IEEE EXPERTS IN TECHNOLOGY AND POLICY (ETAP) FORUM ON INTERNET GOVERNANCE, CYBERSECURITY AND PRIVACY

TEL AVIV, ISRAEL
22 JUNE 2016

Version: 19 August 2016

IEEE

Contents

Executive Summary

The IEEE Experts in Technology and Policy (ETAP) Forum on Internet Governance, Cybersecurity, and Privacy returned to Tel Aviv, Israel, on 22 June 2016 for a session emphasizing biometrics and access control.

The invitation-only event at Tel Aviv University in Israel attracted about 50 experts from the global technology and policy communities. It was the sixth in a series of regionally oriented IEEE ETAP Forum gatherings hosted by the IEEE Internet Initiative over the last 13 months and the second held in Tel Aviv. Keynote presentations and a panel discussion illuminated trends, challenges, and opportunities in technology and policy; attendees voiced their own particular concerns in these areas; and then a breakout session concentrated on the question, what biometric data is appropriate for what circumstances?

Introduction: IEEE Internet Initiative and IEEE ETAP Forum Series

The gap is growing between the fast advance of technology and the policy that is being created to regulate it, IEEE ETAP Forum co-moderator Oleg Logvinov said in opening the 22 June 2016 event in Tel Aviv. The purpose of the gathering was to pursue ways to bridge that gap, he said.

Organized by the IEEE Internet Initiative, the IEEE ETAP Forums on Internet Governance, Cybersecurity, and Privacy bring together technology developers seeking a better understanding of the Internet public-policy landscape to help drive proactive technology design and policy experts seeking reliable technical guidance to make informed Internet public-policy decisions. If the tremendous promise of ongoing Internet innovation and expansion in access for sustainable development, economic growth, enhanced public safety, and security, etc. is to be realized, it will require unprecedented collaboration across the traditionally "silo-ed" worlds of technology and policy. With the Internet of Things (IoT) becoming more of a reality, information is being increasingly shared among machines, in ways that might not be predictable. In addition to the technological complexities introduced by this innovation, there are ethical and legal implications as machines more frequently share our sensitive information with other machines in the IoT. As Mr. Logvinov said at the Tel Aviv event, such implications must be taken into account as technology and policy is developed.

The IEEE Internet Initiative was founded to facilitate precisely the crucially needed two-way dialogue across the technology and policy worlds. Ongoing Internet innovation, sustainability, and market growth depend on sound, informed Internet policy, and effective Internet public policy depends on unbiased, current technical guidance. The IEEE Internet Initiative provides a neutral environment for collaboration among policy makers, engineers, scientists, industry leaders, and others globally on emerging issues in cybersecurity, privacy, and Internet governance—all within the context of advancing technology for the benefit of humanity.

IEEE ETAP Forum events have taken place in San Jose, California, in the United States in May 2015 (http://sites.ieee.org/etap-sanjose/);in Tel Aviv in August 2015 (http://sites.ieee.org/etap-israel1/); in Washington, D.C., USA, in February 2016 (http://internetinitiative.ieee.org/events/etap/etap-forum-in-washington-dc); in Delhi, India, in March 2016 (http://internetinitiative.ieee.org/events/etap/etap-forum-in-delhi-india); and in Beijing, China, in May 2016 (http://internetinitiative.ieee.org/events/etap/etap-forum-in-beijing-china).

The June 2016 IEEE ETAP Forum in Tel Aviv continued the conversation, with a focus on questions arising from the increasing usage of biometrics and access control.

Invited Speakers

The June 2016 IEEE ETAP Forum in Tel Aviv featured keynote presentations from four speakers:

- Iddo Moed, cybersecurity coordinator, Ministry of Foreign Affairs, Israel
- Deepak Maheshwari, director of government affairs across India and ASEAN region, Symantec, and co-moderator of this IEEE ETAP Forum in Tel Aviv
- Dr. Dorit Dor, vice president, products, Check Point Software Technologies
- Professor Isaac Ben-Israel, director of the Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University

Also, five speakers participated in a panel discussion addressing enabling components for closing the gap between policy and technology:

- Limor Shmerling Magazanik, director of licensing and inspection at the Israeli Law, Information & Technology Authority (ILITA)
- Shahar Belkin, co-founder, FST Biometrics
- Jonathan Klinger, Israeli cyberlaw attorney and blogger
- Yuval Elovici, director, Deutsche Telekom Laboratories at Ben-Gurion University
- Boaz Landsberger, Israel Electric Company

Keynote Presentation: Iddo Moed

Many global forums deal with coordinating cybersecurity policy, but there is still a lot of work to be done to bring technology expertise to bear, according to Iddo Moed of Israel's Ministry of Foreign Affairs. It's not that policymakers require so thorough an understanding of technology so as to learn coding language; rather, he said, there must be enough understanding of technology to be able to identify its international context and the processes that are unfolding around its development.

