Enterprise Security Architecture: Key for Aligning Security Goals with Business Goals

Secure Network Design: Micro Segmentation

Secure ERP Implementation

Fallacies in Threat Intelligence Lead to Fault Lines in Organizational Security Postures
DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Feature
14... Enterprise Security Architecture: Key for Aligning Security Goals with Business Goals
By Seetharaman Jeganathan
In this article, the author shares his insights about why security architecture is critical for organizations and how it can be developed using a practical framework-based approach.

Articles
22... Secure Network Design: Micro Segmentation
By Brandon Peterson – ISSA member, Nevada
This article discusses how a secure network design that focuses on micro segmentation can slow the rate at which an attacker moves through a network and provide more opportunities for detecting that movement.

30... Secure ERP Implementation
By Alexander Polyakov
Enterprise resource planning (ERP) and other enterprise business applications play a significant role in a company's architecture and business processes. This article provides four steps to significantly increase ERP security by tuning its architecture. In addition, the author includes a high-level description of ERP security in general, its risks, typical vulnerabilities, and remediation steps.

Also in this Issue
3... From the President
4... editor@issa.org
5... Sabett's Brief
Security Architecture…and the US Congress?
6... Herding Cats
Write That Down
7... Open Forum
The Security Architect and the Security Engineer
8... Gray Hat
A Downside to Red Teaming
9... Security Awareness
Polluting the Privacy Debate
10... Security in the News
12... Association News
32... PCI Guru
Email Security

Fallacies in Threat Intelligence Lead to Fault Lines in Organizational Security Postures
By Jeff Bardin
The article discusses the issues associated with threat intelligence, the need for a common understanding of taxonomy and glossary, as well as presenting a case for intelligence tradecraft as a common standard. Furthermore, the article takes vendors to task for their reporting methods, content, and intent while providing a listing of recommendations and opportunities for organizations that may assist them in their building of organizational intelligence capabilities.

©2016 Information Systems Security Association, Inc. (ISSA)
The ISSA Journal (1949-0550) is published monthly by Information Systems Security Association
11130 Sunrise Valley Drive, Suite 350, Reston, Virginia 20191
703.234.4095 (Direct) • +1 703.437.4377 (National/International)
From the President

Greetings ISSA Members

Andrea Hoy, International President

As the year comes to an end, I am still reflecting upon the wonderful ISSA International Conference in Dallas last month. International attendance was the highest in years with members and non-members coming from at least 15 countries: Bangladesh, Barbados, Canada, the Cayman Islands, Egypt, France, Israel, Kuwait, Liberia, Nepal, Nigeria, Poland, Uganda, the United Kingdom, and the US territory of Puerto Rico. The theme was “Survival Strategies in a Cyber World,” and the conference committee and staff surprised us with tiki torches and even an immunity “armadillo” to kick the conference off before our amazing keynote speakers—Mark Weatherford, Vice President and Chief Security Strategist at vArmour, and Michael Coates, CISO at Twitter—shared their experiences. Attendees took to social media using the conference app and tweeted their thoughts in English and French!

Many of our seasoned and esteemed conference attendees commented favorably on the quality of the speakers and the program in comparison to other conferences they had attended over this past year. It should also be noted that we had a 30 percent rise in attendance with many first-time participants stating they will return and would choose the ISSA conference over others.

And we held our second “Party in the Sky” high above downtown Dallas in the iconic Reunion Tower, allowing for some amazing networking outside of the normal between-conference-track interactions. Thank you to vArmour for their generous support.

The CISO Advisory Council hosted four phenomenal CISO Executive Forums this year: “Innovation and Technology” in conjunction with RSA in San Francisco, “Infosec and Legal Collaboration” where cybersecurity leaders BYOL’d or Brought Their Own Legal Counsel; “Convergence: Securing the World around You” just before Black Hat in Las Vegas that included the first “After Forum Vegas Revitalizer” on The Linq’s High Roller, sponsored by Ensilo; and lastly because we were in Texas, “Big!”

Membership has been growing, and with that growth we have a responsibility to be fiscally responsible to ensure the greatest value and impact to you and the chapters. We must never lose sight of what our chapters and members feel differentiates us from other associations. This year our relevance as an association was reflected by the addition of new chapters in Bangladesh, Columbus, Georgia, and Texas Coastal Bend.

This last quarter, the Board—whom I must thank continually for their hard work, foresight, and passion to see ISSA succeed—has worked on solidifying the strategic plan and aligning budget initiatives to provide the path for 2017.

As a final note, I want to thank those of you who have assisted us throughout the year in generously obtaining/providing much needed sponsorships for our ISSA programs, webinars, chapter meetings, the International Conference, after-hours social events, and annual symposiums at regional levels. Thank you, thank you, thank you!

In closing 2016, I think of ISSA and the many friends it has brought me both professionally and personally. I must remember the seasonal movie, “It’s a Wonderful Life,” where James Stewart reminds us all that “No man is a failure who has friends.”

Moving forward from 2016 to 2017…

The Information Systems Security Association, Inc. (ISSA)* is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

With active participation from individuals and chapters all over the world, the ISSA is the largest international, not-for-profit association specifically for security professionals. Members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial, and government.

The ISSA International Board consists of some of the most influential people in the security industry. With an international communications network developed throughout the industry, the ISSA is focused on maintaining its position as the preeminent trusted global information security community.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.

---

* ISSA Journal – 3

\[ Image: Andrea Hoy, International President \]
Thank you and looking forward to a new year!

Joel M. Weise – Chairman, Editorial Advisory Board and ISSA Distinguished Fellow

And so ends another trip around the sun for the ISSA Journal. Is it me or does it seem like the years go by faster?

I would like to close this year out with a thank you to our membership; the many contributors and authors that provided articles, columns, editorials, and feedback; our International Board for their unwavering support; the Journal’s Editorial Advisory Board for their dedication and hard work in reviewing all of the Journal’s content; and Thom Barrie, our editor, for bringing it all together.

I look forward to another year of the Journal. There are many security, privacy, governance, and other issues we continue to face, and I am sure there will be many to come that we cannot even anticipate. My only ask of the membership is please contribute. This is your Journal. It is only as good as your participation.

We all should be looking for ways to stay engaged and help influence the world of information security.

Joel M. Weise

As the year winds down, across the globe many of our membership are looking forward to the holidays. We wish you all the warmth of family and friends.

We wish you a time of respite from the constant battles of work, travel, commute; We wish you a pause in the incessant keeping of the wolves at bay.

But as one put it: rust never sleeps. And neither do those bent on wreaking havoc, bent on thieving and destroying, bent on laying waste to our personal security, our financial security, even our national security.

So, do relax and enjoy some brief and fleeting moments of rest; revitalize yourselves as you continue to fight the fight, day in and day out, year in and year out.

Happy Holidays and a Prosperous New Year!

The information and articles in this magazine have not been subjected to any formal testing by Information Systems Security Association, Inc. The implementation, use and/or selection of software, hardware, or procedures presented within this publication and the results obtained from such selection or implementation, is the responsibility of the reader.

Articles and information will be presented as technically correct as possible, to the best knowledge of the author and editors. If the reader intends to make use of any of the information presented in this publication, please verify and test any and all procedures selected. Technical inaccuracies may arise from printing errors, new developments in the industry, and/or changes/enhancements to hardware or software components.

The opinions expressed by the authors who contribute to the ISSA Journal are their own and do not necessarily reflect the official policy of ISSA. Articles may be submitted by members of ISSA. The articles should be within the scope of information systems security, and should be a subject of interest to the members and based on the author’s experience. Please call or write for more information. Upon publication, all letters, stories, and articles become the property of ISSA and may be distributed to, and used by, all of its members.

ISSA is a not-for-profit, independent corporation and is not owned in whole or in part by any manufacturer of software or hardware. All corporate information security professionals are welcome to join ISSA. For information on joining ISSA and for membership rates, see www.issa.org.

All product names and visual representations published in this magazine are the trademarks/registered trademarks of their respective manufacturers.
Security Architecture…and the US Congress?

By Randy V. Sabett – ISSA Senior Member, Northern Virginia Chapter

Unless you follow Congress closely you may have missed their recent foray into security and Internet architecture. Some of things that have been discussed, however, actually reflect a viewpoint of one of my very smart friends who knows a lot about this. His approach (several years back) would be to completely re-architect the Internet from the ground up to make it secure. As he has stated, “humans built this thing; humans can tear it down and re-build it.”

So, as a result of high-profile attacks using IoT devices that have highlighted security vulnerabilities, some witnesses at a recent House hearing have called for direct government regulation. House members, however, struck a more cautionary note, calling for greater coordination and adoption of best practices. Coincidentally, immediately prior to the House hearing, NIST released best practices guidance for engineers developing IoT devices. Industry failure to adopt such practices will likely heighten regulators’ resolve to prescribe standards, especially if disruptive attacks continue.

IoT security hearing by the House Energy and Commerce Committee

The committee held a hearing on November 16 to examine the role of the IoT in recent cyber attacks that involved hacked consumer IoT devices. Bruce Schneier characterized the DDoS attacks as a fundamental market failure: “[Y]our security on the Internet depends on the security of millions of Internet-enabled devices, designed and sold by companies you’ve never heard of to consumers who don’t care about your security…[T]he market has prioritized features and costs over security.” Schneier encouraged the House committee to take action: “[T]he only solution is to regulate. The government could impose minimum security standards on IoT manufacturers, forcing them to make their devices secure even though their customers don’t care. [Doing so] would raise the cost of insecurity and give companies incentives to spend money making their devices secure.” Another witness stated that “there may be a role for the government to provide appropriate guidance.”

While expressing concern over the risks associated with connected devices, the members of the House committee were hesitant to endorse legislation as the solution, in part due to concerns over stifling innovation in this burgeoning industry. As stated by the Honorable Greg P. Walden, chairman of the Subcommittee on Communications and Technology: “How do we make ourselves more secure without sacrificing the benefits of innovation and technological advances? The knee-jerk reaction might be to regulate the Internet of Things, and while I am not taking that off the table, the question is whether we need a more holistic solution.”

NIST guidance for engineering trustworthy secure systems

The House committee recognized NIST as the author of a set of security recommendations to which industry and government can look for guidance. NIST Special Publication (SP) 800-160, Systems Security Engineering, represents a holistic approach to creating trustworthy and secure systems, encouraging the incorporation of engineering-based security design principles into the basic architecture and design of a system. The document states at the very beginning that it is meant to be used in a very flexible fashion, in order to meet the needs of a diverse set of stakeholders. Additionally, it is “not intended to provide a specific recipe for execution.” Thus, Chapter Two begins with an overview discussion of the discipline of systems security engineering, including descriptions of a system, the elements of a system, and the associated environment. It then describes a system from a security perspective and introduces concepts that allow the system to be appropriately deconstructed. Chapter Three discusses the processes that define a system life cycle that leads to security. These include agreement negotiations, organizational project-enabling processes, technical management processes, and detailed technical processes. Clearly this is not a document to be consumed by just one type of stakeholder.

So, I’m now going to kick back with an RFID-tagged beer that I pulled from my Internet-connected fridge (the same one I mentioned in my June column), turn on my smart TV, tell my copycat voice-recognition device to find out what’s on C-SPAN, and instead wind up watching the game on my tablet…though I can’t understand why all my favorite sites are so slow or completely down…

About the Author

Randy V. Sabett, J.D., CISSP, is Special Counsel at Cooley LLP (www.cooley.com), and a member of the Boards of Directors of ISSA NOVA and the Georgetown Cybersecurity Law Institute. He was a member of the Commission on Cybersecurity for the 44th Presidency, was named the ISSA Professional of the Year for 2013, and can be reached at rsabett@cooley.com.
very so often, I help out my dad with information technology and security projects. Those who have heard me speak know I sometimes pick on my dad when it comes to information technology around the house, but when it comes to the office, he’s the guy who gets called when stuff breaks. He’s on top of his game when it comes to the office, and he won’t take on any challenge without knowing he has a solid support structure (that isn’t me, by the way) to help him when stuff breaks.

Oh, and for reference, my dad has an undergrad in marketing and a general studies MBA (almost sounds like someone else you know, right?), so IT is not in his training, but somehow it ended up in his bailiwick.

There are times when we have debates about technology or business strategy, and I’ll bring up something around documentation. The default reaction is usually, “Son, that’s big company stuff. We’re a small company.” I sometimes have to remind him that I was once in a company of two—quite smaller than his—and we had some of these basic things documented almost twenty years ago. Small companies tend to be more nimble and reactive, which means that things like months of planning and documentation before investing in a product just doesn’t happen.

Companies in the financial services sector tend to be really good at creating documentation—almost to a fault. I’ve worked for a few over my career and have consulted with dozens. Documentation for the sake of documentation—that is, without a valuable purpose other than to check a box or make an auditor happy—is tough to justify spending time on to get it right. As a consultant, I’ve read through thousands of pages of documentation that resembled a “just get it done so we can clear an audit finding” or “fill out this form so we can pass through the gate.” It was as painful to review as it was to write.

