# Protecting Large-scale IT systems developed and/or managed by eu-LISA from modern threats

A review of recent developments in IT security and associated technologies

## Contact

To contact the main author for further information, please e-mail:
research@eulisa.europa.eu

For enquiries regarding further use of the paper or the information contained herein, please contact:
communications@eulisa.europa.eu

## Legal notice

This report has been produced to provide up-to-date information that can inform discussion on the large-scale IT systems operated by eu-LISA and associated infrastructures at Agency and at national levels. Any views expressed in the report are entirely those of the author acting in his capacity as Research and Development Officer of the Agency and are not necessarily the views of the Agency itself.

Where products made available by specific vendors are referenced, directly or indirectly, this should not be taken as any endorsement by the Agency; references are provided purely for the purposes of embellishing points made in text.

All web-address links provided were confirmed to be functional on August 31st 2016.



eulisa.europa.eu

ISBN 978-92-95208-46-9
doi:10.2857/320307
Catalogue number: EL-01-16-835-EN-N

# Table of Contents

# Executive Summary

Security must be a core element of all activities undertaken in an IT-focussed organisation. eu-LISA, for legislative reasons but also as a centre of excellence in the provisions of IT services, emphasises assurance of system and data security in all of its activities. Modern technology when appropriately chosen and implemented facilitates strong IT security and information assurance. Yet such is the range of technological innovations on the market and in the final stages of product development that appropriate decision making on implementation can be difficult. This document, based on monitoring of technologies and their development in the past year, seeks to report on the state of current and emerging cybersecurity-relevant technologies. Implementation of available and necessary technologies is an important element of this work. It provides an operational, EU and eu-LISA centric viewpoint and should be interesting to the decision makers at Agency level as well as in partner and stakeholder organisations.

Any analysis of technical requirements in the area of IT security requires understanding of emerging threats. In this regard, it is worth noting rather frequent recent instances of zero-day vulnerabilities being discovered in widespread and common software (e.g. POODLE, Heartbleed), an increasing prevalence of highly targeted attacks against government systems (e.g.CosyDuke) and specific end users (e.g. through waterholing) and the rise of hacktivism. In general, the increased frequency and sophistication of external threats should cause concern, while insider threats whether through malevolent or non-intentional actions must always be considered. Technological developments can certainly help to guard against the various threats identified.

Analysis of how appropriate a technology may be for implementation in the organisation also requires assessment of that organisation's capabilities to correctly deploy and subsequently maintain it to the highest standards. For this reason, it is important to reflect, at least briefly, on organisational arrangements that should be in place *a priori* so that one may consider the cutting-edge technologies enumerated herein. Organisations must frequently and comprehensively deploy patches and updates, for example. Collaboration with partners to continually update knowledge on threats is also important, as is training targeting end users who often provide the conduit into a system for determined attackers.

Assuming that such basic arrangements are in place, one can go on to consider the state-of-the-art in cybersecurity technology. Ten technologies/technology categories are identified as being of most interest from the eu-LISA perspective, based both on their topicality but also their capabilities to address emerging threats. The identified technologies are highlighted to help stimulate and/or guide further analyses on the state of technical cybersecurity preparedness against such threats in any organisation.

1. Big data for behaviour-based threat assessment and malware detection
2. Pervasive sandboxing
3. Machine-readable threat intelligence
4. Adaptive access control
5. Permissioned ledgers
6. Hardware random number generators
7. Hashing using SHA-2 or better primitives
8. Encryption key hierarchies
9. Grid computing
10. Advanced DDoS protection

The breadth of technologies identified provides an indication of the rapid pace of change and

development in the domain. It is therefore concluded that monitoring of technological developments in the area of IT security is fundamental in an organisation involved in IT system development and/or management and/or service provision. The topic of IT security will therefore be revisited by eu-LISA in a future report of this nature while technology watch functions will continue to be embedded into the organisation and specifically its security-focussed groups to continuously contribute to the identification of new and relevant developments in the IT security domain going forward.

# 1. Introduction

According to Articles 1(3), 8 and 9 of its establishing Regulation, eu-LISA shall monitor developments in research relevant to the operational management of the SIS II, VIS and Eurodac systems the operations of which they are currently responsible for and undertake investigations of potential relevance to IT systems which may come under the control of the Agency in the future. Knowledge regarding developing technologies and research efforts underway in relevant fields is acquired according to methods and procedures laid down in the Agency Research and Technology Monitoring Strategy 2015-2017. The strategy, approved by the Agency's Management Board at the March 2015 meeting, provides for the publication of bi-annual research reports. This report is the first such report to be released in 2016.

The report examines the cutting edge of technological developments in the domain of IT security. The afore-mentioned establishing Regulation, as well as the regulations associated with the three large-scale IT systems, detail the need for security to be a foundation stone in all IT-related activities, in particular indicating that the Agency 'shall ensure effective, *secure* and continuous operation of large-scale IT systems'.[1] Furthermore, as a result of such regulations or because of stakeholder demands, the Agency's dedicated security team seeks to ensure continuous and secure exchange of data between national authorities and the Agency and to provide for efficient internal and external systems as necessary to provide quality end-user service and to support the Agency's evolution into an EU ICT centre of excellence. IT security is thus very relevant for the operational management of SIS II, VIS and Eurodac. Furthermore, as detailed below, the domain has rapidly involved in recent times, with new threat types and modalities of attack presenting. Technological advancement is necessary to keep up with the pace of change in this domain. This report is prepared, therefore, at an opportune time to take stock of the current state of play in the field of cybersecurity, both in terms of the attack and defence landscapes, as well as to analyse state-of-the-art and developing technologies that might be interesting for the Agency and/or its partners going forward as existing security measures evolve and are enhanced.

The Cybersecurity Strategy for the European Union, issued in 2013, along with the European Agenda on Security, published in 2015, provide the overall strategic framework for EU initiatives on cybersecurity. A roadmap that attempts to translate the Cybersecurity Strategy into concrete actions has been developed. In 2013, the Commission also put forward a proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union; the co-legislators agreed on the text of the so called Network and Security (NIS) Directive in late 2015 with actions to translate the contents of the directive into national law to be anticipated in the coming months. On 25 May 2018 the General Data Protection Regulation of the European Union will become applicable for all activities in which the personal data of EU citizens is processed; the Regulation introduces technologically neutral rules for protection of data, increases the obligations on data processors to disclose the steps they take to protect the data and requires operators to invest in technologies such as anonymization and encryption. Thus, the domains of data protection and security are necessarily related and increasingly overlapping. All referenced documents highlight, amongst other things, the need to enhance cybersecurity capabilities across borders and between different parties, cooperation and information exchange. In the roadmap document following up on the Cybersecurity Strategy, eu-LISA is mentioned as one party that can contribute to wide-ranging efforts to achieve cyber resilience within Europe, including by taking all necessary actions to ensure their

[1] Article 2(a) Regulation (EU) No. 1077/2011.

own security and sharing the knowledge and expertise gained with other parties. This document is one element of work contributing to the drive for enhanced cybersecurity at both national and European levels and one means by which information is being communicated as widely as possible.

## 1.1. Purposes of this report

This report seeks to describe and briefly discuss the most relevant recent technological developments and trends in the domain of IT security.

Discussions are generally limited to identification of technologies alongside their general uses, with reflections on how the technologies identified are applicable to organisations like eu-LISA added where possible and appropriate. In this regard, the overarching goal is to focus on the most recent developments and, where possible, anticipated outputs of cutting edge research. The report may be seen, therefore, as a review of relevant technologies and their recent developments, tailored towards those of most interest to the Agency and thus the security of large-scale IT systems generally.

It is important to note that the current state of security of existing systems is not examined in any way nor is the means to best implement any new technologies in eu-LISA systems. Full consideration of whether any technologies described herein should be considered for actual implementation would require a full security evaluation of the systems as well as a thorough risk analysis that bears in mind the Agency's threat landscape and business requirements, both of which are outside the scope of this document. The material herein should certainly help in the identification of possible technological solutions to address areas of concern that might be noted following execution of such analyses. It also should help to highlight the evolution of the threat landscape itself in recent times as a means of providing input to such evaluations. Finally, by providing an operational, EU and eu-LISA centric viewpoint on new technologies in the field of IT security, the report should provide interesting insight for stakeholders regarding the potential applicability of new and innovative technologies going forward.

It is important to emphasise that the scope of the report is limited and the recommendations made are not intended to form a baseline for preparation of any particular cybersecurity strategy nor define a minimal set of controls that should be undertaken. The recommendations relate to the trends identified from technology monitoring work and thus are more developed in some areas than others. As they emphasise the areas of most recent flux, they touch on areas in which a party may have to develop its capabilities and thus they are anticipated to be a useful reference point for those who already have a baseline cybersecurity strategy and wish to advance it further. However, different resources should be used in order to provide a full mapping of cybersecurity within any entity.[2]

## 1.2. Target Audience

The report is intended for distribution to interested parties within national governments, European Institutions and other European Agencies and will also be used as an input to discussions within eu-LISA. Stakeholders who manage and/or develop corporate or larger-scale IT systems within all of these entities will find material of interest because of the general approach taken to identification of new and interesting

[2] For example, the NIST Framework for Improving Critical Infrastructure Cybersecurity or the ISO 27001 and ISO 27000 family of international standards for information security management.

technologies. Readers are invited to combine the information contained herein with that arising from full systems analyses in order to make positive decisions regarding the evolution of their systems that take a full knowledge of the technological state-of-the-art into account. As eu-LISA's large-scale systems involve deployment of hardware and software that interfaces with systems at Member State level and in other EU Agencies, the Agency encourages all parties to continuously improve the security of their IT infrastructure and to use the most modern technologies as appropriate. It is clear that improved security of systems at all levels will result in enhanced security of the full large-scale IT ecosystem.

## 1.3. A note on terminology

In this report, the terms IT security, computer security and cybersecurity are used interchangeably. As per the NIST definition,[3] cybersecurity is 'the ability to protect or defend the use of cyberspace from cyber-attacks'. The document describes technologies that could be applicable in the implementation of IT- or cyber-security measures that guard against such attacks. It should be noted when speaking of 'attacks', however, that threats can arise from internal or external sources and may result from intentional or accidental actions. Such threats may relate to hardware, software or information on systems and cybersecurity for our purposes involves taking steps to address vulnerabilities in all regards. Although an attack typically involves hostile or unfriendly actions, a cybersecurity risk analysis should also consider the possibility of non-malevolent actions impacting upon systems. In this report, cybersecurity measures targeting all aspects of cyberspace in its broadest sense are covered, including computers and networks and both physical and virtual spaces. In all cases, the main criterion for inclusion of a technology is its topicality in terms of recent developments.

As regards threats to information, information security or information systems security (infosec) is a closely-related field, dealing with protection of information systems against unauthorised access to or modification of information. As all eu-LISA systems contain sensitive information, any attack on its systems is likely to entail a threat to information, and thus for our purposes information security may be considered to be equivalent to cybersecurity.

The term information assurance (IA) has been widely used recently, being the term of choice in the Council decision on the security rules for protecting EU classified information (EUCI).[4] Communication and information systems in Europe need to handle EUCI in accordance with the concept of information assurance, defined in NISTIR 7298 as 'measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.' The concept is also applicable for systems processing sensitive data, such as those managed by eu-LISA. In general, information assurance is considered as being wider in scope than information security. IA has been considered as an important goal in this report and technologies enabling improved information assurance are identified and discussed.

In this report, any technology relevant for protecting and/or defending systems or the data and information thereon, as well as the software and hardware on which the systems run, is of potential interest, no matter the source of the threat.

---

[3] NISTIR 7298 Revision 2. Glossary of Key Information Security Terms. May 2013. Available at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[4] Document 2013/488/EU – Council Decision of 23 September 2013 on the security rules for protecting EU classified information

A frequently noted issue in the field of cybersecurity is the lack of a uniform or consistent vocabulary used by communities or even by individuals within the same communities.[5] In this regard, standardisation efforts have been recently promoted.[6] Until such efforts reach fruition and definitions thus created become widely known and applied, readers should take care to ensure that terms are not misunderstood. Definition of further terms beyond those referenced in the first part of this section goes beyond the purposes of this report. Any other terms used should be understood in the context in which they are used herein only.

## 1.4. Structure of this report

Several frameworks exist in computer security for the categorisation of activities, outcomes, threats or requirements. These frameworks can be adapted across sectors and are typically used to guide organisations as they devise cybersecurity strategies, assess the state of their cybersecurity activities and identify risks. In these regards, the main goal is inevitably to align activities with resources and business needs.

