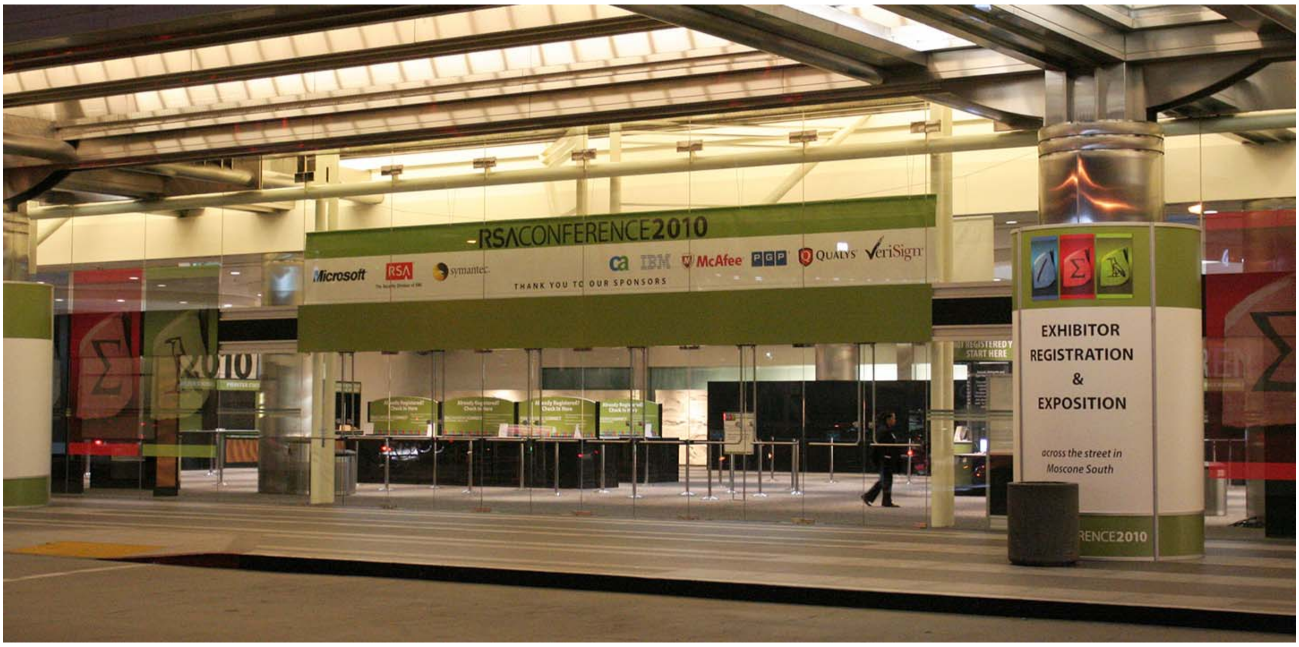
RSA 2010 Conference Report

San Francisco, 1-5.3.2010. Juha Sääskilahti



About RSA

RSA is probably the biggest security exhibition and conference arranged annually. 2010 more than 600 security companies were exhibiting their products and services and the conference had more than 250 different track sessions to choose from. In addition there were a number of key note sessions, in which representatives from the industry shared their views. Cryptography experts such as Diffe, Hellman and Shamir as well as famous names such as Steve Wozniak showed up.

At the lecture room of each track session the participant badge was scanned. The list of track sessions participated was emailed to the participants later. Key note sessions had such a big number of watchers (up to ten thousand?) that the participant badges were not scanned. This report contains my notes from the key note sessions and track sessions I participated. The track sessions I:

AND-304 Threat Modeling: Lessons Learned & Practical Ways to Improve Your Software
BUS-106 Industry Analyst Roundtable
BUS-201 Business Model for Information Security
CRYP-108 Elliptic Curve Cryptography
CRYP-203 Identity-Based Encryption and Signatures
EXP-202 Picking a Yardstick to Measure Your Software Security Practices
GRC-302 The Keys to Successful Monitoring for Detection of Insider Attacks
HT1-401 ZigBee Wireless Ethical Hacking
HT2-108 The End of the Internet as We Know It? Separating Reality From the Hype
HT2-303 Rootkits in the Real World Today
HT2-402 Attacking Mobile Phone Messaging
LAW-301 Information Security Standards and the Law
NMS-107 Secure Virtual Networking: An Oxymoron?
NMS-204 "In-the-Cloud" DDoS Mitigation
PNG-403 DNSSEC - A Right Answer to the Wrong Question
RR-108 Veiled: A Browser Based Darknet
SEM-001 Innovation Sandbox

