Internet of Things: Emerging and Future Scenarios from an Information Security Perspective

M.T. Dlamini[1], M.M. Eloff[2] and J.H.P. Eloff[3]
[1,3]Information and Computer Security Architectures Research Group
Department of Computer Science, University of Pretoria, South Africa
[2]School of Computing, UNISA, Pretoria, South Africa
Tel:+27 12 9999100, Fax: +27 12 9999131
Email: [1,3]{mdlamini,eloff}@cs.up.ac.za; [1,3]{moses.dlamini, jan.eloff}@sap.com;
[2]eloffmm@unisa.ac.za

Abstract— Information security is becoming a major concern for most worldwide telecommunication companies and more so as we move towards the future Internet of Things. In this era, a plethora of digital devices, people and other physical objects have the potential to seamlessly connect and interact on the future Internet of Things. This paper takes a leap forward to proactively discuss the type of threats that we are likely to face in the future Internet of Things. We discuss scenarios of how a botnet of stoves can bring down a power grid, future life threatening health systems and how a distributed denial of service can be used to beat competition and increase revenues of Telcos.

Index Terms— Future Internet, future threats, information security, Internet of Things and scenarios

I. INTRODUCTION

Today's Internet is moving beyond merely connecting billions of computers and hosting web sites towards connecting a thousand times more physical objects. From e-commerce, e-government, e-banking to e-everything, the Internet is moving into the future Internet of smart phones, smart homes, smart offices, smart vehicles, smart classrooms, smart factories to smart everything. The future Internet is an emerging world of highly networked smart items that will be able to autonomously communicate with each other with little or no human intervention.

The Internet has moved from *isolated* and *only when in office* (mainframe computing) connectivity; to *anywhere* at *anytime* (mobile computing) connectivity; to *anywhere* at *anytime* in ***anyway*** (network convergence) connectivity; and now it is moving towards a new era of the future Internet characterized by *anywhere* at *anytime* in *anyway* by ***anything*** (Internet of all things) connectivity [1]. According to Friedemann [2], the Internet is a changing paradigm, which started as a network of computers, grew to include documents, further improved to include people and services in the era of Web 2.0, and will be further extended in the near future to include physical objects (things). Billions and billions of digital devices, people and other physical objects will have the potential to seamlessly connect and interact on the future Internet of Things (IoT).

This paper discusses the key emerging technological trends shaping the future Internet i.e. network convergence in brief and the Internet of Things in more details. These two emerging trends are the bridges that connect the current Internet to the envisaged future Internet. To ensure that the future Internet is built on bridges that will not collapse, it is very important to at least anticipate and prepare for possible threat scenarios that may come as a result of these emerging and future developments. The leap to embrace and leverage the benefits of the future Internet should be a calculated one, taking cognizance of the potential risks involved.

Today's viruses, worms, Trojans, zero-days, phishing attacks and other threats have the potential to spread in just a few seconds to infect the entire Internet space [3]. The main motive is not necessarily to damage the infected machines, but to use them to perform illegal acts (e.g. distributed denial of service and distribution of spam among others) that are often financially motivated and have damaging consequences. Worms are reported in [4] to have brought down alarm phone centers, train signaling systems and millions of computers, all of which have a huge financial impact.

The main problem in the information security domain is that security researchers tend to concentrate on working on the security solutions for today's threats and vulnerabilities and have no time to work on the emerging and future ones. When new threats and vulnerabilities emerge, security experts are often caught off-guard and taken by surprise; as was the case when the DNS vulnerability was discovered by a researcher called Dan Kaminsky in 2008 [5]. The discovery of this vulnerability led to a mad rush to patch DNS servers worldwide. In [6] there were about 10% organisations reported to have been affected by the DNS incident. Imagine the magnitude of this vulnerability in the era of the IoT whereby on top of the usual DNS servers; there would be object naming servers (ONS); one of the enabling technologies of the IoT.