The CIA triad of confidentiality, integrity and availability is a classic paradigm that is often cited in information security circles as highlighting the various areas in which the threat landscape must be assessed. Confidentiality relates to efforts to ensure that information is not available or disclosed to unauthorised individuals. Confidentiality of the personal data present on eu-LISA managed systems is a legal imperative as already mentioned, and therefore of upmost importance. Integrity means assurance of the accuracy and completeness of data without inappropriate or unauthorised modification over time. When considering threats to data integrity, one might be reminded of the words of the US Director of National Intelligence, James Clapper, in September 2015, when he noted that "the next push on the envelope is going to be the manipulation or the deletion of data which would of course compromise its integrity", undermining confidence in data stored. Clearly the risks are high and emphasis must be placed on security systems and data against such attacks. Systems must be fully available when needed in order to serve their purposes, hence the inclusion of the third element of the triad as a crucial component of an information security plan.[7]

Another framework often used describes the different types of activity typically associated with cybersecurity analyses and risk management activities, placing them under the headings – Identify, Protect, Detect, Respond and Recover.[8]

Activities typically covered under the 'Identify Function' are associated with understanding of business requirements, resource availability and risks. Clearly such an analysis will be individual and specifically tailored for any organisation; in this report, 'identify' activities are touched upon only in Section 2 in which recent news and developments of relevance are enumerated – this effort, undertaken here in order to

---

[5] See, for example: At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. David Clark, Thomas Berson and Herbert S. Lin, Editors. National Research Council of the National Academies, Washington DC. 2014. Available at: http://www.nap.edu/catalog.php?record_id=18749

[6] CEN/CENELEC/ETSI Cyber Security Coordination Group. White Paper No. 01. Recommendations for a Strategy on European Cyber Security Standardisation. 2014.

[7] For eu-LISA, continuous operation of large-scale IT systems is a legislative imperative laid down in Article 2 of the Agency's Establishing Regulation.

[8] Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0 National Institute of Standards and Technology. February 12 2014.

examine the changing threat landscape, should contribute to risk assessment efforts.

Activities to protect IT systems from attack often involve implementation of technological solutions alongside measures associated with physical or personnel security. Nevertheless, there is widespread acceptance that no protection mechanisms can be 100% effective and thus efforts to detect a cybersecurity event must also be considered. Such 'detect' activities also frequently involve the use of technology. 'Protect' and 'Detect' functions are thus the core areas of attention herein. Chapter 3 on integrity includes categorisation of technologies according to whether they seek to protect a system or rather detect intrusions, typically through detection of anomalies of changes. It should be clear, however, that technologies like malware scanning seek evidence of intrusions that can lead to compromises of data integrity and confidentiality, and indeed threats to system and data availability.

Activities under the 'respond' and 'recover' functions deal with efforts to deal with a cybersecurity event (e.g. communication, analysed, mitigation etc.) and recover in a resilient manner (e.g. recovery planning, post-event improvement etc.). These activities are typically analysed in detail in an organisation's business continuity plan. Such plans may include technological solutions to enable more efficient or effective responses or recovery to attack and these solutions are covered in some detail in section 6 on availability.

Finally the PDCA approach to security improvement of ISO 27001 warrants mention, specifically describing how one should sequentially undertake plan-do-check-act cycles during deployment and operations of all security-related actions in order to sustain a desired state of security. The approach can be applied to any system, procedure, technology, practice or change and should be applied iteratively.

This report, focussed as it is on technology, doesn't require adherence to any particular framework of approach amongst those mentioned. However, technologies, where appropriate, are identified as being useful for identification, protection, detection, response or recovery. The NIST framework built around the 5 pillars - Identify, Protect, Detect, Respond and Recover – has been used to ensure an over-arching and comprehensive analysis which reflects on technologies for different purposes and with complementary capabilities in the context of an overall security management plan. It is important to note, however, that the technologies themselves, once chosen and deployed, will have to be continuously monitored and frequently improved according to the PDCA approach or similar.

Some elements of a cybersecurity plan are nevertheless transversal and cannot be categorised neatly under the headings mentioned in the previous paragraphs.

The structure of the document is as follows:

- In Chapter 2, emerging threats are discussed as a means to frame the ensuing discussion and highlight the most relevant issues that need to be addressed through technological advancement. Threats of most relevance to eu-LISA are highlighted.
- In Chapter 3, transversal topics are mentioned, taking recent news discussed in the previous section as a basis for identification of tasks and activities that are crucial for any organisation using IT to undertake no matter what their level of risk appetite or the level of resources available.
- In Chapter 4, technologies of note are enumerated, categorised according to their use in a typical organisation's security architecture. Short reflections are also provided as to how and why the identified technologies should be interesting for eu-LISA and its stakeholders.

# 2. Emerging threats

Any effort at full cybersecurity risk analyses and risk assessments requires a good understanding of the cyber threat landscape as it stands. Such full analyses are undertaken by specialist entities regularly, typically to allow tailored development of products for defence, updating of guidelines for protection or similar. In the latter regard, ENISA publish regular analyses, for example.[9] The purpose of this section is rather to focus on those stand-out attacks that are relevant for eu-LISA and its closest stakeholders and/or for large-scale IT systems and those that highlight particular trends that are deemed particularly worthy of note. Additionally, threats that can be addressed through technology are most in focus. Thus, attacks on payment systems, although commonplace nowadays, are not covered. Furthermore, threats associated with physical attacks, disaster, outages or legal issues are not within scope – though they must be covered in any comprehensive security strategy, typical cybersecurity technologies are not useful in these regards.

The threats noted are framed according to the ENISA threat taxonomy.[10]

## 2.1. Recent high-profile events

IT systems are under threat from internal and external actors, through both nefarious and unintended actions. Throughout this document, when we speak of 'attacks', it should be clear that the attacker is not necessarily external to the organisation, and furthermore, his/her actions may not be undertaken with the purpose of compromising that system. Nevertheless, the most high-profile attacks typically involve external parties purposely compromising important computer systems. Technologies that guard against such attack types and vectors are the main focus of this report, although it may be noted that several of the mentioned technologies are also helpful in preventing or detecting internal attacks, even those based on negligence rather than mal-intent.

A number of recent high-profile events are enumerated as an introduction to this section. The selection is made to highlight the variety of dangers that are present, sometimes increasingly so in recent times, and thus to give some indication of the importance of emphasising comprehensive cybersecurity in the enterprise.

High-profile attacks can be described based on:

1. The attacker and target
2. The route used to infiltrate the system
3. The approach to system compromise

Events are chosen to highlight trends associated to each aspect. The events are also categorised according to the most prominent threat that they reveal, using the ENISA taxonomy. However, the event in many cases arose because of exploitation of several threats. Social engineering, for example, can provide a route into a system while malware subsequently placed on the system can allow data exfiltration – in such cases, threats including social engineering, rootkits, worms, Trojans, spyware etc. can all become apparent successively or simultaneously.

### 1. The attacker and target

[9] See, for example, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends
[10] ENISA Threat Taxonomy. A tool for structuring threat information. Version 1.0, January 2016.

### *Attacks on Governments*

### High level threat – Eavesdropping/ Interception/ Hijacking

#### Threat – Interception of Information

In late 2014, the US government confirmed a particularly significant attack against their internal servers.[11] A subsequent attack first reported in October 2015 (so-called CosyDuke) and reported to come from Russia succeeded in providing access to the email correspondence of US President Barack Obama.[12] Security experts indicated that the attack was based on highly specific spear phishing in which people close to the president were induced to click on email links that allowed installation of malware into the system. Interestingly, the malware included notable detection evasion techniques and evolving cryptographic capabilities.[13]

When considering attacks on government, the infiltration of the email account of the CIA director John Brennan is noteworthy to the extent that it demonstrates the possibility of accessing confidential personal and company information through attacks on single parties who may use non-secure personal accounts. It was reported that the hacker was a high school student who obtained access using social engineering techniques targeting the director's service provider.[14] The same hacker/group subsequently went on to release information regarding law enforcement employees and obtain access to other materials, potentially federal arrest records being exchanged through FBI information-sharing portals.[15] In a similar vein, an attack on the US Offices of Personnel Management resulted in the leakage of the personal information of more than 22 million people who had applied for governmental jobs.[16] Recently, the possible detrimental effects of cyber-attacks against national public critical infrastructure were highlighted when part of the Ukraine saw its power grid go dark due following online attacks.[17]

The use of the Regin malware against the Belgian telecommunications company Belgacom is worth noting in a similar vein, particularly as it allowed for the gathering of data belonging to Belgacom customers including the European Commission, Parliament and Council.[18] The sophistication of the malware deployed was highly suggestive of nation-state development.

### *Hacktivism*

### High level threat – Unintentional damage/ loss of information or IT assets

#### Threat – Information leak /sharing due to human error

A number of attacks on private companies in recent years are notable because of the extent to which they have, or at least had the potential to, destroy reputations and/or extort money. Hacking Team is a controversial spyware company that sells intrusion and surveillance software to governments and law

[11] http://readwrite.com/2014/10/29/white-house-confirms-cyber-attacks
[12] http://www.ibtimes.co.uk/russian-hackers-read-barack-obamas-emails-during-white-house-cyber-attack-1498462
[13] https://securelist.com/blog/research/69731/the-cozyduke-apt/
[14] http://nypost.com/2015/10/18/stoner-high-school-student-says-he-hacked-the-cia/
[15] http://www.bankinfosecurity.com/hackers-claim-fbi-information-sharing-portal-breach-a-8667/op-1
[16] https://www.opm.gov/cybersecurity/cybersecurity-incidents/
[17] http://www.cnet.com/news/were-fighting-an-invisible-war-in-cyberspace/
[18] https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/

enforcement agencies worldwide[19] - part of the growing trend of outsourcing coding and sale of code for profit. In July 2015, the company itself was hacked with 400GB of internal documents, email communications, user credentials and even zero-day exploits.[20] Ashley Madison, an online portal for extramarital affairs was hacked resulting in the release of customer names, email addresses and credit card information and the eventual fall of the CEO.[21] Kaspersky, a leading anti-virus software provider, also had its systems compromised in summer 2015 with some corporate files known to have been accessed.[22] The code used was apparently based on the Duqu Trojan and had been used in other environments associated with global political activities.

## 2. The route used to infiltrate the system

### *Exploiting hardware or software vulnerabilities*
### High level threat – Nefarious activity/ abuse

#### Threat – Manipulation of Hardware and Software

Loss of information can arise because of abuse of vulnerabilities in deployed hardware or software. In a typical case, the identification of the so-called OpenSSL Heartbleed bug[23] in 2014 caused great concern amongst the global IT community and teaches some important lessons. In brief, the Heartbleed vulnerability in the ubiquitous OpenSSL TLS encryption protocol allowed an attacker to dump part of the memory from a vulnerable server and potentially thus get access to encryption keys, login credentials and possibly confidential information. Many put the existence of the vulnerability down to the fact that the open-source OpenSSL code was developed by a small and rather under-funded group. This argument was somewhat reduced in standing by the discovery of the POODLE attack[24] later in 2014 that affected the commercially-developed SSL 3.0 protocol, later shown to be applicable in TLS 1.0 – 1.2 protocols even when SSL 3.0 is disabled. Estimates suggested that the vulnerabilities affected some 40-60% of all websites. [25,26] Not long thereafter, researchers identified a flaw in the LibreSSL encryption library[27] that was intended to replace OpenSSL as a more secure alternative. Around the same time, serious flaws in Adobe Flash Player and Windows OS were discovered and patched.[28] The episodes highlight the potential perils of externally-developed code no matter the extent of resources put into development and proofing and thus the likely presence of attack vectors – potentially unknown - in one's own systems when relying on such code and almost certainly in systems that one interfaces to (in the Heartbleed case, users communicating with systems protected by the vulnerable versions of the OpenSSL software could be compromised) and over which one has little if any control. The events also highlight the frequent persistence of vulnerabilities over time – the Heartbleed bug was 'in the wild' two years before discovery.