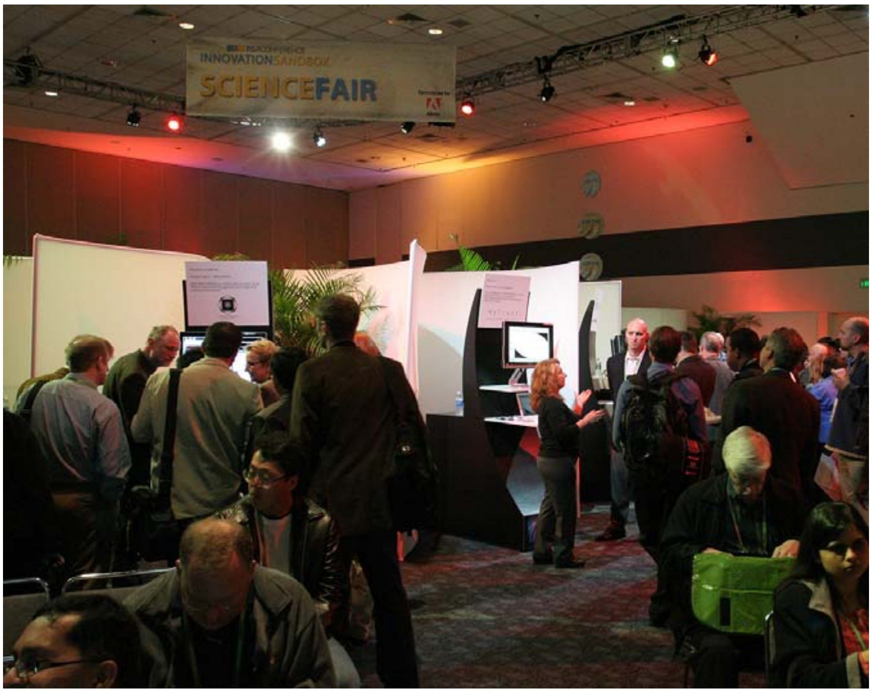
Disclaimer: Everything stated in this report is based on, how I understood the presentations – and I may have misunderstood parts, missed details or made wrong interpretation. Read with discretion.

Day 1 – Innovation Sandbox & Exhibition

Innovation sandbox

The innovation sandbox event consisted of exhibitions of innovative security start-up companies (10 of them), white board sessions discussing current hot topics, and activities to boost entrepreneurship. Also an innovativeness competition among the companies exhibiting in the innovation sandbox was arranged. Altor Networks (virtual network traffic/ access policy/ malicious traffic detection) won the competition. The winner was announced by Ray Rothrock (Venrock, venture capital). The entrepreneurial factors, such as good presentation and good team (start-up company staff) affected the choice.

All of the companies were basically established around single idea/ solution. Characteristic to the companies was great commercialization of their idea. Some of the companies' ideas were rather thin, but still excellent solutions for the niche they presented. For example one company, Envision Security promoted a solution for Risk Communication – a method, how to communicate risks to decision makers in a company to get the right security decisions done. Example of a more technical solution was a web application vulnerability analysis tool (Hacktics), which actually follows also the execution of the program in a debugger –type of view, while attacking and developing new attacks against the system. Other companies' innovative offering included cloud computing –related security mechanisms/tools, security monitoring solutions and password management (eg a visualizing tool for creating numerous safe passwords – KikuSema and password reset tool based on users' preference on certain images – RavenWhite).



Exhibition

The RSA Exhibition was an impressive showroom for *the* players in the security industry, RSA, Symantec, CA, CheckPoint, Cisco, Microsoft, Intel, IBM, Kaspersky, PGP, TrendMicro, Verisign, FBI and NSA to name a few of the best known. NSA even had the classic Enigma on display. The exhibition catalogue contains approximately 100 different categories for security companies – the number of individual companies at the RSA was over 600.

An interesting notion from the exhibition was that Germany was the only country, which was promoting itself as a country (a group of German security companies). No other country had similar branding. Interestingly, China is also emerging to security market – and was present with a couple of companies (eg Bejing Zongguancun) openly promoting the Chinese origin. Juniper/Netscreen was not in the exhibition.