When documentation is done right, it forces us to have tough conversations before products or projects get too far down the implementation path. Imagine for a second that Target had a robust remote access documentation process, including continual validation of those requirements, for the remote management of HVAC equipment. By robust, I mean complete and effective. Perhaps they did have forms and help-desk tickets, but the process was broken, leading to the well-publicized incident we often quote. Had their process been effective, would they even be top-of-mind when it comes to big retail breaches?

One of my favorite areas of security architecture is ensuring business alignment. It’s the documentation that shows all the business and security requirements that must be met before something can move from planning to design phase. These are the discussions that will allow the security team to ensure their basic requirements are met while simultaneously introducing additional requirements based on risk or customized to the project itself. If you do this correctly, all of the controls associated with those requirements can be included early enough to adjust the business model to account for unrealized risks.

Let’s bring this full circle. Documentation is not just a big company thing—it’s an every company thing. It’s critical to your security architecture process as it forces the tough security conversations early. It should be a valuable investment for current employees, auditors and the audit process, and future employees to understand the why of your operations. It’s not something that can be taken lightly, but done right, it’s worth the investment. You must allocate resources to maintain and review your documentation, and you must convince your superiors that it is worth the resource investment. Connect the dots for them and show them how current and future processes can benefit from useful documentation. Remember, good documentation is alive. It will change as your company changes. It should evolve to represent the current state of things. It is a reference for future employees who come in after you and a tome for current employees on your team or in a cross-functional role.

By the way, I’m just seeing if people read down this far (and padding my word count for Thom). Given that it’s the holiday season, tweet something about this article and tag me (@BrandenWilliams). I will enter all those who do so into a random drawing for a $25 Amazon gift card. Happy holidays!

About the Author
Branden R. Williams, DBA, CISSP, CISM, is a seasoned infosec and payments executive, ISSA Distinguished Fellow, and regularly assists top global firms with their information security and technology initiatives. Read his blog, buy his books, or reach him directly at www.brandenwilliams.com.
The Security Architect and the Security Engineer

By David Mashburn and Stephen Northcutt – ISSA member, Puget Sound Chaper

Two essential roles for successful security operations in mid-sized or larger organizations are security architect and security engineer. In the competitive job market for skilled IT security professionals, it might appear that the two roles and skill sets are nearly interchangeable. However, there are some significant differences in scope and perspective between the two roles. These differences should be considered carefully as part of the hiring process to make sure that the candidate most effectively meets the needs of the organization.

Security engineer is a common job title in many organizations. The skills required for this role usually target a specific domain of security expertise with an emphasis on relevant technologies or products. Examples of job requirements or desired skill sets taken from job postings for security engineers include phrases such as “skilled with PKI in a Windows Active Directory environment” and “experience with the maintenance and upgrading of firewalls, specifically Checkpoint and Palo Alto,” highlighting the focus on these important, but possibly narrowly focused and vendor-specific areas of expertise within the security operations of the organization.

If you compare those examples with the following skill requirements taken from a job description posted online for a senior security architect, the following attributes are expected from the candidate: “network security, network hardware configuration, network protocols, networking standards, supervision, conceptual skills, decision making, informing others, functional and technical skills, dependability, information security policies.” Note the descriptions are less vendor or product specific, reflecting the differing role of the security architect.

The security architect designs a defensible architecture that is aligned with the risk tolerance and risk profile of the organization. The architect views security through the lens of organizational need, where the priority is understanding what the organization values, where the organizational assets are located, and how adversaries are most likely to try access that data. The architect must be able to present ideas and designs to vastly different audiences, ranging from technical groups to managers including the C-suite. Because of these priorities, the security architect must not be locked into a product- or vendor-centric view of security and be open to alternatives.

A broad comparison of the two roles reveals the relationships between the two jobs. There are overlaps but also fundamentally different expectations of each role in the security organization.

Security architecture is strategic, while security engineering is often tactical by nature. The architect understands not only the desired end state of a project from the security perspective but also how that aligns with the overall organizational objectives; while a security engineer may primarily be interested in the most efficient and effective way to complete the project from the perspective of IT security.

The security architect designs solutions based on principles of defensible security architecture, leveraging defense-in-depth, data-centric security, and visibility, providing opportunities to break the exploit kill chain. The security engineer is more likely to implement the individual components of the solutions that comprise the entire security architecture, such as firewalls, IPS or IDS, anti-malware products, file integrity monitoring, and data loss prevention solutions. These are essential elements of the organizational security, but an engineer is more likely focused on the specific technology or vendor rather than how all of the elements are combined into the effective end state.

For aspiring security architects, there are a growing number of training and certification resources available. Certifications developed for IT security architects often include training offerings. The (ISC)² organization has created an ISSAP (Information Systems Security Architecture Professional) certification. The SABSA organization offers a set of integrated frameworks—models, methods, and processes—that can be utilized independently or as part of an integrated enterprise solution.

The TOGAF standard and certification program specifically addresses enterprise architecture. While not intended for the security practitioner, these resources could prove valuable in establishing the required business perspec...
A Downside to Red Teaming

By Mark Anderson – ISSA member, Australia Chapter

Red Teaming is seen by many as a very effective means to test the defense of a network. Basically, a team of white hats defend a network, and an opposing team of black hats undertake attacks. At the end, a penetration report is written and can be used to strengthen a network’s defenses. Sounds like a good idea doesn’t it, and in many instances where vulnerabilities have been discovered and closed off, this is a proactive win before an attacker can use an exploit. However, I want to list some hidden costs that can make the exercise pyrrhic if not managed very carefully.

I will refer to a couple aspects of two red teaming efforts my staff and I were involved in where we had our white hats on, supporting the defending team of large classified operational networks. When you are “pen” testing a live, operational network, it’s a bad idea to activate wide-scale responses (e.g., lockdown) if the penetration detected is part of the black hat activities for red teaming. So, one of the typical rules of engagement (ROE) includes the presence of a “trusted agent.” This agent in one of the exercises was an unknown member of the white hat team who had knowledge of an attack by the black hats and can then declare it if the defenders start a massive lock down.

But this seemingly good idea can backfire. Basically, in the first exercise, I observed all the white hats trying to figure out who the trusted agent was and were worried that if the black hats trusted this person then maybe they would do a “double agent” and apprise the black hats of current tactics. In trying to ferret out the identity, distrust was sown right across the team. Unsurprisingly, the team was no longer a team, and it was clear that its effectiveness in defending the network became seriously compromised. Any competent military commander can tell you that trust amongst your unit is vital, and it was mesmerizing when I visited the network site for upgrades during the exercise to see the team’s disintegration. It was amazing to me that we managed to detect any attacks at all; and we got burnt by the black hats.

Given knowledge of previous cultural issues, I was given strict orders to cooperate with the black hats in another exercise to test one of my technologies, as this was a “one team” exercise; there were criteria for the test to set the ROE and a marking scheme that the testing organization comprising the black hats would fill (that’s right, the attackers decided unilaterally on the score). Much better you would think? Firstly, a black hat turned up to look at our signature file citing “one team”; they stated later it was part of social engineering. They later supplied us with a signature of one of their attacks, but it was modified so it couldn’t work, and I wasn’t allowed to remodify it to work, given the ROE. In the end, we actually passed the test much to the black hats’ chagrin but later found out they then added other secret tests with hidden criteria. One of the responses was that the genuine adversary doesn’t follow a ROE, so why should they?

In the cases I alluded to, it destroyed friendships, entrenched a sour relationship between organizations, and caused significant loss of expertise. The testing organization senior management did write a memo to a three-star rank military committee where they noted that my team had significant advanced cyber capability and would be able to assist them in their cyber black hat mission. But the damage was done.

I am a proponent of red teeming, but it needs to be tightly managed beyond just the technical aspects, and the outcomes carefully considered. In the case of trusted agents, they should be known and independent of the white hats so the team don’t keep second guessing each other. In the second case, if the ROE is no ROE, this needs to be communicated to the white hats or factored into the deliberation. Don’t stake your white hats out on an ant hill and then castigate them for getting bite marks defending. ROEs need the same rigor and structure as those found in other military exercises. Otherwise, you might get a list of new vulnerabilities, but you are likely to pay a price much larger than you bargained.

You might think my homily is that if you get a choice, put on a black hat. They appear to have more fun, don’t have to follow any rules, choose when, where, how; and if they fail, it is in secret. But no. Stand proud white hats; it’s the toughest gig. You are openly accountable, have serious rules of engagement restrictions, and somehow the networks are still there. I have worked both sides of the street successfully in the service of the Western Alliance, but I tell you, the white hats are way underappreciated when compared to the seeming “glamour” of the Black Hats.

About the Author

Gray Hat is an ACM Distinguished Engineer and principal inventor for several patented devices and major systems that have entered operational service with the US Armed Forces, as well as other national governments for high-grade information security purposes. He can be contacted at msanderson@ieee.org.
Polluting the Privacy Debate

By Geordie Stewart – ISSA member, UK Chapter

The debate about the balance between privacy and surveillance is important. The problem is that some participants aren’t helping. They’re polluting. Rather than engaging constructively they have resorted to a number of underhanded techniques that distract and obscure.

Firstly, some have tried to deny the trade-off between surveillance and privacy. The FBI’s attempt to force Apple to weaken its security is a good example of this. A world where iPhone users are protected from cyber criminals and repressive regimes is also a world where the FBI won’t always be able to access everything it wants. The converse is also true. If intelligence and law enforcement agencies have backdoors to bypass encryption, then criminals can discover and exploit those same backdoors. We’ve tried backdoors before, and they don’t work. Remember the special TSA approved luggage locks that had special master keys for airport security? Well, instructions on how to make your own are available on the Internet. Those proposing magic backdoors that only the good guys can use don’t know what they’re talking about, or they’re deliberately trying to mislead us. Either way, denying the existence of a trade-off disqualifies you as a credible commentator.

Secondly, cynical attempts have been made to sway the public and avoid a proper debate. An example is using the relatives of terrorist attacks to turn the debate emotional rather than rational. We’re told that if we don’t give law enforcement and intelligence agencies the access they want, then they might not be able to prevent future attacks. Thinking rationally, the same argument can be made about search warrants and attorney-client privilege. These occasionally inconvenience law enforcement but exist to serve a greater good. We would have banned them if making the job of law enforcement easy was our single overriding priority. But it’s not. The irony is that we live in a golden age of surveillance. Law enforcement and surveillance agencies have never had it so good.

Thirdly, there’s an absurd notion that companies like Apple were considering themselves “above the law” by choosing to exercise their right to due process. Companies have a duty to use the courts to represent the interests of their customers and their shareholders. To pretend otherwise is to mislead the public.

Privacy vs surveillance is an important debate. Are companies allowed to design effective security for their systems?

Continued on page 44
How Enterprise Software Development Is Changing

This is a simple overview of where software development is these days. Although the article is not very exciting, it does cover a lot of ground. Furthermore, I agree with the observation that “software development is evolving into a continuous R&D practice.”

What IoT (and Security) Needs to Learn from the DeWalt Mitre Saw

Lance Spitzner, one of my old friends and a guru on security awareness among other things, says it best. “We need to take people into account and make security simple. We have to stop blaming others and look at ourselves. Until we do, the bad guys are going to continue to win.”

American Elections Will Be Hacked

As usual Bruce Schneier does a nice job on pointing out what many have said and thought; namely, the systems used in US elections are at risk. As he says, it’s only a matter of time before those systems are attacked. His suggestion to declare the US election system a critical national infrastructure does make a lot of sense, considering what could be at stake—specifically our democracy—if an election were actually hacked.

Barak Obama, Neural Nets, Self-Driving Cars, and the Future of the World
https://www.wired.com/2016/10/president-obama-mit-joit-ito-interview/

One of my favorite subjects is artificial intelligence. Happily, Obama appears to have a reasonable grasp of AI, and it was interesting to see the interview delve into the sociological and ethical questions that surround the subject. The soon-to-be-former US president is also pretty astute in recognizing the potential threat AI could pose to cybersecurity.

New Leak May Show If You Were Hacked by the NSA
http://arstechnica.co.uk/security/2016/10/new-leak-may-show-if-you-were-hacked-by-the-nsa/

More news from ShadowBrokers. Having spent my formative years at Sun Microsystems, I found it a bit alarming that many of the systems attacked were running Solaris. And for those that like to follow the details of NSA hacking tools, a list of possible tools was published that included DEWDROP, INCISION, JACKLADDER, ORANGUTAN, PATCHICILLIN, RETICULUM, SIDETRACK, and STOCSURGEON.

Why Did We Have to Wait a Year to Fix Our Cars?
https://www.eff.org/deeplinks/2016/10/why-did-we-have-wait-year-fix-our-cars

Section 1201 of the Digital Millennium Copyright Act (DMCA) is the anti-circumvention provision that prevents researchers and others from undertaking evaluation of copyright-protected code. This has lead to a suppression of research and what has been considered a restraint on free speech. With the help of the Electronic Frontier Foundation, rules have finally been adopted protecting such research.

What These CSOs Did on Their First Days
http://www.csoonline.com/article/3137477/it-careers/what-these-csos-did-on-their-first-days.html

It is important to remember that “a security program is an ongoing journey.” Before you can build systems, strategies, and protocols for your organization, you first need to have a good grasp of what you are defending. Although the article focuses on best practices for security executives who are taking on or transitioning to new roles or new companies, these tips could be applied at any time, particularly if it has been a while since your last inventory or risk assessment.