---

[19] http://www.hackingteam.it/
[20] http://www.csoonline.com/article/2944333/data-breach/hacking-team-responds-to-data-breach-issues-public-threats-and-denials.html
[21] http://www.forbes.com/sites/ericbasu/2015/10/26/cybersecurity-lessons-learned-from-the-ashley-madison-hack/#60a30090ed99
[22] http://www.bbc.com/news/technology-33083050
[23] http://heartbleed.com/
[24] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
[25] http://www.techweekeurope.co.uk/workspace/nsa-denies-prior-knowledge-heartbleed-bug-143855
[26] http://www.itpro.co.uk/security/23756/2014-the-year-that-security-broke
[27] http://www.techweekeurope.co.uk/workspace/catastrophic-flaw-libressl-found-fixed-149192
[28] http://news.en.softonic.com/critical-adobe-flash-exploit-leaves-your-data-vulnerable

The Shellshock software bug[29] had the potential to compromise millions of servers on a similar scale to those mentioned above and is thus worthy of brief note. It affects the Unix Bash shell, allowing execution of commands by malicious parties that could allow access to the system itself. Perhaps the most notable aspect of Shellshock was the extent to which hackers exploited vulnerable servers in the days after the bug was first revealed.[30] This was at least partly due to the low complexity of the attack despite the fact that the impacts could be extremely severe. Botnets based on computers compromised based on the Shellshock vulnerability conducted a number of distributed denial-of-service (DDoS) attacks. Targets included the United States Department of Defense.[31] It is notable that patches were already available at the time that the bug was first revealed, with these attacks taking place during the lag period prior to these patches being applied. This highlights that though the initial vulnerability may be unknown, responsiveness in case of patch release is critical and this is solely the responsibility of the end-user organisation.

### *Attacks exploiting the human interface*
### High level threat – Nefarious activity/abuse
#### Threat – Social engineering

The prevalence of social engineering as a means of attack along with the possibility of brute force attacks on user account credentials (as used, for example, to access private files in the Apple iCloud)[32] has encouraged many to turn to password management tools as a means of easing difficulties in administering multiple accounts with different and complex passwords. In this regard, the LastPass hack is noteworthy. Hackers gained access to the addresses, encrypted passwords and password reminder phrases of more than 7 million people that had been stored in the cloud.[33]

## 3. The approach to system compromise

The above mentioned attacks highlight the frequent use of sophisticated malware, spyware and other code that can reside undetected on systems and exfiltrate data or other information. Such malware can be placed following social engineering attacks or through exploitation of system vulnerabilities. It may be targeted in the most sophisticated cases. In some instances, brute force attacks may allow unauthorised access through credential compromise. It may arise through watering hole attacks using websites frequently visited by a particular group. Yet, sometimes, system breach is not required.

### *Denial of service attacks*
### High level threat – Nefarious activity/abuse
#### Threat – Denial of service

Denial of service attacks can target network layers, application layers or both. They are often distributed attacks in which massive numbers of requests are sent to the service simultaneously from a number of

[29] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
[30] http://bits.blogs.nytimes.com/2014/09/26/companies-rush-to-fix-shellshock-software-bug-as-hackers-launch-thousands-of-attacks/?_r=0
[31] http://www.itnews.com.au/news/first-shellshock-botnet-attacks-akamai-us-dod-networks-396197
[32] http://www.theverge.com/2014/9/1/6092089/nude-celebrity-hack
[33] http://www.forbes.com/sites/katevinton/2015/06/15/password-manager-lastpass-hacked-exposing-encrypted-master-passwords/#128ac5d5a666

malicious (often infected) clients. A recent prominent example was the failure of the Australian Census website. [34] The full details of the attack are not yet know, but it demonstrated clearly the threat to government authorities in terms of reputational damage, as well as delayed processes.

## 2.2. Trends in the Threat Landscape

The attacks enumerated above allow us to identify some current trends in the field of cybersecurity. As one undertakes risk analyses, such trend analysis is important as it aids prioritisation in those instances in which the availability of resources to dedicate to boosting IT security are limited. In this document, the trends identified also determine the breadth of focus in the ensuing sections. A number of trends are obvious from the above that are worthy of note for organisations like eu-LISA:

- Increasing frequency of attacks on government entities
- The re-use of exploits and code in malware, with the out-sourcing of malware preparation to external parties and companies (i.e. Crime as a service) and thus the increased sophistication of malware/crimeware
- Increased use of zero-day exploits and exploitation of unpatched vulnerabilities in advanced code
- The increasing prevalence of targeted hacktivism to ruin reputations
- Frequent targeting of end users through theft of user credentials (often through spear phishing or other social engineering techniques), watering hole attacks or similar.
- Internet of Things

*Increasing frequency of attacks on government entities*
In order to better quantify the first point, the Kaspersky Targeted Cyberattacks Logbook[35] provides some useful reference material. It highlights the most menacing Advanced Persistent Threats (APTs) detected in recent years and indicates that only a single notable attack targeting government entities was detected in the year 2011, four were detected in 2012, eight in 2013 and nine in 2014. One company described the emergence of government and international organisations as 'notable targets' in their 2015 report.[36] In response to one attack, German intelligence agencies said that they face about 3000 cyber-attacks daily, of which about five come from foreign intelligence agencies.[37].

*The re-use of exploits and code in malware, with the out-sourcing of malware preparation to external parties and companies (i.e. Crime as a service) and thus the increased sophistication of malware/crimeware*
With regard to the use of Advanced Persistent Threats (APTs) against governments, the Stuxnet worm was something of a forerunner. It specifically targeted the Siemens supervisory control and data acquisition (SCADA) systems in place at Iranian nuclear facilities resulting in slow breakage of equipment. Reports suggested that the worm was jointly developed by the American and Israeli authorities.[38] It was first released into the wild in 2007 and remained undiscovered until June 2010 and only when it was more widely disseminated outside of the nuclear plant infrastructure against which it was targeted, highlighting the covert nature of its activities. The Duqu Trojan was discovered about one year later and appeared to also target Iranian authorities. It was described as being 'nearly identical to Stuxnet, but with a completely

[34] http://www.abc.net.au/news/2016-08-16/census-failure-will-have-far-reaching-consequences/7749446
[35] https://apt.securelist.com/#firstPage
[36] M-trends 2015. A View From the Front Lines. Mandiant 2014.
[37] http://www.bbc.com/news/technology-30724168
[38] http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

different purpose'[39], namely cyberespionage. Interesting aspects include its self-deletion from servers and the fact that it steals digital certificates to help future viruses appear as secure software. Duqu propagates through social engineering. Its modular structure highlights the complex nature of its development and the fact that individual elements can be easily re-used elsewhere. At least some elements of Duqu and Stuxnet were reused in the Flame malware which also targeted Iranian industrial facilities with the goal of covertly obtaining files and data and was described as 'the most sophisticated malware we encountered during our practice; arguably… the most complex malware ever found' by one expert team[40]. Elements were also reused in the Duqu 2.0 code used to attack Kaspersky in 2015 as mentioned above.

When considering the sophistication of modern malware code referenced above, some aspects stand out in terms of the technological nous of developers. The advanced stealth, concealment and camouflage strategies in-built into modern malware, such as the Duqu code's self-suicide switch, make detection in infected systems extremely difficult even in high-security environments. One company reported that the average time from compromise to detection across all sectors is 2015 days[41] – clearly more than ample time for data extraction, monitoring and data gathering, system destruction or otherwise. Another recent phenomenon is the proliferation of so-called two-faced malware that carries out benign processes when run in sandboxed environments, allowing for 'safety clearance' before its malicious processes can be executed.[42] In 2014, up to 28% of all malware was "virtual machine aware".[43] Many modern malware is being developed by so-called 'hackers for hire' with advanced capabilities and the knowledge and experience to continually write new and ever-more advanced codes, re-using exploits while devising new approaches to overcome the defences put in place to defend systems and networks.

*Increased use of zero-day exploits and exploitation of unpatched vulnerabilities in advanced code*
Zero-day vulnerabilities are exploitable flaws in software that remain unpatched, either because of a lack of knowledge on the part of developers or the fact that patches have not been prepared in the time since the flaw was first uncovered. The software bugs mentioned in the previous section were exploited within hours of becoming public, if not before, and are thus cases in point. At least 24 zero-days were discovered in 2014, more than in any year previously.[44] Duqu exploited a zero-day in the window's kernel while Stuxnet took advantage of at least four such vulnerabilities, allowing spread through USB drives, remote code execution and escalation of privileges.[45]

The attacks also make use of increasing availability of backdoors. At the end of 2015, Juniper Networks revealed that some firmware on its firewalls contained two backdoors installed by sophisticated hackers, rumoured to be nation state entities.[46] Interestingly, one such backdoor was built upon a pseudo-random-number generator already back doored by the NSA as revealed by some Snowden leaks.

Cryptographic issues, often due to flaws in the implementation of cryptographic primitives, are the second

---

[39] W32. Duqu. The precursor to the next Stuxnet. Version 1.4 (November 23, 2011). Symantec Security Response.
[40] sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks v1.05 (May 31 2012) Technical Report by the Laboratory of Cryptography and System Security (CrySys Lab) of the Budapest University of Technology and Economics.
[41] M-trends 2015. A View From the Front Lines. Mandiant 2014.
[42] https://blog.digicert.com/emerging-cyber-threats-in-2016/
[43] ISTR 20 - Internet Security Threat Report. Symantec. April 2015.
[44] Ibid
[45] http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities
[46] https://www.schneier.com/blog/archives/2015/12/back_door_in_ju.html

most common type of flaws affecting applications across all industries, according to a recent report.[47] The so-called FREAK flaw let an attacker weaken a connection using SSL/TLS, making it much easier to break the encryption and view the traffic.[48] In more detail, the flaw allows the downgrading of keys to weak 512-bit RSA keys (the modern standard is 2048 bits for this protocol) that can be efficiently revealed using modern computing tools. Analysis of the bug led to a more surprising finding that many hosts shared the same 512-bit public key. In fact, it appeared that manufacturers generated a single key and then installed it on many, many devices – a clear implementation flaw that would leave all such devices vulnerable to attack.[49] The Logjam and Drown flaws were reminiscent of the FREAK flaw with the former allowing downgrading of RSA keys used with SSL while the latter was based on a flaw in the TLS protocol itself rather than on an implementation vulnerability.[50, 51] Further investigation of the issue indicated that millions of HTTPS, SSH and VPN servers use the same prime numbers for Diffie-Hellman key exchange, a key part of the TLS protocol itself. This would allow eavesdroppers to break encryption of connections to such servers in large numbers of cases by performing a single enormous computation to 'crack' a particular prime, thus allowing breaking of any individual connection that uses that prime. Based on an analysis of comments made by top US Officials, researchers postulated that the NSA was exploiting this implementation flaw in the wild using pre-computation techniques, targeting HTTPS and VPN connections.[52] As noted by the authors, 'a one-time investment in massive computation would make it possible to eavesdrop on trillions of encrypted connections.' [53]

On occasions, one discovers implementation flaws that invite significant questions regarding the capabilities of developers or their protocols for secure programming. In one example, self-encrypting hard drives were accessible using a default password even when the user defined his/her own new one. In other cases, keys were used that were based on the computer clock and thus quite predictable.[54] As mentioned at the outset, encryption involves use of primitives, schemes and protocols and the full chain of security must be considered if reliability is to be fully assessed and hopefully ensured.

Some statistics on zero-day exploits make for sobering reading. It has been noted that a typical zero-day attack lasts 312 days on average. Furthermore, after zero-day vulnerabilities are disclosed, the number of malware variants exploiting them increases up to 85000 times and the number of attacks increases up to 100000 times.[55] Evidence suggest that standard safeguards are becoming less effective against zero-day attacks, indicating that new approaches need to be implemented in order to detect attacks exploiting zero-

[47] State of Software Security report: focus on industry verticals. Volume 6. Veracode.
[48] http://www.computerworld.com/article/2892592/serious-freak-flaw-could-undermine-the-webs-encryption.html
[49] Factoring 512-bit RSA Moduli for Fun (and a Profit of $9000). Martin R Albrecht, Davide Papini, Kenneth G. Paterson and Ricardo Vilanueva-Polanco. Available at https://martinralbrecht.files.wordpress.com/2015/03/freak-scan1.pdf
[50] Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springali, Emmanuel Thome, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Beguelin, Paul Zimmermann. Available at: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf
[51] http://www.theguardian.com/technology/2016/mar/02/secure-https-connections-data-passwords-drown-attack
[52] http://www.theage.com.au/it-pro/security-it/revealed-the-encryption-tools-spies-can-and-cant-crack-20141229-12fosh.html
[53] https://freedom-to-tinker.com/blog/haldermanheninger/how-is-nsa-breaking-so-much-crypto/
[54] Got HW crypto? On the (in)security of a Self-Encrypting Drive series. Gunnar Alendal, Christian Kison, modg. Available at: http://eprint.iacr.org/2015/1002.pdf
[55] Before We Knew It. An Empirical Study of Zero-Day Attacks in the Real World. Leyla Bilge and Tudor Dumitras. Proceedings of CCS '12, October 16-18 2012, Raleigh, NC, USA.

day vulnerabilities or at least cope with the consequences.[56]

*The increasing prevalence of targeted hacktivism to ruin reputations*

Hacktivism – the phenomenon in which individuals or groups target others through hacking as a means of political protest or of making a political statement has become increasingly prevalent in recent years, crossing borders and challenging governments and international organisations. Spreading of malware and instigation of distributed denial of service (DDoS) attacks are common elements of the hacktivist's toolbox. Alongside the afore-mentioned Ashley Madison and Hacking Team attacks, one may add recent attacks on Sony Pictures and TV5 Monde or attacks against individuals, typically so-called doxing attacks.[57] What is perhaps most notable in recent years is the confluence of hacktivism with other attack forms – hacktivist attacks frequently follow leakage of user credentials (as noted in the next paragraph) and standard DDoS attacks associated with hacktivism are in fact more frequently being used as cover for the targeted spread of malware and data theft,[58] as seen in the Sony attack as well as in the infamous theft of user data from the UK firm Carphone Warehouse.[59] When discussing information security under the headings of confidentiality, integrity and availability, one should consider to extend the triad to include reputation as a key aspect of many entities relationships with IT.