Conventionally, information security experts respond to information security threats and vulnerabilities in a reactive manner. They rush to produce the countermeasures after a

threat or vulnerability has been discovered. This process takes time and is a little bit costly if discovered after a solution roll-out than if discovered at the development and testing phase. By the time researchers come up with potential solutions, the threats would have already done enough damage and the attackers would have moved on to exploit other avenues [4]. This has created the need to contemplate the emerging and future attacks; to identify and understand trends, visions and technologies that are likely to bring new types of threats.

This paper takes a different approach to the conventional way of doing things. As a first step it discusses the possible and realistic threat scenarios of the future Internet of Things. This paper seeks to proactively provide an understanding of how information security threats might evolve in the near future and years to come. This is done to anticipate and better prepare for emerging and future threats before they could occur.

We also argue that unless security experts get an understanding of the emerging and future threats posed by the future Internet, they will always be caught off-guard and as a result will not be in a position to timely develop appropriate and effective security solutions to defend their information assets from the emerging and future threats [7].

The structure of the paper is as follows: Section I provides an introduction and motivation. Section II discusses the future Internet with specific reference to the key technological concepts that are shaping it. Section III discusses the related work as basis for this work. Section IV discusses the scenarios of the threats to the future Internet and section V concludes and provides future work.

II. The Future Internet

A. Network Convergence

In the near future, the Internet will soon provide a unified platform for the once disparate voice, video and data networks to converge in the next generation networks (NGN) over the Internet Protocol (IP). Voice over IP (VoIP) and IP Television (IPTV) are the starting points. The concept of network convergence over IP presents future Internet users with access to multimedia services over a shared and service independent network. This network is based on an all-IP open standardized architecture. It creates a world where the wired networks merge with wireless, WiMax, Wi-Fi, Bluetooth, GSM, RFID, fixed and mobile networks, vehicular and sensor networks among others.

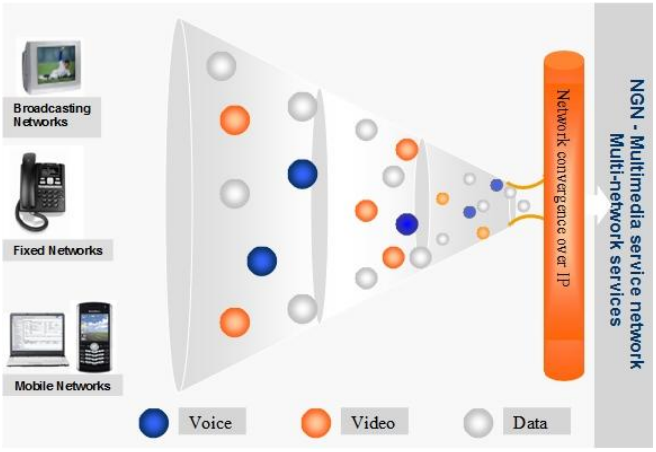

Fig. 1. Voice, video and data converge over IP in the next generation networks.

B. Internet of Things

A full and seamless network convergence over IP leverages the emerging trend of IoT. The IoT builds on the infrastructure of the network convergence by expanding the Internet to real world objects. The IoT is an envisaged world where physical objects seamlessly integrate into the Internet, merging the physical and virtual world; thereby creating real-time end-to-end infrastructures.

Radio frequency identification (RFID) has been coined as the bridge that connects the physical and virtual world [8]. By adding RFID tags to everything, the RFID technology will create an IoT [8][9][10].

In addition, wireless sensor networks are the second bridge that connects the virtual and physical world. Sensors enable physical things to detect and monitor changes in their environment and communicate them back to the virtual world for a response. There exist several enabling technologies such as electronic product code (EPC), ONS, WiFi, MiFi, WiMax, near field communication (NFC) [11], etc as shown in figure 2. These form the lower layer of enabling infrastructure and technologies.

The second layer is the intelligence layer which consists of intelligent agents to interpret a user's context and be able to choose and configure the most appropriate mode of communication to achieve the end-to-end IoT.

