to enabling cooperation between civilian and military first responders: first, all of the organisations have existing infrastructure and information management systems. Secondly, information can be classified at different levels, both from a national security perspective, and also privacy of citizen information – organisations involved in managing the crisis require a controlled

[*] corresponding author

information exchange. Thirdly, no single organisation is in control of all the information. Therefore an approach is required that manages this information exchange but more importantly ensures the separation of the security domains.

The approach demonstrated in this work utilises a MILS [6] kernel to ensure separation of the information domains, with a controlled "content-based security" mechanism to allow specific information flows – encrypted and labelled – to pass between the domains. Furthermore, we have developed a proof-of-concept demonstrator of a content-based key management mechanism on top of the PikeOS [7] MILS kernel, using existing military-hardened equipment. Information sharing has been proved between military Command & Control (C2), implementing NATO STANAG 4677 [2], and civilian-based geo-location based C2 systems. The integration of both military and civilian C2 systems enables the sharing of locations, tracks and information about events between existing systems used by crisis response teams.

Our approach uses the advantages of a dedicated channel for information exchange as well as separate channel for key exchange, ensuring the clear separation of concerns necessary for secure systems. This allows the information to flow between the distinct security domains without issue, as it is encrypted. However, due to the filtering, no data that should not pass from high-to-low will do so.

Although our approach is focused on mobile ruggedised hardware, we have also investigated the use of commodity hardware to enable multiple instances (between many separate networks) in a single hardware instance. Finally, we have also investigated how to integrate LTE into our system. This allows the quick roll-out of emergency mobile communication infrastructure in crisis situations. Furthermore, this allows the use of commodity mobile devices, such as phones, within areas where no infrastructure is available after, for example, a natural disaster. This also allows a dedicated communication channel for authorised users, unaffected by stresses on the normal infrastructure, commonly transpiring during civil emergencies. The remainder of this paper describes the architecture and information flow models and policies used to enable these applications.

The remainder of this paper is organised as follows: Section 2 introduces the concepts behind content based security. The basics of the command and control, both military and civilian, is outlined in Section 3. Both of these concepts are then linked together within a system architecture, as outlined in Section 4. Finally, Section 5 concludes the paper with a discussion and identifies some next steps.

2 Content Based Security

Distributing data between multiple parties in complex organisational structures requires the ability to carefully discriminate and manage access to the data. While traditional approaches have concentrated on either securing access to the system or securing access to the data stores, Content-Based security (CBS) instead secures access to the data items. CBS has a number of distinct advantages, such as the ability for data owners, rather than system owners, to control access to their information. This is particularly important in applications that require collaborative work practices and where asymmetries of trust exist. Our implementation of a content-based security solution, called Martello, provides a federated security solution where the owners of the data manage access to that data. While existing solutions address parts of the problem outlined above, Martello addresses the entire problem in a unique manner.

In a traditional perimeter defence approach, access to the system is controlled at the entry points and centralised authentication and authorisation mechanisms determine the access subjects have to objects within the system. In such systems, centralised authorisation mechanisms, using, for example, Active Directory or LDAP, are typically used in order to mediate access to the system. In such approaches, a centralised decision point (or a set of replicated decision points) are utilised to determine if a subject has access to an object. This approach effectively means that the administrator of the access control system owns all of the information within that system.

In contrast, in a system based on content-based security (also known as information bound security), objects are protected individually and may be freely shared. The security of the system relies upon the strength of the cryptographic algorithms used to encrypt the data. Encrypted data can then be stored in a public location. Furthermore, as such systems are by nature decentralised, such solutions allow the use of both federated and decentralised access control systems.