*Frequent targeting of end users through theft of user credentials (often through spear phishing or other social engineering techniques), watering hole attacks or similar.*

Despite the apparent sophistication of advanced code developed by well-supported expert groups, it is abundantly clear that the weakness in many systems often stems from end-users. Theft of user credentials, typically usernames and passwords, is frequent and particularly dangerous in that it can provide for intrusion and potentially control of anything from single stations to full systems depending on the access rights of the user, the system setup and the skills of the attacker(s). The precision with which social engineering attacks are being undertaken is remarkable, with one monitoring company reporting an 8% increase in spear phishing despite a reduction of 14% in the number of emails sent and a 20% reduction in the number of targets in 2014 compared to the previous year.[60] Furthermore, larger organisations are most frequently attacked while government is amongst the top 5 sectors for spear phishing campaigns as well as by number of incidents in which data was breached. They also reported increased use of social media in such attacks, noting that trust in posts by contacts or 'friends' means that end users are more likely to click on links in such environments compared to in spam email. It has been reported that attacks that gain access to a target's VPN give attackers significant scope to exploit a system without detection[61] and typically follow from use of stolen credentials. Given such access, attackers can easily get a strong foothold in any system using publically downloadable tools that enable acquisition of increased privileges in the system over time[62] - including so-called Crimeware - and taking advantage of well-established stealth techniques to remain undetected even on systems with intrusion detection systems. Maintenance of

[56] Zero-Day Danger: A Survey of Zero-Day Attacks and What They Say About the Traditional Security Model. Fireeye 2015.

[57] Doxing is a term used to describe hacktivist attacks against individuals in which personal details are posted online in order to intimidate.

[58] 2014. The Danger Deepens. Neustar Annual DDoS Attacks and Impact Report. Available at: https://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

[59] https://digitalguardian.com/blog/ddos-cover-data-theft

[60] ISTR 20 - Internet Security Threat Report. Symantec. April 2015.

[61] M-trends 2015. A View From the Front Lines. Mandiant 2014.

[62] For example, the Mimikatz toolkit. Available from https://www.offensive-security.com/metasploit-unleashed/mimikatz/

persistence is a hallmark of modern attackers using so-called Advanced Persistent Threats (APTs). Such is its prevalence that researchers have recently coined the term Ghostware to describe such malware.[63] Prevention of the initial intrusion is paramount but events above highlight that even the most trained individuals can be tricked using exceptionally targeted attacks at the people themselves, their associates or even third parties with whom they are in contact.

Waterholing is a phenomenon also worthy of note to which even the most knowledgeable and cautious of end users can fall prey – and indeed in recent years have done so on many occasions. It typically involves the exploitation of vulnerabilities in web browsers and associated plugins to enable execution of malicious code on the machines of those visiting the infected website(s). A Microsoft Internet Explorer vulnerability[64] discovered in 2012 was apparently being used to target senior US politicians and another[65] to target US Federal Employees.[66] Yet another accomplished watering hole attack dubbed 'Operation Ephemeral Hydra' targeted a website associated with national and international security policy[67] and allowed connection to an external command and control server for remote interaction with the affected machines. Even more recently, in an attack dubbed 'Operation Russian Doll' vulnerabilities in Adobe Flash and Windows were exploited to attack a government entity, or more specifically employees who interacted with a website controlled by the attackers.[68] Researchers have found that some 75% of websites have vulnerability issues, with about 20% of these being critical,[69] highlighting that waterholing may continue to be a popular means of launching attacks going forward.

## 2.3. Trends in Information Technology

Any assessment of novel technologies in the cybersecurity realm requires consideration of emerging ideas and technologies in the IT domain generally. A non-exhaustive selection of technologies is provided tailored to those of some relevance to the security technologies enumerated in section 4 but not covered in detail later. A more complete list may be found in other reports purely focussed on these matters.[70]

*Internet of Things*

No publication on IT-related matters nowadays is complete without some form of reference to the Internet of Things – the term being used to describe the current networked world in which devices, sensors and other 'things' are connected to each other and to more standard IT equipment, providing for a meshed network in which information is gathered, shared, analysed and acted upon. In this regard, commentators have described the current state of affairs in technological development as a 'digital explosion'. Nevertheless, government entities such as eu-LISA depend on core services and guard private and personal information of immense importance and sensitivity whose sharing and dissemination must be controlled, meaning that they must be conservative in their approaches. They are 'guard the jewels'

[63] https://www.hackread.com/ghostware-two-faced-malware-coming-in-2016/
[64] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4792
[65] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1347
[66] Lin. "IE Zero-Day is Used in DoL Watering Hole Attack." May 2013.
[67] https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html
[68] https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html
[69] ISTR 20 - Internet Security Threat Report. Symantec. April 2015.
[70] http://www.cpni.gov.uk/Documents/Publications/2015/05-June-2015-Emerging%20Technologies%202015%20-%20V2_PV.pdf

organisations.[71] Mobile devices and non-core IT may be used but will never be priorities; sensitive and important information will always be produced and retained in core IT. The proliferation of cloud services will be of limited relevance as information will always have to be stored and acted upon solely at the central level. Analytics will only ever apply to the entity's data and never to a composite of this data with other data or information in a cloud-type environment. Therefore, this topic is not developed further in this paper.

*Affective Computing and Emotion Recognition*

There is increasing interest in the field on reading and interpreting the actions and emotions of the human users of technology. Visual, oral or aural cues can be interpreted to make insinuations regarding a person's feelings or thoughts and thereby feed modulating responses. From a security perspective, the main area of interest may well be in terms of user surveillance and user behaviour monitoring and potentially manipulation. User monitoring could be exploited for both positive and negative purposes – for example to ensure appropriate user access but also to associate users to machines and potentially manipulate actions to fit the needs of an attacker. Technologies in this domain have advanced significantly and are already being released onto the market.

*Digital cryptocurrency*

Digital currency can be used for the acquisition of goods or services purchased online, in a manner akin to how normal currency is utilised in the real world. Bitcoin is the most prominent, but far from the only such currency. Fundamentally, cryptocurrency 'wallets' are files containing tokens associated with the currency units. They may be (indeed should be) backed up like any digital file. The token relies on cryptography to secure the records of transactions. The basis for this is so-called block chain technology, referenced later.

*Homomorphic encryption*

Homomorphic encryption is the most commonly-known and utilised encryption method in which the encryption process can be mapped to mathematical functions – implying that encrypted data can be processed without any necessary decryption. Providers, managers or end users can thus manipulate data without actually having access to the intelligible form of that data. There is obvious interest in such technologies to allow for centralised data management while maintaining data protection standards. The technology is also of interest in the domain of biometrics, as referenced in the previous eu-LISA report on the topic.[72] The main issue currently is the computational expense of the process. Predictions suggest that homomorphic encryption will not become mainstream for many years as a result.

*Security Information and Event Management (SIEM)*

SIEM implies the collation of information present in logs based both on events and security logs in order to allow for trends to be analysed and anomalies identified. In this regard, SIEM particularly deals with the collection of information, while big data and analytics capabilities allow for the actual utilisation of the gathered information and the creation of actionable intelligence for follow-up. Big data is the subject of further discussion in Chapter 4.

*Wireless mesh networks*

---

[71] This term has introduced by Gartner to describe such organisations, see: Cybersecurity Scenario 2020 Phase 2: Guardians for Big Change. Earl Perkins. 20 July 2015.

[72] Biometrics in Large-Scale IT. Eu-LISA Research Report 2015. Available at: http://www.eulisa.europa.eu/Publications/p_reports/Pages/default.aspx

Wireless mesh networks consist of disparate devices, each of which may be considered a network node, communicating with each other, generally wirelessly. As a network architecture, advantages include the possible fault tolerance of the network due to the multiple paths across which communications can flow between any two nodes. The nodes may be IoT devices, and hence wireless mesh networks are closely related to IoT. Should such architectures be implemented in any organisation, security matters will doubtless have to be considered. However, such networks would also offer possibilities in terms of improved or diversified surveillance, tactical communications in critical environments and improved automation and monitoring of systems, datacentres etc.

# 3. Transversal topics

Recent developments and news in the domain of IT security and the trends that such occurrences allow us to note, described in the previous section, begin to allow us to devise recommendations for maintaining and advancing system security and information security systems such as those managed by eu-LISA going forward. Some recommendations can be made regarding specific, novel technologies devised or developed for particular purposes, yet others relate to organisational capabilities, strategies and approaches to ensuring cybersecurity or the processes that are put in place in the security domain. The latter category of recommendation can nevertheless relate to technologies – patching, for example, must be organised so as to be undertaken quickly and effectively across an organisation, with the end goal being that deployed technologies are up-to-date.

To be straightforward, any organisation must walk before running, and therefore it would be amiss to even allude to new technologies let alone recommend serious consideration of their implementation without emphasising the fundamental arrangements that must be in place to provide baseline security and in fact, ensure that implemented technologies work. In this section, such transversal requirements are briefly enumerated

***Patching***

Although it is clear that zero-day vulnerabilities are being exploited 'in the wild', evidence also suggests that a particularly crucial aspect of security is the updating of applications and software with released fixes to address discovered and patched vulnerabilities. The Australian Signals Directorate (ASD) has assessed that implementing just 4 basic strategies will mitigate 85% of intrusion techniques seen, of which two relate to patching (of applications and of operating systems).[73] Attackers can take advantage of any delay between a vendor becoming aware of a vulnerability and the release of a patch to address the issues, or indeed any delay between the release of such a patch and the application of the fix to systems. It has been reported that the average time from publication to patching was 59 days in 2014.[74] Yet attackers move far more quickly – some were able to exploit the Heartbleed bug within four hours of it becoming public.[75] In this case, a patch was released at the same time yet over one month later many thousands of the most popular TLS-enabled websites were still vulnerable. Application of patches, while no panacea, should be a priority in the immediate term upon discovery of any vulnerability as the immediate aftermath of any announcement appears to be a particularly dangerous period for attack. The priority given to patching should correspond to the risk vulnerability. Similarly, anti-virus and anti-rootkit tools should be updated with new signatures frequently on all machines, probably at least daily, as should DDoS mitigation equipment and any other devices relying on signatures for their effective functioning. It goes without saying that software that is no longer maintained or developed should not be present on machines, something that should be assured through software whitelisting.

When considering patching, it is also crucial that updates are propagated to all machines of which an enterprise's network is comprised. Thus, the appropriate mechanisms for full patch distribution and auditing of process completion should be in place.

---

[73] http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm
[74] ISTR 20 - Internet Security Threat Report. Symantec. April 2015.
[75] Ibid

***Collaboration***

As borne out in the previous point, information on vulnerabilities, on-going attacks and appropriate defences changes frequently and all parties must be on their toes to adapt to the threat landscape that modulates quickly. Access to information is crucial if appropriate reactive decisions are going to be made. Furthermore, and as borne out above, third parties and partners can act as conduits for attacks against oneself, and therefore appropriate responses to attacks across all partners is in the collective group's interests. When considering threat intelligence, continuous monitoring of developing threats and defence technologies is necessary, as borne out in this particular document. It is important that partners interact and share appropriate information. They may also interact in efforts to examine deficiencies in each other's networks and systems – engaging in penetration testing or red team tests, for example. Generally cooperation with industry should also be encouraged. Bearing in mind above-mentioned reports of backdoors and loopholes in commercial products and software, it is crucial that end users are aware of the provenance of the software that they purchase and have a good relationship to allow full questioning and trust. The EU's cybersecurity strategy emphasises public-private cooperation and information exchange. Recent developments indicate that the need for such exchange is as important as it was in 2013 when the Strategy was drafted, a fact emphasised by the repetition of the emphasis in the NIS Directive whose text was recently finalised.

