2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

The Role of COTS Products for High Security Systems

Robert Koch
Institut für Technische Informatik
Universität der Bundeswehr
Neubiberg, Germany
Robert.Koch@UniBw.de

Gabi Dreo Rodosek
Institut für Technische Informatik
Universität der Bundeswehr
Neubiberg, Germany
Gabi.Dreo@UniBw.de

Abstract: Today, economic pressures and decreasing military budgets enforce a revision of armament projects. While comprehensive and cost-intense equipment acquisitions could be realised during the Cold War, overextension and global economic crisis forced the abatement of projects and broad cutbacks of the residual undertakings.

Based on this, one of the most important tendencies of the last few years is the intense use of commercial off-the-shelf products (COTS) and master agreements with the industry. In contrast to past armament projects, the necessary hardware and software is no longer designed with respect to special military requirements, but products already available on the market are used wherever applicable.

The increasing use of COTS products in all areas of armament is a matter of special importance, opening tenuous points of attack. By that, the number of important security incidents has grown larger in the past few years even with more and improved security mechanisms like firewalls and Intrusion Prevention Systems in place.

On the contrary, through the use of sophisticated and targeted attacks, even highly secured or isolated networks and systems can be compromised. Stuxnet or the attacks on RSA and the subsequent compromise of Lockheed Martin and other companies of the American defence industry are well-known examples. Conficker was another demonstration of the comprehensive infection of secured networks, for example in the Federal Armed Forces or the Royal Navy.

Based on that, a significant security hazard arises which is of essential importance with regard to the Cyber Domain.

This paper analyses the effect of COTS products and proprietary software with respect to the security of military systems. Based on the identified endangerments, conclusions for the recovery of the security of military information systems are presented and implications for the implementation of Cyber Operations are given.

Keywords: *commercial off-the-shelf, high security, data leakage, information operations*

1. INTRODUCTION

Armament projects are often characterised by their complexity, typically in conjunction with high costs for development and acquirement, but also for maintenance during the utilisation period. While comprehensive and cost-intensive equipment acquisitions could be realised during the Cold War, overextension and the global economic crisis forced the abatement of numerous projects and broad cutbacks of the residual undertakings. To be able to reduce costs on new and indispensable projects, the use of COTS products and master agreements with the industry has been widely used in recent years. Therefore, hardware components are no longer designed and optimised for military applications but standard hardware products of the market are used wherever possible. On the one hand, this approach enables substantial cost savings, on the other hand, numerous problems arise which can often only be recognised at a second glance. Through the use of COTS products and widespread proprietary software, various security and supply problems are opened up which can endanger the security and availability of systems. For example, COTS products can be introduced very quickly without the need of additional development costs, but on the other side, there is often no availability guarantee.

Also, numerous systems are using proprietary software, often based on general licences concluded for whole organisational areas and running out-of-date versions of operating systems and applications. Because of the widespread use of these products in civil everyday life, these systems are alluring criminals and numerous malicious programmes are available to attack them.

The paper analyses the role of COTS products and proprietary software for high security and classified systems with respect to information security (defensive) and information operations (offensive). While there was a three-day symposium of NATO in Brussels in the year 2000 which dealt with COTS products in defence applications [1], the main focus was limited to the use of software products. However, numerous important aspects have arisen in the past few years and now, especially, the hardware has to be taken into consideration, too. Therefore, characteristic properties of COTS products – hardware and software – are presented and their vulnerabilities are analysed. After an assessment of the current situation, action needs for ensuring the security of the systems and implications for the implementation of information operations are given.

The remainder of the paper is organised as followed: First, requirements for high security networks and systems are collected in order to scale for the investigation of the role of COTS products. After that, the characteristic properties of traditional, custom-made systems as well as the aspects of COTS products and general licences are briefly described. Following, an analysis of the relevant aspects arising from the use of COTS products in high security domains and cyber operations is given. Based on these results, necessary steps for the current systems in use are drawn and conclusions for information operations are given.

2. HIGH SECURITY SYSTEMS AND NETWORKS

For implementing secure and robust systems and networks, numerous aspects of the organisational and technical domain must be considered, e.g. in the areas of management, infrastructure, systems and networks (for example, see [2]).