2.1 Martello

Martello [4, 5] is an approach to defining and implementing an end-to-end MILS (multiple independent levels of security) solution for data distribution systems using a content-based security approach. The solution aims at protecting the confidentiality and integrity of data objects for their entire lifetime, regardless of the security of the storage and communication media [18]. One of the most critical factors when distributing information between partners is controlling when, where and to whom this information is passed. The fundamental principle within Martello is that data remains under the control of the data owner at all times. This entails not only deciding on the access rights of other users but also retaining the ability to audit accesses that take place. This is managed through the use of standard cryptographic protocols and tools, where the data owners retain control over the keys to their data. Users of the system must negotiate directly with data owners in order to gain access to the data. A particular problem that occurs with such strict security requirements is that it becomes difficult for users to discover relevant information within the shared data space. However, if data owners are willing to grant access to specific processes that can aggregate results and then sanitise this information for specific queries, there is the potential that searching secure information can be achieved. As the data is processed on machines controlled by the data owner, the sanitised information remains under the control of the data owner until it is authorised for release. While it is impossible to guarantee that unscrupulous (but legitimate) users will not intentionally leak sensitive information, the system keeps audit logs that allow post-facto investigations to identify such leaks and thus allow administrative redress. Martello addresses the above-mentioned limitations of existing solutions in the following ways:

- Ensure that at least some critical functionality will remain available (e.g. data exchange between registered participants) even when one or more system components fail.
- Support non-disruptive changes to group membership;
- Support multiple classification systems by multiple authorities;
- Ensure that each information owner maintains control over information released or shared with other authorities, and
- Define an efficient exclusion and revocation mechanisms.

2.2 Deriving Keys

The basic premise supported by Martello is that information consumers are fully trusted to manage information in a domain but information producers are not. This asymmetry of trust reflects the fact that producers can be sensors that are in the field (and hence potential sources of leaks) as well as potentially limited in computational capabilities. However, the asymmetry could be in the other direction, where producers are trustworthy and consumers untrustworthy. Information stored in Martello is cryptographically encoded to ensure confidentiality. Key management becomes the central issue in such a system. Martello addresses this by using a key hierarchy. Each domain manager holds a set of Topic Keys, one for each topic supported by that domain. When an information consumer is successfully authorised to subscribe to that domain-topic, they receive this topic key. In contrast, information producers, who are untrusted, receive instead a key that is derived from the topic key but that is also unique to each producer. Producers encrypt using the derived key; consumers derive this key based on producer identifier. Standard Cryptographic mechanisms are typically used[1]. For example:

- SSL/TLS used to provide communication security for key exchange operations
- KDF2 with SHA256 used for key derivation to enable the asymmetry of trust.

3 Command and Control

In military systems, command and control (C2) is a vital aspect of information management in the field. As stated in [3]:

> The complexity of military operations is increasing as strategic, operational, and tactical levels merge, as operations serve a mixture of military and civil objectives, and as operations are carried out by coalitions of the willing.

Typically, military systems have a well-developed systems of C2, where all units are equipped with GPS and transmit information about their locations and other relevant data within their command structure. Civilian organisations, such as police and civil emergency response, are increasingly deploying similar systems. However, it is difficult to communicate between both the military and civilian systems, due to security concerns and lack of standards.

3.1 STANAG 4677

The NATO STANAG 4677 [2] defines a framework for data exchange between different nationalities, in the sense that its goal is to enable the battlefield information exchange amongst several armies of distinct NATO countries. The key idea to achieve is to set up an interoperability radio-network among the different armies, to grant the access to this network the nations will use tactical radios supporting the associated protocols (in NATO terms these radios are called Loaned Radios), thereby each nation could exchange data with the rest of the partners through these radios. Although, STANAG 4677 primarily defines message data exchange, voice is also possible, but it is not standardized in much detail by the standard. Finally

[1] These are fully configurable and different choices can be used within a shared system

with this objective present, the STANAG defines the specifications for making this interoperability network among nations, the layered structure that should be developed (taking as reference OSI stack model) and the processes that must support the exchange of data.

According to [2] (Page 9), the basic requirement for a system that implements the STANAG 4677, is the ability to read from and write to the standard data format defined, independent of the national soldier management system application and operating system selected. In order to achieve this goal, the STANAG 4677 standard defines how the data should be formatted and processed so as to issue/receive it to/from the soldiers or even to/from another national SBMS through the military network.