The third layer ensures that anything can connect to any service on the Internet at anytime, from anywhere, in anyway possible. The last layer is the envisaged layer of end-to-end IoT. At this layer, all things can seamlessly connect and interact in the future Internet to access web services in the coined Internet of Services (IoS). Organizations are moving towards software as a service, infrastructure as a service, platform as a service and a plethora of other services which will become intense with the introduction of the IoT.

The emerging technological trends of NGN and IoT are driving today's users towards the future Internet which is expected to come along with an unprecedented evolution in the telecommunications landscape. This presents opportunities and challenges. A clear understanding and awareness of these emerging technological trends and the challenges they pose can assist in realizing the opportunities of the future Internet.

Information security is one of the challenges that might hinder the adoption of the envisaged IoT. Even though information security has been viewed as a hindrance or an obstacle to technological developments, it will soon become an enabler and differentiator for the success of the NGN and IoT. Considering security in the early phases of development of the future Internet of Things ensures that we design and build secure, strong and dependable digital bridges that will not collapse.

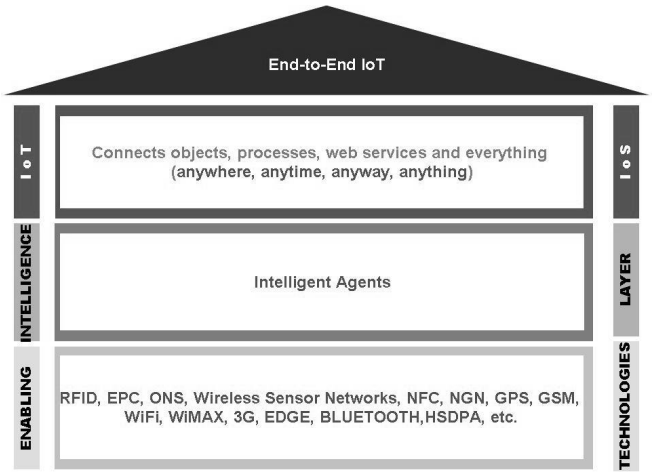

Fig. 2. IoT framework.

C. *Information Security in the Internet of Things*

Information security has not been a top priority in voice communications, yet in the future IP networks, it will become a major concern for all telecommunication companies world wide [12]. Securing information and its IT systems has been mostly regarded as a reactive exercise. Quite often, security experts act after a security breach has already occurred with patchwork solutions to counter individual security threats [7]. Moreover, information security has mostly been bolted onto products as an after-thought.

The future IoT is too critical and it cannot afford to be built on bolted security and patchwork solutions. It must be built on top of a very strong foundation with security as one of its top priorities. This must be done in a proactive manner, by anticipating the future threats and then develop possible countermeasures.

The future of the Internet is uncertain; so is the future of information security. It's easy to identify and protect against the current known threats of the Internet, yet it is almost impossible to predict the emerging and future Internet threats. Therefore, security experts remain ill-prepared to deal with emerging and future threats.

This has created a need to better anticipate, predict and prepare for the emerging and future Internet threats. Hence, this paper acknowledges the difficulty in predicting emerging and future threats and will therefore extrapolate on the current information security threats.

The next section discusses related work to show that the work of this paper does not exist in isolation but is based on other existing work.

III. Related Work

Most researchers dwell so much on annual review and the current information security threats landscape without much focus on the emerging and future threats. For example [13] provides an annual review of web threats from the beginning of year 2008 until the first quarter of 2009. A statistical analysis of email and web threats for the first quarter of 2009 is provided in [14]. Fossi et al. [15] provides an annual Internet security threat report for the year 2009. [6] and [16] focus on the annual threat roundup and unlike [13] and [14], they at least provide a future forecast for the year 2009, which is at least a one year focast.

Even though most work seems to be concentrating on reviews [6][13][14][15][16], there exist some efforts focused on addressing emerging and future information security threats. Ahamad et al. [1] focuses more on the current and emerging cyber security threats, existing or potential countermeasures and how threats might evolve but only for 2009. [18] predict that emerging and future threats will not differ so much from those faced in the past, and argue that the past and current threats will form the basis for the emerging and future threats. As a result, the authors have decided to extrapolate on the current threats to better predict the emerging and future threats.