Cybersecurity is a topic of terrific attention in global forums including the United Nations (UN) and Organization for Economic Cooperation and Development (OECD), he said. A series of seminars in Geneva addressed how agreements need to be applied on export arrangements. In Israel, specifically, there has been debate around a recent export control directive. Similar conversations are going on around the world.

“It can only work in the real world with the technologists, the economists and the politicians sitting around the same table,” Mr. Moed said. “And that is very complicated process, because we speak very different languages.”

The word “stability,” for example, could mean different things in different environments, he said. The language being used to shape policy is political language, not technological language, and he said that’s not necessarily the correct approach. Language for policy around cybersecurity and other technological issues must be more concrete than is often the case in strictly political realms. For example, the Wassenaar Arrangement, a Cold War-era arms control export restriction deal, is not up to the task of dealing with the issue, he said.

Mr. Moed said there exists a UN group of experts from 25 countries, dealing with arms control, that since the late 1990s has discussed international law and how it applies to moral issues, privacy, how norms apply, the need for new norms, how confidence can be encouraged, etc. For example, governments agree not to attack computer emergency response teams (CERTs) and to publish cybersecurity policy for information sharing, and these, he said, are confidence-building measures. The discussions are directed by diplomats but also engage technological experts.

This work is valuable, Mr. Moed said, but “people in technology don’t like to work with government—it’s not exciting, for most people. That’s a fact of life, so we have to find all kinds of schemes and programs to keep technologists on board.”

Keynote Presentation: Deepak Maheshwari

IEEE ETAP Forum co-moderator Deepak Maheshwari with Symantec discussed his own personal views of India’s “Aadhaar” biometric identification program, which aims to help people receive government benefits and carry out financial transactions.

Mr. Maheshwari first offered a socio-economic and political snapshot of India, a secular, democratic republic with 1.2 billion people. Half of India’s population derives their livelihood from agriculture, he said, but that represents only 14 percent of the economy. “So it’s a service economy but an agricultural society,” Mr. Maheshwari said.

There are lots of programs to address poverty and provide subsidies. Delays, denials, and duplication are among the problems with these programs. Delays mean that subsidies and benefits can take a long time to be delivered, he said; duplication and denial mean that, if two people are meant to receive a benefit, one may not get it, while the other may get it twice. “Leakage rate” in the programs is estimated at 85 percent, Mr. Maheshwari said, “and that’s a huge amount.”

At 7.6 percent gross domestic product (GDP) growth, however, India's economy is a bright spot. Internet growth is happening via mobile, he said, thanks to proliferation of low-cost smartphones, prepaid mobile phones, inexpensive recharging and new subscriber identification module (SIM) cards available for less than half a dollar.

Mr. Maheshwari said India has a slew of government identification: passports, licenses, voter IDs, income tax numbers, etc. But not everyone has them, and many people have none. Consequently, people have a challenge in proving their identity—especially if they move villages and no one can vouch for them in their new environs.

Aadhaar is a program intended to give a unique ID to each resident of India (including refugees and non-citizens who are in the country). Every resident is entitled to a 12-digit random number. At this point, getting a number requires an application to provide demographic information and bioemetric information (10 fingers, iris, and face), plus e-mail and mobile number. Aadhaar was voluntary but has emerged as a de facto mandate, Mr. Maheshwari said.

The Aadhaar number in itself does not reveal anything about its user. For example, gender or region cannot be generated from the number alone. Using the number, Mr. Maheshwari said, someone who wants to check a person's identity would enter the person's biometric information and number into the Aadhaar system and get a binary response in return—either a yes or no, confirming or rejecting a match.

The program, he said, operates by first registering people and their biometric information, and then allows any entity to verify their ID technology. Aadhaar either confirms or denies that the person's biometric info matches the ID number. That, Mr. Maheshwari said, can help a leaky and inefficient government benefits programs, which have difficulty getting benefits to the right people.

When Aadhaar is combined with the Jan-Dhan program for Financial Inclusion and mobile access (JAMs), the breadth of options opens, he added. There are already nearly a billion JAMs registered. "You have people who could be anywhere with an online authenticating ID, mobile phone, and bank account," he said "Having these three things you can do quite a lot." Government, for example, can put money into a user's bank account. And people can also do exchange of money, low-value cash transactions.

But the program also faces challenges, Mr. Maheshwari said, such as limiting what biometric data can be shared with whom, and even whether the biometric data is being collected properly with the best equipment. He said key issues around security and privacy have arisen:

- What information is shared among agencies?
- While Indian law is explicit when it comes to demographic data, open questions remain around biometric information.
- If the original biometric data collection isn't good, then in, say, 10 years, "how do I prove that I am who I am or claim to be?"
- Fake credentials could result from people replicating a fake iris scan or lifting fingerprints.

Panel Discussion

A panel discussion of enabling components for closing the gap between privacy policy and technology engaged five experts on interrelated aspects of the topic, such as consumer understanding of privacy agreements, changes in techniques, enforcement issues, and corporate approaches to information flow. The panel also emphasized the importance of educating children from an early age about the implications of using the Internet, as well as various apps, programs, and social networks.