Several guides and recommendations can be used as a guideline to set up secure systems and networks, e.g. NIST-SP 800-36 “Guide to Selecting Information Technology Security Products” [3] or the NIST-SP 800-23 “Guide to General Server Security” [4]. From the software point of view, the basis for a secure system can be a certified Operating System (OS). For the evaluation of the security, the Common Criteria (CC) for Information Technology Security Evaluation[5] (ISO/IEC 15408) can be used. After the completion of the security evaluation, an Evaluation Assurance Level (EAL) can be achieved, where EAL1 is the lowest (functionally tested) and EAL7 is the highest (formally verified design and tested) security level. For example, the system XTS-400 Version 6.4.U4 [6] is EAL5+ certified. seL4 [7] has made a formal verification of what constitutes the basis for a certification for EAL7. Based on a secure OS, the selection of the installed programmes should be minimal and preferably also certified. A minimal set of services, protocols and software should be used.

Especially in a high-secure environment with a strict set of allowed services, the possible links between systems and servers can be monitored and controlled reliably. The use of monitoring software, anti-virus software and Intrusion Detection and Prevention Systems (IDS/IPS) is a crucial point for the surveillance of networks. Often, high security systems are isolated from other networks, or special devices like data diodes are used to secure them. However, the attacks on SCADA networks, e.g. by Stuxnet, demonstrated that offline systems and isolated networks are still not immune from attack. Therefore, the use of IDSs/IPSs is mandatory also for all kinds of critical systems. In particular anomaly-based systems can be of great use: while these systems typically suffer from high false alarm rates when used in networks connected to the Internet, these false alarms can be greatly reduced in high security networks because of the limited set of allowed services and the relatively similar communication processes. Therefore, the main reason for false alarms in traditional networks (the presence of new and unknown benign behaviour), can be excluded.

Based on the level of needed security, further requirements, for example the use of Tempest-proof hardware, high-quality cables with special characteristics regarding physical shielding or Electro-Magnetic Interference (EMI) filters can be necessary. Tempest (discovered by van Eck in 1985, therefore, also called van Eck phreaking) is the endangerment of systems because of their electromagnetic emanation which can be picked up and evaluated, compromising the data processed in a system [8]. All kinds of hardware are at risk, e.g. displays (CRT as well as LCD) [9] and keyboards [10]. Also, data cables of disk drives, etc. can be used for tapping. By using techniques like SVMs, high detection results can be achieved [11].

3. TECHNICAL ASPECTS

An important aspect in context with the origin of high costs of designed hardware is not only the development process itself or the low number of manufactured copies, but also the guaranteed availability of spare parts for a specific period in time. Therefore, the manufacturer is forced to keep spare parts or to be able to rebuild specific parts after plenty of years. Because of the long utilisation period of military equipment of about 10 to 20 years, or even longer, this can be a crucial point when using COTS: Problems can arise if spare parts are no longer available because of the short life cycles, especially in the area of the computer industry. Also, a key design goal of SCSI *is* the backwards compatibility. Therefore, an Ultra-160 SCSI disc should be usable on the bus of a quite old SCSI-1 host adapter. Even though this is possible in theory, device compatibility is often reduced in practice, for example because of different types of signalling (e.g. high and low voltage differentials). Considering other areas, these problems can grow quickly, e.g. see the development of bus architectures in PCs like ISA, VESA Local Bus, PCI, AGP, PCI-X and PCIe and their different revisions and (in)compatibilities. Therefore, it can be difficult to find specific spare parts after several years.

On the other side, the stockpiling of affected material can also be insufficient because of electrostatic sensitivity. It cannot be guaranteed that these parts are still functional after a long time of storage because of different effects, e.g. the behaviour of capacitors. Capacitors are passive electrical components, which are used to store energy in an electric field. They are used to smooth voltages on printed circuits and power supplies, etc. Typically, they consist of two conductive plates, separated by a dielectric. Often, electrolytic capacitors are used which permanently have a low loss rate. If these components are stored, the loss rate is increased based on chemical processes, e.g. the electrolyte can dry out and the capability of smoothing voltages can be reduced. Therefore, the initial current can be so high that the circuit will be destroyed when powering on the system after a few months. This effect *can* but *must not* appear. The quality of aluminium electrolytic capacitors strongly depends on the manufacturing process. The residual current behaviour is an important quantity for the recommissioning of a capacitor after an intercalation. After creating a direct current, it will be quite high and will subsequently drop down to the remaining operational power. However, by switching on the equipment, the current made can be so high that the capacitors are destroyed because of the reduced isolation capability of the dielectric and, therefore, the high leakage current. If high quality components are used, for example high-grade aluminium electrolytic capacitors, the storage time can be up to 10 years or even higher; but if only low-quality items are built in, these effects can occur even after just a few months.

For example, the impact of quality on the duration of life was analysed by a long-term study by Storelab, examining the life-time of hard disc drives (HDDs). For example, the identified failure rate of HDDs produced by Seagate was about 56 percent, while that of Hitachi was as low as five percent. Also, while the operating time of HDDs of Hitachi was about five years on average, that of Seagate drives was only 1.5 to three years, strongly depending on the specific HDD series [12].

