



DIALOGUE

Volume 3 • No. 9 | 2010 June

CONFERENCE REPORT

Border Security 2010

by Silvia Venier, Centre for Science, Society and Citizenship

IN THIS ISSUE

- 1 *Conference Report*
Border Security 2010
- 3 *Focus Group Report*
Identification and
Classification in Embedded
Systems and Ambient
Intelligence
- 7 *News and Notes*

DIALOGUE is published quarterly by The Hastings Center, a HIDE Partner.

PRINCIPAL INVESTIGATOR
Thomas H. Murray, *President and CEO*

EDITOR & PROGRAM MANAGER
Karen J. Maschke, *Research Scholar*

ART DIRECTOR
Nora Porter

MANAGING EDITOR
Joyce A. Griffin

CONSULTING EDITOR
Gregory E. Kaebnick

This work was supported in part by the European Commission under contract FP7-217762 HIDE, Homeland Security, Biometric Identification & Personal Detection Ethics.

On 3 and 4 March 2010, the SMi group held its Border Security 2010 conference in Rome, bringing together leading international experts from the security sector to discuss border management procedures and technologies. As a world leader in business-to-business information, SMi organizes over 150 conferences, workshops, and master classes every year.

The Border Security conference provides a yearly networking opportunity for security professionals and international experts who deal with land, air, and maritime border security. The conference brought together high-level representatives from international border security agencies (such as FRONTEX of the European Union, NATO, and Borderpol); governmental bodies (the Spanish Guardia Civil, the UK immigration advisory service, the U.S. Department of Homeland Security, the Rome Airport Police, and the Romanian Border Guard); various industries (BAE Systems, ARINC EMEA, and Sagem Sécurité); research institutes (Fraunhofer Institute for Computer Graphics Research and the Centre for Asia Studies); and relevant interest groups (the European Biometric Forum).

Advanced Technologies and Effective Border Security

Border security is a process that incorporates a broad spectrum of legal, social, cultural, and political paradigms into specialized national and transnational programs and policies. This year the conference focused

“The aim of border security strategies is to protect the freedom to enjoy our way of life in a safe, just, and tolerant society.”

particularly on the deployment of the most advanced technologies in the management of borders. Participants agreed on the fact that an effective border management system has two main objectives—namely, reaching the highest level of security in order to protect the state from unauthorized entries, while at the same time facilitating the enter/exit procedures for bona fide travelers, which is a paramount feature of the global village.

CONTINUES ON PAGE 2



Conference Speakers

- Keith Best
Immigration Advisory Service, UK
- Edgar Beugels
Frontex
- Jordi Bonet
Police of Catalonia, Spain
- Raffaele D'Orsi
Metropolitan Police, UK
- Marius Dumitru
Romanian Border Police
- James Ferryman
Project EFFISEC
- Bogdan Ivanescu
Romanian Border Police
- Nicodemo Liotti
Rome Airport Police
- Mike McBride
IHS Jane's Information Group
- Andrew Mellors
BAE Systems
- Roberto Mugavero
University of Rome
- Brian Muir
*Association of Chief Police Officers
Scotland (ACPOS)*
- Alexander Nouak
*Fraunhofer Institute for Computer Graphics
Research IGD*
- Bill Puttmann
*Weapons of Mass Destruction Centre,
NATO*
- Julio Serrano
Guardia Civil
- Max Snijder
European Biometrics Forum
- Thomas Tass
Borderpol
- Sandrine Trochu
Sagem Sécurité
- Seshadri Vasan
Centre for Asia Studies, India

With these themes in mind, the two-day conference was organized around the main topics of 1) new priorities and challenges for border management, 2) current and emerging border control technologies, and 3) integrated border control systems and international cooperation on counterterrorism strategies. An interactive panel discussion on “People, Technology, and the Future of Ethical Decision-Making” was organized in the afternoon of the first day to look closely at the key social, ethical, political, and legal problems faced in deploying

emerging technologies in the field of border security.