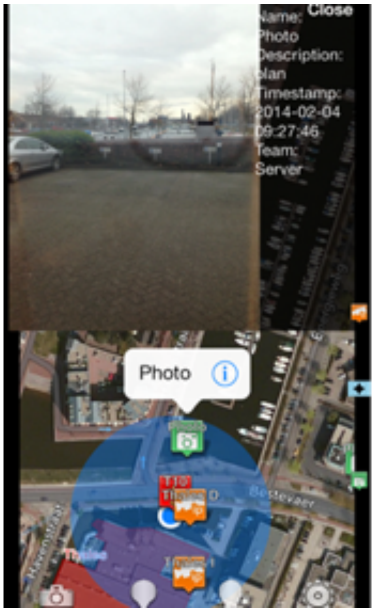
As it has been introduced in the previous section, at the military side, the CiMi-Gateway is going to make use of STANAG 4677, this provides the freedom of using any national BSM on the application layer, increasing thus the possibility for being used by several armies.

3.2 iSecuriTeam

The iSecuriTeam emergency services communications system is a personal communication system, implemented as a smart phone application, that assists the emergency worker with its task. The application provides shared situational awareness to the individual emergency responder. The platform uses standard technology guaranteeing interoperability between the various players in the public safety domain (police, ambulance services, firefighters, defense, professional security services). Figure 1 shows an example of the type of information that can be shown using iSecuriTeam, specifically a photograph, is shown on a map interface.

A prerequisite for achieving and ensuring Public Order and Safety (POS) is the capability for all involved parties to share and to have access to relevant information at the right time and place. To this purpose, Thales has developed the iSecuriTeam concept, which is based on sharing information between the following elements: the individual, the mobile team and the Command & Control-platform (C2).The concept is based on using technology that ensures ‘interoperability of information’ between all parties within the POS domain (Police, GHOR [Medical Assistance in case of Accidents and Disasters], Fire brigade, Defence, and other civil parties).

The main objective of iSecuriTeam is to enable the exchange and provision of data between C2 and elements equipped with iSecuriTeam, in order to enable fast and effective decision making and execution and achieving POS more adequately. This is carried out on the basis of an effective (operational) decision–making process and command & control through, for instance:



lame:
hoto
escription:
lan
imestamp:
014-02-04
9:27:46
eam:
Server

Figure 1: Example of the iSecuriTeam overview (here showing the split-screen functionality).

- A better shared operational overview at all levels, so that e.g. the location of all parties involved is known;
- Effective retrieval of (mobile) information, so that this information can be accessed and processed sooner;
- More effective use of information by sharing filtered and only relevant information and thus achieving efficient use of scarce capabilities;
- Improved collaboration between the various POS parties within the domain,
- Increased security for the individual team members.

The main features supported by iSecuriTeam are as follows:

- Own position and orientation with respect to others (‘blue force tracking’);
- Map information;
- Share plan information of the commander;
- Retrieval of external information (databases);

- Easy reporting of incidents with respect to georeference;
- Small and light system with long operational life,
- Sharing of images from and to C2, aimed at increasing data based on environmental sensors.

4 System Configuration

The basic system architecture, shown in Figure 2, operates on top of an initial prototype, based on bespoke hardware (for civil/military applications) and the PikeOS virtualised embedded real-time system. For the initial testing, the development was based on top of the Pike OS embedded Linux personality, called ELinOS. Martello, whose components indicated with the key logo, is written in Java 7, iSecuriTeam (identified as MOOVE in Figure 2), uses MySQL backend and Perl. The STANAG 4677 converter is written in TCL. ELinOS supports all of these packages and applications, with several modifications to libraries etc.