Limor Shmerling Magazanik

Limor Shmerling Magazanik with ILITA called herself "a strong believer in the necessity of forming policy alongside developing and implementing technology; this way, we may enjoy the advantages while consciously managing the risks."

Ms. Magazanik called privacy both a foundation of consumer trust and basic human right. She noted, for example, research showing that U.S. consumers are growing increasingly concerned about companies selling and governments accessing personally identifiable information (PII). She also cited various government and corporate actions and counteraction around privacy legislation around the world.

"I'm really convinced that privacy is not dead. I really feel we should not give up the fight," she said. "We can do this if we adopt standards to self-regulate the community. … We do our enforcement as government; we try to legislate. But you have to understand that legislation is very lengthy. It's like the turtle trying to catch up with technology, which is must faster … so we really rely on standards."

It is difficult for consumers to understand the privacy conditions they regularly agree to, Ms. Magazanik said. She presented findings that it would take a person 201 hours on average to actually read through all the privacy agreements and terms of service to which he or she agrees each year, at a yearly cost of $3,534—a total of $781 billion. Applications for machine-automated privacy management are emerging to help users more efficiently address the problem. “This is a way to give the consumer more control when he’s managing his affairs on the Internet,” she said.

Ms. Magazanik said that Israel undertook a large-scale project on biometric ID and that its oversight committee considered several options:

- Not having a database
- Having a database but not including biometric info in it
- Making do with a card that minimizes risk
- Limiting biometrics uses
- Collecting face-only biometrics but not fingerprints

While it’s compelling to use biometric information for other purposes, she said, legislation prohibits its usage for other means in order to prevent mission creep. It also establishes an independent regulator for the program. Project organizers still are seeking functionality with better risk management, she said, adding that there was a pilot period for testing and regulating the program and that it is still pending with Israel’s interior minister.

Shahar Belkin

People have proven themselves willing to trade off privacy for convenience, said Shahar Belkin with FST Biometrics, but concerns about terror, fraud, crime, and urbanization are driving market interest in new privacy measures, such as ones using biometric data.

“I’m talking about the problem of using biometrics as a security key, because there are risks,” he said. There are concerns over how people can fake biometric data, letting people who shouldn’t be able to gain access to information into supposedly secure systems.

What are the potential ways that biometric systems can be compromised? One simple method is called a “presentation attack.” This attack cheats or spoofs a system by presenting something other than genuine biometric information such as fingerprint or face (e.g. using a photo instead of the real face). “What the presentation attack doesn’t take into consideration ... is the next level of behavior,” Mr. Belkin said. “When people put their finger on a fingerprint reader, each one does it in a unique way. And behavior is not something that is going to be able to be spoofed soon. We have the tools now, in what is called ‘deep learning,’ to understand what is the behavior of the person. And behavioral is part of the new biometrics.”

The market is moving toward a behavioral approach, he said, that takes into account not only data such as face or fingerprint, but also the way people move, the way they hold their devices, the amount of pressure they tend to use when pressing down their fingers, etc.

Jonathan Klinger

"The question is not how you protect the information you store; it's whether you actually need to store it in the first place," said cyberlaw attorney and blogger Jonathan Klinger. "Because having the best security and best protection in the world won't help you when you have an inside data breach. And, if we're looking to avoid it, we'll be asking, 'Why was it necessary to store this specific information beforehand?'"

People have no idea whether or how their data is being store, used, or sold. "Most of you have applications on your phone," he said. "You install them without hesitation, without reading the privacy policy … The problem is not just that people don't read the agreement, but you don't have any way to monitor your data."

Free apps and more popular apps tend to request more permissions than paid and less popular ones, Mr. Klinger said—the free ones, because that is how they make their money; the popular ones, because the depth of their user base makes their information more valuable.

Not only are privacy policies difficult to understand, Mr. Klinger said they are also effectively impossible to enforce. If a user sends a photo to another user, for example, there is no way to monitor whether that file is subsequently shared. While an agreement might exist that an organization will not sell or share personal information, "there is no technology behind that statement," he said. "It's faith in people, and I have no faith in people—people are the weakest link between technological interfaces."

Mr. Klinger spoke to the need for a standard that attaches itself to personal information, files, call records, browsers, etc., which would create metadata specifying how a user's information can be shared, stored, or passed along. The standard, he said, could allow users to specify, "I allow you to track my location, but don't store it in my database. Or, do store it, but don't send it to other people. Or don't store it; don't send it to other people, and ask me every time. I want this preference to be saved, and when I submit information, I choose how this information could be passed along the way."

Such a standard is necessary, he said, because "the only way to control (information privacy) is not by enacting laws but by creating a standard for technology that people will feel protected if they know that software is compliant with that standard."

Yuval Elovici

Yuval Elovici with Deutsche Telekom Laboratories said, “In general, attackers like security tools because security tools give users a false sense of privacy or security.”