Titanpointe — The NSA’s Spy Hub in New York, Hidden in Plain Sight

An NSA collection site right in New York City? Who would have thought? Therefore, it should not come as a surprise that because the NSA is “presumably operating…to target foreigners…surveillance cannot be neatly limited to non-Americans.”

Facebook’s Fake News Crisis Deepens

Facebook has been under fire for allowing fake news that may have impacted the US presidential election. CEO Mark Zuckerberg has stated, “Of all the content on Facebook, more than 99% of what people see is authentic.” In all fairness to Facebook, users, especially those who take voting seriously, should always question the source of their news and not assume that just because it’s on Facebook or posted by a friend, it’s accurate. Facebook is a social media site, not a news organization.
DIGITAL DANGER ZONE
ISSA 2017 INTERNATIONAL CONFERENCE
October 10-11, 2017  San Diego, California

Sponsorship information: click here

#ISSAConf
ISSA CISO Virtual Mentoring Series

EARN FROM THE EXPERTS! If you're seeking a career in cybersecurity and are on the path to becoming a CISO, check out the latest webinar:

December 8: 1:00 pm - 2:00 pm EST. December Webinar.

Check the archives: 18 webinars from April 2015 through November 2016! Click HERE.

SPECIAL INTEREST GROUPS

Special Interest Group Webinars

Want to hear more from ISSA's Special Interest Groups? Join free here.

Healthcare SIG

December 15: 12:00 pm - 1:00 pm EST.

Auditing and Access to Electronic Health Records.

This timely topic is presented by the Healthcare Special Interest Group to explore the privacy and security needs for auditing access to electronic health records, risk issues, regulatory concerns, and technical deployment of solutions. Auditing of access to records is the primary means of identifying inappropriate access that may lead to a privacy breach or indicate a potential security incident.

Financial SIG

December 9: 1:00 pm - 3:00 pm EST.


Financial institutions have been a beacon for attackers on which to focus their attention for monetary gain, hacktivism, or disruption. The frequency and intensity of cyber attacks by financially motivated or nation-backed assailants has only heightened in the past years. This session will cover topics such as: How has 2016 shaped up? What major lessons have been learned this year? What major changes in attacks have we seen and do we anticipate what is next? What should your priorities be in 2017 to protect your company and customer financial data?

ISSA Chapter Events

December 10: Miami, FL, “SecureMiami.” For details and registration, click HERE.

April 9-11: Dubai, United Arab Emirates, “2nd Annual GCC ICS Cyber Security Forum Dubai 2017.” For details and registration, click HERE.

Get your events published in the ISSA Journal and E-News. You will build chapter activities, and your sponsors will appreciate the extra publicity. Send your events with the following information in this exact format: Date, Chapter Name, Time, Location, Title, Speaker, Sponsor, and a hyperlink to Details and Registration. Email to mdelacruz@issa.org.

For more ISSA and industry events, visit the ISSA Calendar.

ISSACAREER CENTER

Looking to Begin or Advance Your Career?

The ISSA Career Center offers a listing of current job openings in the infosec, assurance, privacy, and risk fields. Visit the Career Center to look for a new opportunity, post your resume, or post an opening. Among current 935 job listings you will find the following:

- Chief Information Security Officer (CISO) – Washington Health Benefit Exchange, Olympia, Washington
- Senior Risk and Compliance Analyst – Verifi, Los Angeles, California
- Network Security Engineer – Bon Secours Health System, Richmond, Virginia
- Lead Information Security Advisor – USAA, San Antonio, Texas
- Cybersecurity Analyst – LMI, Crystal City, Virginia

Visit our Career Center online for a full listing of job openings! Questions? Email Monique dela Cruz at mdelacruz@issa.org.

CSCL Pre-Professional Virtual Meet-Ups

So, you think you want to work in cybersecurity? Not sure which way to go? Not sure if you’re doing all you need to do to be successful? Check out Pre-Professional Virtual Meet-Ups to help guide you through the maze of cybersecurity.

December 6, 2016: 1:00 PM EDT – 2:30 PM EDT. What Should Your Toolbox Look Like?

ISSA Journal | December 2016
Announcing the New Howard A. Schmidt Scholarship

ISSAEF chairperson Sandra Lambert announced the naming of one of its scholarships in honor of Howard A. Schmidt, who retired from the infosec profession this year. She said, “Howard has been a leader of ISSA, a champion of learning, and a staunch supporter of the Foundation, as well as a friend and mentor to many private and public sector professionals. Therefore, it is fitting that this scholarship acknowledges his extensive contributions to education and to the profession as a whole.”

Howard, as many of you know, served on the ISSA International Board of Directors, including two terms as its president. During his career, he served two US presidents as Special Assistant to the President and Cyber Security Coordinator at the Executive Office of the President, White House. During his lengthy career, Howard has been CISO for Microsoft and EBay, an adjunct professor at Georgia Tech and instructor at Idaho State University, and a world-renowned evangelist for the profession. Congratulations, Howard!

Chapter donations

The Foundation is pleased to acknowledge the generous donations again this year from the LA Chapter ($2,500) and the SF Bay Area Chapter ($1,000). The LA Chapter, the first ISSA chapter to be established, has given donations to the Foundation totaling over $15,000 since 2007.

The SF Bay Area Chapter is the second chapter to provide sustained contributions for three years totaling over $4,000. Can your chapter also contribute? Donations may allow the Foundation to increase the amount of its grants to the scholarship recipients and/or the number of scholarships available each year.

Please contact ISSAEF Treasurer Richard Mosher for check-donation information or visit our website for online giving: www.ISSAEF.org.

Annual fund-raiser wrap-up

The ISSAEF annual fund-raiser, held in Dallas, TX, in conjunction with the annual ISSA conference, exceeded our expectations totaling almost $2,000, thanks to prize sponsors SANS, Venafi, TEN, ISSE Service, and ISE Talent. Our heartfelt thanks to all of those who made donations at the conference! See you next year in San Diego!
Enterprise Security Architecture: Key for Aligning Security Goals with Business Goals

By Seetharaman Jeganathan

In this article, the author shares his insights about why security architecture is critical for organizations and how it can be developed using a practical framework-based approach.

Abstract
Enterprise security architecture is an essential process that aims to integrate security as a part of business and technology initiatives handled by any organization. When the security goals and objectives are aligned with organizational business goals and objectives, any organization can make informed decisions about business ventures and protect organizational assets from ever-emerging security threats and risks. In this article, the author shares his insights about why security architecture is critical for organizations and how it can be developed using a practical framework-based approach.

Introduction
Enterprise security architecture (ESA) is a design process where the current state of enterprise security is analyzed, gaps are identified based on effective risk management processes, and the identified gaps are fulfilled by applying cost-effective security controls. It is a life-cycle process that enables any organization to protect itself from advanced security threats. Until recently, ESA was a major technology effort wherein the IT technical team owned the definition, implementation, and operation of security processes and controls. However, this model has created a vacuum with respect to business involvement and has failed to align the IT security functions with the organizational goals and objectives [11].

Security goals and objectives
Traditionally, information security functions have been providing confidentiality, integrity, availability and accountability services to information systems and infrastructure. These services are often referred to as primary goals for information security functions. The primary objective is to secure the overall IT system and business functions as well as support growth of the underlying business. ESA is a key enabling factor to ensure that the security goals and objectives are achieved as per the expectations of the senior management [11].

Why security architecture?
- Security architecture is a key in aligning security functions with the organization’s business functions
- Without a clearly defined architecture, security solutions cannot be balanced between over protection and under protection
- Security architecture functions enable accountability and help obtain support and commitment from senior management
Even though the proposed security architecture framework is a part of the enterprise architecture, it can also be rolled out separately as a new initiative for organizations that are not matured yet with respect to enterprise architecture. In the sections below, the author shares his practical experiences in implementing the proposed framework with several of his industry customers. The primary goal of the framework is to provide an organization-wide security architecture review process to ensure that security is an integral part of all business critical systems and processes [2][7].

Note: Since this article focuses on security architecture in general rather than information security architecture specifically, it will be appropriate to include corporate security, personnel security, and physical security aspects in this exercise.

People factor

This area focuses on several actors (people) who must operate together to effectively roll out the proposed framework. The enterprise security architecture group (ESAG) or enterprise security review board (ESRB) is a governance body that must be formed if not available already, as an initial step. The effectiveness of the framework will be dependent vis-a-vis the involvement and participation of the identified team members. They must fulfill their required roles and responsibilities as effectively as possible. Human resources being expensive assets for organizations, it is indispensable to get adequate support and commitment from the senior management to effectively utilize human resources to protect the interests of the stakeholders. Senior management support can be obtained by developing a charter of this proposed ESA group by identifying key roles and responsibilities of the group members. It is important to map the goals and objectives of this group to the overall organizational business goals and objectives and portray how this group will enable or support the growth of the underlying business functions [1].

Figure 2 depicts the proposed people factor top-down approach model to form the ESA group.

---

**Organizational Governance**
- Executives, Board of Directors, Stakeholders

**Enterprise Risk Management**
- Chief Risk Officer, Risk Management Group

**Enterprise IT / Security Governance**
- CIO, CSO, CISO, etc.

**Enterprise Architecture**
- Enterprise Architects

**Enterprise Security Architecture**
- Framework

**Figure 1 – Enterprise security architecture framework**

- Security architecture functions support IT functions during changes in the business processes
- Security architecture provides a snapshot of an organization’s security posture at any point of time [9]

**Enterprise security architecture framework**

Figure 1 shows the proposed enterprise security architecture framework discussed throughout this paper.

The framework begins with defining the security strategy, based on risk profile of the organization. An organization’s security requirements are derived mainly from security threats and risks faced by the organization [4]. These requirements are analyzed in the framework to clearly define a security strategy for the organization. The framework leverages three major factors; people, processes, and technology to implement the defined strategy across the organization. It is supported by other essential elements such as organizational governance, risk management, and IT governance bodies to effectively achieve total security of the organization. The author has referenced “The Business Model for Information Security” (BMIS) model and designed this article with exclusive focus on the security architecture function. The BMIS model was originally created by Dr. Laree Kiely and Terry Benzel at the USC Marshall School of Business Institute for Critical Information Infrastructure Protection. Later in 2008, ISA-CA adopted this model and has been promoting its concepts globally.

---

**Figure 2 – People factor (top-down approach) model**
The ESA group must consist of people representing all business units of the organization such as HR, finance, R&D, IT, products, manufacturing, etc. It is important to note that the focus of this group is not only securing the information systems but also securing the organization with a holistic approach. Business insights and guidance are essential to derive a holistic “organization wide” security approach. A top-down approach will provide necessary commitment and oversight from senior management; also, when there is a disagreement between business groups, senior management can liaise and resolve critical issues. It is extremely important for this group to cascade the architectural functions and decisions to the entire organization below and/or above them. The head of this group or its representatives must conduct regular “connect meetings” with the business units to provide security architecture overviews and guidance for all their technology and business initiatives [1].

One of the primary expectations and outcomes of this working group should be developing security policies and standards for all organizational functions wherein security is a key requirement. Security policies are directions by the senior management to the organization on what is allowed and what is not allowed from the security standpoint. Security standards are guidelines developed to substantiate/support each policy and set directions for business units on how to adhere to the required policies [8].

Note: The author is highly inspired by the series of books, Information Security Policies Made Simple, by Charles Cresson Wood and recommends them as reference materials to create relevant security policies by any organization. However, the samples provided in the book should be used as an inspiration and must not be adopted directly without careful review. The teams working on defining the policies must also take into consideration industry regulations, country-specific laws, and compliance requirements before defining the policies.

Process factor

This area focuses on how the security architecture review process should work in real time at any given organization. The need for an organization-wide risk management process is now more than ever because information systems and technology are widely used for business functions across the world. Information systems are subject to serious security threats. Threat agents exploit known and unknown vulnerabilities and cause damages to information systems. This will impact the confidentiality, integrity, availability, and accountability goals of security functions. Security breaches can cause permanent damage to organizations and can make them go out of business. Recent laws and compliance requirements make senior management personally accountable for any negligence in securing their customer’s personally identifiable information (PII), financial data, and personal health information (PHI) in the healthcare industry. Therefore, it is critical and of utmost importance that the senior management, mid-level, and lower-level employees of an organization understand their roles and responsibilities in protecting organization’s resources effectively from security risks [1].

Enterprise risk management is focused on managing risks faced by the organization. Security risks are one among several other risks faced, but security risks are more severe than others. Organizations generally follow widely known risk management frameworks (NIST, ISACA, etc.) or custom-made frameworks specific to the organization based on its culture, laws, and compliance requirements. The author discusses and illustrates this article based on the NIST (SP 800-39) risk management process, which suggests that risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level. This enables organizations to make informed decisions about their security activities based on the outcome of the risk management process already in place [10].

Figure 3 depicts the NIST risk management process and multi-tiered organization-wide risk management approach.

Note: As the scope of this paper is not to detail the NIST risk management process, readers are encouraged to read the NIST SP 800-39 document to understand the risk management framework.

