Wireless Pers Commun
DOI 10.1007/s11277-010-0069-6

Location-Aware Mobile Intrusion Detection with Enhanced Privacy in a 5G Context

Nils Ulltveit-Moe · Vladimir A. Oleshchuk · Geir M. Køien

Abstract The paper proposes a location-aware mobile Intrusion Prevention System (mIPS) architecture with enhanced privacy that is integrated in Managed Security Service (MSS). The solution is envisaged in a future fifth generation telecommunications (5G) context with increased but varying bandwidth, a virtualised execution environment and infrastructure that allows threads, processes, virtual machines and storage to be migrated to cloud computing services on demand, to dynamically scale performance and save power. 5G mobile devices will be attractive targets for malicious software, and this threat will in some cases change with location. Mobile devices will store more sensitive information and will also be used to a larger extent for sensitive transactions than they typically do today. In addition, a distributed execution environment in itself gives raise to some new security challenges. In order to handle these security challenges, we have proposed the location-aware mIPS architecture, which benefits from a distributed execution environment where processor intensive services can be outsourced to Cloud hosting providers. The mIPS supports querying location threat profiles in a privacy-preserving way, and ensures that mIPS alerts sent to the the first-line MSS are anonymised. We finally perform an analysis of potential strengths and weaknesses of the proposed approach.

Keywords 5G · Mobility · Security · Personal privacy · Location profile · Intrusion detection and prevention

N. Ulltveit-Moe (✉) · V. A. Oleshchuk · G. M. Køien
University of Agder, Service box 509, 4898 Grimstad, Norway
e-mail: nils.ulltveit-moe@uia.no

V. A. Oleshchuk
e-mail: vladimir.oleshchuk@uia.no

G. M. Køien
e-mail: geir.koien@uia.no

Published online: 08 July 2010

1 Introduction

Mobile terminals are personal devices that can contain a lot of private and sensitive information, and will also be used for sensitive transactions like on-line banking. This means that sensitive information can leak out to criminals or other non-trusted persons via different channels like physical theft, malware or spyware. Security services like antivirus, firewalls, Intrusion Detection Systems (IDS), integrity checking and security profiles may therefore be *required* for all mobile terminals in the future.

However a concern with using IDS integrated in Managed Security Services (MSS), is that the service intended to enforce the security of the terminal itself can leak sensitive information. Leakage of sensitive information can for example occur via alerts sent out from the system or during forensic analysis of suspicious events. Contractual means like confidentiality agreements may not be sufficient to prevent abuse of sensitive information by corrupt insiders. It is therefore important that an IDS also considers the *privacy and sensitivity* of the information sent in the IDS alerts.

It will furthermore not be sufficient with a managed IDS alone, since the mobile device can be out of range for Internet connectivity. It is therefore important that the IDS sensor on the mobile device can act *reactively* on an autonomous basis, if there is poor connectivity towards the central monitoring server. This means that the mobile IDS sensor should be considered as a partially autonomous Intrusion Prevention System (IPS). Some level of autonomy is also important in order to scale the MSS service to a potentially huge amount of mobile devices.

Last but not least, the threat profile can change with the location for a mobile device. Some areas may for example be more prone to Bluetooth attacks, there may be rogue WLAN access points or other threats that are specific to a given location. This means that the mobile Intrusion Prevention System (mIPS) should be *location-aware*. In addition, future mobile devices may support a virtualised execution environment where threads, processes or light weight virtual machines can be migrated between the mobile device and a pay-as-you-go cloud hosting provider on demand, for example to gain additional processing power or to save battery capacity.

Such Cloud-based services would however be sensitive to both the cost and the latency of the service. We assert that 5G services will have the necessary bandwidth to accommodate these services, but in a wireless/cellular setting one must always be prepared for temporal/spatial restrictions on the 5G access (i.e. downgrading to 4G, 3G or even 2G bandwidths). This means that a cloud based execution environment to some extent would need to follow the physical location of the mobile device, which means that some cloud service providers may be more trustworthy than others. In addition, Cloud based services may not be viable where bandwidth is limited, which in our case means that the mIPS needs to be able to run locally as well in some scenarios. This article describes and analyses an mIPS architecture that is a first step towards solving these problems. To the best of our knowledge, a location-aware intrusion detection and prevention system with enhanced privacy handling has not previously been described in the literature.

The article is organised as follows: The next section defines what we mean by 5G. This includes aspects of the communication channels, access security expectations and trusted computing. Section 3 defines mIPS system requirements in a 5G context. Section 4 discusses various sources of privacy leakage in managed security services. Section 5 describes the two-tier privacy-enhanced system architecture and sect. 6 goes in detail on technical solutions for location-aware mobile IPS. This includes discussion about federative, bandwidth and energy saving policies. It goes into detail on how location-aware mIPS policies can be distributed

to the mIPS client in a privacy preserving way. Sections 7 and 8 performs respectively a security and privacy analysis of the mIPS architecture. Section 9 discusses related work and section 10 concludes the article and outlines directions for future work.

2 What Do We Mean by 5G?

For the purpose of this paper, this section defines what we mean by "5G". We first identify a few factors that may help us define the expected properties of 5G.

Bandwidth/Communications Capacity. The ITU has standardised requirements for what 4G systems must provide. This is captured in the ITU-R *IMT-Advanced* definition (see [16]), and is exemplified by LTE-Advanced [3]. The 4G systems will routinely provide *Fast Ethernet* bandwidths of 100 Mbps even for high mobility and up to 1 Gbps for low- or local mobility cases. We expect 5G mobile systems to provide in the order of ten times the 4G bandwidth. Sustained 5G rates, even with low-to-moderate mobility, may be in the order of 1–10 Gbps.

Mobility. Compared to 2G, 3G and 4G systems, we do not expect too many differences in generic mobility capabilities. Idle mode mobility should be similar to 3G/4G idle mode mobility. We estimate that many devices will not need a high degree of mobility.

Coverage. We expect that 5G coverage eventually will be generally good or decent in urban conditions. There may be hotspot coverage in suburban areas, but no general coverage is expected there. Many may enjoy 5G coverage with limited mobility in home femtocells.

Access Security. We postulate that link layer security is needed and is catered for by the radio system. We expect the 4G access security, such as the security defined for LTE (33.401 [2]) to be extended, in order to cater for new nodes and faster bandwidths.

Communications Security is defined to be security specific to the network layer (or above), as opposed to access security. Thus, the communications security will not always be needed, and it will be end-to-end when applied.

Personal Privacy will be more important in the future. For a mobile device, that naturally means that identity privacy and location privacy will be very important. Similarly, higher level concepts such as movement and transaction privacy will also be important for mobile devices, but not necessarily an issue at all for stationary non-personal devices. See [18,19] for background on classical personal privacy issues for cellular subscribers.

2.1 Access Security and Operator Provided Security

We expect that access security mechanisms in a 5G device will be at least as good as for 3G and 4G cellular services.[1] Thus, we generally expect that the 5G link will be adequately protected with respect to data confidentiality and data integrity. This protection includes a reasonable protection against charging fraud, eavesdropping and over-the-air data manipulation. However, as with all access security, the protection will not be designed to be end-to-end, so the user data will potentially be exposed when the data stream exits the mobile network or before it enters the mobile network.