Another aspect is the prohibition of the use of brazing solder in the European Union [13].

From July 2006, new electrical and electronic equipment must not contain lead, mercury and some other materials. For servers and storage systems, an exemption was granted until 2010; for network infrastructure equipment, e.g. switches, an exemption is still given. However, the need for using other (lead-free) materials for solder in the area of servers can have extensive consequences because the lifespan of the solder joints will be greatly reduced if they are not executed perfectly. For example, the Xbox 360 has had hardware failures in up to 50 percent of all sold units in 2006 based on problems with the lead-free solid used. This *must not* happen if high-quality components are used; however, *because* of the financial pressure and, therefore, the use of COTS, often cheap products are bought and integrated without an investigation of the installed components. Therefore, spare parts purchased at the date of the introduction of a new system can already be defective at the time of installation if they are stored for a long period. Also, inadequate air conditioning and storage can additionally reduce the lifetime of the spare parts.

Another endangerment is the used COTS hardware itself, because design and fabrication of Integrated Circuits (ICs) are typically performed by different companies to reduce costs of the fabrication process. Often only limited or no control of the manufacturing process is possible and a modification of the original design is possible. One cannot say if the specifications of a circuit contain all implemented functions or if the manufacturer retains some information. A trivial example is an Athlon-XP processor built by AMD, where a hacker found four undocumented Machine State Registers in 2010 which only could be read out after setting the Extended Destination Index to a specific value and which can be used for debugging purposes, etc. [14]. After a request, AMD confirmed the existence of undocumented registers, however, they emphasised that this is *common practice* for hardware testing and development. While no security vulnerabilities have been opened up by these registers, this example demonstrates the possibility of hidden hardware functions. To overcome this shortcoming, Bloom et al. proposed an approach to increase the trust in IC fabrication by logging forensic information of the fabrication process and printing the information on the chips, therefore, enabling an examination of deviations of the chip from the original design [15]. However, the implementation of the proposed systems requires a comprehensive adaption of the complete IC supply chain and manufacturing process for the integration of the use of a Trusted Platform Module (TPM) and corresponding runtime software. Also, several issues are not covered by the proposed approach, e.g. an insertion of trojan circuits cannot be detected, which is crucial when trying to verify the correct system behaviour of COTS in high-security systems.

Another aspect is the endangerment by pre-installed backdoors or data leakage which can be hard to detect. By the use of covert channels or techniques like steganography, an outward transfer of data can be realised which is able to easily bypass security systems. Not only can the Central Processing Unit (CPU) be manipulated in this way, but also components like the network interface card (NIC): For example, 3Com published the 3CR990 series in 2001 (after being taken over by Hewlett Packard in 2010, renamed to HP Secure), which integrates firewall functionalities directly onto the NIC. This could be a predestined point to intervene into the communication and leak data, almost impossible to detect by the server itself and only detectable by a comprehensive statistical analysis of the network traffic. For example, the timing of events can be perturbed to covertly transmit data [16], or covert channels can be encoded directly by network packet delays [17]. An overview of covert channels and corresponding countermeasures is given in [18].

In particular, the consideration of the hardware is crucial, because the use of an EAL7-certified system is performed ad absurdum if the underlying hardware cannot be tested. It must be remembered that special security elements like a TPM chip are subject to the same problem, too, and that the correct behaviour has to be verified for the *whole* system, which is almost impossible in hindsight.

Further aspects are the software and algorithms in use. Considering government or large company projects, often master agreements are concluded – typically with market leaders of proprietary (COTS) software. On the other side, the open-source market offers a comprehensive collection of all kinds of software and algorithms. Here, two philosophies face each other: security gained by keeping an algorithm, programme, etc. secret and not giving any information about its functionality vs. opening the underlying algorithms and techniques for public examination and discussion. While the former is also known as "Security by Obscurity" and endorsed by some public institutions and industrial companies, the latter one is typically supported by scientists. Presenting an algorithm to research enables the possibility of identifying weaknesses of the design, etc. Various examples over the past few years have demonstrated that the secrecy of algorithms cannot be ensured permanently and that uncovering erroneous designs can have serious consequences, e.g. as seen by the reverse-engineering of the Crypto-1 algorithm of the Mifare-Classic RFID tags [19]. Even when Security by Obscurity can be used to temporarily disguise some limited information, like details about the infrastructure [20], using open-source and the scientific power of the community is a more promising way to gain security, as demonstrated by Hoepman et al. [21].