The meeting was chaired by Mike McBride, consultant editor of *IHS Jane's*, an open-source intelligence provider. McBride opened the conference by noting that border security is one of the three main areas encompassed by homeland security; the other two are internal security and the war on terror. In the globalization era, he argued that effective border security and surveillance continue to be vitally important for contemporary sovereign states. International organizations and governmental border control agencies constantly cooperate to build a common international framework of values and procedures. The final aim of these strategies is to “protect the freedom to enjoy our way of life in a safe, just and tolerant society.”

Challenges in Border Management

The first day of the conference focused on the main challenges to contemporary border management. Nicodemo Liotti, who is responsible for security with the Rome Airport Police, gave the opening address. He began by reporting the latest on the deployment of the whole body imaging technologies (commonly known as body scanners) for a trial period of four weeks at the Fiumicino Airport. He then described the structure of the Italian Civil Aviation Organization, which is divided between the ENAC (agency of the Italian Minister of Transport), the Minister of the Interior, and the National Airport Security Programme (NASP), through which security is maintained at the airport 24 hours a day, seven days a week. The antiterrorism plan, which is approved by the Italian Minister of the Interior, encompasses three main phases: preventing (through the NASP), monitoring (through CCTV, patrols, checkpoints), and repressing (through emerging procedures). The employees in the security sector represent 80% of the Fiumicino staff, who manage the passage of approximately 33 million passengers per year through the airport.

The inaugural address was followed by the presentation on “Border Management: Shifting Priorities and Uncoordinated Missions,” given by Thomas Tass, executive director of Borderpol, the world’s international border police and border management organization. Tass pointed out that the continued threats of terrorism and organized criminality invariably result in increasingly intrusive security measures and the introduction of ever-more-sophisticated border management policies, including a complex set of systems and procedures. During the post-cold war era of the 1990s, the world saw a reduction of border security formalities, but the 9/11 events in the United States resulted in a renewed effort to support security measures. He noted that the biggest challenge in border security today is that “even the likeminded states still cannot bring themselves to agree on a system that will bring about an effective, seamless, and interoperable information-sharing system, allowing countries to notify each other about their nationals who might be traveling from one state to another for legitimate reasons.” Governments have to agree on technological standards and policies that can support a universal and voluntary “trusted citizens” program.

A particular perspective was outlined in the talk given by Keith Best, immigration expert and former chief executive of the UK Immigration Advisory Service, the largest not-for-profit organization giving legal advice and representation to immigrants and asylum seekers in the United Kingdom. In his talk about asylum policy and reinforced border controls, Best presented surveys regarding public perception of illegal immigration in Britain. According to the British Social Attitudes Studies, there was a 10% increase in public hostility toward immigrants between 1993 and 2003. Best pointed out that the most critical issues raised by immigration will be a clear regulation of the Western national citizenship

CONTINUES ON PAGE 4



Identification and Classification in Embedded Systems and Ambient Intelligence

By Karolina Owczynik, Zuyd University

On 26 February 2010, the Infonomics and New Media Research Centre at Zuyd University organized the second HIDE Focus Group meeting on Embedded Systems and Ambient Intelligence in Maastricht, the Netherlands. The Focus Group explored the ethical and social issues related to embedded technologies, one of the four technological areas of work package three on critical issue identification. As only a limited number of embedded systems actually involve personal identification, the partly overlapping technological areas referred to as ambient intelligence (AmI), pervasive technology, ubiquitous computing (UbiComp) and the internet of things (IoT) are also included within the scope of the focus group.

Irma van der Ploeg opened the half-day session, welcoming participants and introducing the theme and ambition of the focus group, as well as the invited speakers. These speakers included Michel Klein of the Free University of Amsterdam, who discussed the new ways in which human knowledge can be integrated into complex AmI technologies, and Maarten Hogervorst of the defense and security division of the Netherlands Organization for Applied Scientific Research (known as TNO), who demonstrated some of the particularities in defining “abnormal behavior” in an EU-funded security project called Automatic

Detection of Abnormal Behavior and Threats in Crowded Spaces, or ADABTS. Van der Ploeg also encouraged the participants to comment on the draft ethical brief that would be discussed during the afternoon roundtable, drawing from concerns, questions, and issues that may (or may not) have been highlighted by the presentations.