Furthermore, the different access networks will have different access security architectures, and inevitably all may not be equally good. This could be a consideration for the

[1] A reasonable account of cellular access security can be found in [20].

platform security in the 5G device, and it might conceivably be part of the access policy considerations taken into account by a mIPS client. The mIPS client should probably also be aware of whether or not the 5G device is connected to the home network or to a roaming network. One should assume that the subscriber has a higher, or at least a well defined, level of trust in the home network. Roaming networks may operate security services at a high level, but the subscriber has less confidence and less reason for trust in the roaming networks.

2.2 Trusted Mobile Computing

We expect the typical 5G devices to have some sort of trusted mobile computing support. This will be realized by hardware, be it a secure device like the UICC (for 3GPP 3G/4G devices [1]) or a dedicated part of the device CPU (like the ARM TrustZone extension),[2] that amongst others can be used for sealed storage, trusted boot and hardware support for encryption/decryption. This both makes new business models feasible as well as possibilities for increased security and privacy handling in the mobile devices.

2.3 Overall Characteristics of 5G

Native 5G connections will be very fast compared to today's networks. This allows for unprecedented levels of streaming services and permits use of services like online storage systems. Ultimately, this also means that much more private information can be managed and exchanged to/from a mobile device. But, 5G systems will not have global coverage. Hotspot coverage, through femtocells, will likely be the most common case. So, the 5G device must be able to function satisfactory with much lower bandwidths than what it can expect from a 5G connection. This means that all services must handle the following scenarios:

1. Periodically the device will have full 5G service
2. Periodically the device will only have 4G (or 2G/3G) connectivity
3. Periodically the device will be off-line[3]

There are many challenges for services operating under these conditions, given that essential services must work satisfactory at all times. This includes security services, basic call connectivity and messaging services. This also means that many of the services must be able to operate more or less autonomously. For the purpose of this paper, we note that this in particular applies to the mIPS service, where one must have a local IDS client integrated into a managed security service, which also can act autonomously (i.e. IPS functionality).

3 mIPS System Requirements in a 5G Context

In the following section we postulate the following system requirements for a mIPS system in a 5G context:

Communications Channel. Peak performance: Very high (5G) bandwidth with low latency. Worst case: Dropping down to 2G (EDGE) bandwidth or losing the connection altogether. The 5G device should therefore have a bandwidth usage policy in place according to the status of the communications channel. In general, there should be sufficient bandwidth for transmitting IDS alerts in areas with 5G connectivity, at least as long

[2] See http://www.arm.com/products/security/trustzone/index.html.

[3] The device may still have limited local connectivity via Bluetooth, NFC/RFID etc.

as the IDS is not subject to a Denial of Service attack aimed at consuming bandwidth. However, due to the risk of large bandwidth variations, there may be times when alert data should be queued until sufficient bandwidth is available for transmitting the alerts. This also means that using XML-based message formats like for example using IDMEF, SAML, XACML or web services should be viable from a bandwidth perspective. Since there is no guarantee that the link will provide sufficient bandwidth for sending alerts, then it is important that the IDS can operate autonomously and perform active responses (i.e. IPS) in order to avoid ongoing attacks. Examples of active responses is to drop connections or block the attacker in the firewall.

Processing Power and Local Storage. The 5G device will have more than adequate processing power for all necessary cryptographic operations and for all local IDS client operations. The 5G device will be able store substantial amounts of data locally. Temporary storage of IDS data and logs is therefore considered unproblematic.

Battery/Power status The 5G device may be run on batteries, or it may be connected to a power source (USB powered/mains cable/etc). There will be situations where power consumption is not an issue (connected to external power source). Correspondingly, the device must also be able to run on a local power source (battery/fuel cell) with limited capacity. In those cases there will be a need to conserve energy.

Virtualisation and Cloud Computing The processor of the 5G device will have full hardware support for virtualisation, and the phone operating system will run as a guest operating system in a virtualised environment. This ensures both increased flexibility in the form of running different user profiles as different virtual machines,[4] and the possibility to increase scalability and reduce battery power usage by migrating threads, processes or lightweight virtual machines to Cloud-based services on demand. It will also provide increased security through isolation between the virtual machines. However, this is under the presumption that the Cloud hosting provider is honest and trustworthy, since introspection of virtual machines from the Virtual Machine Monitor/hypervisor usually is possible [14].

Personal Privacy Profile (PPP). The PPP will depend of the privacy sensitivity of the user. It may also depend on the usage of the device, i.e. according to the perceived risks and threats to the usage of the device. Thus, a device used as a personal authenticator, for example for on-line bank services, is likely to be more privacy sensitive than a device used for games and entertainment only. Different PPP's can be isolated in different virtual machines running on the mobile device[5], to separate data between different profiles. In a mobile setting the location may also affect the personal privacy profile; The exposure level for location dependent threats within your own home is probably fairly low, but may be considerably higher in other more hostile environments. The PPP should be set to reflect this situation.

mIPS Architecture. The mIPS architecture is logically composed from one or more central mIPS servers and one or more mIPS clients on the 5G device. The central server has a global view over the threat situation, but must be assisted by the local clients to update its global view. That is, the local clients acts as sensors for the central mIPS server.

Local mIPS Policy. The central mIPS server provides threat profiles and updated rulesets or similar to the local mIPS clients. The threat profiles help the local mIPS client to

[4] E.g. VMWare Mobile Virtualization Platform http://www.vmware.com/products/mobile/.

[5] The virtual machine for the privacy profile needs to able to run locally on the mobile device for profiles that can be used in low bandwidth (2G/3G) scenarios. Other profiles may require 4G/5G connectivity to work, in which case outsourcing of computationally heavy operations to Cloud based services can be an option to save CPU or battery power.

properly configure itself for the given context. There will be a baseline *user preferences profile*, possibly based on a template for the device type, that can be used to control how much sensitive information that is sent out from the mIPS. The total local mIPS client monitoring policy should be coherent with the mIPS server's provided set of profiles for services and communication interfaces. The battery/power policy aims at reducing power usage as much as possible without reducing the detection efficiency. This can also involve outsourcing computationally heavy mIPS operations for processing by a Cloud hosting provider.

mIPS Alert Handling. The alert messages should be transmitted to the alert database as fast as possible after the IDS has detected a potential attack, to limit the effect of the attack. It is also presumed that end-to-end encryption is used on the connection between the mIPS sensor and the alert database.

4 Privacy Leakage from Managed Security Services

Corporations can in the future be expected to require Managed Security Services (MSS) on corporate mobile terminals. Such services will control firewall settings and run 24×7 monitoring using mIPS to detect attacks on the terminals. mIPS rules from Managed Security Services may leak private and sensitive information. It is therefore a trade-off between the privacy leakage caused by a monitoring organisation running MSS, and the privacy leakage caused by adversaries. It should in this respect be noted that the effects of privacy leakage to criminals can be devastating and is without any regulatory control, whereas the privacy leakage from MSS is presumed to be measurable and under regulatory control. However, it should still be a goal for the monitoring organisation to minimise the harm on privacy and confidentiality for the subjects being monitored, since even a MSS provider cannot guarantee that sensitive information that leaks out from mIPS alerts can not be secretly abused. Another aspect worth noting, is that it may be feasible to forward huge amounts of data back and forth between the 5G device and the mIPS service provider in a 5G environment. This accentuates the need for better handling of personal privacy in conjunction with the mIPS service, in particular for outsourced MSS.

