Information Security and Privacy Advisory Board (ISPAB)

Summary of Meeting

George Washington University
Cafritz Conference Center
800 21st Street, Room 405
Washington DC

December 3 – 5, 2008

December 3

Started at 9:05 A.M.
Ended at 3:50 P.M.

Present:
Dan Chenok
Fred Schneider
Pauline Bowen
Brian Gouker
F. Lynn McNulty
Philip Reitinger
Joe Guirreri (telecom)

Absent:
Howard Schmidt
Ari Schwartz
Rebecca Leng
Alexander Popowycz
Peter Weinberger
Jaren Doherty
Lisa Schlosser

Visitors, presenters, panelists:
Matt Scholl, NIST, Computer Security Division

The Chair, Dan Chenok, opened the Information Security and Privacy Advisory Board (ISPAB) meeting at 9:15 am. He explained the schedule of the 3 day period, which included the Cloud Computing and Cyber Security session on Friday. Dan Chenok welcomed for the first time to board, the first speaker, Michael Howell.

OMB Update
Michael J. Howell Jr.
Deputy Administrator, e-Gov & IT

Mike Howell was previously CIO with the Interior Dept, now is the senior career civil servant for IT at OMB. He is playing an important role in cyber security.

He talked first about using a Social Security Number only for accessing Social Security accounts and no longer using it for identity purposes. He suggested setting up another identity number to get rid of identity theft with Social Security Numbers. Fred Schneider asked, “Why would using a different identity number be any better? You will not help the SSN problem by using a different identity number.” “Fred Schneider suggested that we should eliminate using identifiers to authenticate people”.. Mike Howell let us know that it is just one step toward protecting individuals from risk, with regard to identifiers not authenticators.

He indicated that the Federal CIO Council was increasing its role in privacy and security through new committees.

Regarding the Trusted Internet Connection (TIC) initiative, Mike Howell reported that the number of connections had been reduced from 4500 to 2578, with a target of under 100. TIC providers have to be independently assessed. Additional TIC activity through Networx will occur, but agencies need more information from vendors including C&A. Dan Chenok stated that the Board voted last meeting to send a letter asking questions about this and a plan to review the Einstein-related monitoring by agencies where trusted internet connections were added.

Mike Howell discussed the GSA lead for implementing DNSSEC at top level .gov domain in January 2009 and said that it was on schedule. He said that the agencies will implement the second level by December 2009 and that the agency plans are under review and modification. The schedule is on track. Dan Chenok asked, did this come out of a policy assurance? Howell answered that it was an OMB memo. Dan Chenok suggested that he may want to do a deeper follow up session.

Mike Howell said that agencies had made good progress with Federal Desktop Core Configuration and HSPD 12

Mike Howell discussed the IT Infrastructure Line of Business. He said that this focused on 3 different categories, including End User Computing and Support, Mainframes and Servers, and Telecommunications.

He ended with the upcoming issues that may occur during the transition.

USCERT and Einstein
Mischel Kwon, DHS

Mischel Kwon has been with the committee before. The Chair stated that the board has a great interest in US Cert. Mischel Kwon stated that US Cert has changed an enormous amount, including a large change in organization. They started an Operations portion of US Cert which Mischel Kwon heads; Mike Smith is the acting director of the Federal Network Services (FNS) portion of CERT at this time.

She stated that the mission of US Cert has grown, and that US cert will more than double in size with in the next few years. Reporting out about attacks is a big job for them. US Cert is growing and looking at a larger facility.

She stated that the tech part is not the hard part, the people part is.

Process documentation and certification, is a big interest to them. Process needs to be customer-usable. Mischel Kwon stated that USCERT is working with partners in Intel and security who can share info with US Cert so that they can respond faster and more easily to problems. She said that they have begun more projects, including the Joint Agency Cyber Knowledge Exchange (JACKE). JACKE goes through fed focused threat tactics. Kwon is excited about this new working group, and it benefits partnership with Fed space.

Einstein I has been deployed, 26 locations use this. She discussed the upcoming Einstein II which will help speed up the identification of the attack. Einstein II will try to get rid of flow data which could take days. Dan Chenok asked if this will be at the TIC locations. Mischel Kwon answered, yes and she hopes it will venture to more locations as well. She stated that privacy does come up when Einstein is talked about. She suggested that the committee read the Secretary’s speech about privacy, and said that she will have the relevant quote available for Pauline Bowen. US Cert will provide Privacy training for all of the operators so that they know what to do when handling PII.

They are looking into using more people in a variety of different roles, for a balance of staff, including international cooperation between SOC staffs. Fred Schneider asked, to what extent do you hear alerts? Mischel Kwon said that it will depend, it is a balance, they often play catch up. She said that partner agencies work together every day -- they work with NSA, FBI, and etc., and nothing would be successful without teamwork. She said the new cyber authorities were not needed for her people to do their job. Concluded at 10:22am.