Expert Presentations

The purpose of the expert presentations was to inform participants about state-of-the-art technical developments in fields relevant to the Focus Group topic (http://www.hideproject.org/events/fg-embedded_technology.html). Michel Klein is an assistant professor in the Agent System Research group in the Department of Ambient Intelligence at the Free University of Amsterdam. His research focuses on intelligent technological support for humans, sometimes called “human ambience.” In his presentation, “Human Ambience Integrating Human Knowledge in Ubiquitous Computing Environments,” he introduced several of the research concepts and findings of projects he has conducted with colleagues in the Department of Ambient Intelligence. The approach

of the department toward ambient intelligence focuses on the application of AmI technology to support human functioning. The relevance of this for HIDE lies in the possibility of extend-

“ Human ambience is a human-like understanding of (supportive) environments through the needs and interests of humans. ”

ing this approach to security and crime prevention contexts, where human knowledge will then be embedded in systems for detection of abnormal or criminal behavior.

Klein first described what his research group considers human ambience to be: “a human-like understanding of (supportive) environments” through the needs and interests of humans. This suggests both a narrow and a wide understanding of human ambience, with the narrow perspective involving the application of computational models about human functioning in order to create supportive environments, and the wider perspective including the use of knowledge about human functioning to create intelligent environments. To define human needs and interests,

programs and the broad deployment of electronic documents at borders for citizens and foreigners. He noted that “liberty and justice have been guiding principles for civilization, and we should not compromise them for expediency nor sacrifice the few for the many.”

Integrated Strategies

The second day of the conference was mainly devoted to integrated and automated border control systems and technologies. Roberto Mugavero, from the University of Rome, opened the second day’s proceedings by explaining the successful case of the security strategy put in place by the Italian government during the G8 meeting in Italy last summer. Edgar Beugels followed with his presentation, “European Border Security Challenge.” Beugels is head of the research and development unit at FRONTEX, the European Agency for the management of operational cooperation at the external borders of the member states of the European Union. Beugels talked about the European integrated border security strategy, which relies on border surveillance and border control, with the aim of facilitating registered persons and combating illegal stays. He noted that it is paramount for a European approach on border security to exist so that member states find a common understanding on the concrete meaning of security and its practical applications. This is necessary in order to balance security with freedom and other fundamental human rights.

The issue of coordination among national border security strategies

was also central to the presentation given by Bill Puttmann, civil and military coordination expert of the NATO Weapons of Mass Destruction Center. In his talk on the international border security agenda, Puttmann described the complex functioning of his organization and focused on the NATO strategy to prevent the proliferation of weapons of mass destruction and defending against chemical, biological, radiological, and nuclear threats. This strategy is based on three pillars: prevention through the contribution to global nonproliferation efforts and disarmament; protection through deterrence and vulnerability reduction; and recovery through crisis management, including civil and military cooperation and civil preparedness.

The deployment of biometric technologies for automated border processing was the topic addressed by Sandrine Trouchu, from Sagem Sécurité, and Max Snijder, from the European Biometric Forum. Trouchu’s presentation highlighted Sagem’s long experience in the development of such technologies and summarized the main technical problems faced by her group in implementing them. Snijder described the role of his organization in establishing and promoting dialogue and cooperation among European stakeholders in the field of biometrics. He then gave an update on the current state of such technologies and addressed the use of biometrics in border control procedures. He also mentioned the case of the Dutch passport act, which permits the biometric data of Dutch citizens to be stored as part of the central public

database. With regard to the Dutch policy, Snijder observed that the Dutch Data Protection Authority considered the act to be a “serious infringement of privacy” and had called for it to be reviewed.

In the afternoon of the second day, Alexander Nouak, head of the security technology department of the Fraunhofer Institute for Computer Graphics Research IGD, gave a presentation entitled “Technology Must Adapt to People, Not People to Technology.” Nouak argued that the application of new technologies must never harm human dignity, neglect the privacy of individuals, or, above all, substitute for human—especially police—experience and intelligence. He pointed out that one of the main challenges faced by security staff at border checkpoints is the number of fake documents that travelers use. Nouak described the PRE BORDER LANE project, a technical system for sorting passenger flows into full-screening and minimum-screening streams, based on the idea that the time passengers spend in line to have their passports inspected could be used to scan documents, allowing specific check priorities to be set.