Most of the existing work that has been discussed so far, do not discuss the emerging and future threats with a specific reference to emerging and future technology trends. Moreover, most of those which are at least forward looking make shallow forecast that only projects threats for up to one year ahead, not beyond.

The European community has taken a step forward in discussing emerging and future threats. The ICT-FORWARD and ICT-WOMBAT [19] (Worldwide Observatory of Malicious Behavior and Attack Threats) projects sponsored by the EU Commission under the Framework Programme 7 (FP7) provide the most relevant work to the work of this paper. Both projects started in 2008.

The ICT-FORWARD project promotes collaboration and partnership between academia and industry to better protect their ICT infrastructure. This project seeks to provide an understanding of emerging and future information security threats and adversaries [4][7][3][20].

The ICT-WOMBAT project on the other hand seeks to build a worldwide network to perform early warning and analysis of malware. This project is aimed at providing better means of understanding the existing and emerging threats that are targeting today and future Internet users [19].

The following scenario is adopted from one of the deliverables of the ICT-FORWARD project [21]. In [21], they envisage a scenario where a hacker could take a phone number (e.g. +27799938615) off-line, in such a way that every time when this number is called it responds with the message "The telephone number you called is not available on the Vodacom network". This could result in confusion to the caller and the person who is being called.

Now imagine the loss that an organization can suffer if a hacker decides to take down the company's call-centre number. If you think that is worse, imagine the life threatening situation as a result of the hacker taking emergency service numbers off-line (Ambulance, police flying squad or crime stop) at a time when there is an accident or a bank robbery.

In addition to this scenario, the next section discusses some of the scenarios that could be happen as a result of a blindfolded adoption of the IoT, without considering the risks involved.

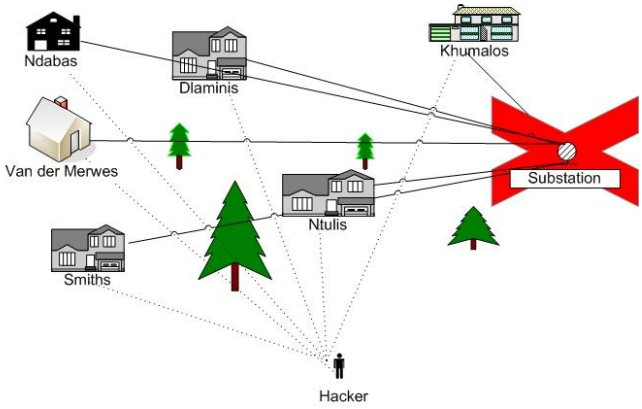

Fig. 4, Substation failure

IV. Scenarios

Scenario 1. A botnet of stoves cause damage to ESKOM power grid

Consider the possible risks accompanying home automation in the era of the IoT. A hacker somewhere in China identifies an exploitable vulnerability in electronic stoves. The hacker discovers that the vulnerability could allow him/her to covertly switch a compromised stove on/off and adjust the heat to whatever he/she likes. The hacker creates an exploit that will search the IoT for all stoves that have not been patched for the identified vulnerability. He sets it free on the Internet. Viola! His exploit identifies a couple of vulnerable stoves on the IoT one of which is owned by Mrs van der Merwe in South Africa.

Mrs van der Merwe left a turkey in her oven ready to cook as she left home for work. She had planned that just before she leaves work she would remotely switch on her stove and let it start cooking slowly while she is stuck in the Johannesburg traffic jam. On a very busy day her trip would take a minimum of two hours and by the time she arrives home the food would be ready and still warm.