Break

NRC CSTB Report Briefing
Herb Lin, NRC CSTB

Herb Lin has a new report out: Protecting Individual Privacy in the Struggle Against Terrorists: A framework for Program Assessment. The committee is headed by Bill Perry. The task of this new report was to address the challenges of technology in fighting terrorists, especially data mining and information fusion, available and emerging surveillance technologies and their IT support, behavioral surveillance, and attendant privacy issues.

Herb Lin discussed 'The ever-present tension?' which is, "Protection of our Nation or Privacy and Civil Liberties". There are a few basic premises of the report. One is that the US faces two real threats from terrorists: first, including terrorist acts themselves second, that the terrorist threat does not justify government activities or operations that contravene existing law and inappropriate or disproportionate responses. Another basic premise would be terrorist challenges do not warrant fundamental changes in our level of privacy protection. Another issue is that science and technology are important dimensions of counterterrorism efforts. Last, counterterrorist programs should provide other benefits when possible. Herb Lin said that the report found that the counter-terrorism community should have the best tools and that our privacy should be protected.

Herb Lin said that the core of the Report would be a Framework for evaluating Information Based Programs for effectiveness and consistency with U.S. laws and values, applicable to all information-based programs for specific government purposes, such as counterterrorism, both classified and unclassified. The report believes this framework is realistic; applicable; consistent with U.S. laws and values; based on common sense, best practice and lessons learned; and will lead to continuous improvement and accountability. Herb Lin talked about the Framework and that to be effective, programs must be robust, have appropriate and reliable data, data stewardship, objectivity, ongoing assessment, and well-documented. The framework should be consistent with U.S. laws and values regarding Data, Programs, and Administration and Oversight.

Herb Lin stated his conclusions on the framework, Privacy, Assessment of Counterterrorism Programs, Data Mining, Deception Detection and Behavioral Surveillance and Statistical Agencies.

- Privacy protection can be obtained through the use of a mix of technical and procedural mechanisms; data quality is a major issue in the protection of privacy, and inferences about intent and/or state of mind can implicate privacy issues to a much greater degree than assessments or determinations of capability.
- Assessment of Counterterrorism Programs can be obtained through program deployment, and use must be based on criteria more demanding than 'its better than doing nothing,' Fred did not agree with this statement and said that the statement could easily be twisted.
- Data Mining: currently, privacy violations arising from information-based programs using data mining and record linkage are not adequately addressed. He also said that data mining has been successful in private sector applications such as fraud detection, and that pattern-based data mining can help analysts determine how to deploy scarce investigative resources and actions. Automated terrorist identification is not feasible. He said that they will never have a perfect profile of what an unknown terrorist looks like and Joe Guirreri asked if there was a terrorist who had been arrested and released without being convicted, would there be enough information to describe him later on. Herb said of course there would be. Continuing on Data Mining, Herb Lin said that systems that support analysts should have features that enhance

privacy protection; however, privacy-preserving examination of individually identifiable records is not possible, and data mining R&D using real population data is privacy invasive -- but that doesn't mean that you can't still use it.

- Deception Detection and Behavioral Surveillance: behavioral and physiological monitoring techniques might help detect: (a) individuals whose behavior and physiological states deviate from norms and (b) patterns of activity with well established links to underlying psychological states. He also said that R&D aimed at automated, remote and rapid assessment of anomalous behavioral and activity with well-established links to psychological states relevant to terrorist intent is warranted and that technologies and techniques for behavioral observation have enormous potential for violating privacy.
- The last conclusion regarded Statistical Agencies. Federal census and survey data has little or no content that would be useful for individual tactically oriented counterterrorist activities, because of their content, sampling fractions, and lack of personal identifiers.

Herb Lin then discussed his recommendations for the framework for the new report.

Concluded 11:40

Lunch

ID Management
Board Discussion with NIST
Elaine Newton, NIST

Elaine Newton has been at NIST for 3 years, with a mainly biometrics background. She and her program are looking to design systems for face recognition. She has recently become program manager.

There are 6 projects within her program, focusing on standards and testing. They are using smartcards, biometrics formats and qualities. She said that she is working on an Identity Management Program. Other work going on at NIST with biometrics are not necessarily in the program. One area that they are not involved in would be biometric revocation.

A question came up as to what revoking a biometric would mean since your fingerprint would never change — Elaine Newton explained it as, to revoke a biometric would be to revoke the transformed data about the biometric. The board asked, is the data stream that biometrics creates cause a problem? Elaine Newton answered that this is not the area that they are in yet, they want to get to that area. She said that she is collecting ideas from the people who are working with identity management and taking ideas from them.

Fred Schneider stated that he has been working on writing a chapter on identity management. He also said that there is not a standard on who can see the information that a person would want them to see. He said that agencies should learn more about what terms and references are out there and not a lot of people have researched what these terms mean. He suggested that NIST write an SP on what terminology there is for this biometrics. Elaine Newton said that she wants to work with the other people around that are using this information rather than NIST starting their own. Fred Schneider said that he would like a Framework guideline on Identity Management and its terms that NIST uses, and a guide for the commercial world to understand Identity Management phrases and regimes. Dan Chenok agreed that having a Framework would help other agencies understand.