The correctness of the software is crucial in high-security systems. Often, a valuation of software based on the number of errors per Line of Code (LoC) is done. There are numerous arguments about which kind of software has respectively fewer programming errors, free and open source software (FOSS) or COTS. However, one always has to take into account the methodologies of the different evaluations and comparisons. For example, often only the sum of the known errors is matched, regardless of the severity of the corresponding vulnerabilities or other important aspects. For example, by investigating the details of the Common Vulnerabilities and Exposures (CVE) database [22], 48923 entries could be found on January 31th, 2012. Therefore, from 2009 to 2012, 185 vulnerabilities were identified in Windows 7, of which 47 percent can be used to gain privileges [23]. Reckoning the vulnerabilities of GNU/Linux, 429 CVEs are known from 1999 to 2012 of which 9.6 percent can be used to gain privileges. With respect to the average vulnerabilities per annum (without the CVEs of 2012 because of the early point in time of the year), Windows 7 has about 60 and the GNU/Linux about 33 vulnerabilities annually. If one considers only the vulnerabilities in GNU/Linux since the release of Windows 7 (July 2009), the average number drops down to about five. It must be taken into consideration that the statistics concerning the number of vulnerabilities often differ and the concrete numbers must be analysed in detail. For example, another evaluation mentions 299 vulnerabilities in GNU/Linux from 2009 to 2011, therefore, about 100 per year. These strong differences can arise because of the considered drivers included, e.g. most of the vulnerabilities do not originate from the core Kernel, but from drivers of peripheries, etc. Sometimes, even utility programmes are included into the statistics, raising the numbers additionally.

Also, the severity of the vulnerabilities must be taken into consideration: For example, the possibility of gaining privileges often *can* be more dangerous than the susceptibility to a Denial of Service (DoS) attack. Therefore, the different vulnerabilities are weighted in the Common Vulnerability Scoring System (CVSS) [24] scores based on three groups (base, temporal, environmental), and their hazardousness from zero to ten with higher values presenting more serious gaps. Regarding Windows 7, the average CVSS score is 8.4, while GNU/Linux has an average about 5.3; looking forward to all vulnerabilities in the CVE database, the average is 6.9. Of course, the real-world endangerment of a vulnerability must be assessed based also on the specific requirements of the operational environment. For example, a DoS vulnerability can be more dangerous in a real-time control system than in a database system.

Also, the number of patches is sometimes used for a comparison. This is quite insufficient, because today patches are often fixing numerous security weaknesses at once, for example on fixed release circles (patch days), therefore, not opening up a comparable base.
It must at least be kept in mind that in the case of COTS software, only the released vulnerabilities can be consulted while the error search is more complex than in the case of FOSS with an available source code. Furthermore, FOSS enables numerous possibilities for security evaluation and hardening, e.g. see Charpentier et al. [25].

However, independent from the kind of software or systems in use, human beings will always produce errors. Panko gives a comprehensive overview of studies investigating how often human errors occur. In the section about programming errors, various studies are given, for example the error rate depending on the number of people in a development team or the influence of the used programming language [26]. Table 1 gives a few examples of the examined error rates.

TABLE 1: SELECTED ERROR RATES IN PROGRAMMING [26].

Reference	System / Language	Error Rate
Graden & Horsley [1986]	Major telecommunications project at AT&T, 2.5 million LoC, 8 software releases	3.7%
Linger [1994]	Formal Development / Cleanroom	0.23%
Jones [1998]	Errors per 100 LoC • Visual Basic • Java • COBOL • FORTRAN • C Average	 1.1% 1.2% 1.4% 1.6% 2.0% 1.5%
Cohen [2006]	300 code inspections CISCO systems	3.2%

Techniques like formal development and cleanroom development, etc. can help to reduce the error rates.

As virtualisation is used regularly today, it also has to be considered. On the one side, security can be enhanced by the use of virtualisation because of the isolation of different instances of OSs and applications. On the other side, the code of the Virtual Machine (VM) can also be erroneous, therefore, opening up serious vulnerabilities which can affect all running VMs. Even if there are no errors in the implementation, virtualisation concepts can be used to control systems, and are practically undetectable. The Blue Pill concept described by Rutkowska [27] is a well-known example of this kind of endangerment. Another threat that is difficult to detect derives from the use of System Management Mode-based rootkits which are able to hide their memory footprint and which are OS-independent [28].