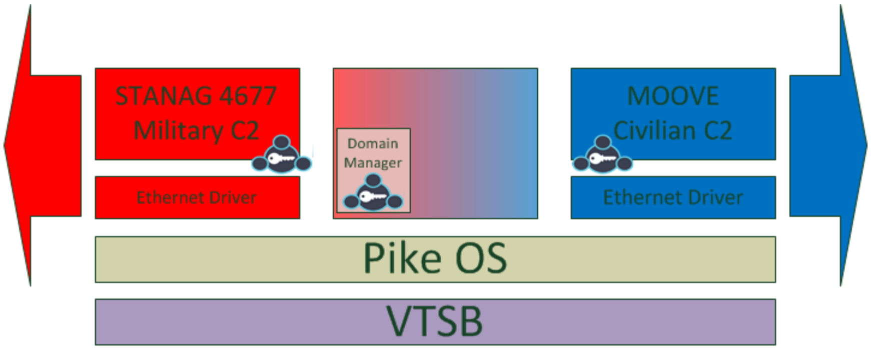


Figure 2: Civil Military Gateway architecture

The slices (virtual machines) were configured as five separate partitions, as shown in Figure 2. There is an Ethernet slice for each interface, civilian (Blue) and military (red). These slices are directly linked to the relevant (red/blue) slice that contained the data (from iSecuriTeam) or converter (STANAG 4677). There is a Martello client operating on both of these slices, handling the data produced by either iSecuriTeam or the military C2 system. Only data that is encrypted is allowed by the filter across the network from the red to the blue area.

The final slice (shown in the middle) operates as the key management system and as a filter checking the validity of packets. In the initial setup A Martello Domain server has been put in the military zone (i.e., under control by a military authority). Note that it needs to be connected to the open half of the gateway in order to be accessible for the civil organisations. Organisations that want to share military information first request access to the Martello domain server via the standard operational procedures common to Martello. Then they get access via the Martello domain server. This is actually a smart combination of two well-known concepts that adds value to Martello, the CimiGateway, and iSecuriTeam.

The CimiGW slice has a single Martello domain manager, under administrative control of the military side. The domain manager controls which military/civil organisation can get access to which information from the other side. In the future this will be two separate slices, each with their own domain manager, one for the red and one for the blue networks. These domain managers manage the keys for data produced by each of the networks. Separate channels, PikeOS queues are then used for communication between the key management services and the Martello clients on each side. PikeOS limits the communication on these channels to key material only.

A specific advantage of Martello in this setup is that without Martello, there would be no further granulation in the separation between the domains in the open (unsecure) world (or: if there would be, it would static) but with Martello dynamic fine grained access becomes possible.

4.1 Hardware

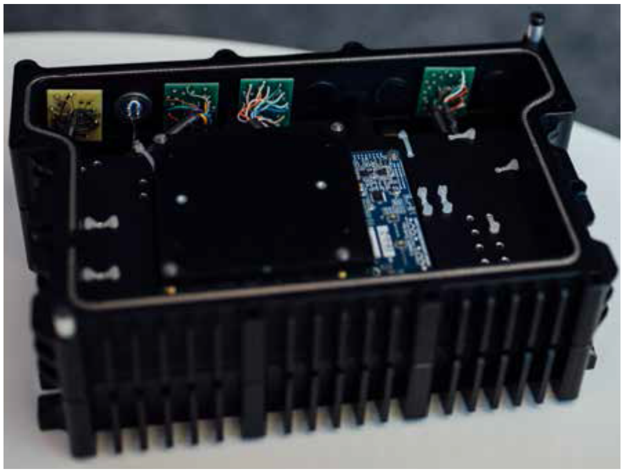


Figure 3: SOTAS Vehicle Tactical Server Platform (VTSP) rev 2 Hardware

The system is running on bespoke hardware, shown in Figure 3. It has the following specifications: Intel Core i7 Processor with 16GB RAM and a SSD HD;

Audio and network interfaces that is passively cooled.

As can be readily identified, this is a standard specification with extensions specifically for military applications, such as passive cooling and ruggedised connectors. The hardware is designed to operate inside military vehicles and to be easily replaceable.

4.2 Pike OS Configuration

ELinOS is a commercial development environment for embedded Linux . It consists of a Linux distribution for the target embedded system and development tools for a development host computer.

PikeOS is a microkernel-based real-time operating system made by SYSGO AG. It is targeted at safety- and security-critical embedded systems. It provides a partitioned environment for multiple operating systems with different design goals, safety requirements, or security requirements to coexist in a single machine.