Lynn McNulty asked, is IAD working with Voice Identification? Newton said no, but EEEL another lab, is working on this. Lynn McNulty believes that this should all be included with each other.

Elaine Newton said that up until this point it has not been addressed by IAD, and that the project has just started up within the past month.

Lisa Schlosser talked about how DOD was up to date with Identity Management with the full deployment of identity credentials and how well it worked there. Fred Schneider stated that there is a problem with having multiple identities. Dan Chenok said that DOD domains are more controllable than the Fed Government as a whole.
Lisa Schlosser talked about YouTube and how President Obama is using this for a weekly video update. She asked, if there was anything that we should look at from a technical standpoint? This could include technical interoperability and standards for open government more generally, as well as continuity of identity over the web.

The board agreed that ID Management is an OMB and a NIST issue. It was noted that GSA was leading a Task Force on this, information is at Biometrics.Gov. The board will be back with NIST about Identity Management, including the idea for a Unified Framework. Elaine Newton was happy to hear feedback from an outside standpoint and stated that she is still doing a lot of standards and testing.

Break

Work Plan (including Privacy Report Update)
Board Discussion

Dan Chenok welcomed back Lisa who was deployed with the military for a year. Fred Schneider stated that Herb Lin's talk was informative. Lynn McNulty said that he felt Mischel Kwon did a very nice job, and he thinks that it sounds like they are organizing themselves well and that it was very candid and forthright.

On the last day they voted on a draft letter that Ari Schwartz did, but when it went up for signature there were a lot of questions. Joe Guirreri stated that in the last meeting he asked that he would have liked to look over the letter before it went out to be signed, but, he never saw it.

Joe Guirreri discussed that there are two levels that can harm the US. He does not want to have open-to-public forums; he feels there is 'classified' information included in this discussion and believes that it is harmful for open public to hear. Ari Schwartz believes that this is not about sensitive information and that it is up to the agency to decide that this information is classified. Brian Gouker says that he sees the point that Joe Guirreri is saying and he went over a list of 5 things that he thinks the letter highlights. Ari Schwartz made some changes to the wording that the board suggested. Then the board agreed on the final version.

Additional agenda items were discussed for the April meeting:

1) DNS Sec Report
2) Standard OMB Update
3) FNS and Tools of CERT
4) Open Government & Security
5) ID Management Framework
6) Supply Chain Risk Management
7) Privacy Report
8) NIST Update

Dan Chenok concluded meeting with thanks to everyone for their participation and he discussed tomorrow's schedule. Adjourned 3:50pm

December 4

Started at 8:23 A.M.
Ended at 4:15 P.M.

Present:

F. Lynn McNulty
Ari M, Schwartz
Philip Reitinger
Joe Guirreri
Rebecca Leng
Alexander L. Popowycz
Peter J. Weinberger
Pauline Bowen
Brian Gouker
Jaren Doherty
Lisa Schlosser
Howard Schmidt
Dan Chenok
Fred Schneider

Absent:

Visitors, presenters, panelists: 8
Donna Dodson, Matt Scholl, NIST's
Computer Security Division

Center for Strategic and International Studies (CSIS) Commission Briefing
James Lewis, CSIS

James Lewis serves as Executive Director of the CSIS Cybersecurity Commission report. He talked with the board about six months ago. He talked about some issues that came up like the difference between homeland security and national security, and does it make sense? The Commission believes that cyber security should be part of national security, and that national security strategy and homeland security strategy should be the same. Commissioners do not believe that DHS is doing a good job with cyber security.

Some of the issues that they talked about were how to fix coordination within the Federal Government. James Lewis said that he thought of Karen Evans' job at OMB for this role, but, she is not the official CIO for the Federal Government. He also said that the Obama campaign might come out with a CTO to resolve this problem.

James Lewis said that Private Sector involvement was a hard issue for the Commission; he said that solutions to secure cyber space are not working. He said that the 2003 strategy was, 'doing everything for everyone', and that did not work out; the Bush administration said that the relationship with Private Sector was worse in 2003 than in 2001. James Lewis said to rebuild these relationships we need to build trust, and personal relationships.

Another issue that he came up with is that there are a lot of different groups. Some groups are handy but they address about 1/3 of what you really need. James Lewis thought they needed an operational group by itself.

James Lewis said that another issue that almost blew up their group was procurement. He said that when the Federal Government purchases IT products it should be delivered in a secure mode. How do you set the standards for having products delivered to you already configured? A recommendation that he had was to build on FDCC. He also said that NIST needs to be involved with this and that they are doing a good job. He stated that if you want to work quickly, do not reinvent the wheel, work together. This needs to be a priority. Jaren Doherty indicated that FDCC is an example of how we do not have the right people involved, he said that no one has gone out to the private sector to coordinate properly.