The three main areas where privacy or confidentiality may be compromised in MSS are:

- alert handling;
- forensic interface;
- and rule handling.

There are numerous ways that the user can be identified or sensitive information can be leak out from network data excerpts or audit traces sent with the mIPS alerts. This can include the location or movement of the user or what transactions the user was doing at that point in time.

Access to a data forensic interface for setting up traces in order to investigate suspicious traffic will violate the user's privacy. Such access therefore needs to be controlled and logged.

IDS rule updating may also be a possible source of privacy violations, since the IDS rules can be designed to return sensitive information by a corrupt security analyst. The IDS rules and threat profiles continually need updating to make signature based mIPS work, since new attack vectors will require new IDS rules to be added. Most of the IDS rules used are based on publicly available rule sets that security companies trust. It may therefore be possible for an insider to attack the mIPS system by modifying the trusted IDS rule set or location threat

profiles. It is therefore important to require unlinkability between the device being monitored and the location threat profile.

Furthermore, a 5G device (with 5G connectivity) will be able to participate in numerous sessions and consume/provide multiple simultaneous services. Scalability is therefore important, since the mIPS must be able to handle fairly large amounts of events, and potentially exchange fairly large amounts of IDS data. Outsourcing mIPS processing to a Cloud hosting provider is one way to improve the scalability of the mIPS both on the client and server side.

5 System Architecture

The location aware mobile IDS system architecture is an extension of the two tier architecture in [33]. The architecture has:

- a *first line* privacy-preserving subsystem, which is operated by security analysts running a 24×7 service;
- a privacy-invasive *second line* service that allows for further analysis by experts, but where all privacy violations are logged;
- built-in *privacy policy enforcement points (PEP)* using eXtensible Access Control Markup Language (XACML) based policies [26];
- mandatory activity monitoring for both first- and second level operation to monitor the privacy and security performance and also for auditability of the MSS operation.

The solution lowers the overall number of privacy violations during MSS operation, by disseminating information on a *need-to-know* basis. Our solution implements this by dividing the security analysis into two tiers, where the first line consists of a group of people performing 24×7 monitoring of the networks using privacy-preserving techniques. The first line monitoring is presumed outsourced to a third-party organisation to reduce the operating cost of running the 24×7 service. The second line consists of security experts that have security clearance and authorisation to perform necessary privacy violations to investigate whether attacks were successful or not. Second line analysts would when necessary provide forensics data to Computer Emergency Response Teams (CERTs) and law enforcing agencies in order to investigate successful attacks.

The Intrusion Detection Message Exchange Format (IDMEF) is used for IDS alerts [8]. It is used in conjunction with the Intrusion Detection Exchange Protocol (IDXP) [10], for transporting alerts from the mobile IDS sensors and to a Security Operations Centre potentially via one or more intermediate proxies. The Security Assertion Markup Language (SAML) is used for authentication in a federated environment, and dynamic eXtensible Access Control Markup Language (XACML) based policies [26] are used for authorisation and security obligations in the mobile device.

The proposed architecture in Fig. 1 provides Policy Enforcement Points (PEPs) that act as intermediaries between IDS monitoring consoles and one or more mobile IDS sensor(s), that enforce a privacy policy on the data transmitted.

The outsourced first-line service receives anonymised alerts with location data, to avoid that sensitive information leaks out. This avoids that location or movement information easily can be linked to the device being monitored. Second line IDS operations can request the real data sessions and set up alert correlating assertions for first-line operation, but can not access location or movement data. In addition, all such requests are accounted for in the activity log.

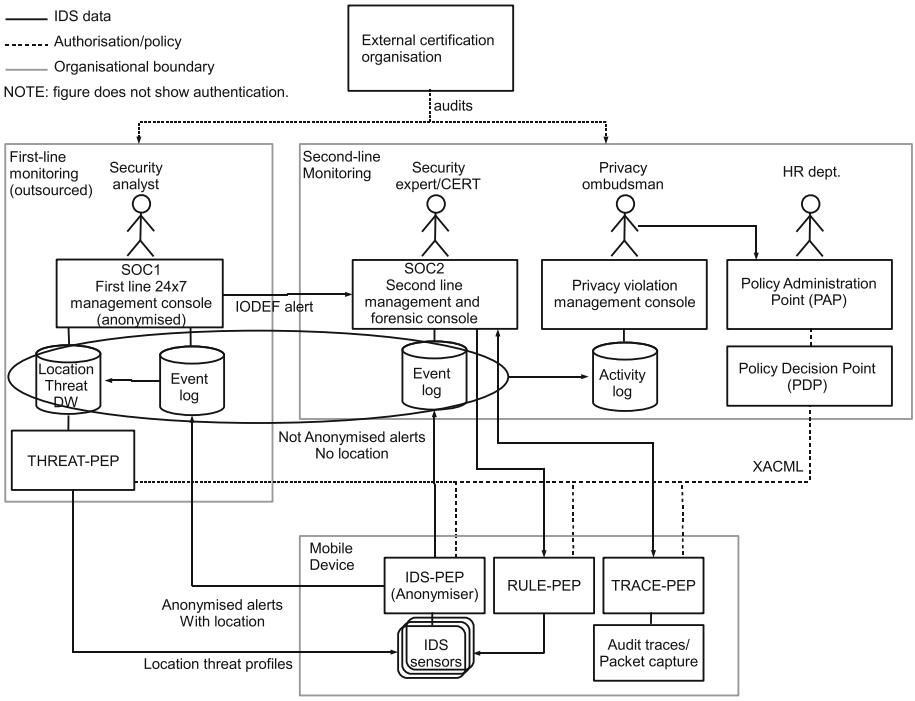

Fig. 1 Location-aware and Privacy-enhanced Mobile IDS Architecture

A privacy-enhanced IDS must obey the principles of data avoidance and reduction [6]. Data avoidance means that the user should be forced to only disclose the minimum amount of information necessary to the IDS. This implies that an IDS does not need to know the identity of a monitored user, until it provably detects an abuse.

Data avoidance is supported by having a two-tiered architecture, where the most labour intensive part, first line monitoring of all incoming events, works in a privacy preserving mode (see Fig. 1).

Data reduction is supported by using XACML obligations which remove data that is regarded as sensitive in the privacy policy. XACML was chosen as authorisation policy language, because it is a mature standard that can use the Security Assertion Markup Language (SAML) for authentication in a federated environment. It fits well into a Service Oriented Architecture (SOA) and has quite broad vendor support compared to other alternatives like the Enterprise Privacy Authorisation Language (EPAL) [28]. We considered XACML to be more general than the Platform for Privacy Preferences (P3P) [23], which focuses mainly on web based authorisation.

The IDS authorisation framework has a Policy Administration Point (PAP) that controls access to first- and second line data. The company's Privacy Ombudsman together with customer and company management is responsible for managing roles (first line or second line) and privacy policies in the PAP. The Human Resources (HR) department defines which role employees belong to.

Law enforcement agencies and CERT teams can be granted access to second line monitoring in order to investigate ongoing attacks. The IDS Policy Enforcement Point (IDS-PEP)

communicates with the Policy Decision Point (PDP) on authentication[6] and access control (authorisation) of the alert data stream.