More than 100 people attended the Border Security 2010 conference to hear the important and timely presentations of representatives from high levels of international and governmental organizations. Additional information about the conference is available at <http://www.smi-online.co.uk/events/overview.asp?is=1&ref=3192>.

Klein noted that certain measurements are required. These measurements were said to be developed through three steps: first, the assessment of the human state; second, the reasoning about this state and an attempt to categorize and interpret it into different quantifiable measurements; and third, an analysis of the consequences of these measuring techniques, which are called “support measures.”

Klein then introduced four contexts in which he and his colleagues try to define and operationalize human ambience. These were attention support, depression therapy, emergency scenarios, and medicine-intake monitoring. He explained that they take an interdisciplinary approach involving human-directed

“By the time complex identification technologies are implemented for security purposes, they may overshadow other legal and ethical principles.”

sciences (such as artificial intelligence and computer science) and rely on the conception of “reflective coupled human-environment systems.”¹ This means that humans and environments reflect each others’ current state through interactive processes. In these processes, Klein argued that hardware infrastructures create possibilities for AmI by using models of cognitive processes and that these can mold, shape, and change human behavior. He referred to this process as persuasive computing, in part because it considers human emotions as a variable in the process and because it can render an augmented cognition to particular computerized systems.

In the presentation, Klein also explained how this understanding of human ambience was put into practice at his research department. First, the team uses informal models of human processes from other

domains, such as psychology, neuropsychology, sociology, or criminology. Second, they formalize these informal models into computational models (e.g., variables, mathematical formulas) and use observations and sensors as input to measure human processes. As an example, he mentioned the trainer project, in which heart rate measuring sensors give advice to the user about how fast or how hard he or she should train in order to remain effective, without getting too tired. Third, the team examines the necessity for a model that could help in assessing whether the computer’s decision satisfies the required support for humans.

Klein then focused on his department’s research into depression therapy as part of the EU-funded project called

ICT4depression. In this project, AmI systems were developed to facilitate patients’ decisions about whether a certain therapy was a good fit for them, and then, in certain

cases, provided further input about what kind of therapy might be an even better fit. The research project used new ICTs to monitor the activities of patients with depression in relation to other people and to detect changes in the patients’ moods. These patients were required to send information via the Internet and mobile phones about how they felt, and in response, they received electronic messages formulated by psychologists and other professionals.

During the question and discussion period at the end of the presentation, the ethical aspects of human ambience applications were raised. Klein described these AmI technologies as looking “through” people, as they assist in discovering hidden emotional and cognitive states. However, he acknowledged that the personal data traces gathered through these systems became almost omnipresent. Klein noted that this has

the potential for a number of unintended implications—thus creating ethical concerns—as these technologies continue to be used and developed. He suggested that further research into these concerns was necessary.

The second expert presentation was by Maarten Hogervorst, a scientific researcher with TNO Defense, Security and Safety and TNO Human Factors in Eindhoven. He introduced the EU-funded security project, Automated Detection of Abnormal Behavior and Threats in Crowded Spaces, or ADABTS. TNO is a partner organization with ADABTS, a project that “aims to facilitate the protection of EU citizens, property and infrastructure against threats of terrorism, crime and riots by the automated detection of abnormal behavior.” Hogervorst described how automated detection of “threat behavior” happens within the security context, noting the major problems and concerns currently affecting the development of abnormal behavior detection. He explained that expert operators (humans) interpret and detect what constitutes abnormal behavior with the help of networked detection technologies. He noted that with the “use of massive amounts of sensor data, manual detection is not feasible.” However, methods for automatic detection often produce many false alarms. Hogervorst said that in order to prevent or minimize the chances of these false alarms, it is necessary to increase the capabilities and infrastructure of the systems—something that often involves procuring expensive new hardware and software technology. However, TNO is focused on developing a less expensive supportive system for the operators that allows them to focus on “interesting data.” To define what constitutes interesting data, TNO draws upon the expert knowledge of current camera operators. Their expertise will be implemented into a combination of video and audio surveillance methods facilitated by low-cost software