The PikeOS RTOS supports the creation of partitions that are fully separated in space (non overlapping memory space) and in time (non-overlapping CPU and I/O hardware access). This guarantees a strong separation between processes belonging to different security domains and strictly controlled information exchange between the partitions and security domains. Communication paths between partitions and security domains are defined during development time and cannot be changed at run time. The PikeOS partitions in the gateway are used to securely separate the Martello Domain manager, the communication content verification algorithms and the virtual I/O device drivers from each other. This prevents the propagation of security risks between domains and the Martello domain manager and quarantines possible exploits in the hardware device drivers.

4.3 Software Stack

As has been stated above, the CIMI Gateway is intended to share information between the military and civilian command and control systems. In the simplest example, geographic locations translated from STANAG 4677 to latitude/longitude information and encrypted using Martello Client using a pre-defined policy. For example, policies exist for geographic location of both the user or the data; and defined time periods. This ensures that, for example, if the consumer of the information is in a certain geographic area, they will receive the key to decrypt the shared information.

There are therefore two channels for communicating between slices: the first for the data shared between C2 systems; the second is the key exchange channel. This second channel is used by the Martello clients to communicate with the domain manager(s). These keys are communicated using UNIX pipes defined in PikeOS. iSecuriTeam C2 authenticated clients contact Martello DM in Secure partition via a separate dedicated channel defined in PikeOS. The iSecuriTeam application has an embedded Martello client that authenticates itself to the domain manager, and then request specific keys. If they are authenticated and authorised, these keys are passed (via a public key encrypted message) to the authorised user. Keys are managed by the the Martello Domain Manager in the Secure Segment.

5 Discussion and Future work

In this paper, we have outlined a system used to allow sharing of information between different security domains, both civilian and military. We have developed a proof-of-concept demonstrator of a content-based key management system on top of ruggedised equipment to enable information sharing between military and civilian-based geo-location based C2 systems. The integration of both military and civilian C2 systems enables the sharing of locations, tracks and information about events between existing systems used by crisis response teams.

PikeOS provides an excellent platform to support MILS solutions. In particular, it supports non-interference, integrity protection and ease of certification for safety and, in this instance, security levels [1, 8]. However, ELinOS is not easily certifiable to a high Common Criteria level due to the size of the codebase. Therefore, future work is investigating developing versions of the Martello, STANAG 4677 convertor, and iSecuriTeam codebases to run natively on either the PikeOS native or POSIX personalities, in order to prepare for EAL validation.

One concrete result is that the VTSP supports multiple software services and provides a stable platform to implement multi organisational data sharing. This work has lead to further investigations towards deploying 4G networks in military vehicles in order to roll out mobile networks in the aftermath of a civil emergency, such as an earthquake, that has destroyed normal infrastructure. This has the benefit that existing devices can be used to help coordinate the crisis response.

Finally, future work is aiming to develop more flexible civil-military gateway devices to enable sharing of information between Non-governmental organisations (NGOs), civilian authorities, and the military, in order to better manage information flow and to improve cooperation in the future.

References

[1] ISO/IEC 15408-1, Information technology – security techniques– evaluation criteria for it security. Standard, ISOIEC, December 2009.

[2] Dismounted soldier systems standards and protocols for command, control, communications and computers (C4) interoperability (DSS C4 Interoperability). Standard NSO/0980(2014)LMC/4467, The NATO Standardization Office (NSO), October 2014.

[3] DS Alberts and RE Hayes. Power to the edge: Command... control... in the information age. Technical report, 2003. `http://www.dtic.mil/docs/citations/ADA457861`.

[4] Thales Nederland B.V. Martello. `https://www.thalesgroup.com/en/martello/`.

[5] Gregor Pavlin, Thomas Quillinan, Franck Mignet, and Patrick de Oude. *Exploiting Intelligence for National Security*, chapter 15.

[6] John M. Rushby. Design and verification of secure systems. In *ACM SIGOPS Operating Systems Review*, volume 15, pages 12–21. ACM, 1981.

[7] SYSGO. Pikeos hypervisor. `https://www.sysgo.com/products/pikeos-hypervisor/`.

[8] U. S. Department of Defense. Trusted computer system criteria. Technical Report CSC-STD-001-83, U. S. National Computer Security Center, August 1983. Known as “The Orange Book”.