James Lewis also discussed continuation with the Common Criteria Testing program and said that we need to move on from this, rather than try to wait for imperfect criteria to be perfected. He said that Common Criteria offers a multilateral vehicle. We need to collaborate with other countries and common criteria helps.

James Lewis suggested that the ISPAB could raise the security profile across the government, and offer real solutions to address privacy and civil liberties.

Lynn McNulty chaired the next portion of the meeting in Dan's absence.

ISC^2 Software Credentialing
Lynn McNulty, Board Member
Howard Schmidt, Board Member

There is an issue of components missing from different agencies. They said that they thought the Software Assurance Forum was coming together and that ISC2 is going to make a big contribution.

Lynn McNulty asked why attackers are attacking applications. He said that attacking systems became harder, perimeter defenses improved, attacking applications became easier, and application software became more vulnerable and more exploitable. Then he asked what is the answer to fixing these attacks. He said that there is not a single answer but a variety of solutions.

He said that the ISC^2 approach is the CSSLP (Certified Secure Software Lifecycle Professional), which is a base credential and professional certification program, which addresses security in the software development cycle, takes a holistic approach to security in the software cycle, and tests candidates' competency (KSAs) to significantly mitigate the security concerns. He said that the purpose of Certification is to provide a credential that speaks to the individual's ability to contribute to the delivery of secure software through the use of best practices, and that the target professionals for this Certification would be involved in the Software Life Cycle Activities.

Lynn McNulty then discussed the overview of ISC^2 Software Assurance Certification and the target audience, including project managers, business analysts, auditors, and industry groups. He went on to the CSSLP Certification Requirements for each person applying for the certification. He discussed the future of CSSLP and stated that there were international marketing efforts, ANSI/ISO/IEC17024 accreditation, maintenance activities and a Cert education Program.

Break

GAO Brief
Gregory Wilshusen, GAO

Gregory Wilshusen runs the GAO security team, and is in a position to be highly influential with the feds. His group has about 38 people and that they work closely with e-security lab which has about 25 people. This was the first time he had been before the board to talk about Information Security.

He spoke about several issues, including GAO Cyber Security Focus Areas; recent GAO Testimonies and Reports on Cyber Security Issues; and Key Findings and Recommendations. He talked about what GAO does in Information Security and Cyber Security Efforts: FISMA, Emerging Issues, Cyber Critical Infrastructure Protection, Consolidated Financial Statements, and Critical IT Systems. He also said that agencies are required to submit annual reports to Congress and GAO, which GAO uses for testimonies and reports. He said that the work that they do is mainly mandated by law or requested by Congress.

Dan Chenok mentioned that the Board is in process of finalizing a letter about Einstein. Gregory Wilshusen said that GAO is interested in this. Peter Weinberger asked if the legislature uses these reports. Gregory Wilshusen answered yes and said that their reports are input, not necessarily a deciding factor.

He stated that agencies are reporting systems certifications, but there are still serious vulnerabilities and said that this is largely due to poor metrics. He mentioned that the first object is to identify particular measures, second would be to go outside of government to see how they use metrics, and third is to identify how other agencies use metrics to identify security issues.

Another request that they have not yet started is the Acquisitions side. With regard to agencies, they have been reviewing and assessing the controls that TSA is in the process of implementing. He said that DHS has now certified that it has met the requirements of TSA requirements. He just received a mandate to look at the component systems and security at NASA and that he finished looking at the DOD security as well as written a report about Los Alamos security vulnerabilities. He said that GAO has became more efficient working inside with agencies and that he often works side by side when writing reviews. Doing an inside review helps.

He continued on, saying that they are looking at the remediation process with other agencies, though the action is not thus far effective. There are a number of vulnerabilities that they have run into. He said that Karen Evans at OMB has testified that certification and accreditation activity is significant. Regarding what's next after C&A, he said that this would involve better risk assessment and mitigation, and improving test evaluation and controls.

Industrial Control System Security, Industrial Control Systems Security
Sean McGurk, Director of Control Systems Security Program, DHS
Lynn McNulty, Board Member

Sean McGurk spent 28 years in the Navy and retired in 2006. He was selected to be the director for the Control Systems Security Program and focuses all of his assets on Industrial Control Systems.

He said that everything has a tieback to control systems, from aquariums to zoos. Peter Weinberger asked if it included badge systems. Sean McGurk said absolutely. Industrial Control Systems are computer based systems (digital to analog), they are connected to integrated systems, they can control critical systems, and usually are remote operations. He said that the term Industrial Control System (ICS) refers to a broad set of control systems, which include SCADA, DCS, PCS, EMS, AS, SIS and a number of other systems. He also discussed control system security challenges, including Anti-virus & Mobil Code Countermeasures and Support Technology Lifetime. He then discussed the 18 Critical Infrastructure Sectors, including Agriculture and Food, Banking and Finance, Chemical; and Nuclear Reactors.

He talked about the Risk Equation: Risk = Threat x Vulnerability x Consequence. He said that threat meant: Any person, circumstance or event with the potential to cause loss or damage. Vulnerability meant: Any weakness that can be exploited by an adversary or through accident. And Consequence meant: The amount of loss or damage that can be expected from a successful attack.