With disclosures, a user doesn’t know what can be derived with the information that’s being collected. “If you knew that your life expectancy could be derived from the information being collected about you, you might not give permission for it,” Mr. Elovici said. Even those who collect the data may not be aware of how it can be used, now or in the future.

A toll road in Israel, for example, bills drivers based on cameras photographing license plates. “I’m always terrified what will happen if the police will come and look at this information,” he said. “Just by analyzing the time that I was photographed in two locations, they can analyze speed and make billions immediately by issuing fines for people. This data was collected for one purpose, but can be used for another purpose.”

Another example is mobile companies’ collection of location data via cellular tower. The companies are supposed to keep the data for seven years for tax purposes, Mr. Elovici said. “If someone steals this data, they will know your location for seven years, even if you don’t remember.”

He noted that there are risks even when permissions are blocked because there are so many ways for private information to be inferred. “Do you think I, as a cybersecurity expert, needs the user to tell me their gender?” he said. “I can even tell if they’re not sure about it.” The number of sensors on mobile devices make maintaining user privacy very challenging; just monitoring the way a mobile phone is physically removed from the user’s pocket, for example, can suggest the user’s gender.

Boaz Landsberger

Boaz Landsberger with the Israel Electric Company (IEC) discussed the organizational model his company uses to keep tabs of information flow, creating a bureaucracy to monitor and evaluate what data is collected, where it is flowing, and how to secure it.

The IEC has data on workers, suppliers, and 2 million households, Mr. Landsberger said. It can be determined when people are home or not based on their electricity usage, because, with smart meters being implemented, readings are being taken more often than the traditional monthly frequency.

Mr. Landsberger said that executive buy-in is critical to an organizational model for tracking information flow and that workforce and money must be allocated for the task. Also, he said it is important in terms of accountability to have a single, go-to person responsible for data-leakage prevention. Owners for each type of sensitive data must be identified, and it is valuable to form a

steering committee of decision makers to, for example, approve what data is released. In addition, a mapping process must be established to define how data is to move from place to place across the organization.

“So,” Mr. Landsberger urged, “take responsibility, map the data, gather sensitive data in a specific location, and have tight monitoring.”

Keynote Presentation: Dorit Dor

Dr. Dorit Dor with Check Point Software Technologies discussed the tradeoff between security that protects consumers and security that helps hackers thrive.

There’s an inherent debate between security and privacy, she said. “The privacy people want to encrypt everything. But, if I let you encrypt everything, I let the attackers encrypt everything, too … If I let all the communication get encrypted, then I have no way of protecting you from what’s in it.”

Without being able to monitor what is in a file, it is harder to detect malware, she said. “Apple wants to convince us that our data is secure and they have no way of opening the phone, because that’s what makes us trust them … but what happens if the phone ends up being used by a terrorist?” she said, referencing the recent stand-off between Apple and the U.S. Federal Bureau of Investigation (FBI) over hacking into a terrorist’s iPhone.

Threats must be addressed quickly, she said; phishing sites, for example, typically shut down within a few hours, so they must be addressed in a very short window. Also, Dr. Dor said, there must be swift action after detection. She related a story of an organization that uncovered a bot but had failed to clear it as of four weeks later.

When it comes to regulation, “there are a lot of buzzwords that are being thrown about … but I think we’re missing the buzzword of prevention.” Prevention is the best approach, she said, as stopping hacks before they start is so much less costly than picking up the pieces after.

A salient problem, she said, is that there are so many points of access that could be weak in the emerging IoT. Networks are growing more complicated, Dr. Dor said, and people are using them for stealing, attacks, wars, political missions, etc. She cited research that forecasts, by 2020, there will be 1 billion smart meters, 50 percent of customers will have wearables, and 100 million smart light bulbs—all of them being potential points through which to wreak havoc. Protection will have to be predicated on the expectation of targeted attacks, she said, and all potential vectors and spaces must be accounted for.

Updates in the IoT present particularly critical challenges. She related a story in which a company many years ago had created a freeware library, resulting ultimately in cookies that introduced a vulnerability being passed through vendors and finally a telco and on to about 12 million user devices. "It's devastating to have something like this …," Dr. Dor said. "It's a very difficult to problem to solve."

A common architecture, she said, is necessary to prevent and monitor threats. Standards are needed in interrelated areas—sharing formats, interoperability (for automation, events, monitoring, etc.), expectations on vendors to solve security issues, expertise, and law enforcement—and will all have to play roles to sufficiently address the threat, she said.

There will never be zero problems, Dr. Dor said, "but we can solve fundamental problems in the industry."

Keynote Presentation: Professor Isaac Ben-Israel

Professor Isaac Ben-Israel with Tel Aviv University discussed the 2010 Stuxnet virus attack against Iranian nuclear centrifuges to demonstrate how the scope of information security had changed.