An important discussion in SP 800-39 is that information security architecture is an integral part of an organization’s enterprise architecture. However, the author from his experience suggests that organizations that do not have a matured enterprise architecture yet must also roll out the security architecture processes in their IT program initiatives. The primary purpose of the security architecture review process is to ensure that specific security requirements are reviewed and cost-effective security solutions (management, operational, and technical) are suggested/developed for qualified risks that must be mitigated as per the risk management strategy. Organizational security requirements could also arise from other factors such as policies, standards, laws, and compliance regulations among others. These requirements must also flow
SecureWorld conferences provide more resources and facilitate more connections than any other cybersecurity event in North America. Our regional events are designed to equip and inspire those defending the digital frontier.

Join like-minded security professionals in your local community for high-quality, affordable training and education. Attend featured keynotes, panel discussions and breakout sessions, and learn from nationally-recognized experts. Network with fellow practitioners, thought leaders, associations and solution vendors.

**Don’t go it alone. Register for a SecureWorld conference near you.**

[www.secureworldexpo.com](http://www.secureworldexpo.com)

Announcing our 2017 conference schedule. In addition to our lineup of 14 regional events, we’re excited to introduce two new markets: Chicago and Twin Cities. Mark your calendars and make plans to attend!

**Spring:**
- Charlotte, NC – March 2
- Boston, MA – March 22-23
- Philadelphia, PA – April 5-6
- Portland, OR – April 20
- Kansas City, KS – May 3
- Houston, TX – May 18
- Atlanta, GA – May 31-June 1
- **Chicago, IL – June 7**

**Fall:**
- Cincinnati, OH - September 7
- Detroit, MI - September 13-14
- St. Louis, MO - September 20-21
- Denver, CO - October 4-5
- **Twin Cities, MN - October 12***
- Dallas, TX - October 18-19*
- Bay Area, CA - October 26*
- Seattle, WA - November 8-9

*Dates subject to change*
After security design recommendations are submitted to the implementation team, it is vital for security architects to provide required support throughout the implementation process and ensure that the proposed design recommendations are implemented as per the suggestions made in the design review. This process is referred to as the security implementation review. Post implementation of a security control, quality assurance testing must be done thoroughly to ensure whether the security control is mitigating the underlying risk(s) as per the requirements. If there is still any gap in risk mitigation, then the whole process must be repeated until the underlying risk is mitigated to the acceptable level. This way, the enterprise security review process could also be aligned with the organization’s SDLC process being followed in the information systems project implementation [8]. Figure 5 describes the proposed review process flow from the beginning to end.

**Enterprise security architecture review process**

An enterprise security architecture review process is primarily conducted to derive the most appropriate security solution(s) for the qualified requirements. Enterprise security architecture review board members should meet and review the security requirements and brainstorm possible cost-effective solutions that could be management, operational, technical, or combination of these controls to mitigate risks to an acceptable level. These steps are referred to as a security requirements review and security controls review. Once a cost-effective security control is identified, a security design review is conducted for functional and non-functional requirements, depending on the type of the security control(s) identified [8].

A high-level summary of the security design review process for each control type is briefed in table 1; this is not an extensive list of design review steps but suggestions to kick start the process [8].

<table>
<thead>
<tr>
<th>Security Control Types</th>
<th>Design Review</th>
</tr>
</thead>
</table>
| Management            | • Conduct current-state assessment and identify gaps  
                        | • Review the associated security policies and standards  
                        | • If required, create new security policies/standards or modify the existing policies to meet the security requirements  
                        | • Document and submit the recommendations |
| Operational           | • Conduct current-state assessment and identify gaps  
                        | • Suggest new or amendments to the operational model/process to meet the security requirements  
                        | • Document and submit the recommendations |
| Technical             | • Conduct current-state assessment and identify gaps  
                        | • Suggest new controls or changes to the existing technical control to meet the security requirements  
                        | • Conduct cost-benefit analysis, security return of investment (SROI) analysis to prove the cost effectiveness of the solutions  
                        | • Provide functional design inputs  
                        | • Provide non-functional design inputs  
                        | • Document and submit the recommendations |

**Technology factor**

This area focuses on the technology aspects of the information systems layer supporting the business functions. The

---

**Figure 4** – Enterprise security architecture process drivers

**Figure 5** – Enterprise security architecture process flow
process begins with creating a blueprint(s) of the current state (“as-is”) of the information systems layer (logical and technical) in the primary and secondary data center(s) of the organization. Figure 6 provides a high-level logical view of the primary data center.

After a high-level blueprint is created, the team has to move on to creating more focused blueprints about the following areas but not limited to:

1. Detailed blueprints about the network segments such as the DMZ layer, internal network layers (intranet), and external networks such as partner networks, Internet, VPN networks, etc.
2. Detailed blueprints about the infrastructure layer such as servers, databases, mail servers, file servers, etc.
3. Request the individual application teams (mission critical and all others) to derive their application-specific architecture diagrams if not already available [4]

Figure 7 depicts a high-level logical and physical deployment sample architecture blueprint of an e-commerce application in a financial services company.

After completion of above mentioned exercise, the architecture team would have relevant information to review and create a detailed inventory of the current state of information security controls in place at the physical, network, infrastructure, and application levels [3].

There are several possible approaches in assessing the current-state security controls of physical, network, infrastructure, and application layer components; one such approach is creating a 3X3 matrix of current security controls classified into types such as preventive, detective, and corrective controls (table 2) [8].

After completing the above exercise at all the levels, the current security posture (“as-is”) of the organization would be created successfully. The next critical steps are:

a) Conduct a gap analysis of current-state security
b) Conduct a risk analysis of critical information systems

An effective risk management process is a key here to find out the gaps in the current state and the residual risk on the business critical information systems. The architecture team must review the gap analysis and risk analysis reports to derive the requirements for the desired (“to-be”) state architecture to adequately protect the identified assets. The requirements must be presented to the senior management, governance board, etc., for approval, funding, and adequate support for implementation. It is extremely important to map the goals of the security architecture with business goals and process begins with creating a blueprint(s) of the current state (“as-is”) of the information systems layer (logical and technical) in the primary and secondary data center(s) of the organization. Figure 6 provides a high-level logical view of the primary data center.

After a high-level blueprint is created, the team has to move on to creating more focused blueprints about the following areas but not limited to:

1. Detailed blueprints about the network segments such as the DMZ layer, internal network layers (intranet), and external networks such as partner networks, Internet, VPN networks, etc.
2. Detailed blueprints about the infrastructure layer such as servers, databases, mail servers, file servers, etc.
3. Request the individual application teams (mission critical and all others) to derive their application-specific architecture diagrams if not already available [4]

Figure 7 depicts a high-level logical and physical deployment sample architecture blueprint of an e-commerce application in a financial services company.

After completion of above mentioned exercise, the architecture team would have relevant information to review and create a detailed inventory of the current state of information security controls in place at the physical, network, infrastructure, and application levels [3].

There are several possible approaches in assessing the current-state security controls of physical, network, infrastructure, and application layer components; one such approach is creating a 3X3 matrix of current security controls classified into types such as preventive, detective, and corrective controls (table 2) [8].

After completing the above exercise at all the levels, the current security posture (“as-is”) of the organization would be created successfully. The next critical steps are:

a) Conduct a gap analysis of current-state security
b) Conduct a risk analysis of critical information systems

An effective risk management process is a key here to find out the gaps in the current state and the residual risk on the business critical information systems. The architecture team must review the gap analysis and risk analysis reports to derive the requirements for the desired (“to-be”) state architecture to adequately protect the identified assets. The requirements must be presented to the senior management, governance board, etc., for approval, funding, and adequate support for implementation. It is extremely important to map the goals of the security architecture with business goals and

<table>
<thead>
<tr>
<th>Preventive</th>
<th>Detective</th>
<th>Corrective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative</td>
<td>• Acceptable usage policy</td>
<td>• Change management policy</td>
</tr>
<tr>
<td>Technical</td>
<td>• Data encryption</td>
<td>• Vulnerability scanning</td>
</tr>
<tr>
<td></td>
<td>• SSL/TLS transport encryption</td>
<td>• Secure coding/review</td>
</tr>
<tr>
<td></td>
<td>• Secure configuration</td>
<td>• Access control</td>
</tr>
<tr>
<td>Physical</td>
<td>• Application-specific control(s) if any</td>
<td>• Application-specific control(s) if any</td>
</tr>
</tbody>
</table>

Table 2 –Sample controls review matrix (e-commerce application)
objectives to garner the support from the management and board of directors [5].

As the technology environment is ever changing due to several factors such as changes in the business processes, environment, technology adoption, automation, etc., security architecture must always be a live and vigilant group in any organization in order to adopt the changes and support the business to function without disruptions. It is essential to remember that IT and security functions must be business enablers rather than creating road blocks for business functions.

Note: Organizations that are matured in information security processes have adopted one or more industry frameworks listed below to implement the minimum required security controls and desired security architecture for effective information security:
- ISO 27001:2013 Information Security Standard
- NIST Cybersecurity Framework
- ISACA COBIT 5 Information Security
- SANS Critical Security Controls, etc. [5]

Incorporating security architecture in enterprise architecture

MIT Sloan School’s Center for Information Systems Research (CISR) defines enterprise architecture as “the organizing logic for business process and IT infrastructure reflecting the integration and standardization requirements of the firm’s operating model. The enterprise architecture provides a long-term view of a company’s processes, systems, and technologies so that individual projects can build capabilities—not just fulfill the immediate needs” [12].

In simple terms, enterprise architecture provides a logical view of the enterprise business layer (functions and processes), the IT infrastructure layer, the data layer, and the applications layer. As enterprise architecture is not the focus of this article, the author would emphasize that security architecture could be part of the enterprise architecture and provide adequate security for all the architecture functions. Figure 8 depicts a security-enabled enterprise architecture view of an organization [13].

Security architecture frameworks

There are several industry frameworks that provide architectural approaches for meeting security requirements. Some of them to be noted are:
- SABSA comprehensive framework for enterprise security architecture and management
- Zachman framework of IBM
- The Open Group architecture framework
- The Open Security architecture group framework
- UK Ministry of Defense architecture framework

- US Department of Defense architectural framework, and much more

Organizations can leverage these frameworks and customize them to meet security architecture requirements. As the scope of this paper is not to review these frameworks in detail, the author notes that organizations must choose an architecture framework that is flexible enough to support business growth and adopt for changes in the business environment and processes [5].

Conclusion

The enterprise security architecture process streamlines security functions of an organization to achieve effective total security. In this article, the author proposed an enterprise security architecture framework and detailed the pillars (people, process, and technology) of the framework. Whether adopting this framework or an industry-recognized framework is a decision to be made by the organization, depending on the culture, business environment, and industry compliance requirements. Any framework will be effective only when adequate support is given. In order to obtain desired outcomes of an architecture framework, it must be understood and supported by the senior management. In today’s economy-centric business environments, a security architecture framework must be increasingly business oriented rather than a technology-centric framework to obtain expected returns on security investments.

References

About the Author

Seetharaman Jeganathan, CISSP, has more than 14 years of experience in IT technology security consulting and program management. He mainly focuses on information systems risk assessments, identity and access management (IAM) solution strategy definition, architecture definition, and design and implementation of IAM security solutions. He also specializes in cloud-based applications security consulting and implementation of IAM solutions in cloud. He may be reached at seetharaman.jeganathan@gmail.com.
Secure Network Design: Micro Segmentation

By Brandon Peterson – ISSA member, Nevada

This article discusses how a secure network design that focuses on micro segmentation can slow the rate at which an attacker moves through a network and provide more opportunities for detecting that movement.

Abstract

Organizations that implement a secure network design will find that the added cost and complexity of micro segmentation is more than offset by a reduction in the number and severity of incidents. In fact, the effort extended in learning, classifying, and segmenting the network strengthens all of the organization’s controls and accelerates incident response. This article discusses how a secure network design that focuses on micro segmentation can slow the rate at which an attacker moves through a network and provide more opportunities for detecting that movement.

Introduction

Secure network design or architecture begins with the understanding that most business processes require network communication to traverse untrusted networks. Certainly the Internet qualifies, but even the business’s own internal networks may be unsafe. Insider threats, hackers in the network, and unintended data leaks are constant threats an organization must anticipate and prepare for. As the world becomes more connected, business risk will increase. For example, the presence of “a huge online population means that even attacks with very low success rates will have significant pools of victims” [11]. The Ponemon Institute estimates the likelihood that an organization will have a data breach involving at least 10,000 records at approximately 26 percent [24]. In addition, the costs of cybercrime to business are also high. Determining the exact cost of cybercrime is tricky, considering the numerous factors involved (e.g., lost productivity, costly security controls, and the lack of information). McAfee and the Center for Strategic & International Studies, in 2014, estimated the annual cost at over $400 billion globally [17].

With the cost, surface area, and volume of attacks so high, it is more critical than ever to protect the organization’s interests with a secure network design focused on micro segmentation. Micro segmentation, also known as protected enclaves, protects the network by breaking it into smaller chunks. This is accomplished through the use of network firewalls, host firewalls, VLANs, VPNs, and network admissions or access control [20]. These techniques add complexity and cost to managing a network. Fortunately, new technology is emerging that can ease the burden and cost of these implementations.