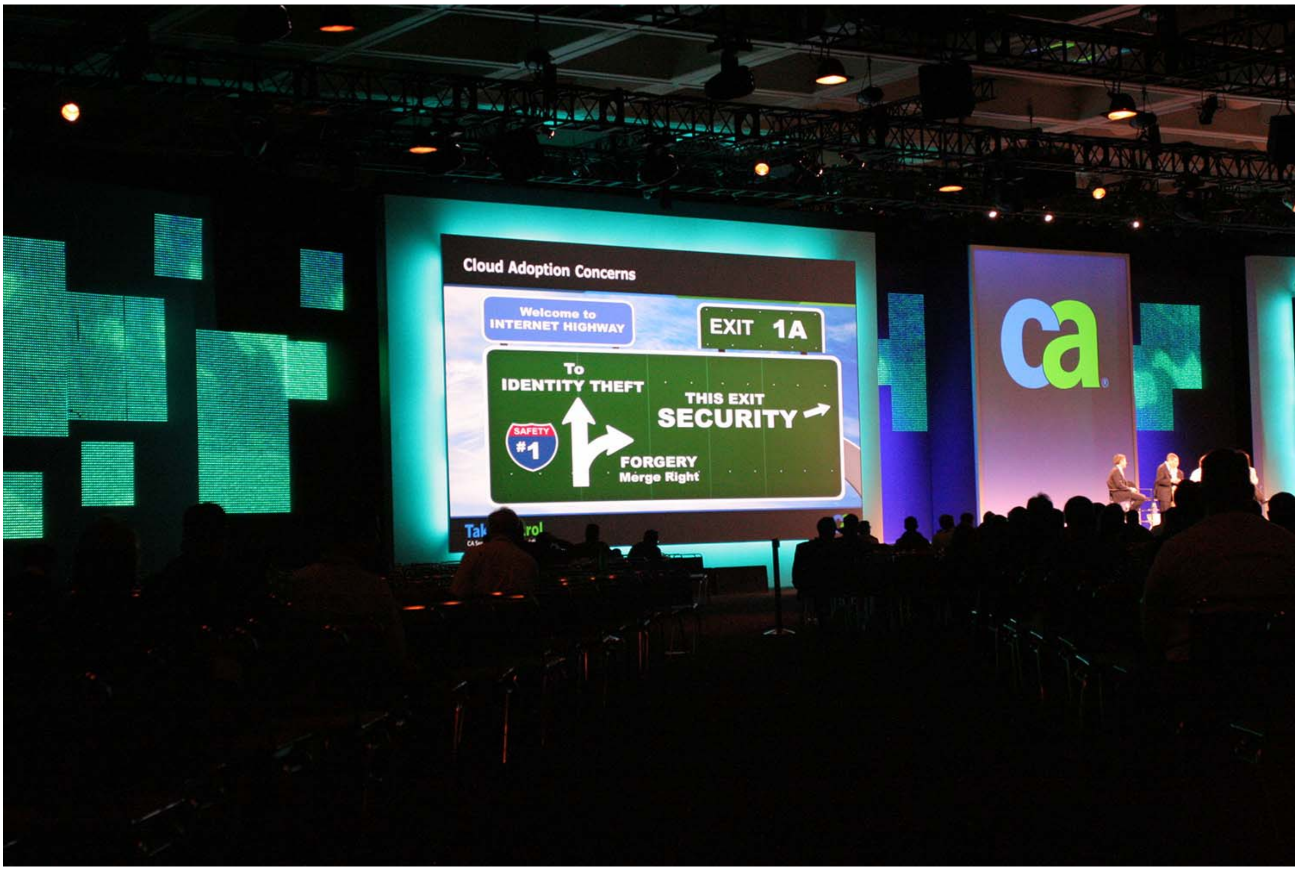
网御神州
SECWORLD
win-win
With Legendsec
Serviced for the 2008 Olympic Games
Ranked second in China's FW/VPN market
Ranked first in China's SOC market (★)
Contributes to the government and works with the World's Top 500 Enterprises, such as China Petroleum & Chemical Corporation and CNPC
Covers 30 provinces and has established 31 district post-sale service centers, 316 customer service networks.Has more than 1000 partners all over the world
(★) Source: CCID (China center for information industry development) 2008-2009 China's Information Security Products Report