Professor Ben-Israel identified three false dogmas in the field of cybersecurity–that cyber warfare is only about, one, stealing or accessing information; two, the Internet; and, three, computers. Until 2010, these were considered the accepted wisdom by most of the experts involved in information security. Collapse of nuclear centrifuges in Iran as a result of the Stuxnet worm, however, demonstrated fundamental changes:

- Stuxnet physically damaged centrifuges; it did not steal or access information. "Many organizations had already information-security functions—we still use the term today 'CISO,' the chief info security officer. But, in this event, it had nothing to do with information … So we learned that (cyberwarfare) is not all about the information. It's *also* about the information, and we have to protect it, of course, too. But, if you judge by the intensity of the damage, it's even more important to block physical damage than damage to the virtual-world information."

- Stuxnet was not delivered by the Internet. The Natanz site in Iran was not connected to the Internet, he said, and, yet, someone succeeded in hacking into the isolated site. "I don't have to tell experts that there are many ways to hack into your computer, even if it's not connected to 'Wi-Fi®' or the Internet or the outside world … You need some way to inject something into your computer—maybe a disk, USB, connection into the wall, something."

- The worm infected industrial equipment, not traditional computers. Nobody knows how the centrifuges were hacked, “but everyone can guess.” They are controlled by supervisory control and data acquisition (SCADA) technology. “The controllers need maintenance. Controllers are produced somewhere. And controllers also have versions of software that need to be updated sometimes.” Potential vulnerabilities are introduced with each process, he said.

So what is cybersecurity today? “Every two years I change my own definition,” Professor Ben-Israel said. “Everyone has their own. It’s not as obvious as it sounds. The way I define it today—I hope this exists more than the 18 months of Moore’s Law—is that cybersecurity is really about the dark side of computing … Computers can be used by bad guys—and there are always bad guys—to harm the society, to cause damage to the way we want to live. So my definition is that cybersecurity is really about the dark side. We try to limit the dark side of this technology.”

Professor Ben-Israel gave the example of a new Bluetooth-connected refrigerator that his wife bought, with communications capabilities that are designed to provide maintenance information. “I’ve stopped talking with my wife in the kitchen about sensitive issues,” he said.

“This is the way we’re going to live five years from now. This is the vision of IoT: Everything will have a chip and some communication to other things. This is why we call it ‘Internet of Things.’ And this will make cyber exponentially more important,” he said. “If we don’t find ways to secure IoT, we won’t have IoT, because every bad guy through his refrigerator will be able to shut down the electricity in to the entire city or some kind of thing like this …”

Breakout Session

The June 2016 IEEE ETAP Forum in Tel Aviv next moved on to a breakout session, led by Limor Shmerling Magazanik of ILITA, focused on discussing what biometric data is appropriate for what circumstances.

Interrelated questions around the increased activity around biometric collection and usage were explored: What is the least amount of information required to achieve the necessary results? Is the collection and use of the data being carried out with consent? How is the definition of PII evolving (from contact info to financial and medical info, location, biometrics, genetics, opinions, religions, ethnic background, and social demographics)? Are different kinds of biometrics more or less harmful to privacy? For example, is facial recognition more damaging than veins? Is there a difference between irises and fingerprints?

Out of the discussion, participants proposed basic principles for implementing/adopting biometrics for authentication:

- Biometrics need not be the default choice. Rather, the decision of what method to use for authentication should be based on the contextual realities and the intended use case/scenario.

- Minimization should be the mantra when it comes to biometrics at each stage (collection, registration, processing, storage, correlation, etc.) The duration of the storage should be minimized; and unnecessary/redundant data, deleted.

- Data should be secured suitably, including strong encryption at rest, in transit, and during processing.

- The method of updating/modifying biometrics data should be easy and not able to be repudiated (to account for, for example, changes in fingerprints in the case of injuries, aging, etc.) An alternative method to authenticate should be offered.

- The enrollment, handling, and comparison of biometric attributes should be done in a place and manner that preserves a person's dignity and does not inflict on them more than necessary for the purpose of use.

- Employees working with biometrics should receive specific training in their handling.

- Special considerations of collecting biometric attributes from minors, people with disabilities, people who are legally incapacitated, and the elderly should be addressed.

- Biometrics should be used along with some other method for multi-factor authentication. Choose biometrics attribute(s) suitable in terms of risks involved, technological and infrastructural maturity, use case, and business model.

- Human intelligence should be used for decision-making over and above the biometrics, where needed.

Participants proposed that the principles be socialized with ISO/IEC JTC 1 SC37/WG 6 through the IEEE liaison in its forthcoming meeting in July 2016. Optionally, a white paper could be developed to outline policy scenarios (legislative provisions or lack thereof), technology choices (e.g., smart card versus online authentication using just a number), use cases, and business models.

Next Steps and Wrapup

Event co-moderator Oleg Logvinov said that one of the primary challenges that the regional IEEE ETAP Forum gatherings regularly illustrate is that, while technological change remains a global phenomenon, policy is fractured in localized variations. Through the IEEE ETAP Forum events such as the June 2016 gathering in Tel Aviv, he said, "we're trying to bring those local discussions to the worldwide stage and create a community that is global."