Determining enclave boundaries

With the advantage of time, hackers can float throughout a network for months looking for additional access or data to steal. By micro segmenting the network, an organization creates boundaries that the attacker has to cross before gaining access to another subset of data. These boundaries are created in a way that only allows the minimum necessary services through. These services are then closely monitored to detect any unauthorized use.

Determining what boundaries or VLANs to create and what resources should be placed in those boundaries is one of the more challenging aspects of designing a secure network. In general, the need for an enclave arises “when the confidentiality, integrity, or availability of a set of resources differs from those of the general computational environment” [25]. A value threshold should also play a role in selecting enclave boundaries. For example, an e-commerce website may want to separate the webserver handling its store operations from a webserver handling its jobs and recruiting page. Both sites may require 24/7 availability and contain sensitive information; however, the e-commerce site represents a far greater impact on business operations if its availability is negatively
impacted. ERP applications are another example of high-value applications that warrant their own segment. The organization’s work flow may dictate that additional services be segmented. Email, file shares, and custom applications may all justify segmentation.

A good measure of business impact for a system can often be found in an organization’s disaster recovery or business continuity plans. These plans often provide details on the priority of systems or data. Typically, the lower the Recovery Point Objective (maximum allowable time period that data might be lost due to an incident) and Recovery Time Objective (time within which the business process must be restored after an incident) times are, the more critical the systems are to the business. Figure 1 shows a sample recovery objectives table from a disaster recovery plan.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Recovery Point Objective (RPO)</th>
<th>Recovery Time Objective (RTO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>2 hours</td>
<td>24 hours</td>
</tr>
<tr>
<td>E-Commerce Website</td>
<td>0</td>
<td>&lt;10 seconds</td>
</tr>
<tr>
<td>Intranet</td>
<td>7 days</td>
<td>14 days</td>
</tr>
<tr>
<td>Payroll</td>
<td>8 hours</td>
<td>3 days</td>
</tr>
</tbody>
</table>

**Figure 1 – Disaster recovery objectives table**

The table makes it clear that these systems all have different value to the organization. At a minimum, a segment for the e-commerce website should be considered.

Another key segmentation boundary is compliance. It is far easier to manage compliance if the number of systems under scope can be reduced through segmentation. While segmentation is not strictly required for PCI compliance, “Without adequate network segmentation (sometimes called a “flat network”) the entire network is in scope of the PCI DSS assessment” [23]. The PCI requirements document has a flowchart for determining if card holder data is segmented and if scope can be reduced. Clearly, it benefits the organization to segment when compliance is involved.

Physical security can play a role in determining if another segment is needed. For example, imagine an office building with 100 identical workers spread across two floors. The bottom floor is in an area with access to the public. The top floor only allows employee access. The information on all 100 systems has the same value and security needs. However, the additional risk presented by the physical access to the systems on the bottom floor means that additional controls are necessary. Network segmentation should be one of the controls considered.

Wireless should be considered another segmentation qualifier. Due to the fact that it is nearly impossible to physically secure a wireless network, it should be segmented on a private VLAN. On a private VLAN, attached devices are not able to directly communicate with each other. This separation helps prevent compromised systems and rogue users from spreading to other systems on the wireless network.

Figure 2 shows the enclave boundaries flowchart that may help network administrators decide when to create a segment.

**Network access control**

Once an enclave is created, it is important to ensure that only approved devices are granted network access. Network Access Control (NAC) refers to technology that restricts network access to devices that meet certain policy controls (e.g., antivirus software, patch level, host firewall), provide sufficient user credentials, or match a certain physical (MAC) address.

802.1x Port-Based Network Access Control allows clients to authenticate using credentials such as passwords or certificates to gain network access. The client sends an authentication request to the switch using the Extensible Authentication Protocol over LAN (EAPOL). EAPOL allows an EAP request to be encapsulated and transmitted over Ethernet. The switch acts as a proxy and takes the encapsulated EAP request and converts it into a RADIUS request, sending it on to the authentication server. The responses returning from the server are then sent back to the client via the switch.
authentication server are then converted back into EAPOL for the client. These transmissions happen until the client is approved or rejected by the authentication server. Once approved, the port on the switch is activated and the client is assigned a VLAN ID [7]. Unapproved devices may be segmented into a guest VLAN or denied network access.

For devices such as printers, scanners, copiers, etc., that do not have the capability to do 802.1x authentication, there are a couple of options that can be used, depending on the scale of the network. One option is to simply use port security to lock down the port on the switch to a specific MAC address. This method becomes cumbersome if used on more than a handful of devices. Another option is to use MAC Authentication Bypass or MAB. According to Cisco documentation, “Standalone MAC Authentication Bypass (MAB) is an authentication method that grants network access to specific MAC addresses regardless of 802.1x capability or credentials. As a result, devices such as cash registers, fax machines, and printers can be readily authenticated, and network features that are based on authorization policies can be made available” [6]. MAB can be configured as a fail-over method of authentication should 802.1x fail. In MAB, the device’s MAC address is used as the credentials to authenticate with.

After the device has been authenticated and assigned to a VLAN, the DHCP server can be set up to only assign IP addresses for known MACs. While a static IP address assignment easily bypasses this control, it does help prevent users from sharing credentials. Figure 3 shows the first two phases of a device as it connects to the network in a NAC environment with DHCP MAC filtering.

Many vendors offer proprietary network access control solutions that extend the IEEE 802.1x protocol further. They offer capabilities like dynamic VLAN assignment, antivirus, and patch scanning. Dynamic VLAN assignment allows users to take a laptop, for instance, to another part of the network and automatically be assigned to their correct VLAN. Patch and antivirus scanning ensures that machines are in compliance with corporate security policies. Machines failing the compliance check are connected to a quarantined VLAN until the machine is brought back into compliance. Most solutions also offer the ability to send unknown machines into a guest VLAN. This allows guests to gain limited network access without having to tie up limited IT resources. Unfortunately, network access control on its own may not be enough to prevent rogue machines or individuals from gaining network access.Spoofing MAC addresses is trivial. User credentials can easily be stolen or purchased on the black market. At DefCon 19, Alva Duckwall IV demonstrated defeating 802.1x using a Linux machine as a bridge [9]. Previously at BlackHat 2007, Ofir Arkin gave a presentation on bypassing NAC. His methods included purposely getting a machine quarantined in order to infect other machines in the quarantined area. The legitimate machines would likely be brought back into the network with his malware intact [2].

Rogue device detection

Not all organizations have the resources to properly implement network access control to automatically restrict devices connecting to the network. Frequently, even networks that use NAC have enough exceptions that they still need a tool to help notify them of devices that connect to the network.

Arpwatch is a free open source tool developed by the Network Research Group at Lawrence Berkeley National Laboratory. It monitors the network for MAC and IP address pairs. Arpwatch sends an email alert when it notices a new pair, a pair that has not been used for six months or longer, or a MAC or IP address pair in the Arpwatch database detected using a different MAC or IP. In figure 4, an email from Arpwatch alerts administrators to an IP address associated with two different MAC addresses within a short period of time.

In the case of the rogue device such as a rogue wireless access point attaching to the network, Arpwatch would detect either a new pair or a new MAC associated with an existing IP. Arpwatch would send an email alert the network or security ad-
DNS is a perfect example of a nearly ubiquitous service that can be used as a covert channel. Using an encoding scheme such as base32, a covert channel can be used to transmit binary information through DNS. The encoded data is sent in the form of a DNS query. The leftmost or host side of the query contains the embedded data. The authoritative name server that is controlled by the hacker then returns data embedded within a DNS txt record. Using this technique, researchers were able to achieve data transfer speeds as high as 4.7Mbps using tools such as DNS2TCP [1].

In practice, understanding that most segments do not require recursion for txt records or queries on longer hostnames can help you configure your name servers securely or catch such requests as they traverse the network. With a policy in place that details acceptable business use and an understanding of the underlying technology, a network security administrator can begin to apply controls to monitor and detect deviations.

Network monitoring architecture

To facilitate network-level monitoring, organizations need to ensure they budget for and include monitoring hardware and software as they build out the network. The goal is to duplicate enough of the traffic at critical locations to catch anomalies. On a small scale, this can be accomplished simply by mirroring ports on the switch or inserting a network tap. Most organizations will eventually overload their monitoring and security scanners with critical feeds they wish to monitor. Figure 6 depicts the issue of aggregating too many feeds into a scanner. It is readily apparent in this example that even with a quad 10Gb Ethernet card there is potential to overload the server. Investing in additional hardware at the monitoring server quickly becomes cost prohibitive.

Several network vendors have come up with a solution to this problem. Gigamon, one of the leading makers of network visibility, sells products to create what they call Visibility Fabric [10]. Rather than send all the tap feeds and mirror ports directly to the server, they are sent to a device that first processes the network traffic. These devices can de-duplicate traffic, strip headers or payload off the packets, decrypt encrypted traffic, generate Netflows, and more prior to sending the traffic on to the monitoring server. Another useful feature they

Figure 4 – ArpWatch email alert

Figure 5 – Compromised network segment

Figure 6 – Aggregate network monitoring feeds

Secure Network Design: Micro Segmentation | Brandon Peterson
Segmentation forces the traffic to cross key junctions where the traffic can be captured and analyzed.

Vulnerability scanning

It is important for an organization to validate its security controls such as patching, secure baseline configurations, and proper user access rights. Vulnerability scanners are able to scan a variety of different devices on the network for insecure software or configurations. They can also aid in detection of rogue devices on the network.

Micro segmentation allows security analysts to derive more value out of a vulnerability scanner by tailoring scans to match the micro environment. Figure 9 shows a page from a Nessus report targeted to a PCI-scoped segment.

The machine in the scan did not meet compliance requirements. The Nessus report details why the device failed and contains information on how to fix the issues.

In some cases, organizations find it useful to create custom scans for their unique environment. Many organizations have developed and deployed custom applications. For instance, a share is the ability to aggregate multiple feeds into one. This allows the server to process many times the network traffic it would otherwise be able to handle. As network speeds get faster and the number of connections grows, the need for network-level aggregators and packet-manipulating devices will increase. Keeping the impact of these devices in mind, “Forecasts from analyst firms such as Gartner, Frost & Sullivan, and others paint a clear picture of the significant growth we can expect in the network monitoring space over the next few years” [21].

Detection

Once the network traffic is aggregated it can be sent to a number of different monitoring and security products for inspection. For example, Tenable’s Passive Vulnerability Scanner can detect new hosts on the network, identify vulnerabilities in both client and server side traffic, and detect other anomalies. Figure 7 shows the top 20 anomalous events detected by Tenable’s PVS on a sample network.

Drilling down into the “login-failure” event shows the details of traffic that triggered the event. As seen in figure 8, Tenable’s PVS detected several failed login attempts to a database between two segments on the network.

Without segmentation, this traffic would have remained “hidden” on the local subnet. Segmentation forces the traffic to cross key junctions where the traffic can be captured and analyzed.

Vulnerability scanning

It is important for an organization to validate its security controls such as patching, secure baseline configurations, and proper user access rights. Vulnerability scanners are able to scan a variety of different devices on the network for insecure software or configurations. They can also aid in detection of rogue devices on the network.

Micro segmentation allows security analysts to derive more value out of a vulnerability scanner by tailoring scans to match the micro environment. Figure 9 shows a page from a Nessus report targeted to a PCI-scoped segment.

The machine in the scan did not meet compliance requirements. The Nessus report details why the device failed and contains information on how to fix the issues.

In some cases, organizations find it useful to create custom scans for their unique environment. Many organizations have developed and deployed custom applications. For instance, a
it’s reasonable to consider moving the PCI systems into their own dedicated environment and limiting their interaction with non-PCI technology. This helps reduce the number of critical systems to be reshaped into compliance and will enhance security by placing them in a controlled and monitored environment” [19].

In addition to limiting the scope of compliance, an effective micro segmentation implementation will satisfy many compliance requirements without additional work. The environment will already be well documented. Also, several layers of security controls including monitoring and vulnerability scanning will be in place.

**Incident response**

Micro segmenting a network provides advantages when dealing with incidents. Once detection has occurred, the subsequent phases of incident response are also made simpler by micro segmentation.

**Containment**

Containing a threat or attacker before doing more damage or spreading on the network is critical. An entire segment can be quickly isolated to contain a threat, as in figure 10.

Since the segment sizes are relatively small, there are fewer business units affected by the interruption of service. If containment is limited to just a few machines within a micro segment, the network architecture lends itself to rapid isolation. Most micro segmentation is accomplished through the use of 802.1Q tagging. An “Isolation VLAN” can be created throughout the network beforehand that only incident responders can access. This allows network administrators to easily and remotely move a compromised machine to an isolated VLAN.

**Eradication**

Once isolated, incident responders can safely begin to eliminate the threat. This may be as simple as running malware

custom scan could be written to track the version of a custom application. If a particular version has issues, support staff would know which machines had the trouble versions.

**Data loss prevention**

Data loss prevention (DLP) tools help organizations “discover, classify, and monitor sensitive information, wherever it’s stored or used, on and off of corporate networks” [4]. This is technically accomplished in a variety of different ways, depending on the solution. Email, web, endpoints, databases, and even social networks can be scanned for data classified as sensitive. Organizations need to understand that “installing DLP on everything, everywhere can be very expensive and difficult to maintain. Think about the key applications and teams within your business that really need DLP technology due to the sensitivity of the data they have access to” [8]. Micro segmentation aids DLP implementations by shrinking the surface area to monitor and assisting in the classification of data. As an example, in a micro segmented network, it may not be necessary to scan a custodial segment for HIPAA or PCI data. This helps target DLP where it is most useful and should keep licensing and implementation costs lower.