***Training***

Bearing in mind the afore-mentioned targeting of end-users through spear phishing and waterholing, not to mention the risks associated with social media use, use of mobile devices and other issues less discussed in this paper, education becomes crucial. Like cybersecurity defences themselves, education of users should be targeted, bearing in mind the most significant risks to an organisation and the likely attack vectors and modified over time to reflect changing realities. Knowledge gaps should be identified through continuous monitoring and novel approaches to learning tested when possible and feasible – for example, gamification and practical exercises can be used. User education should be complemented with user-focussed steps that are discussed in many other documents such as access control and rights management, password management and policies, device and application management per user and account monitoring, with training being tailored to match the rights accorded to individual users and the risks that they thus present. Training should additionally respond to the threat environment generally as well as that faced by the specific organisation. Additionally, IT departments should make user-based attacks more difficult by implementing two-factor authentication schemes while highlighting their benefits to the users in training sessions.

***Layered security***

No technology currently deployed or available, including those mentioned herein, will be vulnerability free or immune from compromise or penetration. The capabilities of attackers to overcome defences are clear in every case. Perimeter defences can be penetrated through user impersonation, signature-based monitoring is not built to deal with the ever-increasing spectre of zero-day-based malware, reputation-based defences cannot cope with brand new attacks and sandboxing is being defeated with two-faced malware. A layered approach to security providing so-called defence in depth is advisable, therefore, employing all of the above and more. Such an approach also offers benefits in terms of isolation of any breaches that may occur. Networks should be segmented with minimal interaction between segments – so-called 'air-gapping' - and the creation of DMZs between layers where possible, while network privileges should equally be controlled in order to hinder attacks requiring higher privileges and to control interfacing between network segments. Intrusion prevention systems should be complemented by intrusion detection systems at both network and host levels and using both signature-based and behavioural analysis tools.

Device and software whitelisting, device configuration controls, DDoS mitigation measures, packet sniffing technologies and penetration testing should all be considered as relevant components of a cybersecurity plan.

***Monitoring and response***

Organisations may expect that they will, at some stage, be compromised. Attacks are becoming more targeted and sophisticated as mentioned and an attacker must only succeed once in order to get a foothold within a system. Monitoring and response, encompassing incident response plans business continuity and recovery, need to be emphasised as core components of any security strategy as a consequence.

# 4. New Technologies to Address Challenges in IT security

Given the increasing risks prevalent in the cybersecurity domain and the subsequent requirements for continuous evolution of IT security capabilities in organisations such as eu-LISA, there is a need to identify possibly relevant technologies that could boost protection of systems or the data thereon, help to detect and/or respond to attacks or already compromised systems and thereby ensure more speedy recovery. Such identification will act as a prelude to more detailed needs assessment and is the purpose of this section. Ten technologies are identified, in no particular order, based on the cutting-edge of IT development generally – which provides some foresight regarding the types of architectures and implementations that will be pursued in the near future and thus the concomitant risks that may become most relevant – the emerging threats faced by eu-LISA and its stakeholders and the Agency's security requirements borne out of the applicable legal bases. The following are the Top 10 technologies for IT security identified by eu-LISA this year:

1. Big data for behaviour-based threat assessment and malware detection
2. Pervasive sandboxing
3. Machine-readable threat intelligence
4. Adaptive access control
5. Permissioned ledgers
6. Hardware random number generators
7. Hashing using SHA-2 or better primitives
8. Encryption key hierarchies
9. Grid computing
10. Advanced DDoS protection

### 1. Big data for behaviour-based threat assessment and malware detection

***Activity classification (NIST): Protect, Detect***
***Threats addressed (ENISA classification): Information leak, erroneous use or administration of devices and systems, malicious code/software/activity, manipulation of hardware and software, manipulation of information, unauthorised activities, targeted attacks***
***CIA classification: Integrity, Confidentiality, Availability***

Perimeter defences are the first line of any security strategy and undoubtedly important. They may include deployment of firewalls, intrusion detection systems, application proxies, VPN servers, demilitarised zone (DMZ) perimeter networks and similar. The preceding discourse highlights the various channels through which attacks can progress and indeed bypass all of these defence mechanisms, however. The ShellShock vulnerability, as an example, was overlooked for some 25 years before being noticed, highlighting the extent to which malicious parties are now seeking (and indeed finding) exploitable vulnerabilities in order to obviate obstacles arising from improved perimeter defences. Similarly, the rise of spear phishing highlights the new goals of attackers to piggy back into systems with trusted users and the ingenuity of attackers to find new means to access systems. Waterholing can be tackled by blacklisting suspicious websites but the foregoing discourse highlights the vulnerability of many reputable sites while spam filters only offer medium protection against phishing attacks – indeed very limited protection as spear phishing becomes more commonplace.

Thus, typical defences have more recently included anti-virus and anti-malware scanning and rootkit removal based on known signatures in order to detect threats that may have breached the perimeter. By definition, these tools can only detect known and confirmed threats. Previously-mentioned criminal groups engage in code morphing to get around these classic defences.

The advent of big data capabilities offers new opportunities in terms of behaviour-based threat detection at the perimeter as well as scanning/removal possibilities. Scanning should imply searching for all types of malware – spyware, viruses, Trojans, rootkits and backdoors should all be considered. Additionally, as advanced malware can seek out the existence of anti-malware and malware scanning capabilities on a system and adapt itself to obviate these defences, the inclusion of some form of disguised presence on the system is advisable. Automated monitoring of audit logs for atypical behaviour is also advisable. Advances in machine learning and neural networks need to be considered - through comprehensive system monitoring over time and application of sophisticated analytics, any anomalies that may be cause for concern should be detected accurately and quickly. Advanced machine learning was noted as one of Gartner's Top 10 Technologies for 2016 and can certainly be applied in the field of anomaly detection for IT security.[76] Developments in this regard should therefore be monitored closely in the coming years and consideration given to roll out of the new methods that will become available. Going forward, the blending of signature-based and behavioural-based methods will become crucial.

Such developments may also lead to improvements in packet analysis or packet 'sniffer' technologies, another component of the security setup required to protect system integrity and confidentiality. Packet analysis systems should be deployed to check on all incoming network traffic. Nowadays, such tools can be signature-based or anomaly-based and in the latter case, the merits of big data analysis may lead to improvements that should be considered for incorporation to managed IT systems.[77]

Behavioural analytics may also be used to monitor user behaviour and detect anomalies that could arise as a result of malicious insider attacks or unintended activities. User behavioural analytics can utilise the significant volumes of data that SIEM, system logs and other tools gather,[78] identifying suspicious behaviours that deviate from those of individuals and/or the group. Follow-up can be based on reporting to system monitors or the immediate and automatic implementation of measures at network, firewall or system levels.

*The eu-LISA perspective:* Perimeter defence systems, scanning technologies and packet sniffing processes will be important as part of layered security approaches implemented in both large-scale IT systems and corporate infrastructures. In order to defend against and/or detect malware, behavioural analytics based on big data can surely complement more traditional signature-based methods, covering in particular unknown attacks which, as referenced above, are becoming increasingly commonplace. The possibility to detect and guard against insider threats and damaging activities that might arise due to unintended actions is another advantage of such technologies. When deployed in a user agnostic manner with global

[76] http://www.gartner.com/newsroom/id/3143521
[77] F. Mansman, L. Meier, D. A. Keim. "Visualization of Host Behavior for Network Security". VizSec 2007.
[78] C. Griffy-Brown, D. Lazarikos, M. Chun. "How Do You Secure an Environment Without a Perimeter? Using Emerging Technology Processes to Support Information Security Efforts in an Agile Data Center" (2016) J Appl. Business Economics 18(1): 90-102.

reporting and follow-up, perhaps even automatic follow-up, there is no threat to the individual user from a privacy and data protection perspective and therefore the use of user behavioural analytics in the workplace may be recommended. Real time adaptive security based on analytics should become a core component of network and system security models in operational settings.

## 2. Pervasive sandboxing

***Activity classification (NIST): Detect***
***Threats addressed (ENISA classification): Malicious code/software/activity, targeted attacks, remote activity (execution)***
***CIA classification: Integrity, Confidentiality, Availability***

Pervasive sandboxing can be seen as belonging to the air-gapping category of system defences, protecting the system and the data thereon by separating code, typically executables, in physically or logically separate layers and/or separating systems from networks where threats may arise. It should be noted, however, that the concept of air-gap malware was introduced by scientists in 2013. [79] The communication of air-gapped systems with networked systems and/or mobile phones using acoustic signals, electromagnetics signals[80] and thermal signals[81] has been demonstrated in practice. Although the bandwidth available in such communication is limited, it is typically sufficient to countenance leakage of packets of information such as passwords, key logs etc. No attacks based on the demonstrated approaches appear to have been uncovered in the wild and they therefore appear to be more theoretical in nature at this stage. However, given how technology advances, it should be noted that air-gapping alone may not be a sufficient means of protecting system integrity going forward.

Pervasive sandboxing focuses on the separation of executables from core systems. By including isolated virtual containers within a system architecture, executables and content can be run in such environments upon first encounter and the virtual machines monitored for indicators of compromise (IOC), typically comparison of what is seen in the sandboxed environment with what is observed on actual endpoints. Gartner identified pervasive sandboxing and IOC confirmation as one of its Top 10 Technologies for Information Security in 2014.[82]

A related technology worthy of note is Data Execution Prevention (DEP).[83]

*The eu-LISA perspective:* Spear-phishing is a significant threat to government authorities who are specifically targeted by various nefarious actors. Malicious attachments and links containing dangerous executable content can arrive via email, CDs and storage devices and provide a foothold into individual systems before propagating more widely, inflicting system damage, exfiltrating information or otherwise. The large-scale IT systems, though air-gapped from public networks, are nevertheless exposed due to the needs to connect to national infrastructures and for devices to be connected at central level. Sandboxing can be an important component of defence both at central systems and within national infrastructures to

[79] Michael Hanspach and Michael Goetz, "On Covert Acoustical Mesh Networks in Air," Journal of Communications, vol. 8, no. 11, pp. 758-767, 2013. doi: 10.12720/jcm.8.11.758-767
[80] http://cyber.bgu.ac.il/content/how-leak-sensitive-data-isolated-computer-air-gap-near-mobile-phone-airhopper
[81] Mordechai Guri, Matan Monitz, Yisroel Mirski, Yuval Elovici. BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations. arXiv:1503.07919
[82] Available at http://www.gartner.com/newsroom/id/2778417
[83] Data Execution Prevention implies that only data in a marked 'executable' area of memory can be run.

which the systems connect. Needless to say, use in corporate infrastructures where threats are even more evident is advisable.

## 3. Machine-readable threat intelligence

***Activity classification (NIST): Protect, Detect***
***Threats addressed (ENISA classification): Information leak, erroneous use or administration of devices and systems, malicious code/software/activity, manipulation of hardware and software, manipulation of information, unauthorised activities, targeted attacks, remote activity (execution)***
***CIA classification: Integrity, Confidentiality, Availability***

The need for collaboration amongst authorities was mentioned in Chapter 3 of this report. A major benefit of collaborative approaches is the sharing of intelligence between parties regarding threats and attacks. This allows for the tailoring of defences and when considering signature-based malware detection and scanning technologies, refinement of the patterns that are searched when executing perimeter checks or seeking to identify already compromised systems.
The amount of data and information available increases as the networks of collaborating partners expand, however, making it more difficult or entities to follow-up in the most appropriate manner in the short timescales available to act. Machine-readable threat intelligence allows for the automated implementation of such responses; like big data, it allows for the improved use of the significant volumes of data being amassed, rendering data as actionable information.

Machine-readable threat intelligence is a recent trend, highlighted in Gartner's Top 10 Technologies for Information Security in 2014.[84] Machine readability offers benefits in terms of the speed with which updates can be incorporated into live software and the possibilities of integrating alerts and content from diverse sources. Governmental authorities should therefore probe possible integration of real-time machine readable threat intelligence and reputation scoring into active anti-malware processes.