The entire monitoring organisation should in addition be audited by an external quality certification authority at regular intervals, and these audits should include an analysis of how privacy-invasive the operation is compared to other companies in the same sector.

After authentication and authorisation, the IDS-PEP accepts IDMEF messages carrying alerts from a set of IDS sensors. The IDS-PEP then forwards streams of IDMEF messages with location data anonymised according to the security policy of the receiving manager application. Data streams authorised for first line operation will be anonymised according to the obligations presented in the XACML security policy for the role *firstLine*. It is sufficient to anonymise data in the Policy Enforcement Points (PEPs), since the outsourced organisation is presumed to not have access to manage the sensors.

If the first-line Security Operations Centre (SOC) identifies a suspicious message, then it will alert the second line SOC using an IODEF message. The alert identifier can be used by the second line operations centre to identify the full non-anonymised alert. The verdict from the incident analysis needs to be sent to the location threat datawarehouse in order to keep an updated threat picture.

The security policy for the role *secondLine* removes the location, however the rest of the alert, including payload is sent to the second line server. This means that location privacy and movement privacy is preserved, as long as the first and second line service do not collude. Both first and second line operations will in addition have the XACML obligation for access to data that all operations will be logged. This is in order to ensure traceability for the MSS operation both from a privacy and a security perspective. The purpose is to be able to monitor that both the first and second line operations perform their duties without shirking or doing excessively privacy invasive surveillance. Access to the forensic interface is governed by a separate privacy policy enforced by the TRACE-PEP. The TRACE server policy will only grant access to security analysts with role *secondLine* with the XACML obligation that all operations are logged.

The Privacy Ombudsman will have read access to summary data from logged activities. This implies that the system also needs a policy for the role *ombudsman*. A separate security policy *ruleManager* is required for updating the IDS rule set, because the Security Operations Centre typically delegates this responsibility only to a subset of the second line security analysts.

6 Technical Solutions

6.1 Federative Policies for Privacy and Security

Mobile terminals can be considered sensitive from a business perspective. The mobile terminal of an employee can technically be fully integrated into a company's intranet today, however there are no common solutions for enforcing the security configuration and policies for the mobile terminal.

This problem can be overcome on 5G devices by allowing mobile terminals to be used in federations of systems in a service oriented architecture, for example based on the Security Assertion Markup Language (SAML) and eXtensive Access Control Markup Language

[6] It is envisaged that the Security Assertion Markup Language (SAML) will be used for authentication. SAML also fits well into the authorisation architecture, since it supports transport of XACML request and response messages.

(XACML). The mobile device will therefore support different privacy and security profiles depending on which context they operate in. Some examples of such profiles are listed below:

Corporate profile The user participates in the work federation. The monitoring organisation can only see what is required for efficient attack detection. Focus on privacy and confidentiality towards third-party monitoring organisations. Perhaps somewhat less focus on personal privacy towards the employer.
Personal profile Access to private resources. Focus on personal privacy and confidentiality. May even have different mIPS subscription or provider in order to separate work and personal security handling.
Guest profile Restricted access to only make ordinary calls and send messages in case someone borrows the phone. No access to install anything. Attempted profile violations may be reported via the mIPS.
Payment profile Access to on-line e-banking applications. Higher security obligations required to reduce chance of fraudulent activities from malware like transaction hijacking for payment or e-banking. The payment profile used to log on to the bank's federation can for example have an *obligation* of continuous and updated antivirus and IDS operation to authorise the payment profile to run.
Forensic profile The CERT team can access everything on the device. Access typically requires consent either by the user or a court order.
IDS profile Used by the mIPS sensor. Gives the sensor software access to the MSS provider's location-aware mIPS service for sending alerts with locations or receiving updated threat profiles according to location.

These profiles mean that future mobile terminals will act as multi-user and multi-role devices utilising role-based access control instead of being single-user devices, which is the standard for mobile technology today.

Furthermore, each profile may be related to the federative environment the user interacts with. This means that the environment poses security and privacy obligations on the device. It is in this respect important that the system can trust that security services perform the job they claim to do. One way to implement this would be an obligation to check against an acceptable list of cryptographically signed security applications.

The federative policy and the mIPS policy are separate policies, in particular for outsourced managed security services. However the federative policy can require the mIPS policy to be active as a criterion for authorisation. This means that security and privacy requirements will change according to *time*, current *user role* and *location*. Different security and privacy profiles are needed in trusted environments like the home network or at work compared to when an employee is connecting to the network via an untrusted network provider like a WLAN source or a roaming provider. Even stricter security and privacy requirements may be required in environments known or expected to be hostile. Furthermore, different security requirements may apply during work hours, at home or when traveling.

Virtual machines can be used to provide a sufficient level of isolation between different user profiles. This would also give the user the opportunity to install any software that is desired on the personal profile, however virtual machine images for certain purposes could also be standardised and migrated from cloud services to the mobile device, based on a clean configuration in a trusted environment, to ensure that such profiles will not be infected by any malware initially when they are being run by the user. Another advantage with running the profiles in a virtual execution environment, is that a scheduler for the virtual execution environment would be able to optimise the processing of these profiles by migrating

threads or processes between the Cloud hosting provider and the mobile device, depending on connectivity and battery saving policies.

6.2 Forensic Interface

Mobile devices will not have the capacity to log information about all network traffic sent or received to the device. Digital forensics interfaces like Time Machines [22], that store some information from all network sessions, is therefore not viable for mIPS services on the mobile terminal. Such processing would take too much CPU power and battery. It would also be problematic from a privacy perspective. It is however possible that mobile devices in the future may have some kind of digital forensic interface to query the mobile terminal about network activities. For example using the Real-time Internetwork Defense protocol (RID) to set up traces to analyse malicious traffic [25]. There would also be sufficient bandwidth in 5G to perform remote export of logs, for example to a log server process outsourced to the Cloud hosting provider. Another alternative is if the logs were stored locally on the mobile device, and rather were protected from removal by adversaries by utilising a separate security domain (alternatively isolated in a separate virtual machine) protected by encryption. This could be done by leveraging future Mobile Trusted Platform Module's hardware support for encryption and access control via signed applications.

6.3 Bandwidth Policies

The amount of alerts may need to be reduced if the bandwidth is reduced or the link is overloaded. This will most likely not be an issue for 4G and/or 5G connectivity, but could be an issue for 3G services and would certainly be an issue if one is forced down to 2G services. Some possibilities for handling low bandwidth situations are:

Alert prioritisation Alerts can use a priority queue system to handle overload situations.
Data triage Another possibility is to use a technique similar to data triage[7] [29], to reduce the load when either the IDS is overloaded; the link is overloaded; or battery status is low.
Rule reduction Noisy rules with a majority of false positives could be prioritised down. However, this causes a risk of real attacks going undetected.
Data compression or reduction Reduce the overhead by sending compressed data or reduce the amount of data sent with IDS alerts.

Data reduction can cause an increased risk of missing true attacks, something that must be considered. Reduced alerting could for example be exploited if the attacker is able to limit the bandwidth and then hide an attack that is under the radar for what alerts that are being transmitted to the central server. This means that Rule reduction should be used with care, also because this causes a potential bias in the central location threat database. Data triage has similar problems like rule reduction in that this will cause a potential bias against the alerts not being transferred as part of the sampling process the data triage does. However, data triage can certainly be useful if the IDS is being overloaded, for example during Denial of Service (DoS) attacks.