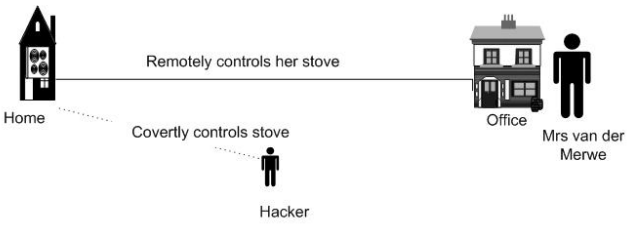

Fig. 3

Unknown to Mrs van der Merwe, the hacker decides to take control of her stove and puts it at maximum power to burn the turkey. She comes home to find the house in smoke. The damage is minor, delayed dinner, an increase in electricity bills and if worse could result in the house burning down.

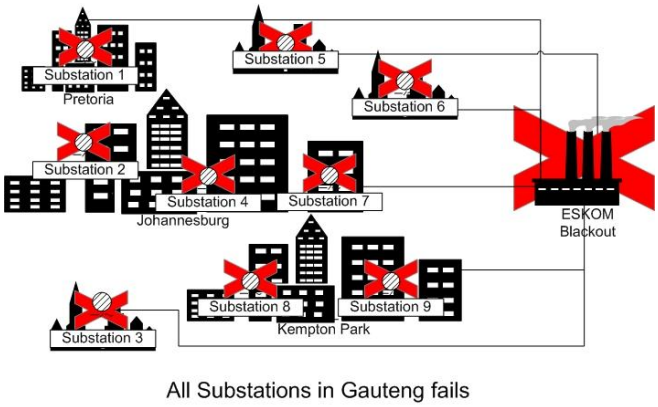

Fig. 5. ESKOM failure

Now consider the same hacker (bot herder) taking control of an entire suburb's compromised vulnerable stoves (botnet of stoves), covertly and simultaneously switching them to maximum power for four or more hours while everybody is at work. This will not only affect the individual owners of the compromised vulnerable stoves; but it could also overload and bring down their substation as shown in figure 4.

If the hacker decides to take control of the entire Gauteng province as can be seen in figure 5, ESKOM would eventually go down causing major loss in production and the normal load-shedding strategy will not help in such a situation.

Apart from the financial losses as a result of a hacker overloading the power grid, future threats could also result in loss of lives as can be seen in the next scenario.

Scenario 2. Life threatening health systems

Imagine a day in life when patients just walk past a health facility and gets a reminder on their mobile phones about their medication and checkups schedules. In the southern sub-Sahara region where the prevalence of HIV/AIDS is high, such reminders could be very helpful for the HIV/AIDS patients.

Now consider a hacker from somewhere in the east getting hold of the health systems that send the reminders and temper with them in such a way that it confuses the patient records; e.g. exchange Mr Du Toit's and Mr De Villier's health records, both HIV positive patients.

Mr Du Toit notes that his next appointment is approaching, but not yet sure of its exact date, decides to walk past his nearest clinic expecting a reminder about his

next appointment for collecting his medication. Unfortunately, the health systems under the instruction of the hacker identifies him erroneously as Mr De Villiers, whose next appointment is due in two months, and sends Mr Du Toit a reminder that his next appointment is only in two months time. This could possibly result in the death of both patients.

Now imagine a situation where the hacker starts to temper with the entire database systems holding HIV/AIDS patient records. The results could be so devastating.

Scenario 3. Fixed vs. Mobile Telco's

In today's telecommunication business environment where switching costs have been reduced considerable, billions of dollars can be made and lost in a matter of days or weeks. For example, consider a Telco that deals with fixed lines competing against three Telcos dealing with mobile services. The fixed line Telco does everything possible to raise its bar against its competitors and all the times it fails to do so due to its competitors' dominance in the market and its inability to innovate among other factors.

With profit margins going down, the fixed line Telco decides to put into place cost cutting measures and start retrenching some of its workforce. An old IT specialist, in a bid to keep his job, decides to send a targeted and distributed denial of service (DDoS) to the mobile Telcos. Indeed the mobile Telcos' systems go down for a week and their customers switch to the available fixed lines. All of a suddenly the profit margins start stabilising for the fixed line Telco at the expense of the mobile Telcos. The fixed line Telco decides to stop their cost cutting measures and the IT specialist keeps his job.