**Compliance**

The regulatory and compliance requirements organizations operate in continue to change as the threat landscape evolves. PCI DSS, HIPAA, and SOX have all undergone changes in the last few years and have added additional requirements. Micro segmenting typically allows organizations to limit the scope of compliance requirements. This becomes necessary in most organizations because compliance is expensive to enact across an entire organization. To combat such costs,
removal software or as involved as a complete wipe and restore from backup. Fewer systems in the segment means that the compromised segment or systems can be cleaned more rapidly.

**Recovery**
The affected business unit, once satisfied the threat has been eliminated, may choose to return the system to production. Once again, the micro segmentation network architecture means fewer systems are involved. The affected business unit can be brought back into production faster, and it is far easier to monitor for post recovery attacks.

**Follow-up**
With the system back in production, the security responders, administrators, and business personnel should have a lesson learned meeting to discuss what process improvements or system changes should be made. A micro segmented network, built around well-defined business processes, provides a clear and well-documented foundation for this discussion. Every port, protocol, and application allowed in and out of the segment should be analyzed to determine if it is necessary. Moreover, as part of the analysis, the team should determine if additional controls or monitoring is necessary.

**Emerging trends**
The architecture of the data center rather than the network may drive the latest wave of micro segmentation. As data centers have evolved they have become more and more virtualized. In what has become known as the Software Defined Data Center, a logical layer of networking, compute, storage, and applications is deployed over physical infrastructure—both on premise and in the cloud. This allows businesses to rapidly provision and reallocate resources in a secure manner.

Emerging products such as VMware NSX or vArmour focus on simplifying the process of micro segmenting. Using policies or templates, these products can spin up a virtual machine, add it to a virtual switch on the correct segment, and apply firewall rules. As the case with VMware NSX, “every virtualized workload can be protected with a full stateful firewall engine at a very granular level. Security can be based on constructs such as MAC, IP, ports, vCenter objects and tags, active directory groups, etc.” [27]. This allows each and every virtual machine to be segmented: the true definition of micro segmentation.

**Conclusion**
Organizations and their networks are constantly attacked from multiple angles and today’s defenders must use a systematic and rigorous approach to protect them. A key element to that approach is micro segmentation. Micro segmentation segregates the network in a manner that provides rapid incident response, simplified compliance, and greater visibility through continuous monitoring.

Micro segmentation begins with an understanding of the business process and how that translates into network behavior. Without that understanding, security controls will be frustrating for the users and ineffective at preventing or detecting attacks. Devices on the network are separated by their business function and security needs. Normal communication between segments is documented and any deviation from the norm should be examined.

If an incident occurs, the module nature of a segmented network simplifies the incident handling process. The segment can be rapidly isolated and the limited communication channels make determining how far the attack has spread much easier. The network and security teams will have an accurate understanding of the business units and processes disrupted by the incident. The relationships formed through the process of understanding the necessary and normal business traffic will be invaluable during an incident. It will bring an understanding of priority and aid in communication with the business leaders.

Micro segmentation provides value to the business in many ways beyond detecting and preventing attacks. It greatly simplifies compliance and reduces associated costs. Compliance scope can be limited and the controls are well understood and documented. Other often arduous tasks such as business continuity and disaster recovery planning benefit from the efforts of micro segmentation and vice versa. Micro segmentation affords IT an excellent opportunity to demonstrate their worth to organization. The result is a more secure, robust, and capable organization.

**References**


About the Author
Brandon Peterson leads the Desert Research Institute’s Cyber Security and Incident Response team. Brandon has spent the last 17 years managing IT infrastructure and security for banking, media, higher education, and research. Brandon is also a community instructor with SANS. He may be reached at brandon.peterson@dri.edu.
Secure ERP Implementation

By Alexander Polyakov

Enterprise resource planning (ERP) and other enterprise business applications play a significant role in a company’s architecture and business processes. This article provides four steps to significantly increase ERP security by tuning its architecture. In addition, the author includes a high-level description of ERP security in general, its risks, typical vulnerabilities, and remediation steps.

What is ERP?

Enterprise Resource Planning (ERP) is the system responsible for managing all of a company’s resources. Many years ago, people used to store all the information about employees, materials, products, clients, etc., on paper; then Excel spreadsheets were used. But when the number of employees involved in business processes increased and the need for automation grew significantly, ERP systems were developed. Those systems now store and process all the “crown jewels” of a company. However, they also pose a huge risk if not secured properly.

A typical cyber kill chain consists of multiple steps such as initial reconnaissance, initial compromise, establishing a foothold, escalating privileges, gaining access to the mission-critical system, internal recon, and, finally, stealing the data or changing some critical configuration parameters (see figure 1).

There are plenty of security solutions (firewalls, WAFs, endpoint protection systems, etc.) intended to detect or even prevent initial intrusions. They are mostly focused on the first stages of an attack, but some of them can aid as well when an attacker is already inside the system.

Every year we witness more and more data breaches while most victim companies have common security mechanisms implemented. It seems to suggest that getting access to a corporate network is not a difficult task for skilled attackers. In my opinion, this situation will not change in the near future: if something is valuable, someone will try to steal it.

So, the most reasonable strategy is to focus security efforts on the most critical assets, which is a completely different task compared to boundary protection.

Imagine our network is a castle. The security measures are implemented: a moat swarming with crocodiles, castle ramparts, and towers with guards. It seems secure. However, if a mole digs a tunnel under the wall and gets inside, he will gain access to the treasure within because there is almost no security equipment inside the perimeter. It is obvious that we should focus at least on the following areas of cybersecurity:

- Network security
- Web application security
- Endpoint security
- Identity and access governance
- Incident detection and response
- Business application security

The last topic—business application security—deserves greater attention as it is responsible for business-critical pro-
cesses. The truth is that all our networks, web applications, endpoints, and identity systems exist mostly to provide access to those business applications such as ERP systems. Without them, all IT infrastructure features turn out to be almost useless.

**Why should we care?**

What can happen if somebody breaks into the most critical assets such as enterprise resource planning system, supply chain management, and product life cycle management?

- **Espionage** (breach of confidentiality) includes theft of financial information, corporate trade secrets, intellectual property, and customer data

- **Sabotage** (violation of availability) can be in form of intentional product quality deterioration, production spoilage, equipment corruption, manipulation of supply chain, compliance violations, and tampering with financial reports

- **Fraud** (violation of integrity) There are different kinds of fraud that can relate to raw materials, finished goods, financials, etc.

- **Terrorism** (such as explosion) now is also among the cybersecurity risks.

All this can happen because of a single vulnerability in an ERP system.

There are different ERP systems available on the market. The most common systems are SAP ECC, Oracle EBS, Oracle JDE, Microsoft Dynamics, and Infor. Despite the fact they differ in details, they are quite similar in general and represent a three-tier architecture consisting of fat client or web browser, application server or multiple application servers with a load balancer, and a database as a backend.

What’s more important, they vary from traditional applications in the following ways:

- **Complexity.** As a rule, complexity kills security. Just imagine, an ERP system from SAP (238 million lines of code, as for 2007) contains more source code strings than Windows 7 + Mac OS Tiger + Debian 5 altogether (85 + 65 + 40 million lines of code). So, there may be many different vulnerabilities at all levels, from network to applications [5].

- **Customization.** Every business application such as ERP is more like a framework, on top of which customers develop their own applications in a specific language. For example, programmers use the ABAP language to extend functionality of SAP systems; for applications such as Oracle PeopleSoft the language is PeopleCode; and the X+ language is used to customize Microsoft Dynamics.

- **Criticality.** This type of software is rarely updated, as administrators are scared the systems can be broken during updates due to backward compatibility and connection with legacy systems. Sometimes instances of SAP systems have not been updated for several years [3].
• **Closed nature.** ERP systems are mostly available inside the company, which is why business applications are considered a closed world. Very few security experts have access to study these systems [7].

**What can happen – typical attack vectors**

To illustrate typical attack and architecture issues, I will provide examples of SAP ERP, as it’s the most widespread, installed in 85 percent of Fortune 2000 companies [9].

The risks of insecure configuration of ERP systems and other business applications are as follows.

**Attacks via vulnerable services**

Most ERP systems have dozens and even hundreds of services installed by default, including web-based services. Some of them are responsible for different administrative functions. For example, SAPControl—the SAP management console—allows remote control over the SAP system. Its main functions are remote start and stop, which one must know username and password to perform. However, there are functions that can be used remotely without authentication. Most of them allow reading different logs and traces and sometimes system parameters.

Research from the SAP Cyber Threat Report 2016 [8] revealed that 3465 management console services were exposed to the Internet. Moreover, internal penetration tests demonstrate the higher number of vulnerable services. Approximately 80 percent of companies’ scanned servers, which I or my team analyzed during penetration tests or security assessment services, turned out to be susceptible to issues. This is just a single example of numerous unnecessary services.

**Privilege escalation by insiders**

When users connect to the server via a client application such as SAP GUI, they can execute different functions; for instance, if they want to create a payment order or a new user or fill up a form, they need to enter a particular transaction name in the SAP menu. The system will open a dialog window where a user can specify different parameters. For instance, if users execute the transaction SU01 to create a new user in the system, they will see a screen where they need to fill in all details about the newly-made user and then click on the “Create” button. If data is correct, the new user will be created in the system.

However, connecting via SAP GUI and running transactions are not the only way to perform SAP functionality. SAP systems are complex and one action can be performed multiple ways. For example, other ways to execute functionality in SAP system include:

• Running a background job using RFC (remote function call)

• Calling the same function via a SOAP interface—a web-based interface to run RFC programs remotely

• Executing the Web Dynpro application, a web-based frontend for SAP systems that can be used if workers do not have a client application but have a web browser

As you can see, all of these methods require a different approach for protection, for instance, segregation of duties (SoD). This is an important factor when dealing with different responsibilities and job profiles within an enterprise.

**Malicious developers**

Programs written in the ABAP language (SAP proprietary language intended to extend functionality of SAP systems) may have vulnerabilities, and more importantly, this language can also be used for writing backdoors that can provide malicious functionality such as sending details of every another to get it delivered. The only reason email messages were directly delivered server to server was if the receiving email server happened to be the next email server in the relay chain. As a result, in order to keep email private and secure, the messages themselves had to be encrypted using PGP or something similar.

With the advent of today’s Internet, relaying became less of the problem as email servers communicated directly, and the threat was replaced by an attacker using tcpdump (now known as WireShark) or similar to copy the network packets containing email—what was commonly referred to as taking email “off the wire.” To circumvent this issue, organizations began implementing TLS connections between email servers they regularly communicated with to encrypt those communications. With the advent of

---

**Email Security**

By Jeff Hall – ISSA member, Minnesota Chapter

THIS CONVERSATION WAS IN REGARDS to the securing of electronic mail. In particular, an organization’s requirement of implementing TLS between business partners. Not that this practice is necessarily a bad thing, but the rationale of doing it has changed a lot since it was first used. However, I encounter a lot of organizations that are trying to implement TLS with everyone so that they can secure email orders with cardholder data (CHD) that come via email.

As I have found out from the bad experiences I have encountered when this issue has come up, a bit of background is required so that people can appreciate why this is not the issue they think it is. Back in the very, very old days of ARPAnet, the predecessor of the Internet, electronic mail was relayed from one mail server to
Secure ERP Implementation

Alexander Polyakov

Unfortunately, development inside a company is largely uncontrolled. You can monitor the occurrence of new programs in the system and potentially find a developer, but you cannot detect exactly what every new program is doing unless you read every single string of the source code. Thus, without using additional solutions, nobody knows exactly what developers perform in the system. There are no control measures at all; they can develop insecure code, miss adding access control checks in the program, or send money to their bank accounts and nobody will be able to discover it unless one looks at the source code. Thus, lack of control over developers makes them a kind of lord of SAP, and their actions should be analyzed.

Insecure connections

You have to connect different applications to automate business processes. For example, if you want to generate an invoice in a SAP system automatically and send money to a particular banking account via the banking system, you need to connect ERP and the banking system. Business application systems are connected to each other like a spider web. In reality, there are dozens of similar connections and all of them can be critical in terms of security. For example, these connections may store usernames and passwords. Moreover, the systems are intertwined not only inside the corporate network but also with partner networks via the Internet or with other providers such as banks or insurance companies. Some of the systems are connected directly to an ICS/SCADA network via particular SAP systems such as SAP xMII (Manufacturing Integration and Intelligence) or SAP PCo (SAP Plant Connectivity).

Technically, this process is managed by RFC (remote function call) and other connections between SAP systems, which usually store credentials to access a satellite system. RFC connections are developed by SAP to transfer data between two switched networks, attackers found it was easier to just compromise an organization’s email server or user’s email client(s) than to try the old fashioned way of taking it “off of the wire.”