Sean McGurk said that the threats to Control Systems are Crackers, Insiders, Hostile Countries and Terrorists. He discussed the Cyber Threat Trends with a chart showing how threats become more complex as attackers proliferate. He then discussed the Vulnerability Lifecycle with examples. Actual incidents include industrial control networks: Davis Besse Nuclear Power Plant; Olympic Pipeline Explosion; Maroochy Waste Water, direct attack; Texas City Explosion, not a direct attack, but a cyber event; Harrisburg, PA water facility, not a direct attack, but a cyber event; Polish Trains; and Insider Threat, Hacking into LA's lighting system.

He discussed the highlights of Industrial Control Systems, saying that Control System security can no longer hide behind proprietary configurations and special training (Security by Obscurity), Control Systems are no longer isolated systems that require special skills. Hackers are smart, the prevalence of information available via the internet makes attacking control systems easier, and Control Systems are migrating away from their traditional shared and unrestricted configurations to more secure ones.

Sean McGurk then talked about the CSSP Strategic Overview. He said that most of industry doesn't understand their service agreements when purchasing equipment, and that they need to raise the level of awareness -- that is why he is putting this document together. He agrees that they need to write a common framework for all of this. He said that there is web-based training for Cyber Security for Control Systems Engineers and Operators and that there is hands-on training provided to government.

The Board discussed having DoD and DOE on a future agenda, to address issues like future NIST guidance and potential procurement language. Howard Schmidt agreed to lead this activity.

Lunch

After lunch the minutes from the last meeting were approved and the Einstein letter was finalized.

The board talked about the agenda for the next meeting on April 1- 3. Dan Chenok asked if there were any other topics that the board would like to do follow up on? No one had any really big issues. Few topics from the day before that the board would like to follow up on are DNS Sec, OMB back after admin change, FNS and Tools part of Cert, we only got the ops part from Mischel Kwon, follow up on mass collaboration (Which Lisa Schlosser was happy to do). The board decided that they would like to hold a meeting on the update of the new administration and that there is a lot of direction stuff that needs to be listened to when the new administration starts. Donna Dodson clarified how Supply Chain places a role in counterintelligence. Ari talked about Privacy Act items, privacy act amendment bill and how he would like to get them to speak to the board.

Threat Analysis, DOD vs. Civilian Government

Matthew Stern, LTC (Retired), Former Commander, US Army CERT

Matt Stern has a role as a deployed army reservist. Matthew Stern was commander for the Army computer response team for 2 years. He is learning and understanding the cyber threat through the Army. He retired 2 months ago. He is now the Program Manager for Cert with General Dynamics.

Matthew Stern talked about the characteristics of today's cyber threats are very determined, sophisticated, agile, and stealthy; they are not deterred or encumbered by laws or policy; they are motivated by money, politics, pride or thrills; and they are probably better at it than average security staffs.

He also talked about "For every action, there is an equal and opposite reaction," including anti-virus programs = polymorphic viruses; two factor authentication = exploits against service accounts; locking down ports and protocols = encrypted traffic over port 80; and MD5 Hashing = Evil twin. There are papers on how you can get around MD5 hashing. (Note: MD5 is not approved for use within the federal government)

Matthew Stern explained that by 'they' he means ALL hackers. When he was in command, a soldier came to him and had the idea of trying to figure out where the next threat was going to come from, he came up with an idea of where to get that from and started to go to conferences to learn the cutting edge. They attended the Black Hat at Deathcon in Vegas. The people attending the conference really showed them how smart these people were that they could hack into so many things.

He talked about the Exploit Vectors: Social Engineering and Phishing, Web browsing attacks, and SQL injection methods against vulnerable websites. DoD considers using thumb drives as a risk. Matt discussed the DoD Cyber Security Community's tools, analyst training, great model to focus intelligence efforts, rehearsals to validate processes and operational concepts, and Certification.

Matt Stern discussed the procedure and certification that his students go through to be trained. They go through analyst training and are recertified every 3 years. A question arose, 'How do you train someone to not click on an email from their commanding officer that may be a phishing email?' Matt Stern explained that it is hard to not actually do that and that it was too hard to completely outsource this expertise. Matt Stern was asked 'if someone were to come up to you and ask what do I do? What would you tell them?' He said that he would make sure that your network is as secure against DDoS as it can be. Assess risk and figure out what is acceptable or not, he said that you will never be able to keep them out entirely.

Identity Management Framework

The Board went into discussion on a potential letter about identity management. They urged Donna Dodson to do more research on the properties on Identity Management: will it really have any effect on the way NIST feels about this? Elaine Newton is very open on the way Identity Management is going and will be open to a letter. NIST took a look at the people from CSD and ISO and said that a lot of things that they were doing with Identity Management made sense. 800-63 was not meant to be the general framework but it seems it turned into a framework. CSD is putting some resources into Identity Management framework. What impact would it have on the consumers of the document? Identity Management for Authenticating People should be the topic of the letter. The letter should be on various kinds of problems you would want to solve in Identity Management. NIST did not have input to this at this point.