*The eu-LISA perspective:* Public authorities constantly work in an environment in which resources are limited. Resources for security are shared where possible with those available for other functions in the organisation or entity. Efficiency is key and the added value of activities a critical area of focus. Anti-virus and anti-malware solutions are undoubtedly effective, as are packet sniffing tools for network security, network and system scanning tools and other approaches to detection of threats and/or compromise. Yet frequent update of the signatures and profiles sought by these pattern-recognition tools is critical. Manual update in response to intelligence is time-consuming. It may also be subject to error or subjectivity. Machine readable threat intelligence addresses these challenges and is thus an enabler of operational implementation of other technologies, including those referenced in this document

## 4. Adaptive access control

***Activity classification (NIST): Protect***
***Threats addressed (ENISA classification): Abuse of authorisations, remote activity (execution), compromising confidential information, unauthorised installation of software, unauthorised activities***

[84] Available at http://www.gartner.com/newsroom/id/2778417

***CIA classification: Integrity, Confidentiality, Availability***

Strict control of access rights and administrative privileges is a basic yet effective strategy in any enterprise cybersecurity plan. In fact, minimisation of administrative privileges is one of the four afore-mentioned basic strategies identified by the ASD as being sufficient to minimise 85% of all threats. Yet a blanket minimisation of privileges has its limitations and in some organisations may be impractical, impinging significantly on user experience and adding demands in terms of administration of systems. Equally, providing heightened privileges to limited users renders them targets for attack and when applied in a standard manner, allows for spear phishing and identity theft targeting such users to become a viable means of system entry.

Adaptive access control is a very relevant modern development that aims to balance trust elevation against risk taking into account the context in which a process or transaction is being requested or run. Thus, any access decision made will reflect the conditions applicable that may include aspects of timing, device used, one's history of activity, dynamic risk assessments or any other factors that may be considered relevant in an overall risk analysis. Additionally, second checks can be instigated for transactions if necessary. A much wider array of access right categories can thus be managed compared to standard permissions models that are based on users and their status only. It is notable that some of the world's largest and most technologically aware companies are making the move away from perimeter security models towards adaptive access systems.[85] The move is driven not only by the perceived advantages of such a model but also by the availability of increased memory volumes at affordable prices – such access schemes typically involve management of huge volumes of data that are processed in an automated manner.

A related technology worthy of note in the context of access permissions and controls is Mandatory Integrity Control (MIC). It is a perimeter defence in which integrity levels are representative of the trustworthiness of a running process. Policies can be set based on these levels to restrict access permissions, for example.

When considering access control, a note on password usage is warranted that takes into account recent research in the area. The use of passwords as the foundation stone of user authentication protocols has been shown to be fallible over time on account of the facts that users often choose simple passwords or alternatively write complex passwords down and tend to re-use these passwords across sites and services. While the use of password management plugins or applications could be considered as one means of dealing with the password management dilemma, the afore-mentioned LastPass breach highlighted some dangers in this regard, while it should also be noted that such password managers introduce single points of failure in a system – namely the master password that provides access to all others. Consideration of these facts have already led some researchers to recommend use of simple passwords across most sites and services that demand limited security on the users' part.[86] Furthermore, issues can arise if passwords are stored in plaintext in system memory as these, along with other authentication modes can be stolen and/or replicated following initial system breach.[87] Most parties will choose to implement rigorous password policies but will be unable to stop users re-using these passwords or indeed recording them

[85] http://www.computing.co.uk/ctg/news/2453699/google-reveals-its-shift-to-an-open-security-architecture
[86] Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. D Florencio, C. Gerley and P.C. van Oorschot. Usernix Security 2014, August 20-22. Available at: http://research.microsoft.com/pubs/217510/passwordPortfolios.pdf
[87] M-trends 2015. A View From the Front Lines. Mandiant 2014.

elsewhere. Consideration of two-factor authentication, potentially including biometric usage, may be considered to address many of these issues and is worthy of consideration going forward.

*The eu-LISA perspective:* Adaptive access control is more relevant for corporate infrastructure and national systems than for large-scale IT. Considering the former in the context of the Agency, it seems apparent that considered implementation of such advanced technologies can bring benefits. In particular, it may simultaneously enable increased management of one's own systems by the IT experts in the Agency who are doubtless knowledgeable and capable of such while also guarding against insider attacks or nefarious activities arising through identity thefts.

## 5. Permissioned ledgers

***Activity classification (NIST): Detect***
***Threats addressed (ENISA classification): Unintentional change of data in an information system, loss of integrity of sensitive information, manipulation of information, compromising confidential information, destruction of records.***
***CIA classification: Integrity, availability***

A distributed ledger is a database shared across sites or entities on a network. Like a traditional paper-based ledger, they can record assets and changes thereof. In digital format, their security can be increased significantly through the use of PKI infrastructures, digital signatures etc. that can control access and permissions and ensure non-repudiation of data; thus digital distributed ledgers can be used as a means of ensuring data integrity by tracking all modifications to a file and associating them to actors. Additionally, as they are distributed, they are difficult to attack because of the multiplicity of copies at various locations.

The technology has enjoyed something of an uptick in attention amongst governmental authorities in recent times. Estonia is moving health care records and other sensitive personal files to a database in which distributed ledger technology provides a key safeguard. For security reasons, the ledgers are not centralised master files but are rather broken into blocks each referring to the block that was created previously, hence the name blockchain for the technology that underlies many modern distributed ledgers (and incidentally underlies the 'bitcoin' digital cryptocurrency). Modifications in any block would imply computationally difficult work on all subsequent blocks until caught up to present if they were to go undetected, rendering illicit modifications or changes to existing ledgers virtually impossible. In this manner, the set-up guards against privileged insider attacks as well. Earlier this year, the Chief Scientific Advisor in the UK suggested that such technologies 'could transform the delivery of public and private services and enhance productivity through a wide range of applications.'[88]

Important attributes of distributed ledgers and blockchain technology include possibilities to reconcile datasets using cryptographic methods, duplicate data sets to improve system resilience and availability and implement advanced access control. The attributes allow proposition of a number of possible use cases that would interest governmental authorities – traceability of transactions in databases to increase trust, reductions in the costs of system administration and protection of critical infrastructure against cyberattacks. The latter is obviously of most relevance to this report and warrants brief additional explanation. The basis of security through distributed ledger technology is the capabilities that are offered

[88] Distributed Ledger Technology: beyond block chain. A report by the UK Government Chief Scientific Adviser. Government Office for Science. 2016.

in terms of monitoring for illicit changes. The integrity of data, code, software and other information within a database and being added or removed from a system can be verified. This would be the case no matter who was interacting with the data or where they are within the network.

*The eu-LISA perspective:* Given on-going development in this area, it is anticipated that the technology will become increasingly attractive for governmental organisations in the short term. Thus, 'permissioned' ledgers should be considered for implementation in networked systems in which data integrity, data sharing, transparency and trust are important. This is doubtless true for large-scale IT systems such as those managed by eu-LISA, and though the use of such ledgers would represent a paradigm shift in system architectures, their use should be examined, including from security perspectives. In particular, as an evolving technology, the safeguards necessary in implementation should be carefully analysed and security and privacy implications assessed. The lessons being learned from trailblazers in the use of digital distributed ledgers should be assessed.

## 6. Hardware random number generators (encryption)

***Activity classification (NIST): Protect***
***Threats addressed (ENISA classification): Abuse of information leakage, manipulation of information, compromising confidential information, interception of information***
***CIA classification: Confidentiality***

Technologies 6 and 7 relate to the encryption of data, a critical step in maintain the confidentiality and integrity of data at rest and in transit. Encryption has been heavily discussed and debated in popular media in recent times. The legal wrangle between Apple and the US FBI regarding decryption of the contents of a mobile phone[89] brought the concept to the attention of the wider public.

Perhaps hastened by recent discussions and public attention being paid to the issue, a number of technology providers quickly introduced encryption for data passing through a network – often end-to-end[90] - to their services.[91, 92, 93] Full disk encryption – i.e. encryption of data at rest - has been established practice amongst many providers for some time.[94] Efforts have even been made to force website providers to move away from vulnerable encryption algorithms and protocols, thereby improving global security.[95]

Cryptographic processes involve primitives – i.e. the cryptographic algorithms that are responsible for the mathematics-based data scrambling, as well as aspects such as key length – schemes (implementations of the primitives to achieve actual encryption services) and protocols that determine the full means of application of the schemes to the data in order to ensure confidentiality. Optimisation of processes will involve consideration of all aspects. The ENISA Algorithms, key sizes and parameters report[96] collates a

[89] See http://www.digitaltrends.com/mobile/apple-encryption-court-order-news/ for a discussion of this story's timeline
[90] End-to-end encryption describes the encryption of data at all points from sender to receiver so that no eavesdropper along the way can have access to the decrypted data.
[91] http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/
[92] http://arstechnica.com/business/2016/03/go-ahead-make-some-free-end-to-end-encrypted-video-calls-on-wire/
[93] https://www.google.com/transparencyreport/saferemail/?hl=en
[94] Apple introduced full disk encryption on its OS X Panther system in 2003, with the option becoming default in 2014. It became mandatory on Android handsets in 2015.
[95] http://www.wsj.com/articles/google-to-boost-encrypted-websites-in-rankings-1407384244?mod=yahoo_hs
[96] Algorithms, key size and parameters report – 2014. ENISA. November 2014. DOI 10.2824/36822

series of proposals for algorithm and keysizes and is thus a useful resource for decision makers seeking more information on which primitives should be considered within their systems, bearing in mind risk analyses that they should carry out ahead of making such decisions. An example rule emanating from the document is that 128-bit security is a minimum for new systems being deployed, and should remain viable at least in the near-term. Similar documents are available within Member States and at international level.[97]

Amongst the most primitive elements is random number generation. Good random numbers are fundamental to almost all secure computer systems. Any possibility to predict the random number assigned to a particular user or process introduces vulnerabilities, and hence cryptographically secure random number generators should be fully unpredictable. In reality, the majority of random number generation processes are in fact pseudo-random, being based on some form of computer algorithm. Typically, they take a seed value to generate a new random number, and thus this seed must be itself randomly generated.

The case of Dual_EC_DRBG random number generation highlights the importance of the number generation process. Elliptical curve cryptography (ECC) has been promoted as the future of public-key cryptography as it typically requires use of a smaller key size than traditional algorithms based on the intractability of factoring large prime numbers. This implies reduced storage and transmission requirements. NIST has endorsed ECC in its suite of recommended algorithms, specifically Elliptic Curve Diffie-Hellman (ECDH) for key exchange, as being suitable for protection of materials to the level of TOP SECRET.[98] Problems with some forms of ECC were first widely noted with NIST's abandonment of the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG) that it first ratified in 2007. By 2013, Dual_EC_DRBG was the default random number generator for several products from the security company RSA, used to create the secret keys for public-key ECC. In such use, the supposition of randomness is crucial as any control over or ability to predict the numbers produced can break otherwise secure cryptographic algorithms, as demonstrated on many occasions previously.[99] In the case of Dual_EC_DRBG, the values of the seed points used in the random number generation were found to be related, creating a backdoor.[100] A working proof of concept backdoor was published in late 2013 [101] leading to NIST's advice to transition to another approved algorithm. Further research suggested that a second NSA tool exacerbated the RSA software's vulnerability, allowing cracking of encrypted data in seconds.[102]

Recently, the US NSA recommended that parties that have yet to integrated ECDH into their protocols avoid its use, citing concerns about future developments in quantum computing.[103] Given the apparent lack of maturity in the quantum computing field at this stage, many found the NSA's announcement curious and indicated that some rather more discomforting realisations might lie at the root of the

---

[97] See https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml for specification of the US National Security Agency's Suite B algorithms; The German BSI publish recommendation on cryptography within the TR-0212 series of documents, available at https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[98] https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[99] https://news.ycombinator.com/item?id=639976

[100] On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng. Dan Shumow, Niels Ferguson. Available at: http://rump2007.cr.yp.to/15-shumow.pdf

[101] http://blog.oxbadcode.be/archives/155

[102] http://www.rawstory.com/2014/03/nsa-infiltrated-internet-encryption-tools-even-more-deeply-than-thought-study/

[103] http://arstechnica.com/security/2015/08/nsa-preps-quantum-resistant-algorithms-to-head-off-crypto-apocolypse/

announcement – for example that solving the elliptic curve discrete logarithm problem (ECLDP) may not be as intractable as initially thought.[104] Given the ambiguity around the usefulness and reliability of ECC and the afore-mentioned faults deeply embedded in at least some of the primitives involved, it is difficult to advocate for its use despite its general apparent mathematical rigorousness.