Three major trends could be observed (subjective view of the author):
-Clouds and cloud security are the key words. Nearly every company present at the exhibition was promoting something cloud- and cloud security related. In the key note session later CA noted that there were 170 companies at the exhibition claiming to provide solutions particularly engineered for cloud security.
-Signature-based security filtering is getting more and more difficult – and companies seem to be moving from signature management to trust management – and in a way towards whitelisting the trusted things (eg web sites, email providers, programs or content in general) rather than blacklisting the bad signatures. It seems that same approach is being adapted to virus protection and spam protection.
-Nothing really new. It seemed that most companies presenting at the exhibition were not presenting anything radically new – rather upgrades and minor improvements to the old existing solutions.

Confidence in a connected world.
SO YOU THINK YOU KNOW SYMANTEC?
HOW DO YOU SECURE YOUR INFRASTRUCTURE?
IBM

Day 2 – Key Note Sessions & Track Sessions

Key Note Sessions



Key note sessions at RSA conference are the main show – having high profile speakers and thousands of people in the audience.

The key note session was opened by announcement of a security lifetime achievement winner. Whitfield Diffie was awarded the prize this year for decades of work in the field of cryptography, and particularly on papers on public key cryptography in the 70's.

First key note session was about cloud security. It was claimed that the cloud computing will totally change how companies manage their IT. Today around 2/3 of company's IT spending may go to only maintaining status-quo of their IT systems. Cloud computing will enable pay-as-you-go model, and radically change the expenditure on IT. The cloud will, anyhow, need security – it must surpass the security of the fixed way of working. There are some major challenges, however. One paradigm change is that the focus needs to be shifted from perimeter protection to data and individual protection. Another major change is that IT personnel roles will change; today there are different teams taking care of storage, network, etc – in cloud model this will all change. Particular challenges will be also seen in multi-tenancy.

A four step evolution path was presented for clouds' evolution:
1) Modern enterprises (Test environments/non critical systems)
2) Virtual enterprises (critical business environment)
3) Internal clouds
4) External clouds

Before the second key note, an excellence award for security practices was handed to Malcolm Harkins (CISO, Intel) for creating educated & well designed security practices for Social Media.

The second key note session was presented by Microsoft – about their trustworthy computing. The main message of the a bit messy presentation seemed to be that the Microsoft's trustworthy computing model can handle the particular needs/challenges (shared accountability, co-tenancy, identity & privacy & jurisdiction) of cloud computing. The components of MS trustworthy computing model are: identity meta-system, trusted stack (people, data, SW and HW), management/ audit and security/privacy fundamentals (development lifecycle, defense in depth & threat mitigation). Microsoft is to publish some security products during 2010: Forefront Indentity Manager, uProve (related to cooperation with Fraunhofer and public identification system in Germany.) They also noted that everyone should be responsible of their own computer health and security.

Third key note session was by Symantec. They stated that the signature-based threat identification is getting challenging. In 2008 there were 1.6M signatures, 2009 2.9M, and the growth speed is increasing. Some kind of a reputation-based system will replace signatures. They also acknowledged the first mobile virii and thought that those may become a real issue along with the heterogenous smart phones. Virus protection will be more and more cloud-based solution. Symantec is also to launch a Cloud Store data storage system and Datainsight data ownership management solution.

A couple of more excellence awards were handed; one for a group – a Public Policy Award. Mathematics award was handed to David Chaum, who has worked on digital cash, electronic voting and privacy related things.

Fourth key note session was a panel discussion with a lively group of academics. Diffie, Hellman, Rivest, Shamir – and Snow were discussing. The last one representing NSA. A few notes from the discussion:

- 768bit RSA has been broken. It was assumed that 1024bit will be broken within a decade – so the recommendation is to move to eg 2048bit RSA.
- Credit card chip security is jeopardized. There is 700-pages standard on, how the credit card chip works; simply – the reading machine of the chip will input the pin code entered by the user to the chip on the credit card, and the credit card chip itself will do the check, whether the code is correct. The problem is, however, that if the code is right, the card will return code "9000". It is trivial to replace the chip with chip which returns "9000" for any code whatsoever.
- When everybody moves everything to the cloud – it will be "the wet dream of the government", since they no longer need even a warrant to collect whatever information. This far they have needed at least a warrant to wiretap or make a house search.
- Some note was made about AES-256 security vs AES-128 (but I missed what was the point)