Cloud Computing Session

The board agreed that they should keep a few minutes at the end of the discussion for Q&A. No questions during the panels, Lynn agreed to bring 3x5 cards for questions and on the index cards, identify who you are and what your question is. Starting 8am tomorrow morning.

Adjourned at 4:12PM

December 5

Started at 8:05 A.M.
Ended at 5:15 P.M.

Present:

F. Lynn McNulty
Ari M, Schwartz
Philip Reitinger
Joe Guirreri
Rebecca Leng
Alexander L. Popowycz
Peter J. Weinberger
Pauline Bowen
Jaren Doherty
Howard Schmidt
Dan Chenok
Fred Schneider

Absent:

Brian Gouker
Lisa Schlosser

Visitors, presenters, panelists: 8
Donna Dodson, Matt Scholl, NIST's
Computer Security Division

Friday 12/5 Dan Chenok opens the meeting at 0805 AM.

Dan Chenok provided the audience an overview of the board, its mission, its charter and its members.

Dan Chenok then introduced some of the concepts of cloud computing and why they are relevant to privacy and security.

Dan Chenok then introduced Karen Evans from OMB.

Opening Keynote
Karen Evans, OMB

Karen Evans, OMB opened with a discussion on the importance of Cloud Computing and importance it has on Critical Infrastructure Protection (CIP), and discussed the possibilities of a Line of Business (LOB) opportunity for the federal government. The LOBs in place today lead the way in acceptance of cloud computing concepts and these new ways of business have potential for significant cost savings and enhanced security.

Issues when looking at cloud computing for the federal government:

1) How do agencies connect into the cloud with multifactor authentication?
2) What are the definitions of interior and exterior networks? This will need to be modified due to the nature of the cloud.
3) How does encryption policy on mobile data apply? An evaluation is needed.
4) Requirements will still exist such as FOIA, Privacy Act, Records Retention Act, E-Gov, FISMA, Paperwork Reduction Act, E-Discovery.
5) How does the IG evaluate these external systems?

Many agencies are currently doing inventive things with mass collaboration technologies. Some example agencies cited were USA.GOV, CDC, DOT, Smithsonian, EPA, and OMB. Specifically discussed was the nationwide mass collaboration discussion with NAPA on health information and privacy. A Report will result on lessons learned from technology, users, communications and results.
OMB did not publish any printed material on the budget this year. Instead they used the federal PKI bridge with GPO, using PIV to sign docs, and sent the budget electronically to the hill. The result was a significant savings in cost and time for OMB relative to their operating budget.

Panel One

Dan Chenok introduced Howard Schmidt and the Cloud Computing Basic Panel. Howard Schmidt moderated the panel.

Industry Trends
Bill Whyman, International Strategy and Investment

Bill Whyman provided an introduction of what the Cloud is and expects a shift of applications, data and markets to the cloud. He discussed his thoughts on how that shift will be disruptive.

IT services will be offered through the cloud, along with tools to build your own cloud. However, there is no agreed-on concept of a private cloud and regulatory issues will be front and center along with the international dimension. This will also affect the underlying network infrastructure.

What is the cloud?
1. Services,
2. Scalability,
3. Sharing,
4. Outsourcing to the internet,
5. New business model. No licensing, now subscribing.

Why do this? Lower total cost. Provides the customer flexibility to scale up and down and is agile and responsive.

There are concerns surrounding security and availability, but the root issue is about trust.

The question for the federal agencies is, does the government really want a cloud or just some aspects of a cloud?

Government Adoption Case Studies
Mike Wojcik, Manager, Risk Compliance Practice, Acumen Solutions

Security challenges exist and need to be integrated into the development process. Federal standards must be applied. Cloud computing does not relieve these requirements but requires them to be re-evaluated to ensure they are being applied properly.

Government CIO
Robert Carey, CIO, Department of the Navy

Trust and loss of control is an issue in the transition to a cloud computing environment for the government. A cloud type of environment was the original intent of Navy Marine Corps Internet (NMCI) but not realized. Issues arose concerning how is information controlled and assured on a military Command and Control (C2) network.

A large issue for the Navy was establishing trust in the Cloud and how to implement once trust, risk and security is understood.

Security Challenges
John Pescatore, Gartner Fellow

Cloud computing is a concern/interest for Gartner clients. There will be private clouds to large outsourced cloud service providers and the entire spectrum in between. This is because compute cycles and data storage is a commodity. If there are requirements beyond basic commodity needs then the cloud gets modified. ACAMA is an organization that is doing cloud and security well.

Best practices may be a cloud in your data center where security is important, and an outside cloud for public facing information. Encryption alleviates some of the requirements for location needs of stored data, but does not solve issues of processing that will not be encrypted. An interesting research area he sees currently is how we can use cloud for new security purposes.