Returning to the issue of Dual_EC_DRBG specifically, it is clear that random number generation is crucial for any cryptographic protocol, no matter what the general algorithms used in the end-to-end encryption process. True, rather than pseudo-randomness, must be sought. Hardware-based random number generation facilitates true random number generation most effectively, generating random numbers from a physical process (e.g. thermal noise, the photoelectric effect, quantum optics) rather than a computer program. The presence of unpredictability in these phenomena can be justified by the theory of unstable dynamical systems and chaos theory. They may be used alone or to create the seed for more speedy pseudo-random number generation while adding extra entropy. In encryption generally, system entropy levels should be monitored. Finally, multiple phases of random number generation using different approaches could be advocated in high security environments.

It is briefly note that those analysing the state-of-the-art in the encryption field suggest that quantum cryptography may become widely available in the near future and address many of the issues noted above – although commercially available, its take up appears to be limited thus far. Theoretically, quantum cryptography should ensure that eavesdropping would be revealed through monitoring of changes at the quantum bit level. Research in the field is on-going, with vulnerabilities (although typically addressable) already being found and remedies proposed.[105]

*The eu-LISA perspective:* For our purposes, encryption is particularly important for private and sensitive personal data, the disclosure of which to unauthorised parties or others with malicious intentions could result in negative effects on the person. Under EU law, persons or organisations that collect and manage personal data must protect it from misuse. As per Directive 95/46/EC 'the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.'[106] The draft General Data Protection Regulation[107] that will supersede the afore-mentioned Directive builds upon this further, mandating both data controllers and processors to 'implement appropriate technical…measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.' Essentially, the principles of privacy by design and security by design are being mandated by legislation. Furthermore, personal data breach must be notified except in limited circumstances that include cases where the data controller 'has implemented appropriate technological protection measures [that]…shall render the data unintelligible to any person who is not authorised to access it.'

[104] A Riddle Wrapped in an Enigma. Neal Koblitz and Alfred J. Menezes. Available at: http://eprint.iacr.org/2015/1018.pdf
[105] http://phys.org/news/2015-12-quantum-cryptography-vulnerable-hacking.html
[106] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281 , 23/11/1995 P. 0031 - 0050
[107] COM 2012/0011

Given appropriate knowledge of the state-of-the-art in encryption and the primitives used therein, it is relatively facile to make use of the most appropriate options when implementing systems. Documents such as those produced by ENISA, along with analyses like those undertaken for the preparation of this repot, enable identification of the best approaches from the technical perspective. Hardware-based random number generation can be implemented without significant difficulty and at low cost. Its use, along with the use of other highly secure primitives not mentioned in this document but discussed elsewhere, is a legal and operational imperative.

## 7. Hashing using SHA-2 or better primitives

***Activity classification (NIST): Protect***
***Threats addressed (ENISA classification): Abuse of information leakage, manipulation of information, compromising confidential information, interception of information***
***CIA classification: Integrity***

Hashing and encryption are closely-related processes often undertaken together to assure both data integrity and confidentiality. Strictly speaking, hashing is the process whereby any modification of data will be detected whereas encryption is implemented for the purposes of keeping such data secret so that unauthorised access is prevented. As hashing is typically irreversible – hashes are calculated by sender and receiver in one direction only and compared – it cannot be used as a mechanism of encryption itself.

Hashing may be considered a primitive element in the encryption process. Common hashing algorithms include MD5, SHA and AES. Vulnerabilities in the MD5 algorithm were exploited by the afore-mentioned Flame malware and it should be considered deprecated. In the afore-mentioned ENISA document, the SHA-1 hash function is included as suitable for legacy use and it is still used within protocols for the protection of information at rest as well as a basis for communication security in protocols such as TLS, SSL, PGP and SSH. More recently, the SHA-1 hash algorithm has been demonstrated to be flawed.[108] Nevertheless, despite being developed in 2002, the SHA-2 algorithm, at least until recently, lagged in terms of use behind SHA-1. The situation is slowly improving - at the beginning of this year, some internet browsers began to display security warnings when visiting sites presenting SSL certificates signed with SHA-1 hashes,[109] thus expediting a transition away from the former standard. It seems timely to emphasise the need for such a move away from SHA-1 in this document. Additionally, although the recommended AES algorithm may be considered safe, recent research indicating successful shortcut attacks on AES variants should be followed with interest in the coming years.[110] We advocate that any hashing executed on files in transit, document signatures and digital certificates, should be executed using the SHA-2 primitive or equivalent standard algorithms. Given its greater security, SHA-512 is favoured, certainly for data being stored long term, although ENISA have considered that 256 bit security is sufficient in the near term. Given recent revelations regarding purposeful introduction of backdoors into such algorithms, the use of open algorithms (like SHA-2) is also advocated.

It may be noted that NIST introduced the SHA-3 standard in August 2015,[111] based on the outcomes of a

[108] https://eprint.iacr.org/2015/967
[109] http://cloudsites.rackspace.com/browsers-phasing-certificates-sha-1-encryption/
[110] https://www.schneier.com/blog/archives/2011/08/new_attack_on_a_1.html
[111] https://www.federalregister.gov/articles/2015/08/05/2015-19181/announcing-approval-of-federal-information-processing-standard-fips-202-sha-3-standard

competition to create a new hash standard. It is not intended to be a replacement for SHA-2 and doesn't purport to offer more security, merely to act as a complementary algorithmic option. Although widespread use and acceptance of the algorithm is likely to be years away, developments in this regard may be monitored. Another alternative complementary algorithm is the Whirlpool primitive that produces a 512-bit hash output. As it is based on different mathematics to the SHA family, it may be used in scenarios where algorithmic diversity is required.

*The eu-LISA perspective:* When considering which primitives to use to achieve appropriate strength encryption, choices regarding the hashing algorithms to deploy are perhaps more vague than most. There is a constant need to balance the strength of the algorithm with the convenience of its use. Additionally, as is clear from the foregoing discussion, vulnerabilities in any particular algorithm may not be apparent and may only come to light after deployment.

Given the importance of the technology to eu-LISA and its stakeholders, implementation decisions should err on the side of caution when necessary, hence the recommendations made in the previous paragraph. Nevertheless, the possibility that issues may come to light at any stage means that organisations should also retain the flexibility and capability to change the algorithms used as necessary.

## 8. Encryption key hierarchies

***Activity classification (NIST): Protect***
***Threats addressed (ENISA classification): Loss of sensitive information, failure of devices or systems, malfunction of equipment, interception of information, abuse of information leakage, compromising confidential information***
***CIA classification: Availability, Confidentiality, Integrity***

There is no such thing as encryption without keys, and thus this implies a need to consider encryption key management. The concept of key use may become particularly complicated in an organisation such as eu-LISA, where encryption of data at rest and in transit must be undertaken both on production and on backup systems. Authorised individuals working in disparate locations and for different organisations will require the appropriate keys to decrypt the data when required. Clearly, straightforward application of symmetric or indeed asymmetric cryptography is not appropriate. Encryption key hierarchies should be used with encryption of production and all backup volumes and/or partitions using a hierarchical set of symmetric and asymmetric keys. A root symmetric key will typically be created for each instance of a server or OS in existence that stands at the top of this hierarchy and can only be decrypted by the service account under which it is created or by the computer account, i.e. the computer is tied to the system where the key is created. In case that the system becomes unavailable and restoration of a backup to a different system is required, it is vital that this key be backed up. It should therefore be stored in a secure, off-site location and itself encrypted using a strong method as alluded to previously.
Below the root key, one typically makes use of other symmetric keys themselves encrypted by the root for each instance of a database or other partition (and that should also be stored securely and be encrypted) and asymmetric keys stored on certificates that are protected by the higher level keys that can be used for regular decryption. In the latter case, it goes without saying that the private key must also be kept securely. Although apparently complex, appropriate defined procedures can ensure that all encryption processes based on hierarchical keys run smoothly and securely.

*The eu-LISA perspective:* eu-LISA manages a complex mesh of complementary systems that are physically located in different locations. The need for protection of all information on these systems no matter their

location is paramount, implying a need for strong encryption of data at rest and in transit and therefore secure key management. The use of hierarchical symmetric and asymmetric keys as described is critical and alluded to herein on the basis of its importance for the organisation.

## 9. Grid computing

***Activity classification (NIST): Protect***
***Threats addressed (ENISA classification): Failure of devices or systems, malfunction of equipment (devices or systems)***
***CIA classification: Availability***

A fundamental component of any strategy to ensure data availability will be implementation of suitable data back-up protocols. Data must be backed-up regularly to guard against loss due to infrastructural damage, natural disaster or perhaps more nefarious causes such as ransomware. Beyond such measures, systems can be implemented to high levels of technical advancement so that they are robust to failure. These systems are termed high availability (HA systems).

High availability can be achieved through the use of redundant hardware in cluster-type systems to ensure availability or through the use of software resistant to single points of failure in a system. Common interpretation of high availability indicates at least 99.999% availability and thus no more than 5 minutes of downtime per year.[112] Given the failure rates of modern systems are still high,[113] this is not an easy benchmark to reach. Harvard Research Group have classified availability levels according to five tiers. The lowest tier, AE-0 implies tolerance to data loss or corruption and the highest availability level, AE-4 dictates that business computing availability is continuous, no transactions are lost, no performance degradation occurs and 24x7 operations proceed.[114] The classification also provides a good overview within which to frame discussion of evolving technologies for HA systems.

As per AE1 level systems, the most fundamental aspect of a HA system is data availability, implying data backup as already discussed but also log-based or journaling file systems to identify and recover incomplete transactions that may have been running at the time of failure. AE2 systems must have some form of functional safeguards while AE3 systems must be continuously operational during core hours but can be taken offline for system upgrades or similar. Organisational measures such as maintenance and implantation of measures to improve resistance to environmental influences will certainly help to improve availability, but modern technologies are playing an increasing role in ensuring the high levels of availability that could not be dreamt of many years ago as huge and complex devices and unreliable cabling requiring high levels of maintenance were used. Technologies that can provide such high levels of availability include fault-tolerant hardware in which faults detected through self-checking (e.g. error-correcting code (ECC) code memory can be used to detect and correct internal data corruption and may be advocated in organisations like eu-LISA where data corruption must be absolutely avoided) are contained and/or repaired. Repair brings massive benefits in terms of availability but is only possible in HA systems

[112] High Availability Computer Systems. Gray, J. and Siewiorek, D.P. IEEE Computer Magazine 1991. Available at: http://research.microsoft.com/en-us/um/people/gray/papers/ieee_ha_swieorick.pdf
[113] Google recently indicated that for an application running on 2000 machines, the average number of machine failures per day is greater than 10. See Twitter University: Cluster Management at Google. Video available at: https://www.youtube.com/watch?v=VQAAkO5B5Hg
[114] http://www.hrgresearch.com/pdf/AEC%20Defintions.pdf

when modifications can be executed online (e.g. with hot-swappable disks). When such an approach is feasible, downtime arising from physical devices failures can be virtually eliminated but it does not prevent software issues because hardware-level comparisons will typically not detect software faults. Thus, one must also consider inclusion of sanity checks in software to examine inputs, outputs and data structures and lead to isolation or repair of identified faults and comparators in software that compare the outputs of various modules to ensure consistency in operations. System pairing increases availability further, with two distinct systems (possibly at different locations to guard against environmentally-induced failure) typically taking shares of user load when run in an active-active configuration and automatic failover allowing for one system to take over a full load if necessary. Theoretically at least, there should be some benefit to be had through independent design of each of the two systems to bring design diversity and guard against design faults, although this must be assessed against the higher costs that are implied with such an approach.

Looking forward, most hype in the field has surrounded the use of grid computing.[115] This involves on-demand sharing of software and computational resources that are not subject to centralised control, with the power of distinct and disparate resources harnessed to reach a common goal. Compared to classic high performance computing, each node within the grid performs a single task or runs a single application, and therefore true parallelism is not achieved at the nodal level but rather across networked computers. In typical cases, some form of middleware acts to apportion activities across the individual machines. Provision of a high availability system utilising grid computing can be envisaged through the use of grid technologies to create self-healing systems that can accept new servers and configure themselves flexibly and continuously without downtime. However, the need for security, predictability in terms of performance and resource availability and reliance on one self rather than others would appear to suggest that grid computing as classically envisaged cannot be a paradigm for IT service provision by entities like eu-LISA.