Do not get me wrong. It is not that an MPLS or other switched network cannot be hacked. It is that such a hack creates a significant number of issues that make the success of that hack very problematic including but not limited to: (1) it is extremely difficult to pull off unless you have a lot of inside information, (2) you need to know what protocols are being used by your target(s) since MPLS carries a number of protocols from ATM to BISync to Ethernet, (3) your hack will hardly go unnoticed to the carrier because your changes to their equipment will generate significant numbers of network alerts, and (4) requires a significant amount of network information to only pull the packets you want unless you have prepared for the terabytes of data per minute you will be intercepting (i.e., drinking water from a fire hose). The bottom line is that the real threat has moved from the network back to the email server(s) and email client(s). However, organizations continue to push for TLS connections between email servers to cover a risk that is, for all intents and purposes, non-existent.

Since the threat is with email servers and email clients, PGP, secure messaging servers, and the like are going to secure email server(s), and the like are going to secure email messages and attachments better than a TLS connection. And since the threat is with email servers and email clients, PGP, secure messaging servers, and the like are going to secure email messages and attachments better than a TLS connection. And since the threat is with email servers and email clients, PGP, secure messaging servers, and the like are going to secure email messages and attachments better than a TLS connection.

How to protect?

Protection of ERP systems is a challenge. A good comprehensive project may take years to be completed, especially when dealing with large landscapes. However, it is worth investments. Here are some basic steps that will help you to securely design your SAP implementation while you are in the planning stage. You can also apply this methodology to protect your systems from the most common attacks.

External attacks – disable insecure services

Any more or less complex application has large functionality that is needed in general, but unnecessary in particular cases. Almost all this functionality in a typical ERP system is enabled by default.

About the Author

Jeff Hall, CISSP, CISM, is a Principal Security Consultant in Optiv Security’s Governance, Risk & Compliance practice and focuses on payment card industry and related security projects. Jeff has over 30 years of technology and is a PCI QSA. Check out PCI Guru or contact him at Jeff.Hall@optiv.com.
As usual, a SAP installation includes approximately 1500 various web services, which are available remotely on behalf of any registered user if the service is enabled by default. About 40 services are even accessible to anonymous users. The SAP paper, “Secure Configuration of SAP NetWeaver Application Server Using ABAP” [10], points out 13 critical services.

I recommend that you apply recommendations from the guideline mentioned above as soon as possible—disable all services accessible to anonymous users, analyze which of the installed services are necessary, and additionally restrict the access by implementing authorization checks.

The SAP system architecture should include a web-based proxy (SAP Web Dispatcher) that will restrict access to all unnecessary services from the outside and allow access only to the necessary ones. SAP Web dispatcher lies between the Internet and your SAP system. It is the entry point for HTTP(S) requests into your system, which consists of one or more SAP NetWeaver application servers. The SAP Web Dispatcher therefore contributes to security and balances the load in your SAP system. Additional information about SAP Web Dispatcher can be found in the related documentation from the vendor [1].

The most important thing is that Web Dispatcher can only prevent access to unnecessary web services from the Internet; to prevent access to the services from the local network, you still need to manually disable all unnecessary web services.

As for non-web services, they should also be protected from any network except an administrator network. Here is the list of services that should not be available to the user network:

- SAPControl service (ports 5NN13 where NN is from 00 to 99)
- SAPHostControl service (port 1028)
- Message Server service (ports 36NN where NN is from 00 to 99)
- Message Server HTTP service (ports 81NN where NN is from 00 to 99)
- Database (port 1527 for Oracle)

Apply SoD principles

SAP solutions have various functional options, which are implemented through programs, transactions, and reports. Access to these objects should be strictly regulated, based on the authorization values defining users, methods, and objects allowed for access. Access to critical actions (e.g., access rights to modify transactions or to read any tables) enables users to perform attacks on SAP systems, escalate their privileges, or steal critical data.

Segregation of Duties (SoD) is a security method to prevent conflict of interests, for instance, to avoid two or more access rights which, being granted together, may give rise to a risk of fraudulent actions (e.g., the ability to create and approve a payment order).

The first step is to minimize the number of users with a SAP_ALL profile or those having access to critical transactions such as SE16 (Table Modification), SM59 (RFC Connections Configuration), and SE38 (Execution of ABAP Programs). As the next step, apply the SoD controls, at least those mentioned in the ISACA guidelines, “Best Practices to Resolve Segregation of Duties Conflicts in Any ERP environment” [2]. Below is the list of seven most common SoD violations:

- Create a fictitious purchase order and then enter the payment
- Release an existing purchase requisition, accept these goods in a specified warehouse location, and post an inventory adjustment to falsify their removal
- Create a fictitious customer account and subsequently approve a credit
- Create a fictitious vendor and initiate purchases from it
- Create a fictitious customer and then issue invoices to it
- Process the purchase of an unauthorized fixed asset, and once paid or received, adjust the fixed asset records to conceal the purchase and possibly obtain or use it
- Create a fictitious customer account and establish inappropriate customer pricing for that account

Separate development from test and check for vulnerabilities

To protect from malicious developers, first, design separation between test, development, and production infrastructures, meaning that nobody from a development team should be able to get access to test and production environments, and in its turn, nobody who has access to the test environment should be able to get direct access to production and develop...
opment environments, and so on. In other words, these systems should be separated on the network layer. Otherwise, developers can change code in production systems without any evidence.

Afterward, we should disable all the transport requests from development to production systems. Transport requests should go only from development to test and from test to production; direct transport requests from development to production should be restricted. If not, new code fragments would be implemented into production without prior testing. Finally, to securely architect separation between test, development, and production systems, make sure that there are no connections at the application layer, which transmit credentials from systems with low priority (development systems) to systems with high priority (production systems). These connections are only allowed to store technical connectivity configurations and authenticate the user for each access. Without this measure implemented, an attacker who penetrates into the development network will be able to get access to production system credentials.

Management of those connections can be performed via SM59 transaction noted above.

As you may know, OWASP (Open Web Application Security Project), focused on improving awareness in web application security, provides its top 10 list of the most dangerous vulnerabilities affecting web applications. When we deal with enterprise applications, it is not so trivial a task to understand what issues we need to check first.

Enterprise Application Security Project (EAS-SEC), a non-profit organization aimed at increasing awareness in the enterprise application security space, consists of separate projects, one of which covers code security: Enterprise Application Systems Application Development Guide (EASAD). This guide describes nine general categories of source code issues for business languages. These categories are universal and the same for the majority of business applications such as SAP, Oracle, Microsoft Dynamics, and Infor and their custom languages. The categories are sorted, based on criticality of vulnerability and probability of exploitation:

- Injections (Code, SQL, OS)
- Critical calls (to DB, to OS)
- Missing or bad access control checks (missing authentication, mistakes)
- Directory traversal (Write, Read, SMBRelay)
- Modification of displayed content (XSS, CSRF)
- Backdoors (hardcoded credentials)
- Covert channels (open sockets, HTTP calls, SSRFs)
- Information disclosure (hardcoded users, passwords)
- Obsolete statements (READ TABLE, kernel methods)

A secure developing process should include at least checking for code vulnerabilities of these nine categories.

Secure connections

As each system is connected with others, understanding which system can be attacked, how SAP is connected with other enterprise applications, how an attacker can escalate privileges, and what assets you should protect first is essential. We should analyze which system is the most important and start solving issues on that particular system.

First of all, we need to assign severity for each asset. Then analyze connections between assets, whether or not they are secure, and finally prioritize assets by their overall impact on the whole landscape security. For example, you have a low-risk asset: a test system without any critical data. This system has a connection with the production system, and this production system, in its turn, has a connection with the industrial control systems (ICS) infrastructure. Taking into account all the connections, this test system may have a high impact on all landscapes, and we should care about its security.

In addition to mechanisms of an application server, servers may often be connected with a number of other mechanisms. For example, SAP solutions may be installed on Windows servers, which are a part of a single domain and run with privileges of a common account. In this case, getting access to one server almost always means access to all other servers, no matter how properly they are protected at the application level. This is also possible when links or trusted connections are implemented via DBMS. DBMS often store references to other databases with pre-defined authentication data, thus making other DBMSs accessible. Further, the scope of such mechanisms includes any other possible methods to penetrate a neighbor system, which security experts usually use in penetration tests (i.e., an attempt to login into a neighbor system with the same or similar passwords both at OS, DBMS, and application levels, as well as all kinds of searches for passwords in plain text in the file system; update, integration, backup scripts, etc.). All these options should be checked to eliminate any risk of penetration through one weak link to all systems.

Another risk of insecure connections is data leakage. SAP systems should encrypt data while transferring it.
As for DIAG and RFC protocols, encryption can be implemented via Secure Network Communication (SNC).

SNC without single sign-on capability is available to all SAP NetWeaver customers for SAP GUI using SNC client encryption and for all RFC communication between SAP servers. Basic single sign-on capabilities are available in environments where SAP servers and SAP GUI clients run Microsoft.

**Summary**

Enterprise resource planning and business application security is a complex task. However, just taking four high-level steps can significantly improve the security level of your ERP system. Only after implementing the architecture securely, it makes sense to take further steps such as vulnerability management and incident response.

**References**


**About Author**

Alexander Polyakov is CTO and founder of ERPScan, president of EAS-SEC.org Project, accomplished R&D professional and Entrepreneur of the Year (by Golden Bridge awards in 2013 and Hot Companies and Best Products Awards in 2013). He is an expert in security for business-critical software like ERP. He has received due recognition having discovered over 100 vulnerabilities, as well as publishing multiple security whitepapers such as the annual award-winning “SAP Security in Figures,” surveys, and a book devoted to information security research in SAP and Oracle. He was invited to speak and train at more than 70 conferences in 20+ countries. He may be reached at a.polyakov@erpscan.com.
Fallacies in Threat Intelligence Lead to Fault Lines in Organizational Security Postures

By Jeff Bardin

The article discusses the issues associated with threat intelligence, the need for a common understanding of taxonomy and glossary, as well as presenting a case for intelligence tradecraft as a common standard. Furthermore, the article takes vendors to task for their reporting methods, content, and intent while providing a listing of recommendations and opportunities for organizations that may assist them in their building of organizational intelligence capabilities.

This article is partially written in analytic writing format, starting with the conclusions first. The conclusion section does not include normal analytic paragraphs and alternative analysis following standard intelligence tradecraft analytic writing. Instead, the recommendations and opportunities section represents supervisory actions. The article uses the Admiralty System or NATO System as a method for evaluating collected items of intelligence recognized by a letter/number combination found after article citations. The article discusses the issues associated with threat intelligence, the need for a common understanding of taxonomy and glossary, as well as presenting a case for intelligence tradecraft as a common standard. Furthermore, the article takes vendors to task for their reporting methods, content, and intent while providing a listing of recommendations and opportunities for organizations that may assist them in their building of organizational intelligence capabilities. The focus is on intelligence as it relates to cyber security/information security in as much as the length of this article allows.

Conclusion
Organizations follow inaccurate definitions of threat intelligence, leading to poorly conceived cyber threat intelligence programs. Vendors communicate threat intelligence definitions supporting their offerings, propagating the fallacy that threat intelligence solves numerous security problems. Cyber threat intelligence functions being built on a foundation that is not supported by standard intelligence tradecraft. Many programs support a fraction of the intelligence needs, yet stakeholders hold unrealistic expectations based upon expenditures.

Information security capabilities marginally improve as spending skyrockets and security posture improvement is limited to after-the-fact discoveries communicated as prevention.

Continued purchases of “threat intelligence” tools based upon the see-detect-and-arrest paradigm ensures slow improvement and loss of data expansion. Intelligence program builds focused on technology capabilities repeat the historical problems of information security when firewalls and antivirus represented the core of security programs.

Recommendations and opportunities normally located in this report position follow below in the recommendations and opportunities section.

Access to organizations that may be more advanced presents gaps in data available for this article. We based evidence upon direct access to a number of Fortune 500 organizations, discussions during cyber intelligence training classes, and actual intelligence program build activities.

Common taxonomy
A general Internet search on “threat intelligence” returns 11 million results in .36 seconds, demonstrating the intentional propagation of a term intended to generate revenue. Information and cybersecurity vendors, well-known training organizations, and companies use the term so often it has lost any
real meaning. Most vendors use the term as if intelligence is easily created, readily available. Products are sold with the expectation that threat intelligence is the panacea CISOs have sought for years. This is a general misnomer and cyclical in the regular creation and use of buzzwords and catchphrases that change annually. Vendors create years of capabilities based upon the jargon that just yesterday no one even knew existed. One of those buzzwords is threat intelligence.

What is threat intelligence? Gartner indicates this to be:

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard [5]. C3

Solutionary (NTT) uses this definition from the Central Intelligence Agency:

Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us. The prelude to decision and action by US policy makers. Intelligence organizations provide this information in a fashion that helps consumers, either civilian leaders or military commanders, to consider alternative options and outcomes. The intelligence process involves the painstaking and generally tedious collection of facts, their analysis, quick and clear evaluations, production of intelligence assessments, and their timely dissemination to consumers. Above all, the analytical process must be rigorous, timely, and relevant to policy needs and concerns [12]. A1

NTT Security then goes on to say that instead of providing military or political intelligence to government stakeholders, the current focus within the information security industry is to deliver threat intelligence to an organization’s stakeholders about digital threats to their enterprise systems [12]. A2

Data and information need definition as well. Many reports and daily deliverables are termed to be intelligence when they only meet the criteria of data or information (figure 1).