- NSA: “Trust meltdown” will happen.
- NSA: Companies: Put some money to vulnerability analyses, damn it! (There is a lot of luridiculous long-known vulnerabilities even in new products [pointing at MS – recent product launch with a vulnerability disclosed 17 years ago])

Track Sessions

The track sessions during the afternoon were of varying quality. There are tens of simultaneous tracks – some more, others less interesting – and with varying quality. This report is about the track sessions followed by the author.

First track session was about securing virtualized (VMWare) environments. Virtual machines market is worth 2 billion dollars, and VMWare has 90% market share. The main messages of the protection strategy were: 1) don’t combine different functions (eg DHCP, DNS, LDAP etc) into a single VM, make separate ones. 2) Enforce at least access control in VM. 3) Bind sensitive VMs to separate physical interfaces. Also highlighted were VM lifecycle management and importance of deployment of virtual sensors similar to fixed systems.

Second session was industry analysts’ round-the table. IDC, Forrester and Gartner were in the panel. The following summarizes some of the key notions made:

- Ecosystems for spamming, identity theft etc DO exist. Botnets can be hired at low cost, and governments (secret services) are using the information in the Internet – eg if you support free Tibet, someone will find that out, and your relatives in China might get in trouble.
- Cloud security is happening – standardization is needed. It was estimated that the cloud providers will need to provide the security – it will not (cannot?) be added afterwards, as done with today’s networks (virus protection etc add-ons). Security SaaS market is $1B today.
- There are very high expectations on mobile clouds’ security – eg “this is from at&t – this must be secure”
- Compliance business has become a monster and is drawing money from ‘real security’; a lot of bureaucracy, and it doesn’t necessarily guarantee security (eg PCI or ISO27001).
- Don’t believe that mobile malware will be an issue (vs Symatec’s view)
- Cryptographic technologies and tokenization will see mergers & acquisitions
- Big trend: big companies are forced to allow end users to use computers/software/mobiles they like; eg Apple computers, social networking etc; they can’t just block facebook anymore.

Third session was about, whether Secure VPNs (virtual machine virtual networks) are an oxymoron. Big issue with virtual machines is that they may have also virtual switches – and virtual switches will hide a lot of information from the physical switches: eg there is no traffic statistics available for analysis. Virtual switches may not have same policies enforced as the physical ones. The list of threats associated with VMs in general was as:

- Transient effect (on/off randomly -> impossible to perform network scans regularly)
- Non-progressive timeline (rollback to earlier version easy; virus patches might disappear etc)
- Ease of diversity (large number of O/S versions; old and new)
- Mobility (VM may move from machine to another with a mouse click. They may also be easily cloned, as they are stored as a single ‘drag-droppable’ file.)

- Management of identity (MAC address of virtual machines = ?)
- Performance loss
- Consistent policy enforcement (eg FW policies should end up in virtual switches etc)
- Traffic visibility (virtual switches not monitorable by eg Netflow)
- Creating secure topologies/ security domains

802.1X challenges & opportunities; challenges even with fixed NW. Latest versions (2010) have improvements taking into account some virtual aspects.

Fourth session was about optimizing computing performance of elliptic curve cryptography. Very mathematical (Brazilian PhD presenting…) presentation about, how the performance can be improved. Two methods were identified. One was related to use of new Intel Core architecture special commands, which increase performance of cryptographic functions, in low-level code optimization. Second approach was applying parallelism to cryptographic functions. An algorithm for Miller-functions capable of utilizing parallelism (performance benefits up to 32 parallel threads was observed, over that the algorithm developed seemed to start to lag in performance benefit).

Day 3 – Track Sessions & Key Note Sessions

Track Sessions

The first track session was about business models for security. ISACA program director discussed about ways of approaching security. The key points seemed to be that quick point solutions should be avoided – as they usually come back as bigger problems – and that security should be handled holistically, involving different disciplines to the security planning (organization, people, technology and process). He also presented that having dual-roles in organization would be good for security – eg a sales team is usually not security conscious; augmenting sales team with a security expert, who would report both sales manager and security chief officer, could improve security consciousness significantly.