It is presumed that data compression will be provided by the end-to-end encryption method used for conveying IDS alerts. Further lossy data reduction may be possible, however we

[7] The term triage stems from the sorting of and allocation of treatment to patients and especially battle and disaster victims according to a system of priorities designed to maximize the number of survivors. (see http://www.merriam-webster.com/dictionary/TRIAGE).

believe that an opportunistic approach where the IDS system performs temporary queueing of IDS alerts until sufficient bandwidth is available should suffice in all but extreme cases, like under DoS conditions. Also because the system is able to operate autonomously using the IPS functionality in low bandwidth areas.

Note that the design decision to have reactive IDS functionality means that the mIPS will be able to function autonomously in most cases. It is however important to prioritise serious attacks first in case of limited bandwidth, for example alerts indicating successful compromise of the mobile device that the IPS has not managed to deter. If a priority queue system with disk caching is used, then all alert messages can be sent when the bandwidth situation allows it, so that the IDS datawarehouse can get an updated threat picture also over areas with low or no internet connectivity.

It should be noted that the threats for a mobile system does not necessarily disappear if connectivity is lost. The reason for this, is that a mobile terminal usually has got several network interfaces (WCDMA, WLAN, Bluetooth) and supports both Internet and Telephony protocols. It may therefore be possible for malware like worms, viruses or Trojans to replicate even though Internet connectivity is not available, for example because the device entered an area with GSM-only coverage but without Internet connectivity and then was attacked locally via Bluetooth. This means that it may make sense to use a priority queuing system for alert data so that all alerts eventually will be sent, provided that the mobile device has sufficient disk space for intermediate alert storage.

6.4 Energy Saving Policies

The mobile terminal, including the mIPS, needs to follow an energy saving policy. It is in that respect important that the policy does not compromise the security and privacy of the device due to lack of battery power, since this would make the system more vulnerable to malicious attacks. The energy saving policy is therefore a local policy that aims at saving battery power without lowering the security of the device. It is designed to enforce that the IDS rules of disabled or powered down devices, inactive services or not installed programs are inactive. This avoids the mIPS from wasting CPU cycles on non-relevant tests. The user of a mobile device with almost empty battery could choose to power down Internet connectivity temporarily, in order to have sufficient battery capacity for ordinary calls or SMS-es. The mIPS would still operate, but now only checking SMS and phone connections on demand. The phone would not try to send any IDS alerts unless it reported a critical event, in which case enabling an Internet connection could make sense to transmit the message to the security operations centre.

Another way to save battery power, presuming that the phone runs a virtual machine with process migration support, is to use a power-aware scheduling mechanism that aims at migrating processes that are highly processor intensive with low to moderate I/O load to the Cloud hosting provider. It could for example be possible to migrate the mIPS monitoring to the Cloud in order to save battery power on computationally heavy intrusion detection processing and also leave more CPU power for other processes on the mobile device. This would not necessarily waste any radio bandwidth towards the mobile device if traffic can be routed from the mobile provider via the Cloud based mIPS and then to the mobile device, meaning that the mIPS basically would act as a router, anti-virus and application level firewall for the mobile device.

Using Cloud based virtual machines for performing the mIPS monitoring would be less efficient in other scenarios. For example if the mobile device is used as a modem or router,

then more than one network interface would be in use. In this case, packets towards the Internet would be routed via the mIPS, however the other interface would need to route traffic from this interface via the mIPS and then back to the device, which would be less efficient. In this case it may be more efficient to migrate the mIPS back to the mobile device, or operate with two mIPS instances - one in the Cloud and one on the device, to protect both interfaces. It would also be important with fail-over functionality, so that the mobile device is able to start its own mIPS instance in case it loses connection with the Cloud based mIPS instance.

6.5 Updating the Location Policies

The threat for a mobile device will to some extent change according to location. Some locations may be extra prone to physical theft based on prior information. Other locations may have a trusted 5G link, but has got a malicious WLAN link in the vicinity. Furthermore, there may be specific locations where Bluetooth attacks are more likely to occur and there may even exist rogue 5G providers. The Cloud computing environment may even to some extent need to move with the mobile device, in order to keep network latencies at an acceptable level. Roaming between different Cloud hosting providers means that there will be a different level of trust with different service providers.

This means that different threat profiles will be required in different locations. More invasive monitoring and stricter security obligations will therefore be required in less safe areas. In general, the home network can be expected to be more trusted than other networks the device roams through. Different profiles are in other words required in the home network compared to in other networks. Furthermore, one can not presume that WLAN networks are being actively managed, which implies less trust.

In order to handle location-based threats, the IDS sensor feeds location alerts (alerts with location data embedded) to the IDS PEP on the mobile device. The IDS PEP will then process the alert message differently for first-line and second-line operation. First-line operation operates in anonymised mode, and is allowed to store location data together with anonymised alerts, in order to perform first-line IDS operation and also maintain the location threat profiles. This ensures both that the first-line MSS service can monitor incoming mIPS alerts and that the IDS datawarehouse's location threat database can be updated continually.

The second-line operation gets access to full alerts, but not location data, in order to preserve the location and movement privacy of the user of the mobile device. It is here presumed that the second line CERT team will not have access to joining alert data with first-line location data. This means that the CERT team will not know the physical location of the mobile device until they potentially decide to investigate a suspicious event. In addition, a privacy preserving protocol for negotiating the threat profile from the THREAT-PEP for a given location is required. A solution for this is outlined in the next subsection.

6.6 Location-aware Privacy-preserving Solution for Mobile IDS

We assume that there is a finite set of threat profiles P that define protection measures, depending on the current threat level within the areas they are located and type of devices. Informally, a treat profile p from P may for example deny using Wi-Fi or Bluetooth communication when the user is physically located in some "less secure" area. We assume that there is a threat map M composed of sub-areas S_i with different security threats. Formally

we assume that $M = \{S_i | i = 1, \ldots, k\}$ such that $M = \bigcup_{i=1}^{k} \{S_i\}$ and $S_i \bigcap S_j = \emptyset$ for $i \neq j$. The mIPS sensors are continually updated when relevant threat policies in M change due to changes in the underlying threat picture. Each threat policy is represented in the form of a function $h : M \rightarrow L$ where $L = \{l_1, l_2, \ldots\}$ is a set of threat levels recognized by by the mIPS sensor and $h(S_i)$ denotes a current threat level within S_i where l_i is a threat level from L. Based on the type of mobile device *dev* and location sub-area S, the IDS defines what profile that should be used for protection. It can be defined as a value of a function $g(dev, l) \in P$ where $l = h(S_i)$.

The threat level $l \in L$ for each sub-area $S \in M$ is defined based on previous and current experience of security threats in this area. It depends on the number and kind of threats reported via IDS location alerts from the area. Therefore the location threat datawarehouse of the first-line MSS service needs to monitor the threat situation continually in order to adjust threat levels and inform the mIPS sensors in mobile devices when they need to update the profile.