Questions from the Board

Will lack of standards and proprietary solutions lock in consumers and create vendor risk?
A: Open standards are being used fairly well and vendor risk does exist. Service Level Agreements (SLAs) are important. This will be an issue. Some major businesses do not want to get into the commodity market.

Will the cloud be useful in a wartime/combat zone?
A: No, combat zones need trusted, tested and validated technologies. Cloud technology right now is too new and lacks control for trust.

Is there a need for new legislation/Policy/Standards to push this technology?
A: These existing items need examination to evaluate if coverage still occurs. FISMA and DIACAP are based on individual systems and specific system descriptions. Boundaries are difficult to define in a cloud. The focus needs to be on the data rather than the system.

Is there any risk during mass collaborating with identity and control of responses to public communications and how do we know who is responding?
A: Targeted messages and restricted responses on an open message are helpful. Knowing that a lack of identity exists during this type of exercise and filtering your data through that lens is important.

What should NIST do to assist with cloud computing issues?
Standards and Guideline selection/harmonization/development to be sure that cloud computing applies.

Board took a break at 0945 AM.

Panel Two

At 1000AM the Cloud Security Panel was presented, moderated by Rebecca Leng.

John DeVoe, Salesforce.
Currently there are no restrictions on co-mingling of data that are known in the NIST security guidelines.

John DeVoe provided an overview of the security controls in place, including technical controls from Salesforce.com and how that is used by a mobile workforce for multiple business who need security and do not have the ability to provide an existing, secure infrastructure to a geographically diverse and mobile workforce.

Questions from the board:
Does Salesforce also conduct other compliance activates outside of FISMA such as PIA/SORN etc.?
A: Not at this time. Currently salesforce provides a Certification and Accreditation (C&A) package to certain agencies upon request.

Is there a data ownership issue when the data is co-mingled?
A: No, the data always belongs to the data owner and the data can be segregated logically rather than physically. To date, this has not been an issue.

Eran Feigenbaum, Google
In Google, system patching and patch management in an outsourced cloud environment is taken care of. Issues of data loss, backup and recovery are also solved with the implementation of a cloud environment. The lack of a central infrastructure to patch and the broad distribution of data greatly assist with these issues.

Benefits of using a cloud are multiple. Largest is cost savings due to the scalable nature of a cloud to provide only what is needed, and guaranteed resource estimations due to the cloud's flexible nature. Security is "better". The cloud can be more secure than our traditional environments. The cloud can provide a better user experience and greatly extend capabilities to the remote worker. End users are given full platform independence.

Google makes it own servers for use in the cloud to minimize the risks that unneeded hardware and applications may introduce, and all platforms are the same to maximize control and ability to maintain.

Stephen Schmidt, Amazon
The cloud will reduce the overhead needed in the delivery of services to your customers. The scalable nature of cloud will totally eliminate any issue of resource estimation risk. This will

ensure that your organization is fully operational with what it needs and not too much. You get just enough and only pay for that. Security and Availability (according to Amazon) can be assured and validated through multiple means depending on your SLAs.

Pat Arnold, Microsoft
Microsoft offers cloud services. Identity is integrated with XML and with open PHP. Movement to this space will be governed mostly by trust.

Questions from the Board:

What is the biggest challenge of selling security of the cloud?
A: The biggest is overcoming existing culture and lack of knowledge of cloud technology. There also needs to be an acceptance of 3rd party auditors along with collaboration with government. There is a general feeling that not all data should go to the cloud right now. Transition into the cloud is a change and the current rules/regulations are focused on the physical existence of a machine, rather than a cloud environment.

What do you recommend for the Government?
A: Anything that touches an open source network can and should be moved into a cloud environment. These require the least trust and can serve as a baseline to expand understanding and work out any issues that may arise with rules and requirements.

How does investigations/forensics work in the cloud?
A: The cloud will actually enhance record keeping. All data has meta-data for the purposes of auditing. This should facilitate the needs for investigations and forensics.

How is physical and personnel security managed?
A: Physical security is managed very tightly. Guards, man traps, CCTV, Video etc. are all deployed and used at all physical sites where the cloud is distributed. The only personnel allowed in the data centers are technicians for hardware services. No data access is allowed from the data center(s). No administrator accounts are kept on the data servers.

Is the SAS 70 the baseline or is more assurance asked for?
A: The security documentation can be provided but on a trusted basis only. External or additional assurances are made on a case by case basis.

Can you support continuous monitoring?
A: Yes to some extent, but this is not fully defined at this point. Scanning by external organizations is not defined. If external scanning breaks something that multiple parties depend on for data availability, who is responsible? Specifics on continuous monitoring abilities of the customer and liabilities must be specified in the contract.

Will the cloud get filled? Will there be a situation when a customer will run out of space?
A: No, never. Use your SLA to specify service requirements. You will only run out of space if you have a limit specified in your SLA. If not, you can expand to the size needed upon request or on an as needed basis.

Break for lunch:

Panel Three

At 1:00 PM, the Virtualization Panel was presented and moderated by Lynn McNulty.