Second track session discussed metrics of software security. SAFEcode and BSIMM were briefly presented by McGraw. Microsoft presented their software security maturity model, where security of a software is measured on scale (basic, standard, advanced and dynamic) based on status of following items in software development: training policy & organizational capabilities, requirements design, implementation, verification and release & response. EMC also presented their software security maturity model. They have product security policy as the main place holder for measured objects of Architecture & design standards, coding standards and process. These yield in two measurements, product risk and organizational maturity, both having 4 levels.

Miscellaneous notes from the session:

- A governmental institution ordering software from a company, might want to measure organizational security maturity rather than the final product security.
- It was noted that culture matters, when choosing metrics, the metrics should be chosen so that they match the organizational culture.
- Microsoft does privacy and risk assessments to their products. They say that some companies assess risks on protecting their IP rather than on protecting the end user, which is wrong.
- About Agile methods:
    - Take customer requirements in efficiently; the problem is that customers rarely have security requirements on the list – they should come from the vendor
    - “Code first, only then think what the heck was done”
        - Architectural analysis very challenging
        - No way to set security requirements in the agile process
- Bad SW security metrics:
    - Count “25 most typical bugs”
    - # of xx certified programmers
    - # of vulnerabilities found
- Good SW security metrics
    - The less code, the better (the more code there is, the more bugs there are)
- Today there are NO standard based measurement models that work

- Security mindset (hacker thinking) cannot be taught to all programmers – need some specialists in the team – yet the more security aware the programmers are, the less security bugs they make – involve to threat analyses

The third track session discussed about encryption algorithms. A study was presented on digital signatures, which allow part of the message to be changed by a 'trusted 3pp'. The technical detail of the presentations went to level of mathematically proving certain properties of certain digital identity – based algorithms (HIBE). More detail on the work can be found in the proceedings of the conference (cryptography track).

The fourth track handled in-the-could (D)DoS mitigation. Peak volume of a single (D)DoS attack has increased from 400Mbps (in 2001) to 49Gbps (in 2009) – and (D)DoS is a serious problem in the internet. There is a 1Gbps attack every 26 minutes and 10Gbps attack every 190 minutes. The type of the attacks has evolved from pure bandwidth attacks to more target-specific. Typical (D)DoS mitigation techniques include: source-based ACL, destination-based ACL, BGP RTBH and rate limiting. In addition to these there are more sophisticated methods including intelligent NW-based filtering (active challenge-based filtering, statistical modeling and deep packet inspection), outsourcing IT (no longer own problem), ISP-based solutions (ISP-filtering, upstream filtering) and could based solutions.

Cloud-based solution was claimed to be efficient, as it doesn't require huge bandwidth over provisioning and technology at every site. In case of an attack, the traffic can be routed inside the cloud to an appropriate 'scrubbing center', to clean-up with various methods the incoming data flows from the attacks. One method is to send a 302 redirect to the incoming packets – good clients will follow the redirect, bad ones will send a new get. User agent field contained in many (D)DoS attacks can help to identify that the packet is an attack (databases of 'bad' user fields exist).

Key Note Sessions

The first key note session was a panel discussion, how to deal with sophisticated threats without creating a big brother. It was discussed, what is the role of governments in the threat mitigation. It was stated that the Chinese steal terabytes of confidential information, and USA is not doing much to prevent that. It was also questioned, whether USA does the same. It was noted that deep packet inspection (particularly on an ISP/ governmental level) creates an efficient tool for profiling people, which may lead to all kinds of (commercial/ non commercial) 'nasty things'.

In the second key note session, Qualys manager explained that the cloud computing will change the world – it will be easy for the companies to switch from one cloud provider to another, unlike with current way of working. What will be needed for cloud computing are secure single-sign-on to the cloud, and a secure browser.

At the third key note session, secretary of Department of Homeland Security, Janet Napolitano shed some insight on US government thoughts related to Cyber Security. She quoted that according to Obama 'these networks are part of critical national infrastructure and they are attacked continuously'. She explained that the Department of Defense is responsible for military security (through NSA) and the DHS is responsible for private sector. Their top priority is the fight against terrorism, but cyber security has recently got a new strategy and is very important on the list. She said that similarly as private organization have silos, the governmental organizations have stovepipes. (If understood correctly) they are developing EINSTEIN(?) and national IPS for network and threat monitoring on a national level. How to pre-emptively attack against cyber threats? From private sector she wished: Automation of security, Interoperability and Privacy –enhancing authentication.