Thus we assume that mobile devices will send threat related information to the location threat datawarehouse, which will include at least location *loc*, time *t*, device type *dev* and threat identifier *tid*. It will not include user identifying information to protect user privacy. Based on these data, the IDS will calculate the current threat level for the sub-area containing the location *loc* based on how severe the reported threat is. (We assume that all threats are weighted with respect to devices.)

One possible way to calculate the threat level is to calculate the weighted average within some specified period of time (day, week, month, etc.). However since both location sub-areas and threat levels of sub-area are changing during active use, threat profiles adopted by users need to be continually updated. The IDS will send new profile updates when it discover that either the user moved to a new sub-area or the threat level of the current sub-area was changed.[8] However our purpose is to propose a solution that preserves user privacy. We therefore require that the user's identity is unavailable to the first-line MSS. At the same time, each mobile device knows its own location.

In the rest of this section we sketch location privacy preserving solutions in the sense that exact user location can be negotiated without revealing the location of interest or the device identity to the first-line MSS.

In the first step, based on its location, a mobile device may anonymously (that is without disclosing the device identity) require from the first-line MSS a subset of $M' \subseteq M$ containing a specific set of one or more areas of interest. To do so, the IDS does not need to know the device identity, but only proof that device is a member of the IDS subscriber group. Many different approaches can be applied to solve the problem. SAML 2.0 for example supports the use of transient pseudonyms between the ID provider and the MSS service provider, meaning that the real identity of the user does not have to be revealed during federative authorisation [4].

Another possibility is a privacy preserving group membership based on homomorphic encryption [13,17]. This approach is feasible since authentication requests will not occur very often. It will depend on user mobility and the size of the subset of M used in the request, taking into consideration the capabilities of 5G as described in the previous sections. If necessary, the profiles sent out can be protected by broadcast encryption techniques [5], in order to ensure that only valid customers can decrypt the set of IDS profiles they subscribe to.

[8] It is better that the mIDS server pushes changed profiles to the clients than that they poll for changes, since it is not known in advance when profile changes will occur. This ensures an updated threat profile on the client and reduces the load from empty poll requests when there are no changes.

In the second step, by having partitions of M, each mobile device may send a threat profile update request to the first-line MSS provider each time it changes to a sub-area outside M'. The first-line MSS provider will at the same time remember those who requested threat profile updates and their subareas of interest M'. Each time the first-line MSS provider updates the threat levels for some sub-areas, it will inform those who requested such updates. Both to reduce communication intensity and protect user privacy, we assume that the user decides how large subset M' of M that should be used. By selecting bigger M', containing more sub-areas, users reduce the chance of being identified by increasing the anonymity set, at the cost of increasing the communicational load. Thus it will always be a trade-off between acceptable level of privacy and communicational load.

7 Security Analysis of mIPS

In this section we analyse new security attacks that may occur for location-aware mobile IPS systems.

7.1 SA1: Stalking Attack

7.1.1 Attack Description

A potential risk with an adaptive threat policy, is that the attacker can exploit variations in the threat profiles. The attacker can for example subscribe to the same IDS service provider as the victim using similar hardware, in order to reveal the location threat profile of the victim's mIPS system. The attacker may then be able to launch more targeted attacks to exploit weaknesses at locations where the location threat profile has weaknesses. One way is to stalk the victim and attack him at a location where the IDS profile is weak.

7.1.2 Mitigation

This attack is inherent in a system that presumes that threat varies according to location. The MSS provider therefore needs to design the IDS profiles with this attack in mind. The threat policy should in other words not be relaxed excessively, even in areas where attacks never have occurred.

7.2 SA2: Threat Elevation Attack

7.2.1 Attack Description

The attacker could also decide an opposite strategy - to elevate the threat level as much as possible by creating IDS alarms, to reduce the chance that certain network interfaces or providers were used or in the worst case cause denial of service, for example in order to steal bandwidth on that channel.

7.2.2 Mitigation

The practical implementation needs to consider these new attack strategies when composing threat profiles for location-aware mIPS. Location threat profiles should not have so strict security requirements that it causes a risk of Denial of Service for high threat profiles.

7.3 SA3: Malicious Cloud Hosting Provider

7.3.1 Attack Description

If the mobile device connects to a malicious Cloud hosting provider, then the confidentiality, availability and integrity of part or all of the virtual execution environment could be compromised. This could for example be passive surveillance based on virtual machine introspection or malicious virtual machine images.

7.3.2 Mitigation

The trustworthiness of a Cloud hosting provider could also be part of the location-aware mIPS service, in order to recommend the user to avoid services that may be dubious or malicious, or to select services based on a trustworthiness level that satisfies the current user's requirements. Furthermore, virtual disks should be encrypted. However a weakness may be that the virtual machines do not support encrypted memory, so that it can be hard to avoid that a persistent Cloud hosting provider can monitor the executing virtual machine. This can for example be done by inspecting the memory of other virtual machines, using functionality in the Virtual Machine Monitor/hypervisor that runs in Ring 0 with access to all physical memory.

7.4 SA4: Cloud Hosting Provider Unavailability

7.4.1 Attack Description

The virtual execution environment may temporarily or permanently become unavailable due to variations in the bandwidth or even that the link goes down. (We presume that the probability of the Cloud Hosting Provider going down is negligible compared to bandwidth problems.)

7.4.2 Mitigation

Important virtual machines, like for example the mIPS service, may need to be cached on the mobile device, so that they can be restarted locally in case of lost connectivity. In a similar way, a Cloud based mIPS service should have a watchdog timer that suspends the mIPS service if it loses connectivity with the mobile device.

7.5 SA5 Denial of Service Attacks

7.5.1 Attack Description

An adversary may perform Denial of Service (DoS) attacks, either based on attacking the radio channel for example using radio noise, bandwidth consuming attacks like Distributed Denial of Service (DDOS) attacks or targeting system vulnerabilities that cause Denial of Service. These attacks mean that Internet connectivity may be drastically reduced or in the worst case lost. In addition, some of these attacks may cause alert flooding of the mIPS.

7.5.2 Mitigation

IDS attacks causing alert flooding can to some extent be handled using threshold based rules, that send an alert with aggregated attack data when the threshold is reached. In other cases, it would be important that the mIPS is able to take over locally when connection to potential Cloud-based services is lost. In addition, alerts can be stored and transmitted once the attack is over. A further risk is that the mIPS itself may deplete the mobile device of CPU resources or battery under DoS attack. The mIPS can in this case notify the user, and tell that this device apparently is under a DoS attack, so that the user can decide to inactivate the network device under attack to save battery and CPU resources.

8 Privacy Analysis of mIPS

In this section we perform an analysis of privacy attacks against a Location-aware mIPS. We presume a Wireless Personal Privacy Intruder that basically has got Dolev-Yao intruder (DYI) capabilities for attacks via the communication channel [9]. The attacks we present are special in that they work by using the location-aware intrusion prevention system against the user.

Note that when we use phrases like "identifying the user" we do not necessarily mean that the intruder has knowledge of the actual user identity, but rather that the intruder can uniquely distinguish the user from other users. Thus there will be the concept of an implicit "acquired identity". We note that such an acquired identity may be specific to a certain service level (communications level/threat level). The intruder may therefore aim at artificially provoking the client to maintain a certain specific status in order to be able to track the 5G device.

If the user can be tracked though the acquired identity, then the intruder may reveal the true system identity of the device/user, for example using data mining techniques.