Mr. Logvinov said IEEE ETAP Forum organizers hope to share conclusions and actionable items from the regional events during the Internet Governance Forum in Guadalajara, Mexico, on 6-9 December 2016.

Join the Conversation

The IEEE Internet Initiative is a cross-organizational, multi-domain community that connects technologists and policymakers from around the world to foster a better understanding of, and to improve decisions and advance solutions affecting, Internet governance, cybersecurity, and privacy issues. There are many ways to engage through the IEEE Internet Initiative. Please visit http://internetinitiative.ieee.org or email internetinitiative@ieee.org for more information.

Appendix I: Program

Date: 22 June 2016

Location: Tel Aviv University, Berglas School of Economics Building, Room 012, Tel Aviv, Israel

Theme: Biometrics and Access Control

Moderators: Oleg Logvinov, Founder, IoTecha, and Deepak Maheshwari, Director of Government Affairs Across India and ASEAN Region, Symantec

Start Time	End Time	Tentative Program
8:15 am	9:15 am	Registration and Networking breakfast
9:15 am	9:45 am	Opening remarks and self-introduction by participants Oleg Logvinov, Founder, IoTecha, moderator Oleg is the President and CEO of IoTecha Corporation, an industrial IoT solutions provider. In March 2016, Mr. Logvinov co-founded IoTecha Corporation. Prior to joining IoTecha, Mr. Logvinov was a director of special assignments in STMicroelectronics' Industrial & Power Conversion Division, where he was deeply engaged in market and technology development activities in the area of industrial IoT, including the applications of IEEE 1901 powerline communication technology in harsh environments of industrial IoT. During the last 25 years Mr. Logvinov has held various senior technical and executive management positions in the telecommunications and semiconductor industry. After graduating from the Technical University of Ukraine (KPI) with the equivalent of a master's degree in electrical engineering, Mr. Logvinov began his carrier as a senior researcher at the R&D Laboratory of the Ukraine Department of Energy at the KPI. In January 2015, Mr. Logvinov was appointed as the chair of the IEEE Internet Initiative. The IEEE Internet Initiative connects engineers, scientists, industry leaders, and others engaged in an array of technology and industry domains globally with policy experts to help improve the understanding of technology and its implications and impact on Internet governance issues. In addition, the Initiative focuses on raising awareness of public policy issues and processes in the global technical community. He is also a past member of the IEEE Standards Association (IEEE-SA) Corporate Advisory Group and the IEEE-SA Standards Board. Mr. Logvinov also chairs the industry engagement track of the IEEE IoT Initiative and has created a series of worldwide IoT startup competition events. Mr. Logvinov actively participates in several IEEE standards development working groups that focus on IoT and communications technologies. Mr. Logvinov is chair of the IEEE P2413 "Standard for an Architectural Framework for the Internet of Things" Working Group. He helped found the HomePlug Powerline Alliance and is the past president and CTO of the Alliance. Mr. Logvinov has 24 patents to his credit and has been an invited speaker on multiple occasions.

Start Time	End Time	Tentative Program
9:45 am	10:05 am	Keynote Iddo Moed, Cybersecurity Coordinator, Ministry of Foreign Affairs, Israel After joining the Israel Ministry of Foreign Affairs in 1992, Iddo Moed was posted in several missions around the world including the Dominican Republic, The Hague, Singapore, and Beijing (DCM). Positions in Israel have included assistant to the director general, Water and Multilateral Affairs at the Middle East Division; Middle Eastern Economic Affairs; and head of the Training Department. In June 2013, Moed was appointed as Cyber Security Coordinator at the Strategic Affairs Department, MFA. In this role Moed is responsible for coordination of policies regarding international cooperation in cyber security.
10:05 am	10:25 am	Keynote—India biometrics Deepak Maheshwari, Director of Government Affairs Across India and ASEAN Region, Symantec Deepak Maheshwari is director of government affairs for Symantec across India and ASEAN region. A public policy and regulatory affairs professional, he has a keen interest in the interplay of technological innovation with socio-economic development. An oft-invited speaker, author and columnist, he has played a pivotal role in evolution and development of Internet policy and digital ecosystem as an industry spokesperson and thought leader. He served two consecutive terms as elected secretary of ISP Association of India (ISPAI) and co-founded the National Internet eXchange of India (NIXI). He is a charter member of IEEE Experts in Technology and chairs the BSA Asia-Pacific Policy Committee., An engineering graduate from Indian Institute of Technology as well as a law graduate, he has previously worked with Microsoft, MasterCard, HCL and Sify.
10:25 am	10:35 am	Break