Nevertheless, incorporation of grid computing concepts into more traditional high availability systems may be a route towards the building of more scalable and flexible systems going forward. Traditional high availability systems will likely involve some form of parallel computing, with co-ordinated locking arrangements in place to prevent conflicts between servers and 'spare' server instances available to take over application execution in case faults occur (achieved using hot-standby servers or disparate mirror data). Parallelisation can be effected and coordinated at application or OS levels or through middle-ware. Fault monitoring and reporting will typically be achieved through clustering at application and server level. Grid type concepts can be introduced through use of standard, open and general-purpose protocols and interfaces that allow horizontal expansion at all tiers of the system and thus removal of single points of failure. Use of load balancing devices at appropriate locations between tiers enables suitable apportioning of job execution across available servers and sharing of the appropriate data required to associate jobs across servers and prevent data loss. Use of standard protocols also facilitates integration of new applications from vendors who typically prefer not to tailor their software for specific setups.

While the use of scheduling and load balancing techniques can support sharing of jobs between nodes or machines, short transient unavailability can nevertheless occur due to sudden increases in incoming data rates for jobs or sudden unanticipated processing demands arise. Techniques such as load shedding and

[115] Foster I., Kesselman C., and Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International Journal of High Performance Computing Applications, 15(3):200– 222, 2001.

traffic shaping[116, 117] can alleviate these spikes, but it is nevertheless advisable that capacity to recover from transient failures is implemented. Typically a choice is offered between active standby, in which two or more jobs are run independently on different machines so that a failure of one doesn't affect the other (only one machine sends results onwards for further processing)[118], or passive standby in which a second machine can take over from the first in case of failure provided that the failure is detected and a reaction is quickly instigated. Recent research has focussed on hybrid methods that balance the pros and cons of each method.[119] Implementers would do well to consider such methods when trying to balance availability with cost demands.

Virtualisation technology has been widely used in high availability systems because it permits each physical machine to be logically divided into several virtual machines. It is worthwhile to briefly consider whether parallelisation and standby systems mentioned in the previous paragraph can work appropriately in virtualised environments. Without particular efforts to the contrary, a failed physical machine automatically fails all virtual machines running on it. Mechanisms to recover virtual machines on other physical machines must be implemented as a result; fortunately such systems have been developed in recent years.[120]

Given the above discourse, technology trends indicate that the most relevant development in the field of high availability computing in recent times is the increasing availability of grid computing and technologies based on grid computing principals.

*The eu-LISA perspective:* For eu-LISA and other entities focussed on provision of IT services to end users, ensuring availability is a key task. Indeed, as per its establishing regulation, the Agency's core task of operational management consists of all tasks necessary to keep large-scale IT systems functioning. The management of a secure back-up site in Austria implies significant organisational and financial overhead – the fact that it is deemed necessary highlights the criticality of ensuring data and system availability. Thus, the Agency also continues to consider any technological advancement that can boost availability (and when possible, performance simultaneously) at the single system level. The technologies mentioned above are obviously interesting and the subject of much study by the Agency already in order to investigate their possible use.

## 10. Advanced DDoS protection

***Activity classification (NIST): Protect***

---

[116] Babcock B., Datar M., and Motwani R.. Load shedding for aggregation queries over data streams. In ICDE '04: Proceedings of the 20th International Conference on Data Engineering, page 350, Washington, DC, USA, 2004. IEEE Computer Society

[117] Tatbul N., Cetintemel U.C., and Zdonik S.. Staying fit: efficient load shedding techniques for distributed stream processing. In VLDB '07: Proceedings of the 33rd international conference on Very large data bases, pages 159–170. VLDB Endowment, 2007.

[118] Tanuwidjaja E., Li J.N., Soroudi A., Franklin M., Kubiatowicz J.D. High Availability on a Distributed Real Time Processing System. Technical Report UCB/EECS-2015-144. Berkeley University. May 15 2015.

[119] Zhang Z., Gu Y., Ye F., Yang H., Kim M., Lei H. Liu Z. A Hybrid Approach to High Availability in Stream Processing Systems. Proceedings of the 30th International Conference on Distributed Computing Systems (ICDCS) 2010, pp 138-148.

[120] Wang W.J., Huang H.L., Chuang S.H., Chen S.J., Kao C.H., Liang D. Virtual machines of high availability using hardware-assisted failure detection. Proceedings of the 2015 International Carnahan Conference on Security Technology (ICCST), pp. 1-6.

***Threats addressed (ENISA classification): Denial of service***
***CIA classification: Availability***

When speaking of availability, it is clear that systems must remain functional and fully available when faced with high demands on performance or, perhaps, attacks that attempt to affect their performance. Catastrophic loss of system availability can occur in case of external attack by malicious parties, typically involving so-called denial of service (DoS) attacks that exhaust the computing and/or network resources of the primary victim within a short period of time. These attacks are of concern for any user of computer systems connected to the internet. Distributed DoS (DDoS) in which attackers hijack many (secondary) victim systems to wage a coordinated attack against their targets (the so-called primary victims), thereby making the target unavailable for its normal and legitimate users, are particularly dangerous. Guarding against these attacks requires specific steps to be undertaken that differ from those mentioned in the previous section.

Technologies to prevent denial of service attacks against web servers are very relevant, therefore. Such technologies have seen significant advancement in recent years, responding to an increased frequency of attack referenced earlier. The increases are related to the fact that DDoS attacks are relatively simple to implement, with user-friendly tool kits available.[121] Furthermore, attackers use diverse and constantly-changing methods, altering the types of packets sent and their sources in order to obviate defence mechanisms that are put in place. Thus, guarding against DDoS is a continuous arms race between attackers and security experts. Tool deployment is also complicated by the fact that DDoS attacks vary in terms of the level of automation, the vulnerabilities in networks, OS, applications or protocols exploited, the dynamics of the attack and thus the impacts experienced. There are few, if any characteristics common to every DoS or DDoS attack. Thus, a combination of defence mechanisms is typically required if robust defences are demanded. Nevertheless, it is important to note that any solution will be partial at best aside from complete disconnection from the public internet.[122]

Defence mechanisms have often been categorised according to their main goals, with four categories of activity typically mentioned – intrusion prevention, intrusion detection, intrusion mitigation and intrusions response. They can also be categorised according to the location of deployment – whether on the victim network, intermediate network or source network.[123] The focus herein is on methods that can be deployed at or near the perimeter of an entity's internal system or on an internal network itself and that therefore do not rely on the cooperation of others.

History-based IP filtering[124] is a method focusing on intrusion prevention that can be deployed at edge routers to analyse incoming packets according to pre-built IP address databases. The databases themselves are typically based on previous connection history - infrequent or unknown IP addresses are not trusted. While robust, the methods are subject to manipulation by attackers who purposely obviate the

[121] Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks 44 (2004), pp. 643-666.
[122] Specht S.M., Lee R.B. Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures. Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, September 2004
[123] Douligeris C., Mitrokotsa A. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks 44 (2004), pp. 643-666.
[124] Peng T., Leckie C. and Ramamohanarao K. Protection from Distributed Denial of Service attack using history-based IP filtering, in: Proceedings of IEEE International Conference on Communications (ICC), Anchorage, USA, 2003.

defence by preparing in advance and ensuring that their attack servers are listed. The use of secure overlay services is similar, but access in these cases is restricted to nodes, called servlets.[125] Thus, client machines need to be modified to allow access to the central server, making the method unsuitable for public services. Intrusion detection methods are typically based either on anomaly detection (analysing packet headers, routing information, packet rates or similar)[126, 127] or misuse detection. While the latter rely on well-defined patterns of known exploits – so called intrusion signatures – the former are self-training systems that rely on recognition of abnormal patterns within the background. Thus, they can benefit from the advances in machine learning alluded to earlier in this report. Indeed, a number of methods utilising advanced machine learning have been developed and noted in recent years and security officers should pay heed to these developments closely given their potential to provide continuous high quality defences respondent to novel DDoS attacks over time.[128, 129, 130] Intrusion response mechanisms are more primitive, relying on IP traceback – made difficult by the lack of source accountability in the TCP/IP protocol. Intrusion mitigation mechanisms meanwhile have been developed in response to the realisation noted earlier that complete protection against DDoS attacks cannot be achieved. Fault tolerance – essentially provision of high availability systems that can overcome faults at single locations – is achieved largely using methods mentioned in the previous section. Quality of service measures assure delivery of predictable results for certain application or traffic and can include specific allocation of resources to certain packet types[131] or application of queuing systems that take into account the traffic or packet types.[132]

*The eu-LISA perspective:* As eu-LISA's large-scale IT systems are not connected to the public internet, the threat of DoS attacks is limited. The discussion herein is relevant for corporate IT systems in any case, but it presented mainly because the connection of large-scale IT, or at least databases containing some of the data contained within the systems, to the public internet, will be likely in the coming years. In particular, the Entry-Exit System proposed will have a webserver that travellers can connect to in order to check on the validity of a proposed trip with the terms that apply to their stay in the European Union. The proposed ETIAS system would have an online application interface similar to that implemented by the USA with the ESTA system. DoS prevention will be critical for these web-interfaces. Considering this, it is noted that none of the mentioned technologies alone fully protect against denial of service attacks. A combination of perimeter defence technologies should be implemented in connected systems. In particular, anomaly detection and misuse detection approaches should be used in combination. IP filtering and/or secure

---

[125] Keromytis A., Misra V. and Rubenstein D. SoS: secure overlay services, in: Proceedings of the ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM Press, New York, 2002, pp. 61–72.

[126] Thang T.M.. and Nguyen V.K. Synflood Spoof Source DDoS Attack Defence Based on Packet ID Anomaly Detection – PIDAD. Information Science and Applications (ICISA) 2016, Lecture Notes in Electrical Engineering (376) pp 739-751. 2016.

[127] Qin X., Xu T. and Wang C. DDoS Attack Detection Using Flow Entropy and Clustering Technique. Proceedings of the 11th International Conference on Computational Intelligence and Security (CIS) 2015 pp. 412-415.

[128] Patel J and Katkar V. A Multi-classifiers Based Novel DoS/DDoS Attack Detection Using Fuzzy Logic. Proceedings of International Conference on ICT for Sustainable Development. Advances in Intelligent Systems and Computing (409) 2016. Pp 809-815.

[129] Vrat B., Aggarwal N. and Venkatesan S. Anomaly Detection in IPv4 and IPv6 networks using machine learning. Proceedings of the annual IEEE India Conference (INDICON) 2015.

[130] Jadidi Z., Muthukkumarasamy V., Sithirasenan E., Singh K. Flow-based anomaly detection using semisupervised learning. Proceedings of the 9th International Conference on Signal Processing and Communication Systems (ICSPCS) 2015.

[131] Geoffrey M.B., Xie G. A feedback mechanism for mitigating Denial of Service attacks against differentiated services clients. Proceedings of the 10th International Conference on Telecommunications systems 2002, pp. 204–213.

[132] Brustoloni J. Protecting electronic commerce from Distributed Denial of Service attacks. Proceedings of the 11th International World Wide Web Conference, ACM 2002, pp. 553–561.

overlay are particularly reliable approaches that may be utilised in certain instances.

# 5. Conclusions

Technologies for protecting information technology infrastructure and the data and information stored on and transmitted within them continue to develop at a rapid pace, meeting the requirements demanded by an evolving threat landscape and a broadening of the types of adversaries that those charged with IT security must consider. This overview of technologies takes a broad view of areas in which technological developments are particularly relevant and emphasises those in which the state-of-the-art has progressed most rapidly in recent years. The number of technologies enumerated is large. Thus, it should become apparent to the reader that technology will be a cornerstone of IT security efforts going forward.

The implications for IT security organisation within the enterprise are clear. IT security requires specialist technical knowledge and this must be embedded in the appropriate manner within the teams tasked with ensuring security. Nevertheless, it is also clear that decision making can never rely on knowledge of technical matters in isolation, as the possibility to implement a given technology and the benefits that one can expect to achieve will depend on, among other things, the architectures of the systems to be protected, the types of data and information that they contain, the risks and threats apparent and the legislative landscape in which the organisation is working. Thus, security teams should implement some form of specialised task force to discuss and decide upon technological implementations, taking all necessary opinions and perspectives into account.

The monitoring of technological development will obviously be important to initially identify possible developments in system protections that may bring benefits and address identified risks or issues and to feed the necessary discourse between specialists within such a task force. For eu-LISA, the technology watch function will by necessity have to include examination of IT security technologies on a sufficiently regular basis to keep up with the pace of change in the field. It is imperative, therefore, that a follow up document on the same topic will be prepared in due course. In the interim period, contributions to the afore-mentioned discourse are planned as necessary.

EL-01-16-835-EN-N



ISBN 978-92-95208-46-9 doi:10.2857/320307