The same could happen within the mobile Telcos. Imagine two of the three mobile Telcos dominate the market; the third Telco with few subscribers could use a targeted DDoS to bring down the dominant Telcos and hence improve its revenue as people switch to use its services.

The above scenarios are just a glimpse of what we must expect in the future IoT. They might be considered to happen in future in the southern sub-Saharan context, but some of them are already reality in some parts of the world. For example, [22] already indicate that targeted attacks have caused power outages in some USA cities and all the intrusions were made through the Internet. It is just a matter of time before life threatening threats start emerging.

The next section concludes this paper and provides possible future directions.

V. Conclusion

Today, the worst damage that current information security threats could cause is a loss of revenue. Yet the damage of future threats could be severe and could cause loss of lives. It is therefore of vital importance for information security experts to proactively combine their efforts in comprehending and trying to understand the kinds of threats that they are likely to face in the future Internet of Things. The currently well known Information Security services such as confidentiality, integrity and availability will be insufficient and has to be drastically expanded to include services such as access control for real-time end-to-end-environments and critical infrastructure protection.

Future work could take this further by discussing possible countermeasures to prevent the identified threat scenarios and their devastating consequences.

Acknowledgment

The support of SAP Research CEC Pretoria/SAP Meraka UTD towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at are solely those of the authors and cannot necessarily be attributed to SAP Research CEC Pretoria/SAP Meraka UTD.

References

[1] G. Rittenhouse, "Internet of Things," 2008, available at: http://www.iot2008.org/, accessed [27 November 2008]

[2] M. Friedemann, "Towards the Internet of Things," Mar. 2008, available at: http://www.iot2008.org/,accessed [27 November 2008].

[3] E. Markatos, S. Ioannidis, and C. Kruegel, "From the World of Security - A Word from the Experts Tracing the Changing Nature of Cyber-attacks," *ENISA Quartely Review*, vol. 4, Dec. 2008, p. 4.

[4] H. Bos, S. Ioannidis, E. Jonssom, E. Kirda, and C. Kruegel, "Future Threats to Future Trust," *Proceedings of the Future Trust in Computing Conference*, Berlin, Germany: 2008, http://www.ict-forward.eu/media/publications/fia-whitepaper.pdf, accessed [14 April 2009].

[5] S. Friedl, "An Illustrated Guide to Kaminsky DNS Vulnerability," 2008, available at: unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html, accessed [14 April 2009].

[6] R. Richardson, *2008 CSI Computer Crime & Security Survey*, USA: 2008, available at: http://www.gocsi.com/forms/csi_survey.jhtml, accessed [10 December 2008].

[7] H. Bos, E. Jonssom, S. Ioannidis, C. Kruegel, K. Dimitrov, E. Djambazova, and E. Kirda, "Anticipating Security Threats to a Future Internet," 2008, http://www.ics.forth.gr/dcs/Activities/papers/fot.pdf, accessed [08 March 2009].

[8] L. Heuser, "Towards the Future of the Internet," April 2008, available at: http://www.iot2008.org/,accessed [27 November 2008].

[9] Intenational Telecommunication Union (ITU), *ITU Internet Reports 2005:The Internet of Things*, 2005, available at: *www.itu.int/osg/spu/publications/**internetofthings/InternetofThings**_summary.pdf*, accessed [27 November 2008].

[10] C. Kruegel, "Who is moving forward," Vienna, Austria, 2008, available at: http://www.ict-forward.eu/, accessed [07 May 2009].