Another important aspect is that the software can also be used to integrate backdoors – with much less effort compared with hardware. Especially when proprietary software is used and no control of the source code is possible, the risk of data leakage and pre-installed backdoors is high. The integration of rootkit-technology in DRM software on music CDs manufactured by SONY-BMG [29], or the Energizer DUO USB Battery Charger trojan which opens a backdoor on a TCP port 7777 [30] are well-known examples. Other examples can be found in the area of smartphones, where several incidents have been known in recent times, e.g. the government spying tools built into Nokia, Blackberry and iPhone smartphones as the hacking group Lords of Dharamraja released early in 2012 [31], or the rootkit software developed by CarrierIQ which is installed on approximately 140 million Android, BlackBerry and Nokia devices and acts like a spyware, e.g. logging keystrokes [32].

4. ORGANISATIONAL ASPECTS

Several organisational aspects must be taken into consideration when dealing with COTS in high-security environments. On the hardware end, by using COTS in security-sensitive systems, an important threat is opened up: because of their application area, COTS typically are not optimised or checked for radiant emittance further than the requirements of electromagnetic compatibility necessary to fulfil the directives of, e.g. the European Union transposed national laws (directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity [33] or directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility [34]). With respect to security-related systems, these directives are not sufficient: for example, electromagnetic compatibility is defined in Article 2 in 2004/108/EC as the ability of equipment to function *satisfactorily* in its electromagnetic environment without introducing *intolerable* electromagnetic disturbances to other equipment in that environment. With respect to Annex I, “1. Protection requirements, number a, equipment shall be designed and manufactured that the electromagnetic disturbance generated does not exceed the level above which radio and telecommunications equipment or other equipment cannot operate as intended.” In particular, no threshold values are given by the directives. Therefore, protection against the tapping of COTS cannot be ensured by the certified electromagnetic compatibility based on the directives. Beyond these obvious possibilities of leaking data, more sophisticated attack possibilities must be taken into consideration, also known as side channel attacks: For example, it is possible to intercept keyboards by the sound emanated when typing. By the execution of an acoustic triangulation attack, whole sessions can be attacked with high recognition rates. Only publicly available tools and hardware is necessary, therefore, the attack can be performed even by non-technical people [35].

Because of this, adequate organisational measures must be conducted when COTS are used in applications relevant to security, e.g. the selection of inside rooms, measuring of the radiant emittance or consequent encryption of transmitted data.

In the context of high-security systems, software versions as well as system configurations must be released by the responsible competent authority. On the one side, these processes can be quite time-consuming, typically lasting several months or even longer. Therefore, the software products, e.g. operating systems are used for as long as possible during the life-span after the acceptance test and approval. On the other side, master agreements often do not include every new software release because of financial reasons, also introducing delays in the software regeneration. For this reason, the used software does not keep up with its life-cycle carried on by the manufacturer, resulting in out-dated and vulnerable installations in security-related systems.

One must also bear in mind that isolated systems and networks are no longer protected against attacks as examples like Stuxnet demonstrated. The weaknesses of human beings and today's sophisticated social engineering techniques [36] compromise even isolated and high-security systems. The successful attacks on RSA and the subsequent compromise of Lockheed Martin, Northrop Grumman and other companies of the American defence industry (e.g. see [37]) is only one example from recent years.

Several manufacturers of proprietary software have introduced so-called patchdays due to organisational and practical aspects, e.g. Microsoft, Oracle or Adobe (e.g. see [38]). On the other side, this policy unnecessarily delays patches, enabling crucial points of attack. Also, it is not guaranteed that the manufacturer will include all necessary patches, as the example of the thumbnail hole in Windows demonstrated: even though a Metasploit module for creating corresponding malicious files was released almost simultaneously with the security advisory of Microsoft, no patch was included in the subsequent patch day [39]. Another problem of proprietary software is the dependency to the vendor and his promises. For example, Microsoft announced to continue the support of Windows NT 4 until the end of 2004. Even so, the company stated they would not provide a patch for a new security vulnerability in NT 4 early in 2003 [40]. In contrast to FOSS, where it is always possible to fix an identified vulnerability, one is adhered to the vendor in the case of COTS.

Another aspect which must be mentioned in this context is what Bruce Schneier calls "bad civic hygiene". A rising trend in recent years is that governments force companies to redesign their communication systems and information networks to facilitate surveillance [41]. This is based on their desire to be able to pursue criminal activities. Even though this is a homemade problem, by introducing such backdoors, serious security vulnerabilities are opened up which can also easily be exploited by an attacker.