Virtualization Models
Chong Yi, VMware

Virtual Machines can scale, isolate, and secure, and are an essential part of the cloud. With VMs you can greatly expand your computing ability in the cloud on a scalable manner to accomplish essential tasks on demand. Security can be realized through tight control of the virtual machines used and the ability to issue “fresh” machines each session to ensure the lack of malicious code.

Security and Virtualization
Lee Badger, NIST

Lee Badger presented to the board the mechanics of HW virtualization. Discussion centered on how calls to the virtual environment must pass through the user environment and be re-interpreted by the virtual machine. This is a complex procedure that requires a complex instruction set and a large library of code. This is not fully understood from a security perspective. Bottom line is that VM can provide benefits but security concerns remain.

Virtualization is not a simple box view. There are different layers of virtualization. Virtualization is complicated and has complicated software that will and does have security issues. Configuration of VM layer is important and complicated. Malicious Virtualization risks exist and have potential to be further exploited as an attack vector in the future. If the attacker can enter zone 0 then detection and forensics is extraordinarily difficult, if not impossible.

Virtualization does give you another security layer. It can provide the user a much better Intrusion Detection System (IDS). Snapshots and rollbacks of configurations are easier and can be conducted quickly if not immediately. Security policies can be specified for and enforced for VMs. These are all good security features that VMs provide but more Research should be done on understanding any new vulnerability VMs may introduce into an environment.

Government Adoption
Jimmy Sorrells, GreenHill

Jimmy Sorrells presented on how to secure a hypervisor. His organization states “You don’t get security just through change.” Green Hill believes that VM is needed to keep users with a familiar user experience while letting their organization tackle a security issue in the back areas. Virtualization can provide economy while maintaining security.

New Security Tech
Anthony More, Vir2us

Anthony More presented an outline of Vir2us capabilities that they offer the federal government in a cloud environment. The Cloud and VM gives an opportunity to re-do large complex architectures that did not have security built in at the start. We should do our best to take advantage of this opportunity to ensure that security is understood and implemented in the initial requirements as this new architecture matures.

Questions from the Board:

What is the fix for ring 0 access vulnerabilities?
A: Don’t have VM machines that allow any access to ring 0.

The Board took an afternoon break.

At 2:45, the Cloud Computing Perspective panel, presented and moderated by Ari Schwartz.

Relevance of Current Standards
Peter Mell, NIST

Peter Mell discussed the current standards and how they may apply to clouds. In order to have standards the item must first be defined. Peter proposed a definition and identified characteristics of a Cloud.

He believes that standards are lacking for the cloud architecture. Cloud interfaces are key standards that are lacking. These are needed to define services to architecture and services to users.

Enterprise cloud infrastructures are a place where standards could be useful. This is where organizations build their own clouds. This will greatly assist organizations in identifying where the cross over is in cost effectiveness in having your own cloud rather than outsourcing the cloud. The government could ID minimum standards for interoperability to ensure collaboration if each builds its own cloud.

What could the Federal Government do?

1. Use third party clouds where possible,,
2. Increment into the cloud based on compliance, security, privacy issues,
3. Get a single USGOV cloud,
4. Let agencies build multiple non-interoperable clouds,
5. Work toward standards in interoperability to ensure cross over.

DoD and the Cloud
Chris Kubic, DOD

The cloud is an effective tool in getting information out to the customer (war fighter) in a timely, accurate and effective manner. This must be tempered with the need for confidentiality and the ability to maintain trust in this environment.

Privacy
Dan Weitzner, MIT

There are many privacy issues that the cloud will raise. Transactional data will overcome the data in the cloud and that will raise its own privacy issues. What is the legal status of those transactional records? Can those transactional records be subpoenaed? Who is the true owner of that data? Will cloud providers need lawyers to respond and sort legal requests? Will there be privacy issues with advertising potential and use in the cloud? Will the Communications and Law Enforcement Assistance act (CALEA) be in effect for this?

Procurement
Mike Sade, GSA

Good procurement processes apply to obtaining cloud services as they do to any other large, complex and new procurement. The cloud environment does not mean a change to federal acquisition regulation, or the absolve need to for an agency to conduct due diligence and exercise due care in selecting a service provider. Mike estimates this to have its biggest impact on software licensing. He is hopeful that it will result in cost savings to the agencies. Currently, no standard contractual language exists for contracting cloud services but this is under research. Mike Sade is unsure how the pricing will be established.

A discussion ensued on the potential for a federal government only cloud. The board was undecided on this issue and stated that it will require more examination.

Closing Comments
Dave Wennegren, DASD IT and CIO, Vice Chair of the Federal CIO Council

Mass collaboration and trusted computing from un-trusted computers is a new way to work and is potentially the way of the future. Authentication and Secure information sharing are also key. Change is disruptive. Be disruptive and be prepared to be disruptive. Drive change in your organizations and make it change for the better.

The Chairman adjourned the meeting at 5:15

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Daniel Chenok
ISPAB Board Chairman