Start Time	End Time	Tentative Program
10:35 am	11:20 am	Panel discussion Shahar Belkin, Co-Founder, FST Biometrics Yuval Elovici, Director, Deutsche Telekom Laboratories at Ben-Gurion University Jonathan Klinger, Israeli Cyberlaw attorney and blogger Limor Shmerling Magazanik,, Director of Licensing & Inspection at the Israeli Law, Information & Technology Authority (ILITA) Boaz Landsberger, Israel Electric Company **Shahar Belkin** In 1995 Shahar founded his first start-up, called OzVision. Developing live video streaming over RF radio and telephone lines, and one of the first, digital video recorders for security, OzVision achieved a leading position as a supplier of remote video solutions in the US security market. It also patented a unique video compression and streaming algorithm. In 2006 Shahar co-started a new startup called FST Biometrics, developing a new concept and technology of visual identification that provides motion biometric Identification, patenting several algorithms in biometrics and in fraud detection. Today the company is a global market leader in the biometric physical access control market **Yuval Elovici** Yuval Elovici is the director of the Telekom Innovation Laboratories at Ben-Gurion University of the Negev (BGU), head of BGU Cyber Security Research Center, Research Director of iTrust at SUTD, and a Professor in the Department of Information Systems Engineering at BGU. Prof. Elovici holds B.Sc. and M.Sc. degrees in computer and electrical engineering from BGU and a Ph.D. in information systems from Tel-Aviv University. He served as the head of the software engineering program at BGU for two and a half years. For the past 11 years he has led the cooperation between BGU and Deutsche Telekom. Prof. Elovici has published articles in leading peer-reviewed journals and in various peer-reviewed conferences. In addition, he has co-authored a book on social network security and a book on information leakage detection and prevention. His primary research interests are computer and network security, cybersecurity, web intelligence, information warfare, social network analysis, and machine learning. Prof. Elovici also consults professionally in the area of cybersecurity and is the co-founder of Morphisec, a startup company that develops innovative cybersecurity mechanisms related to moving target defense. **Jonathan Klinger** Jonathan Klinger is an Israeli Cyberlaw attorney and blogger, acting as a legal consultant for several high-tech companies and start-ups. He serves as a legal counsel for Hamakor, Israel's Open Source Society, Eshnav, People for Intelligent Internet Use, Israel's Digital Right Movement, and others. Jonathan taught computer game development law at Beit Berl College and teaches media law. He volunteers at the Digital Rights Movement free speech clinic, where he takes cases relating to strategic lawsuits against public participation (SLAPP). **Limor Shmerling Magazanik** Adv. Limor Shmerling Magazanik is Director of Licensing & Inspection at the Israeli Law, Information & Technology Authority (ILITA). ILITA is the Israeli data protection authority, in charge of enforcing the Israeli Privacy Act provisions in the digital sphere with regards to the fundamental human right to privacy. Her responsibilities in the past eight years have included managing ILITA's regulation and enforcement activities over both private and public sectors. These include investigations and legal proceedings, in cases of privacy law infringements, over issues such as consent, purpose limitation, and data breaches. Ms. Shmerling has also managed the regulation of digital identity via digital signatures in Israel. She is a frequent participant in policy framing in Israeli government information systems and data projects, promoting compliance with privacy regulation. She was part of the oversight committee supervising the program for the establishment of a biometric database alongside the smart identity card project. Previously she worked as legal advisor in the fields of corporate law, property law, and banking, and she has held product and project management positions in the high-tech industry. Ms. Shmerling is a graduate of Tel-Aviv University, holding bachelor's and master's degrees in law and a master's degree in literature.

Start Time	End Time	Tentative Program
11:20 am	11:40 am	Keynote Dr. Dorit Dor, Vice-President, Products, Check Point Software Technologies Dr. Dorit Dor serves as Vice President, Products for Check Point Software Technologies. She manages all product definition and development functions for both the enterprise and consumer divisions of the company. Dor's core responsibilities include leading the company's product management, research and development (R&D), and quality assurance (QA) initiatives from concept to delivery. Dor has served in several pivotal roles in Check Point's R&D organization. She has been instrumental to the organization's growth and managed many successful product releases. She has been published in several influential scientific journals for her research on graph decomposition, median selection, and geometric pattern matching in d-dimensional space. In 1993, she won the Israel National Defense Prize. Dor holds PhD and MS degrees in computer science from Tel Aviv University, in addition to graduating cum laude for her Bachelor of Science degree.
11:40 am	12:00 pm	Rapid-Fire identification of issues Oleg Logvinov
12:00 pm	12:20 pm	Keynote Professor Isaac Ben-Israel, Director of the Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University Major Gen. (Ret.) Professor Isaac Ben-Israel serves as director of the Interdisciplinary Cyber Research Center (ICRC). Additionally, he serves as chair of the Yuval Ne'eman Workshop for Science, Technology and Security, chair of the Israeli Space Agency, and chair of the National Council for Research and Development in the Ministry of Science. Professor Ben-Israel studied mathematics, physics, and philosophy at Tel Aviv University, receiving his PhD in 1988. Professor Ben-Israel joined the Tel Aviv University as a professor, teaching at and leading the Security Studies Program and at the Cohen Institute for the History & Philosophy of Sciences and Ideas. He also serves as deputy director of the Hartog School of Government and Policy. In 2011, he was appointed by the Prime Minister to lead a task force that formulated Israel national Cyber policy. Following that he founded the National Cyber Headquarters in the Prime Minister's Office. Professor Ben-Israel has written numerous papers on military and security issues.
12:20 pm	1:00 pm	Lunch
1:00 pm	1:20 pm	Review of key issues from previous ETAP Forums Deepak Maheshwari
1:20 pm	1:45 pm	Synthesis and selection of high-priority areas Oleg Logvinov
1:45 pm	2:00 pm	Break