[11] E. Fleisch, "The Internet of Things: What it is, and what Europe can do," 2008, http://www.iot2008.org/, accessed [27 November 2008].
[12] Nokia Siemens Networks, "Security Solutions: Secure your network and monomize the risks," 2008, available at: www.nokiasiemensnetworks.com/NR/rdonlyres/C9FC39F5-3A48-479F-B4DF-979340C6F709/0/csi_security_solutions_brochure.pdf, accessed [03 March 2009].
[13] Sophos Inc, *Security Threat Report:2009*, Boston, USA: Sophos, 2009, available at: *www.sophos.com/sophos/docs/eng/marketing_material/sophos-**security-threat-report**-jan-**2009**-na.pdf*, accessed [07 May 2009].
[14] McAfee Avert Labs, *McAfee Threat Report: First Quarter 2009*, Santa Clara, CA, USA: 2009, available at: *img.en25.com/Web/**McAfee**/5395rpt_avert_**quarter**ly-**threat**_0409_v3.pdf*, accessed [07 May 2009].
[15] M. Fossi, E. Johnson, T. Mack, D. Turner, and J. Blackbird, *Symantec Global Internet Security Threat Report: Trends for 2008*, Cupertino, CA, 95014, USA: 2009.
[16] Trend Micro Inc., *Trend Micro 2008 Annual Threat Roundup and 2009 Forecast: Security Your Web World*, Cupertino, CA, 95014, USA: Trend Micro Incorporation, 2008.
[17] M. Ahamad, D. Amster, M. Barrett, T. Cross, G. Heron, D. Jackson, J. King, W. Lee, R. Naraine, G. Ollmann, J. Ramsey, H. Schmidt, and P. Traynor, *Emerging Cyber Threats Report for 2009*, USA: Georgia Tech Information Security Center, 2008.
[18] J. Strand, "Future Security Threats: Enterprise Attacks of 2009," 2009, available at: http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1344178,00.html?track=sy320, accessed [14 April 2009].
[19] H. Debar, "Worldwide Observatory of Malicious Behaviors and Attack Threats," 2009, available at: http://www.wombat-project.eu/, accessed [07 May 2009].
[20] C. Kruegel and S. Ioannidis, "On Looking FORWARD," *ERCIM NEWS*, vol. 76, Jan. 2009, pp. 62 - 63.
[21] S. Ioannidis, "Security and Privacy in a Networked and Mobile World," 2008 Crete, Greece, 17-20 June 2008, available at: http://www.ict-forward.eu/media/publications/fidis2008-presentation-forward.pdf, accessed [14 April 2009].
[22] T. Claburn, "CIA Admits Cyberattacks Blacked Out Cities," Jan. 2008, available at: http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=205901631, accessed [09 May 2009].

Mr Moses T. Dlamini received his BSc Computer Science and Mathematics in 2002 at the University of Swaziland. In 2005 he became a teaching assistant at the same University. In 2006, he received his Honours BSc Computer Science at the University of Pretoria; where he also worked as an assistant lecturer. He is now working towards finishing his MSc in Computer Science at the University of Pretoria. He has presented research papers on information security at international and national conferences. As part of his research based MSc, Moses is currently employed as a Masters Research associate at SAP Research CEC Pretoria/SAP Meraka Unit of Technology Development since the beginning of 2008.

Prof Mariki Eloff received a PhD Computer Science degree in 2002 and gained tertiary teaching experience by lecturing at various tertiary institutions in South Africa for more than 20 years. Since October 2002 she is appointed as an associate professor in the School of Computing at UNISA. She is a member of the College of Science, Engineering and Technology Executive and Research Committees at UNISA. She participated in many information security management research projects and contributed to the development of various information security- training modules for industry. She has presented research papers at international and national conferences mostly focusing on information security. She has assisted in the organization and management of international conferences in information security.

Prof Jan Eloff has been Head of the Department of Computer Science at the University of Pretoria, South Africa since October 2002. He was a full professor in Computer Science until February 2009. He is currently appointed as the Research Director at SAP Meraka UTD focusing on creating new software platforms for emerging economies. He is a member of Technical Committee 11 (Information Security) of the International Federation for Information Processing (IFIP). From 2004 to 2007 he was the President of the South African Institute of Computer Scientists and Information Technologists (SAICSIT). Jan has published extensively in a wide spectrum of accredited international subject journals and he is a member of the Council for Natural Scientists of South Africa. He has received a B-rating from the NRF as a researcher who enjoys considerable international peer recognition for the high quality of his recent research outputs.