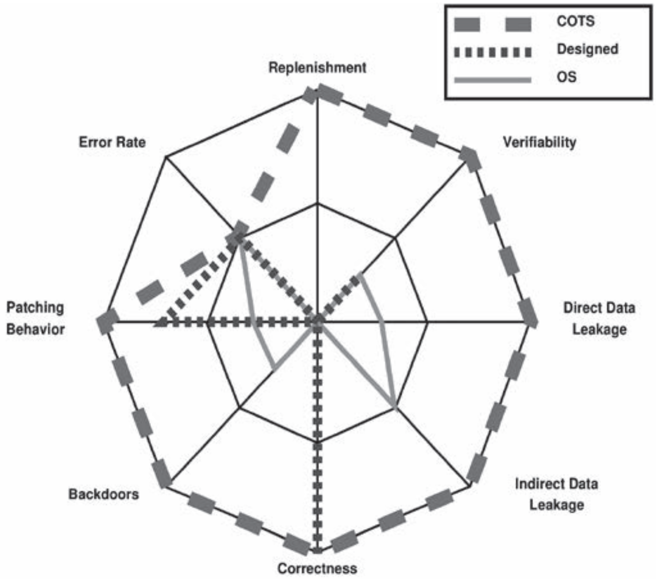
5. USING COTS PRODUCTS IN HIGH SECURITY SYSTEMS

Based on the identified influencing factors, the crucial aspects for using COTS, open-source and designed products are summarized qualitatively in Figure 1.

In detail, the following aspects must be taken into consideration:

- **Replenishment:** Especially for COTS products, the availability can be challenging after a few years. This cannot necessarily be compensated by storage because of the electronic components used. When using designed products, the supply can be governed by contract, typically reflected in high costs. Open-source enables the remanufacturing as needed; however, only a few circuits are available as open-source.
- **Verifiability:** While designed as well as open-source products can be verified with respect to their implementation, this is quite difficult for COTS.
- **Direct Data Leakage:** COTS products often implement undocumented functionality for statistical evaluation, etc. Also, a hardly detectable outward transfer of data can be integrated in COTS products.
- **Indirect Data Leakage:** Because of their cost-oriented design and fabrication as well as the fuzzy regulations, COTS products are strongly at risk of leaking data by radiation. Open-source can also be endangered by that phenomenon, but can be adapted and secured more easily. On the other side, designed products can be shielded per se.

FIGURE 1: INFLUENCING FACTORS ON SECURITY DEPENDING ON THE PARADIGM, *COMMERCIAL OFF-THE-SHELF, OPEN-SOURCE AND DESIGNED SYSTEMS.*



- **Correctness:** The public analysis and discussion of algorithms and procedures can reveal design errors in an early state. While Security-by-Obscurity can be quite effective in restricted military domains, it typically will not be in the public market and the use of widespread COTS.
- **Backdoors:** The difficult and limited test and control opportunities of COTS open up an endangerment by backdoors.
- **Patching Behaviour:** In the case of vulnerabilities, COTS depends on the manufacturer. Also when using designed products, later requests for patches can produce high costs. In contrast, fixing open-source can be quite easy due to the available code, even when there is no support.
- **Error Rate:** The error rates of all paradigms strongly depend on the design and development principles and techniques, and are not predictable.

To control the presented threats opened up by the use of COTS, several actions should be taken; on the other side, corresponding vulnerabilities in target equipment can be exploited for information operations in cyber space. The following aspects have to be considered:

- The communication of high-security systems should be statistically analysed to detect covert channels and unwanted behaviour. Because of the limited number of services in high-security networks, anomaly-based detection can be used to detect unwanted behaviour while achieving low false alarm rates. However, this may not be enough if a malicious behaviour is implemented from the beginning into a new device, because the correct traffic characteristic has to be known by the security system. Here, the use of unsupervised learning techniques can be an approach.
- Measurements of the radiation emittance must be done in areas where no adequate structural protection can be guaranteed by the buildings. It is important to include all possible media and connections, e.g. electromagnetism over the air, acoustics, interlinking in the power network, etc. While Tempest can be very powerful if cyber components are able to operate in the target area or adjacencies, the typical information operation will be conducted over long distances and, therefore, not able to exploit this valuable information.
- When using COTS in environments relevant to security, only long-term supported software and hardware should be used. Especially, only high-quality products should be purchased, including sufficient spare-parts. Suitable and controlled storage is a must-have for enabling adequate replenishment.
- If COTS are used in high-security systems, a doubling of systems can be used to strongly increase security while keeping costs reasonable. By the use and implementation of two independent products and the comparison of their calculations, anomalies and manipulations can be detected more easily.
- Where possible, COTS should be replaced by suitable open-source software and algorithms as well as open standards to be able to minimise design errors, etc.

Table 2 summarises important threats and attack opportunities related to COTS products.