Rest of the day’s key note sessions were of varying level and content. The interesting notion from McAfee was that quite often the security of the software repositories is awful. Apart from stealing IP from those, inserting malicious code or backdoors by malicious parties is typically very easy.

The day was finished with a bit different presentation by Dr John Donahue regarding human-machine interaction. They have conducted the first clinical trials on inserting a microchip in paralyzed person’s head – and have been able to allow person to move mouse cursor on a computer screen by only thinking of hand movement (albeit being paralyzed from neck down). Interesting evolution possibilities on the human-machine interaction – somehow Star Trek come to my mind.

Day 4 – Track Sessions and Key Note Sessions

Track Sessions

The first key note session handled about law and security standards. It was noted that standards can be created by anyone; private organizations, national organization and international organizations. Examples: ANSI, ISO and PCI. It was stated that no law requires security certification, but in the court a security certification may show that security has been taken seriously. Apparently law in Massachussets requires the organizations to have risk-based security measures. The first part of the law requires risk-based approach to security methods selection – but the second part particularly requires that firewall, virus protection on personal devices and encryption of the portable devices. For case of someone suing company, all security measures should be properly documented – so that it can be shown in the court that adequate security measures have been taken – and cases have started to appear, where this has helped the companies the escape the charges.

The second track session handled effective insider attack detection. Carnegie Mellon university has created a database of insider attacks, which can be used for studying characteristics of insider attacks. Three major categories of attacks were identified: sabotage (112 cases), fraud (129 cases) and IP theft (62 cases). 38 cases didn't fall into these categories. The sabotage is typically carried out by ex male employee, who has had a system admin (or other privileged) role. Fraud again is typically carried out by low-level worker (male or female) while being employed. IP theft again is carried out by employees who are about to leave, or who are actual spies. Mitigation strategies suggested were:

- Follow HR radar – audit computers of people identified by HR
- Monitor logs
- Monitor privileged user accounts
- Scan computers for malicious software (many sabotage cases were characterized by user having hacking/ malicious tools on their computer)
- Check log edits
- Check killed services (eg logging services)
- Scan for dormant accounts; eg make a script to compare employee lists against account lists; find “James Bonds and Donald Ducks”

The third track session handled evolution of the rootkits. The latest rootkits (such as TDL3) are incredibly smart and difficult to remove from the computer. There seems to be also an ecosystem around the rootkits. The session contained several demonstrations of detection and removal of different generation rootkits from the computer. It was advised not to use system as an administrator, upgrade to 64bit O/S and to use bitlocker with tpm (?) to avoid rootkits. It was also stated that as it is very difficult to detect the rootkit in the computer, monitoring network traffic may be an effective way of detecting a rootkit. In a single computer, the rootkit might have an own invisible IP protocol stack, so monitoring or protecting with SW firewall may be inefficient.

The fourth track session handled threat modeling. Microsoft, EMC discussed about their risk modeling practices in software design. Microsoft gave following cost factors, depending on which software lifecycle phase a security flaw is found (referred to similarities with quality in general): design 1 – implementation 6.5 – testing 15 – maintenance 60. Their threat modeling was based on architecture & design vs threat modeling interaction. Threat modeling again interacted with training/planning, source code analysis, security test plan and customer documentation. They said that two lessons have been learned from threat modeling, firstly threat modeling is really hard – and sometimes “scary” (=avoidable) experience for the coders and secondly that “assets” are not really known in the design phase – as the customer environment can in practice be anything. www.microsoft.com/sdl web-site should have free material and tools for risk modeling.

EMC added to the threat modeling that checklists work better than open-ended questions to the coders – and EMC relies on engineers to perform the threat modeling. EMC had following process for threat modeling: 1) draw data flows 2) identify threats with checklists 3) assess risk of threats (with a simple Excel(?) tool) 4) plan mitigations using prescriptive guidance. They also had a threat library (for eg c/c++; risks such as buffer overflow etc). Average risk assessment at EMC takes ~8 hours, involving 2-5 engineers, yielding to average of 6 high and 3 medium risks.