8.1 PA1: Traffic Analysis Attack Based on Recognizable/Distinguishable IDS Setting

8.1.1 Attack Description.

The device user has set the IDS policy such that the IDS client is continually, or at least frequently, in contact with the central IDS server. Traffic analysis may reveal that the IDS communication, while properly protected as such, may be recognizable by the WPPI as being IDS message exchanges. If the IDS policy generates specific patterns, then the WPPI may identify the user and determine its location using techniques like for example triangulation.

If the IDS traffic is continuous and/or executed on regular (fairly frequent) intervals then the WPPI may also be able track the user. Depending on circumstances, this may even allow the WPPI to break the confidentiality of user transactions, i.e. to derive statistically that the user took part of a said transaction.

8.1.2 Attack Mitigation

An efficient mitigation of this attack is to migrate the mIPS service to a Cloud hosting provider, which means that IDS message exchanges would not be visible on over-the-air interfaces. The attack can also be mitigated using best practices against traffic analysis. For example to send data at random points in time or continuously in order to make traffic analysis more difficult. It is also possible to route the IDS location alerts via Mixes [7].

Another mitigation strategy the user could use in this case, is to opt out from sending IDS alerts, but still subscribe to location threat profile updates. However, this would lower the security somewhat, since the first-line MSS provider would not be able to see events that indicated a successful attack on the mobile device.

8.2 PA2: Traffic Analysis Attack on the 5G Device

8.2.1 Attack description.

In the following scenario we assume that the WPPI issues an attack on one or more devices located in a confined area (called $Area_{A1}$).

The purpose of the traffic analysis attack is primarily to trigger the local IDS sensor such that it reports the incident to the central IDS datawarehouse. We now assume that the WPPI is able to detect such IDS status change through observations of the communications channel. Thus, this may permit the WPPI to selectively identify users. In itself this provides little information to the WPPI, but it may make it possible for the WPPI to individually target users within $Area_{A1}$. Thus identity- and location privacy may be compromised.

We furthermore assume that the WPPI triggered incident provokes the local IDS client and the IDS client to engage in more frequent communication (transfer of logs etc) then there may emerge a pattern which is recognizable to the WPPI. In this case that WPPI may be able to track the devices for the duration of the increased IDS communications activity. Thus, the WPPI may be able to intrude on the movement privacy of the user. If the tracking can be maintained for prolonged periods it will statistically be increasingly more likely that the intruder also learns about specific user transactions.

8.2.2 Attack Mitigation

This attack can be mitigated using the same techniques for traffic analysis avoidance as described in Sect. 8.1.1.

9 Related Work

This article builds upon similar ideas as the two-tier IDS architecture described in [33]. However, this article is extended to support a location-aware mobile scenario that includes partially outsourcing the execution environment to a pay-as-you-go Cloud hosting provider. It also contains a new privacy preserving algorithm for updating location profiles in mIPS. This includes separating location and movement privacy from transaction privacy by keeping the location data in the anonymised first-line service, whereas full IDS alert data without location is sent to the second line operation. Furthermore, it is not viable and probably not desirable from a personal privacy perspective to use continuous packet logging techniques like Time Machines on mobile devices for forensic purposes. Our solution instead proposes that it may be possible to add trace requests using the Real-time Internetwork Defense mechanism on devices undergoing forensic investigation.

Mobile IDS is still in its infancy, partly due to hardware and software limitations in some of the existing mobile platforms. Packet filtering, IDS and firewall functionality is for example not yet widely available for smartphones. However it can be expected that these limitations will disappear as mobile terminals evolve and mature. There exists a few prior examples of mobile IDS systems. An anomaly-based IDS for smartphones is presented in [30]. The

proposed system uses a small set of features that provided the best correlation for clustering a known set of malware attacks based on a principal component analysis. The features investigated are: the amount of free memory, number of TCP/IP connections, CPU usage, battery charge level, user idle time, disk space, threads and network cell ID. The system exports a set of feature set samples at regular intervals (every 20s) to a central unit that performs the anomaly detection based on amongst others self-organising maps. This is an interesting concept that should be viable also for today's phones. It is however limited what kind of intrusions that can be detected using such a scheme, so future IDS systems will probably also need to use other technical approaches.

The BRO IDS supports a way to anonymise the payload of a packet instead of removing the entire payload [21,27]. Our solution is different, since it anonymises IDS alerts instead of anonymising the captured packet traces. This is sufficient in a scenario where first-line security analysis has been outsourced.

There exists some earlier work on privacy-enhanced host-based IDS systems that pseudonymise audit data and perform analysis on the pseudonymised audit records [6,11,15,31,32]. A similar approach is further elaborated in [12], which builds the privacy policy into the IDS rules by defining a privacy-preserving rule language that pseudonymises payload and other information that is defined as sensitive. Kerberos [24] is used for authentication. This approach focuses on reversible protection mechanisms using cryptographic techniques for pseudonymisation. However neither of these consider the location and mobility aspects of mobile IPS systems.

10 Conclusions and Directions for Future Work

We have suggested a two-tier architecture as a first approach towards better privacy protection for mIPS. A potential disadvantage with the proposed architecture, is that IDS alerts are duplicated and sent both to the first- and second line operation. However, we regard the extra bandwidth requirement to be unproblematic under normal conditions in 5G networks and can be handled by techniques like priority queues and Data Triage during DoS and other overload conditions.

The proposed solution supports querying location threat profiles in a privacy-preserving way. In addition, it may be beneficial to migrate the mIPS service from the mobile device and to a Cloud hosting provider in order to save battery power and CPU processing capacity. However the mIPS must also be able to run on the device, for example if there is no or insufficient Internet connectivity, or if the mobile device is routing packets between several interfaces.

We have also outlined how profile handling could be done for an envisaged 5G mobile device under changing environments like bandwidth variation, limited battery capacity and connection to different federative systems. The profile handling can furthermore benefit from isolating the execution environment of different profiles in different virtual machines running on the mobile device. Furthermore, there are some potentially new attacks on the anonymity of location-aware mIPS and we have suggested mitigation strategies for these.

The most serious new attack against location-aware mobile IDS systems, is perhaps so-called *stalking attacks*, where the adversary can exploit potential weaknesses in the location threat profiles by subscribing to the same service, and then stalks the mobile user and attacks him at a location where the IDS service has a weak profile in order for the attack to go undetected. The managed security service provider and the mobile user subscribing to such

services should in not presume any area to be unconditionally safe. There should in other words be some minimum level of security built in to all threat profiles.

We intend to continue our work with some of these promising research directions with the objective to demonstrate a working prototype of a mobile location-aware reactive IDS system. This will both provide empirical data on the efficiency of the proposed solution and improve the strategies for rule profile handling.

Acknowledgments This work is funded in part by Telenor Research & Innovation under the contract DR-2009-1.