TABLE 2: REQUIREMENTS FOR ENSURING SECURITY WHEN USING COTS PRODUCTS AND ATTACK POSSIBILITIES IN INFORMATION OPERATIONS RELATED TO COTS PRODUCTS IN THE TARGET ENVIRONMENT.

	Hardening	**Information Ops.**
Verifiability	High	Low
Direct Data Leakage	High	Medium
Indirect Data Leakage	High	Low/High
Correctness	Medium	Medium
Backdoors	High	High
Clearance	Medium	High

6. CONCLUSION

COTS products are used in ever more areas, for example for high-security systems and networks, and for hardware as well as software. By the use of COTS in areas relevant to security, numerous endangerments arise. Not only evident aspects like the lack of verifiability, but also secondary factors like replenishment and long-term availability must be taken into consideration. Therefore, the use of COTS products for mission-critical applications poses an imminent challenge. Even so, this endangerment is widely neglected at the moment: Based on the ongoing proliferation of attack tools and the numerous vulnerabilities opened up by the use of COTS, current and especially prospective military missions can be easily compromised: on the one side, effective attacks can be conducted even by an amateur. On the other side, aspects like reliability and supportability can strongly affect missions. With respect to the increasing financial pressure and the comprehensive use of COTS, it is crucial to address these challenges in depth. Therefore, an assessment of the usability and endangerment by the use of COTS in high-security environments must consider all layers in use, hardware as well as software. Based on the identified shortcomings, the high risk opened up by COTS can be attested. Appropriate countermeasures must be taken to overcome these endangerments, e.g. the statistical analyses of network communication. On the other side, an appropriate protection and examination of COTS can produce important knowledge about attack vectors, usable for own information operations in the cyber domain. Therefore, own system vulnerabilities must be identified and closed, and weaknesses must be known to keep superiority in information operations and to be able to defend from countermeasures.

ACKNOWLEDGEMENT

This work was done at the Chair for Communication Systems and Internet Services, led by Prof. Dr. Dreo Rodosek, part of the Munich Network Management (MNM) Team.

REFERENCES:

[1] NATO Research and Technology Organisation, “Commercial Off-the-Shelf Products in Defence Applications (The Ruthless Pursuit of COTS)”, in *Information Systems and Technology Panel (IST-016)*, 2000.

[2] Federal Office for Information Security. (2007). *IT-Grundschutz Catalogues* [Online]. Available: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues

[3] T. Grance *et al., “Guide to Selecting Information Technology Security Products,”* NIST Special Publication 800-36, 2003.

[4] K. Scarfone *et al., “Guide to General Server Security,”* NIST Special Publication 800-123, 2008.

[5] *Common Criteria Common Methodology for Information Technology Security Evaluation*, Common Criteria Recognition Arrangement, 2009.

[6] *Security Target, Version 1.22 for XTS-400, Version 6.4.U4,* BAE Systems Information Technology, Inc., London, UK, 2008.

[7] G. Klein et al., “seL4: Formal Verification of an OS Kernel,” in *ACM Symp. Principles of Operating Systems (SOSP)*, Big Sky, MT, 2009.

[8] M. Kuhn and R. Anderson, “Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations in Information Hiding,” in *LNCS 1525*, 1998, pp. 124-142.

[9] M. Kuhn, *Compromising Emanations: Eavesdropping Risks of Computer Displays*, University of Cambridge, Computer Laboratory, Cambridge, UK, Tech. Rep. UCAM-CL-TR-577, Dec. 2003.

[10] M. Vuagnoux and S. Pasini, “Compromising electromagnetic emantations of wired and wireless keyboards,,” in *Proc. 18th Conference on USENIX Security Symp. (SSYM09)*, USENIX Association, 2009, pp. 1-16.

[11] Z. Hongxin *et. al*, “Recognition of electro-magnetic leakage information from computer radiation with SVM,” in *ScienceDirect Computers & Security*, no. 28, issues 1-2, pp. 72-76, 2009.

[12] Storelab. (2010). *(Comparison of the reliability of hard drives of the main producers)* [Online]. Available: http://www.storelab-rc.ru/sravnenie-nadezhnosti-hdd.htm

[13] *Directive 2002/95/EC of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment*, COD 2000/0159 extended to the EEA by 22003D0147, 2003.

[14] Czernobyl. (2010). *Super-secret debug capabilities of AMD processors* [Online]. Available: http://www.woodmann.com/collaborative/knowledge/index.php/Super-secret_debug_capabilities_of_AMD_processors_!

[15] G. Bloom *et al*., “Fab Forensics: Increasing Trust in IC Fabrication,” in *IEEE Int. Conf. Technologies for Homeland Security (HST)*, Waltham, MA, 2010, pp. 99-105.