Start Time	End Time	Tentative Program
2:00 pm	3:00 pm	Breakout sessions—delve deeper into highest priority issues
3:00 pm	3:30 pm	Report from Breakout Sessions Breakout leads
3:30 pm	3:45 pm	Next Steps and Wrap-up Oleg Logvinov

Appendix II: Participants

The following individuals attended the second Tel Aviv IEEE ETAP Forum:

Danny Akerman, The Standards Institution of Israel

Eddie Aronovich, Computer Science Tel-Aviv University

Shahar Belkin, Co-Founder, FST Biometrics

Professor Isaac Ben-Israel, Director of the Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University

Ortal Benjamin, B. Benjamin

Chaim Cohen, CDO webIntegrity

Tamar Cohen

Lucian Cristache, IOT Architect LucommTechnologies

James Denaro, Hyperco Partners

Jermy Dery, Dan Hotel Tel Aviv

Dr. Dorit Dor, Vice-President, Products, Check Point Software Technologies

Niv Elis, Reporter Jerusalem Post

Yuval Elovici, Director, Deutsche Telekom Laboratories at Ben-Gurion University

Ori Freiman, Bar-Ilan University

Chaim Greenberg, Appsec-Labs

Asaf Hecht, Researcher Cyberark

Ariel Hochstadt, co-founder vpnmentor.com

Noam Ifat

Vladimir Jotsov, Full Prof. ULSIT

Gil Keini, Founder CEO Firmitas

Jonathan Klinger, Israeli Cyberlaw attorney and blogger

Dafna Kovler, Project Manager ICRC

Ilan Lamdan, CEO NetExpert Computer Systems LTD

Boaz Landsberger, Israel Electric Company

Yossi Lavon, Appsec Labs

Gadi Lenz, Chief Scientist AGT International

Inbal Levi, Student

Oleg Logvinov, IEEE Internet Initiative, Chair; IEEE P2413 Internet of Things (IoT) Architecture Working

Group, Chair; IoTecha Corporation, President and CEO

Limor Shmerling Magazanik, Director of Licensing & Inspection at the Israeli Law, Information & Technology Authority (ILITA)

Deepak Maheshwari, Director of Government Affairs Across India and ASEAN Region, Symantec

Sebastian Maier, Managing Partner Maier | Schumann | Partners LLP

Shuki Maman, Architect Huawei

Sharon Mashhadi, Bank Hapoalim

Avraham Menachem, Consultant OCS

Iddo Moed, Cybersecurity Coordinator, Ministry of Foreign Affairs, Israel

Ido Naor, Kaspersky Lab Senior Researcher

Mary Lynne Nielsen, Global Operations and Outreach Program Manager IEEE

Daniel Perez

Tomer Reuven

Rinat Ron-Selzer, Embassy of Israel Washington DC

Adi Sagi, BGU

Florian Schutz, Business Development Cyber & Intelligence RUAG Schweiz AG, RUAG Defence

Asaf Shelly, CEO Engage ioT

Eva Shelly, COO Engage ioT

Shachar Siboni, PhD Student BGU

Rami Tsalka

James Voorhees, Cyber Defense Analyst Common Securitization Solutions

Albert Waldhuber, Manager, Global Standards Solutions & Content Marketing IEEE Standards Association

Dalia Yogev

Appendix III: Combined Issues List, All IEEE ETAP Forums

Tel Aviv, 22 June 2016

- What biometric data is appropriate for what circumstances?

Beijing, 17 May 2016

- Cyber-threats to critical infrastructure, including eGovernment/eCommerce
- Transparency as a source of obtaining data for evidence-based decision making
- Biodiversity in the Internet ecosystem

Delhi, 4 March 2016

- Protecting Internet traffic, managing meta-data analysis, and how to implement both security and privacy at scale
- Multi-stakeholder Internet governance
- Options and challenges in providing universal access for social and economic inclusion

Washington, 5 February 2016

- Data localization
- Education and ethics
- End-to-end security/privacy by design
- Technology-policy development process

Tel Aviv, 10 August 2015

- User assessment of trustworthiness of devices, enterprises, and governments
- Educating users about characteristics of information society
- Machine-readable privacy agreements and who enforces them?

San Jose, 18 May 2015

- Threats and opportunities in data analytics
- Multi-stakeholder Internet governance
- Protecting Internet traffic, managing meta-data analysis, and how to implement both security and privacy at scale
- Fragmentation of the Internet due to local policies and how to avoid it
- Algorithmic decision making that exacerbates existing power balances and ethical concerns
- How to best engage IEEE as a platform for contributing to the resolution of these and related issues