Focus Group Participants

- Wieslaw Bicz
Optel
- Maarten Hogervorst
TNO
- Michel Klein
Free University of Amsterdam
- Miriam Leis
TNO
- Katja Lindschow
Lancaster University
- Geert Munnichs
Rathenau Institute
- Karolina Owczynik
INM, Zuyd University
- Irma van der Ploeg
INM, Zuyd University
- Jason Pridmore
INM, Zuyd University
- René van Schomberg
EC, DG Research
- Silvia Venier
Centre for Science, Society and Citizenship (CSSC)

technology.

In their current research, TNO focuses on large-scale events and on mass transportation. Hogervorst explained that their project analyzes several elements of the detection process, such as what the users' needs are; what the norms are that distinguish normal and abnormal behavior; how experts define normal and abnormal behavior; and how these parameters can be interpreted and implemented into the operation of various sensor technologies and systems. In order to test certain applications in the design phase, his project observes and uses as an example the experiences of the gaming industry (e.g., casino security systems that detect cheating.)

Hogervorst further explained that the ADABTS research considers the legal and ethical restrictions on certain technologies and the implications for privacy, but the research does not involve specific personal identification features and techniques such as

face or voice recognition. He suggested that automated detection without human operators is currently impossible and would lead to an extremely large number of false positives. Therefore, he added that the "ultimate judgment will always be done by humans." However, he emphasized that research shows human operators need to be increasingly "enhanced" by supportive detecting technologies, since the continuous picture and data analysis is an extremely labor-intensive activity.

Roundtable Discussion: Critical Issues and Ethical Brief

Prior to the focus group meeting, participants received a draft copy of the ethical brief, as well as critical questions to generate and steer the debate. These critical questions were posed in light of the expert presentations and aimed at informing the ethical brief by generating input through the roundtable discussion. Van der Ploeg outlined some of the major critical issues and concerns of identification and detection technologies. Among those she emphasized were the covert and distant nature of data capture; the sensitivity of using "body data"; the "black-boxing" of contestable and sensitive categorizations; and the normative nature of "normality" during various classificatory processes (e.g., "if classification has inherent normativity, how can you contest the norms?"). In addition, she pointed to the potential contradictions and frictions with existing EU laws and general principles. How does user awareness and empowerment happen and how can users consent to the transfer of their data if processes get increasingly embedded (hidden) and automated? These are important ethical starting points for several other principles, including proportionality, nondiscrimination, the presumption of innocence, and bodily integrity.

Drawing on the themes of the

expert presentations, another principle seemed especially interesting and generated heated debate: "the freedom from automated decisions." Van der Ploeg noted the massive amount of automated steps involved in identification processes, the severity of which are often overlooked. Geert Munnichs of the Rathenau Institute emphasized the need to make technology-intensive processes as transparent as possible. This was criticized by other participants, who felt that too much openness could in itself result in unintended consequences (e.g., breach of confidentiality or trust relations). Maarten Hogervorst added that algorithms are almost impossible to make transparent. Van der Ploeg then asked, "What are the possibilities to defend ourselves as citizens from accusations?" and elaborated about how, in the case of security measures implemented to combat terrorism, more grandiose security measures are seen as acceptable because the fear of terrorism has increased. René von Schomberg (European Commission, DG Research) emphasized that by the time very complex identification technologies are implemented for security purposes, they are seen to overshadow other legal and ethical principles.

After an enlightening session and vigorous discussion, the contributions from the expert presentations and the participants in this focus group meeting will be used to inform the draft ethical brief as the main focus group deliverable. For background documents and the agenda, please visit the HIDE Web site at:

http://www.hideproject.org/events/fg-embedded_technology.html

1. Jan T. On human aspects in ambient intelligence. In: Mühlhäuser M, Ferscha A, Aitenbichler E, *Communication in Computer and Information Science*, vol. 11. Berlin, Germany: Springer, 2008, 262-267, p. 262.