Both EMC & MS stated that getting started the risk/ threat evaluation is very difficult, and particularly if the engineers scare/ get bored in the situation. MS has developed a card game to be used & ease risk finding process. A good practice of a threat evaluation session is to involve different people from project management to coders, so that later everyone part of the software development will have a right mindset.

Key Note Sessions

The key note sessions were getting lighter and more repeating towards the end of the conference. Majority of the discussion was around cloud security, and how clouds can be used for (D)DoS protection. FBI mentioned that they have >1000 computer forensics experts on their payroll – and that cyber terrorism (Georgia & Estonia mentioned) and espionage are a real threat. The last key note session handled about ‘robot revolution’. Robots are increasingly replacing humans in different situations; US army has over 7000 robots and over 12.000 unmanned vehicles in use. Roadside bomb checking robots are in daily use in Iraq – and if the Moore’s law keeps its pace with robots, there will be some kind of a robot evolution in the future.

Day 5 – Track Sessions

The first track session handled about ZigBee wireless ethical hacking. ZigBee is a low-power short range wireless protocol, which is designed to be used in eg house control appliances (such as thermostat control, remote controls etc but was mentioned to be in use on eg dam floodgate control and other more critical applications. It was mentioned that MGM City Center – brand new hotel in Las Vegas – has 10.000 ZigBee thermostats, 5.000 touch screens and 7.500 other controllers). ZigBee is designed to be a low-power competitor to eg Bluetooth (battery life designed to be years rather than hours, stack size is <120kB; with max data transfer rates of 250kbit/s). Zigbee has been recently designed, and it does include some security – but according to the track session, severe security flaws do exist (particularly interesting towards eg house key applications, controls of critical infrastructure such as floodgates etc). Joshua Wright (Inguardians Inc, SANS trainer) has developed a "KillerBee" toolkit for ZigBee security testing. Some of the potential weaknesses include:

- DSSS (802.11b) – no channel hopping – easy to sniff
- Max frame size 127 bytes (fragmenting -> fragmentation flaws do already exist in implementations)
- Shared-secret (often pre-installed by manufacturer; what if someone steals one physical instance of a ZigBee remote device – and then finds out the key [possible, demonstrated – easy through memory dump]; has full access to all house ZigBee devices.
- Vulnerable to replay attacks (capture & re-transmit eg door opening signals)
- When powered up, the device gets the shared-secret key over the air – unencrypted

The second track session was about mobile phone messaging attacks. A research group had studied SMS and MMS vulnerabilities. (Technically they didn't seem to know much about mobile systems underneath the messaging). Few highlights from the presentation:

- Phone is an interesting attack target: always on, personal
- Possible to do low-level attacks, as more open phone operating systems (such as android) come to the market
- Operator-sent SMS commands to change phone settings open an attack vector – have tried out spoofing fake settings SMS to phones -> works; eg possible to change Internet proxy to some MiTM machine; or change MMS server address to a fake one.
- Different manufacturers' chips allow sending different types of SMS (some do more filtering than others).
- Old phones (and modem sticks) store incoming SMS in raw format (on SIM) which enables testing, what kinds of messages come through.
- Operators (at&t) do notice 'weird' messages & spoofing -> contacted the phone owners
- Android UDH parsing flaw; sequence #00 crashes phone process (valid range for sequence numbers is 1-ff)
- IPhone SwirlyMMS -> possible to cause cyclical restart/crash; impossible to fix without other phone
- Windows Mobile WAP push SL "vulnerability"… With configuration change SMS, it is possible to make the phone load and install whatever software!!
- T.A.F.T JailBroken iPhone @ redsn0w.com (hacking tools?)
- Have reported these issues to GSMA

Last track session of the conference was about DNSsec. The track session speaker didn't take very technical stand-point to DNSsec – rather said that, one should carefully consider, whether implementing DNSsec or not – as it could potentially be used as a political tool. Already now there is a Shanghai treaty signed by US allies & enemies to oppose US proposal for ICANN having the 'root certificate' – as the root certificate owner would have total top level domain control. Conspiracy theories of US government's intentions with DNSsec were hinted. The main point was that if DNSsec – like systems are to be designed, they should not be designed with single choke point, as there will be national interests. Rather SSL or some other existing security mechanism than DNSsec should be selected. DNSsec protects against cache poisoning attacks, but not eg domain name capture using fake name holder, DDoS or hosts.txt –attacks.