[16] G. Shah *et al*., “Keyboards and Covert Channels,” in *15th USENIX Security Symp*., USENIX Association, 2006, pp. 59-75.

[17] V. Berk et al., *“Detection of Cover Channel Encoding in Network Packet Delays,”* Dartmouth College, Hanover, Tech. Rep. TR2005-536, 2005.

[18] S. Zander *et al*., “A Survey Of Covert Channels And Countermeasures In Computer Networkprotocols,” *IEEE Commun. Surveys & Tutorials*, vol. 9, no. 3, pp. 44-57, 2007.

[19] K. Nohl and D. Evans, “Reverse-Engineering a Cryptographic RFID Tag,” in *17th USENIX Security Symp*., USENIX Association, 2008, pp. 185-194.

[20] Dafyyd and Stuttard, “Security & Obscurity,” in *ScienceDirect Network Security*, no. 7, pp. 10-12, 2005.

[21] J.H. Hoepman and B. Jacobs, “Increased security through open source”, *Commun. ACM*, vol. 50, no. 1, pp. 79-83, 2007.

[22] The MITRE Corporation. (2012). *Common Vulnerabilities and Exposures* [Online]. Available: http://cve.mitre.org/

[23] cvedetails.com. (2012). *CVE Details: Windows 7 Vulnerability Statistics* [Online]. Available: http://www.cvedetails.com/product/17153/Microsoft-Windows-7.html?vendor_id=26

[24] P. Mell *et al*. (2007). *Common Vulnerability Scoring SystemVersion 2.0* [Online]. Available: http://www.first.org/cvss/cvss-guide.html

[25] R. Charpentier and M. Debbabi, “Security Evaluation and Hardening of Free and Open Source Software (FOSS)”, in *Information Systems and Technology Panel* (IST-091), NATO Research and Technology Organisation, 2010, pp. 18-1–18-16.

[26] R. Panko. (2008). *Ray Panko’s Human Error Website* [Online]. Available: http://panko.shidler.hawaii.edu/HumanErr/Index.htm

[27] J. Rutkowska, *Subverting Vista Kernel For Fun And Profit*, presented at the Black Hat Japan, Tokyo, 2006.

[28] S. Embleton et al., "SMM rootkits: a new breed of OS independent malware", in *Proc. 4th Int. Conf. Security and Privacy in Commun. Networks (SecureComm '08)*, 2008, pp. 11:1-11:12.

[29] D.K. Mulligan and A. Perzanowski, "The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident", *Berkeley Technology Law Journal*, vol. 22, pp. 1157ff., 2007.

[30] US-CERT. (2010). *Energizer DUO USB battery charger software allows unauthorized remote system access (Vulnerability Note VU#154421)* [Online]. Available: http://www.kb.cert.org/vuls/id/154421

[31] NDJ World. (2012). *Secret Government Spying Build Into Smartphones* [Online]. Available: http://www.nodeju.com/17809/secret-government-spying-build-into-smartphones.html

[32] T. Eckhart. (2011). *Android Security Test: CarrierIQ* [Online]. Available: http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/

[33] Directive 1999/5/EC, 1999.

[34] Directive 2004/108/EC, 2004.

[35] A. Hiu and Y. Fiona, *"Keyboard Acoustic Triangulation Attack"*, M.S. Thesis, Chinese Univ. of Hong Kong, Hong Kong, 2006.

[36] S. Gold, "Social engineering today: psychology, strategies and tricks", *ScienceDirect Network Security*, vol. 2010, issue 11, pp. 11-14, 2010.

[37] F.Y. Rashid. (2011). *Northrop Grumman, L-3 Communications Hacked via Cloned RSA SecurID Tokens* [Online]. Available: http://www.eweek.com/c/a/Security/Northrop-Grumman-L3-Communications-Hacked-via-Cloned-RSA-SecurID-Tokens-841662/

[38] R. Lemos. (2003). *Microsoft details new security plan* [Online]. Available: http://news.cnet.com/2100-1002-5088846.html

[39] H Security. (2011). *Microsoft warns of thumbnail hole in Windows* [Online]. Available: http://www.h-online.com/security/news/item/Microsoft-warns-of-thumbnail-hole-in-Windows-1163562.html

[40] P. Roberts. (2003). *Failure to Patch NT Flaw Causes Concern* [Online]. Available: http://www.pcworld.com/article/110054/failure_to_patch_nt_flaw_causes_concern.html

[41] B. Schneier. (2010). *Web snooping is a dangerous move* [Online]. Available: http://edition.cnn.com/2010/OPINION/09/29/schneier.web.surveillance