HIDE Upcoming Events

- **14 September 2010**
Focus Group Meeting on Technology Convergence. Paris, France.
- **8 October 2010**
Focus Group Meeting on Embedded Technology. Maastricht, the Netherlands.

Recent Publications

- Bayly D, Castro M, Arakala A, et al. Fractional biometrics: Safeguarding privacy in biometric applications. *International Journal of Information Security* 2010;9(1):69-82.
<http://www.springerlink.com/content/wpw7221459105u35/>
- Cavoukian A, Snijder M, Stoianov A, Chibba M. Privacy and biometrics for authentication purposes: A discussion of untraceable biometrics and biometric encryption. *Ethics and Policy of Biometrics*. Berlin, Germany: Springer, 2010, p. 14-22.
<http://www.springerlink.com/content/430jr47273973g48/>
- Friedewald M, Wright D, Gutwirth S, Mordina E. Privacy, data protection and emerging sciences and technologies: Towards a common framework. *Innovation: The European Journal of Social Science Research* 2010;23(1):61-67.
<http://www.informaworld.com/smpp/content~content=a922417231&db=all>
- Parker T. Are we protected? The adequacy of existing legal frameworks for protecting privacy in the biometric age. *Lecture Notes in Computer Science*, vol. 6005. Berlin, Germany: Springer, 2010, p. 49-46.
<http://www.springerlink.com/content/d5t4t51575238523/>
- Rahter NK. Privacy protection in high security biometrics applications. *Ethics and Policy of Biometrics*. Berlin, Germany: Springer, 2010, p. 62-69.
<http://www.springerlink.com/content/0862m718627g4824/>
- Serwaa-Bonsu A, Herbst AJ, Reniers G, et al. First experiences in the implementation of biometric technology to link data from Health and Demographic Surveillance Systems with health facility data. *Global Health Action* 2010;3:1-8.
<http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2830803/>
- Sustrop M. Ethical issues in governing biometric technologies. *Ethics and Policy of Biometrics*. Berlin, Germany: Springer, 2010, p. 102-114.
<http://www.springerlink.com/content/138n66k2425352w2/>
- Van Dijk N. Property, privacy and personhood in a world of ambient intelligence. *Ethics and Information Technology* 2010;12(1):57-69.
<http://portal.acm.org/citation.cfm?id=1731510>
- Weber RH. Internet of things—new security and privacy challenges. *Computer Law and Security Review* 2010;26:23-30.
http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VB3-4Y7WYVD-4&_user=483702&_coverDate=01%2F31%2F2010&_rdoc=1&_fmt=high&_orig=search&_sort=d&_docanchor=&view=c&_searchStrId=1364345242&_rerunOrigin=scholar.google&_acct=C000022720&_version=1&_urlVersion=0&_userid=483702&md5=b51cfee4ccbc7495cd99302fec667977
- Woo RB. Challenges posed by biometric technology on data privacy protection and the way forward. *Ethics and Policy of Biometrics*. Berlin, Germany: Springer, 2010, p. 1-6.
<http://www.springerlink.com/errors/500.mpx?errorid=1c15a963-3507-4e2b-9535-b26ebac15b5f>
- Zhai X, Renzong Q. The status quo and ethical governance of biometric in mainland China. *Ethics and Policy of Biometrics*. Berlin, Germany: Springer, 2010, p. 127-137.
<http://www.springerlink.com/content/amx361k344120480/>

Centre for Science, Society and Citizenship
Rome, Italy

Centre for the Economic and Social
Aspects of Genomics
Lancaster and Cardiff, UK

Centre for Biomedical Ethics—Yong Loo
Lin School of Medicine
Singapore

Eutelis Italia SRL
Rome, Italy

Fraunhofer Institute for Computer Graphics
Research
Darmstadt, Germany

International Biometric Group
London, UK

Optel Ltd
Woclaw, Poland

Sagem Sécurité
Paris, France

The Hastings Center
Garrison, NY, USA

University of Ljubljana
Ljubljana, Slovenia

Zuyd University
Heerlen, the Netherlands