References

1. 3GPP TS 31.101. (2009). 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; UICC-terminal interface; Physical and logical characteristics (Release 9).3GPP, Sophia Antipolis, Valbonne, France, 12.
2. 3GPP TS 33.401. (2009). 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture; (Release 9). 3GPP, Sophia Antipolis, Valbonne, France, 12.
3. 3GPP TR 36.913. (2009). 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Requirements for further advancements for Evolved Universal Terrestrial Radio Access (E-UTRA) (LTE-Advanced) (Release 9). 3GPP, Sophia Antipolis, Valbonne, France, 12.
4. Alrodhan, W., & Mitchell, C. J. (2008). A delegation framework for liberty. In *Proceedings: 3rd conference on advances in computer security and forensics, (ACSF 2008)* (pp. 67–73). Liverpool, UK: Liverpool JMU.
5. Attrapadung, N., & Kobara, K. (2003). Broadcast encryption with short keys and transmissions. In *Proceedings of the 3rd ACM workshop on digital rights management* (pp. 55–66). Washington, DC, USA, ACM.
6. Büschkes, R., & Kesdogan, D. (1999). Privacy enhanced intrusion detection. In G. Müller & K. Rannenberg, *Multilateral security in communications, information security* (pp. 187–204). Reading, MA: Addison Wesley.
7. Büsckes, R. & Kesdogan D. (1999). Privacy enhanced intrusion detection. In *Multilateral Security for Global Communication - Technology, Application, Business*. Addison-Wesley-Longman.
8. Debar, H., Curry, D., & Feinstein, B. (2007). The intrusion detection message exchange format (IDMEF). http://www.ietf.org/rfc/rfc4765.txt.
9. Dolev, D., & Yao, A. (1983). On the security of public-key protocols. *IEEE Transactions on Information Theory, 29*(2), 198–208.
10. Feinstein, B., & Matthews, G. (2007). The intrusion detection exchange protocol (IDXP). http://www.ietf.org/rfc/rfc4767.txt.
11. Fischer-Hübner, S. (2007). *IDA-An intrusion detection and avoidance system (in German)*. Aachen: Shaker.
12. Flegel, U. (2007). *Privacy-respecting intrusion detection*. Newyork: Springer.
13. Freedman, M. J., Nissim, K., Pinkas, B. (2004). Efficient private matching and set intersection. In *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *Lecture notes in computer science* pp. (1–19). Springer.
14. Garfinkel, T., & Rosenblum, M. (2003). A virtual machine introspection based architecture for intrusion detection. *In Proceedings network and distributed systems security symposium* pp. (191–206).
15. Holz, T. (2004). An efficient distributed intrusion detection scheme. In *COMPSAC Workshops* pp. (39–40).
16. ITU-R (2008). REPORT ITU-R M.2133, Requirements, evaluation criteria and submission templates for the development of IMT-Advanced. Technical report, ITU, 12.
17. Kissner, L., & Song, D. (Aug 2005). Private and threshold set-intersection. In *Proceedings of CRYPTO '05*.
18. Køien, G. M. (2007). Subscriber privacy in cellular systems. *Telektronikk ISSN, 0085-7130*(103), 39–51.
19. Køien, G. M., & Oleshuck Vladimir, A. (2007). Personal privacy in a digital world. *Telektronikk ISSN, 0085-7130*(103), 4–19.
20. Køien, G. M., (Oct 2009). *Entity authentication and personal privacy in future cellular systems*. The River Publishers Series in Standardisation.

21. Lawrence Berkeley National Laboratory. Bro intrusion detection system. http://bro-ids.org.
22. Maier, G., Sommer, R., Dreger, H., Feldmann, A., Paxson, V., & Schneider, F. (2008). Enriching network security analysis with time travel. *SIGCOMM Computer Communication Review, 38*(4), 183–194.
23. Marchiori, M. (Ed). (2002). The platform for privacy preferences 1.0 specification. http://www.w3.org/TR/P3P.
24. MIT Kerberos Team (2009). Kerberos: The network authentication protocol. http://web.mit.edu/Kerberos.
25. Moriarty K. M., & Trammell, B. H. (2008). IODEF/RID over SOAP. http://www.ietf.org/internet-drafts/draft-moriarty-post-inch-rid-soap-05.txt.
26. Moses, T. (Ed). (2005). OASIS eXtensible Access Control Markup Language (XACML) Version 2.0. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.
27. Pang, R., & Paxson, V. (2003). A high-level programming environment for packet trace anonymization and transformation. In *Proceedings of the 2003 conference on applications, technologies, architectures, and protocols for computer communications* (pp. 339–351), Karlsruhe, Germany ACM.
28. Powers, C., & Schunter, M. (Ed) (2003). Enterprise privacy authorization language (epal 1.2). http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/ .
29. Reiss, F., & Joseph, M. H. (2004). Data triage: An adaptive architecture for load shedding in TelegraphCQ. In *In ICDE* pp. (155–156).
30. Schmidt, A.-D., Peters, F., Lamour, F., Scheel, C., Çamtepe Seyit, A., & Sahin, A. (2009). Monitoring smartphones for anomaly detection. *Mobile Networks and Applications, 14*(1), 92–106.
31. Sobirey, M., Richter, B., & König, H. (1996). The intrusion detection system AID - architecture and experiences in automated audit trail analysis. In *Proceedings of the IFIP TC6/TC11 international conference on communications and multimedia security* pp. (278–290).
32. Sobirey, M., Fischer-Hübner, S., & Rannenberg, K. (1997). Pseudonymous audit for privacy enhanced intrusion detection. In *Proceedings of the IFIP TC11 13th international conference on information security (SEC'97)* pp. (151–163).
33. Ulltveit-Moe, N., & Oleshchuk, V. (2009). Two tiered privacy enhanced intrusion detection system architecture. In *IEEE International workshop on intelligent data acquisition and advanced computing systems: technology and applications, 2009. IDAACS 2009* (pp. 8–14).

Author Biographies

Nils Ulltveit-Moe is a research fellow at University of Agder in Norway. He holds a B.Sc. in Telecommunications from University of Agder (UIA, then AID) and a M.Sc. in Cybernetics from University of Stavanger (UiS, then HSR). He has previously worked with software development for Ericsson and computer security for Proseq AS. He furthermore participated in the EIAO IST project doing research on large scale automatic assessment of web accessibility. In addition, he has worked as Assistant Professor at UIA since 1998, giving courses amongst others on data communication, client/server programming, operating systems, directory services, Python programming and computer security. He is currently pursuing his Ph.D. doing research on privacy enhanced network monitoring systems.

Vladimir A. Oleshchuk is Professor of Computer Science at University of Agder, Norway. He received his M.Sc. in Applied Mathematics (1981) and Ph.D. in Computer Science (1988) from the Taras Shevchenko Kiev State University, Kiev, Ukraine, and his M.Sc. in Innovations and Entrepreneurship (2007) from the Norwegian University of Science and Technology (NTNU). From 1987 to 1991 he was Assistant Professor and then Associate Professor at the Taras Shevchenko Kiev State University. He has been working at University of Agder since 1992. He is a member of IEEE and a senior member of ACM. His current research interests include formal methods and information security, privacy and trust with special focus on telecommunication systems.

Geir M. Køien is a postdoctor at the University of Agder, Norway, where he works with cellular system, access security, personal privacy and similar topics. He holds a B.Sc. hons in Computing Science from the University of Newcastle upon Tyne, England, a M.Sc. in IT from the Norwegian University of Science and Technology (NTNU, then NTH), and a Ph.D. from Aalborg University (AAU). Køien has previously worked for Telenor R&I, and participated in security standardization in 3GPP during 1999–2009 as the Telenor delegate. He has worked extensively with access security in GSM/GPRS, UMTS and LTE.