Definitions misunderstood

Herein lies one of the most inherent issues that vexes many organizations today, whether understood or not. The myopic view that the missing cog needed to protect an organization is technical threat intelligence. We couple this with additional fallacies a bit later, fallacies that create massive fault lines in our cybersecurity postures guaranteed to lead to unrealistic expectations and program gaps.

Definitions for intelligence range in scope and depth based upon who is using the term. We tend to stay close to traditional tradecraft definitions such as those below:

The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning adversaries (script kiddies, novices, cybercriminals, nation-states, hacktivists, political activities, insiders, whitehat/blackhat hackers, cyber terrorists, competitors, investigative reports, academics) hostile or potentially hostile cyber elements, or areas of actual or potential operations [6]. A1

Also, a body of evidence and the conclusions drawn from what is acquired and furnished in response to the known or perceived requirements of consumers. It is often derived from information that is concealed or not intended to be available for use by the acquirer [7]. A1

Alternatively, data and information that is sourced openly, and when placed through a process of decomposition, analysis, recomposition, and synthesis, becomes intelligence.

It gets quite confusing. Which definition should we follow? For pure terminology, MWR InfoSecurity in the United Kingdom seems to have a solid handle on the threat intelligence definition.

MWR proposes a model that breaks down threat intelligence into four distinct categories based on consumption: strategic, operational, tactical, and technical [10]. B3 MWR’s model (figure 2) is well defined, detailed, and something organizations should read and recognize.

Strategic, operational, tactical, and technical intelligence – defined with respect to threats

Strategic intelligence is defined as the high-level information, consumed at board level or by other senior decision makers and stakeholders at the business leadership level [10].
Operational intelligence is defined as information about specific impending attacks against the organization and is initially consumed by higher-level security staff, such as security managers or heads of incident response. Operational threat intelligence also includes attacks in progress, day-to-day situational awareness, surveillance, and warning while focusing on adversary intentions [10].

Tactical intelligence is defined as tactics, techniques, and procedures (TTPs) and is information about how threat actors are conducting attacks [10].

Technical intelligence is defined as the information (or, more often, data) that is normally consumed through technical means. IP addresses, domains, domain information, MD5 sums, log monitoring, technical data feeds from internal and external technologies, and providers are included in this listing and are often termed to be indicators of compromise (IoCs).

The problem with this model is the exclusive focus on threat intelligence. Threat intelligence is a subset of intelligence. Threat intelligence assumes a certain amount of collected data and information is collected, creating intelligence that is then aligned to organizational threats. Threat intelligence does not always include the correct data. Most times, the data is tactical and technical in nature, leaving significant gaps. Other times that data is skewed by the inherent bias of the technologies through which it is collected and filtered. In the end, it lacks in scope, depth, and breadth, including lacking tradecraft. Other types of intelligence reporting rarely covered in organizations include basic and foundational intelligence, research intelligence, competitive and estimative intelligence. For more information on types of intelligence, see cia.gov. Traditional warning intelligence is what the information security industry calls threat intelligence.

What is tradecraft?

Unfortunately, most of what is produced are data and at best, information. This starts with the misunderstanding as to what data is versus information as opposed to actual intelligence. The term is a core component of sales neglecting the difficult process of creating intelligence, while presenting data and information as actionable intelligence. Creating intelligence is a process that requires hard-nosed collection, attention to detail in production, structured methods and techniques, awareness of critical thinking and cognitive bias, the use of analytic methods, and the patience and perseverance that comes with knowledge creation. This is called tradecraft.

Let’s not confuse tradecraft as being something that is military intelligence. Many believe intelligence tradecraft is military in form and function. This is not true. The intelligence tradecraft of which I speak is rooted in CIA capabilities honed over years of trial, error, mistakes, and triumphs. The writings of Sherman Kent, long held as the father of intelligence analysis, defined methods of intelligence analysis used today. Kent’s analytic standards, doctrines, and practices need to be applied today within cyber threat intelligence functions [3] A1

The writings of Richards J. Heuer Jr., a 45-year CIA veteran, describe issues with critical thinking, cognitive bias, and structured analytic techniques used today as well. The writings of both men are directly applicable to information security efforts to create threat intelligence. Their use enables organizations to see beyond the limited view of “see, detect, and arrest,” while progressing to data collection, analysis, and intelligence creation use to prevent and eventually predict adversary actions. In addition, tradecraft is the underlying framework for intelligence upon which military and non-military programs should be built.

Many of the fallacies we face as cybersecurity professionals relate to a lack of understanding of what it takes to be an intelligence professional. The two are not mutually inclusive. Security operation centers are not populated with intelligence professionals. They are not occupied by analysts skilled in the arts professed by Sherman Kent and documented by Richards Heuer. In fact, most cybersecurity professionals find tradecraft to be distasteful and a general waste of time. This conclusion is drawn from the many engagements across the globe with cybersecurity professionals. When we come onsite to help build the intelligence program, we immediately face
resistance if the focus is not on low-level, technical activities. Yet most do not have a grasp, respectfully, surrounding the need for a well-built intelligence program that is top-down as opposed to technically oriented, bottom-up. Most have not had training in intelligence analysis or tradecraft. Real-world intelligence analysts endure rigor, structure, and focused training that specializes in the craft of intelligence analysis: the core function of any intelligence organization. They learn how to think, write, and brief. They study analytic tools, counterintelligence issues, denial and deception, analysis, and warning skills [1].

Another fallacy is that former military intelligence soldiers and National Security Agency staff are skilled in tradecraft. Not to say that they are not capable or that they have not had intelligence courses, but the courses are largely focused on physical, military action. Their version of tradecraft is specific to their missions and requirements. The NSA trains collectors to collect and analysts to analyze and most times, never the twain shall meet. We have direct knowledge of these methods. The protocol is compartmentalization and separate of duties as a higher priority over continuity of effort and understanding. The intent here is to point out that their skills are very focused on many different areas associated with intelligence. Whether the type is signals based or human, the methods do not include the end-to-end scope of traditional intelligence tradecraft. What we have found is their adoption to be much faster, their understanding of the model more inclusive than cybersecurity professionals. In general, the ability to adapt, adopt, and incorporate the tradecraft model is not a stretch for these men and women due to their backgrounds.

The daily crises

We spend countless hours preparing daily reports, responding to daily incidents, and dealing with the issue de jour. Morning stand-up meetings are preceded by a daily data push many call intelligence. We establish serialized reporting where each day we deliver a threat report; each week a weekly threat roll up; each month a roll up of each week and so on. We spend so much time gathering current data and fighting daily issues we never get to a point where we can actually perform intelligence-type work. This is largely self-inflicted. This fallacy in our process ensures we will never have the ability to analyze data based upon historical collection. The collected data is all current. The scope for that data is immediate. The data is not arranged in such a way as to facilitate long-term analysis. Of course, there needs to be a balance between the long-term analysis and the short-term reporting. The fallacy is that the short-term reporting is communicated as an intelligence-analysis product when it is mostly a regurgitation of open source data and readily available vendor reports.

Letting the enemy know what we know

Vendor reports with cute names dot the landscape, documenting the tactics, techniques, and procedures (TTPs) of adversaries. Detailed lists of adversary IoCs populate the appendices of said reports. The reports list the capabilities of the vendors verifying their prowess at uncovering adversaries. Adversary mistakes are lauded with great swagger. The reports list many conclusions without citation, with little discussion of likelihoods, limited communication of confidence levels, and no discussion of gaps in their collection, production, or analysis. The reader is left to fully trust the report at face value. The reports are positioned as absolute in their reasoning, yet the logic may be poorly crafted. Sweeping conclusions that oversimplify the problem hallmark the reports. Blanket statements used to persuade the reader are repeated in the reports, serving to hammer home the need to purchase services from these vendors.

Written to market and sell products and services, the reports do not discuss the potential for denial and deception. Could the data be forged or faked before vendor acquisition? Is it possible their collection methods or sensors are in error or misinterpreted? How did the vendor determine source credibility and reliability? Is there any bias in the technology used or human analysis of the data collected? Are adversaries using heuristics to lull vendors into comfort levels of consistency all the while they are deceiving vendors with traditional maskirovka, the well-honed Russian use of deception? The belief is yes; our vendors are being lulled into comfort levels. As we clearly communicate what we know about them, our adversaries adopt new methods to deny and deceive us all the while they continue to project activities that reflect old TTPs. On the contrary, deception existed as far back as recorded time. The Trojan horse, double agents, and tactical deception are strategies that turn the tide of battles.

The practice of deception to trigger an action is a key method of generating data that can be turned to intelligence. Triggering an action leads to the collection of data not only from the primary ripple in the so-called pond, but from second and third order effects. An old USAF tactic is to circle with fighter jets near the 12-mile limit of a country’s ocean border. The jets circle and circle while an RC-135 is nearby collecting data. Eventually, one or both of the jets turns on the afterburners crossing the border. Acquisition radars turn on, missile sites light up, all the while the RC-135 is collecting data. A treasure-trove of information is collected as radio chatter fills the air waves. The jets turn back and the collection slowly subsides. The intent clear. The data collected, great. Our adversaries use the same tactics in the cyber environment to determine our readiness posture, technical capabilities, and methods for defense.

Is this sedition?

The real travesty with the vendor threat reports is the fact that they are openly published. Cyber warfare is upon us. Adversaries and enemies scour blogs, forums, chat rooms, and personal websites to piece together information that is used to harm governments, commercial organizations, and individuals. They utilize methods of espionage extracting sensitive data at unprecedented rates. When discovered, cybersecurity vendors feel a need to publish every TTP, each IoC, and their malware and individual hacker courses of action to the world.
The damage done by these actions is pure negligence. Very surprising that the government does not ask the vendors to suppress the details. If one of their own were to release such data, we would be reading reports for charges of treason. The reports serve to bolster vendor sales while informing the enemy what we know about them and their TTPs. Many of these reports reference other vendor reports on the same topic, providing circular reasoning that further, albeit falsely, solidifies their conclusions (demonstrated clearly in the reports on Rocket Kitten). This behavior serves to drive the enemy to increasingly creative and undetectable methods of scanning, penetration, and data exfiltration. They change these methods more frequently in light of the constant barrage of vendor reports—many timed just before or during well-known cybersecurity conferences. The organizations who have penetrated the enemy and adversary forums, chat rooms, and new methods of communication while using the access to learn more about them, may miss the “frequency change” due to the vendor reports. By frequency change I refer to the old methods of rolling up on a radio frequency, learning about the enemy including alternative frequencies, and making the change to that frequency when the request is broadcast. Today the methods are much more dynamic, the communications many times encrypted, and the changes very subtle.

Fallacies that create fault lines

As discussed above, we believe the fallacies in threat intelligence stem from a lack of agreed upon glossary and taxonomy. In addition, the industry’s acceptance of vendor solutions to provide actual intelligence, and vendor reports taken at face value without source validation or citation. The organizational placement of intelligence within information security, the inaccurate understanding of what an intelligence professional is, and the inability of organizations to see beyond purely defensive measures for information security all contribute to the issue. These fallacies, understood to be non-inclusive, create inherent fault lines in our security programs.

Recommendations and opportunities

Changing behaviors

What can we do to rectify the path of fallacies we continually choose to follow?

First (in no specific prioritized order), we must educate everyone in information technology, information security, and the C-suite on the standard taxonomy of intelligence. This provides a shared understanding and baseline glossary upon which to build communication.

Secondly, we must treat each vendor report as nothing more than another source of data, data that must be evaluated for credibility, reliability, and relevance. To do so, we can use the NATO Admiralty Code [9] (figure 3) A1 used throughout this article to rate sources in the format of (A1, B2, B3, etc.). The code helps organizations evaluate sources of data and the credibility of the information provided by that source. Evaluate each vendor report using this coding method while documenting ease of data extraction, relevance to your organizational issues, type of intelligence (strategic, operational, tactical, and technical), and value in solving your security problems.

Thirdly, begin to grow and expand your intelligence program functions. Learning methods of anonymity, open source data collection, collection management and planning, production management of intelligence functions, analysis, analytic writing, and dissemination adds immediate value to your organization. Understand that intelligence is not the same as incident response or a core component of the security operations center. These skills are unique and must be shared, but to bury them within these areas is a mistake. We faced this for years (and still do), putting information security under information technology and treating it as a solely technical issue. We should not make the same mistake with intelligence. Intelligence functions need direct access to organizational stakeholders.

Fourth, create standard processes to seek out malicious actions within your information technology environment. Use adversary TTPs to drive your “hunt and detect,” but understand that, albeit a valuable capability, it is not a proactive function. They are already inside the wire and must be removed. Organizations need to do this for proper hygiene.

Fifth, develop methods within your organizational risk model to collect open source data regularly. Like our third point above, we must grow this function so we collect data and information and develop intelligence that is pertinent to our stakeholders and our organization. Capture priority intelligence requirements, create information requirements prioritized and vetted, focusing on all sources of data including open source collection. Devise methods for mission management that drive targeting for passive collection.

Accuracy of data

1 - Confirmed by other sources
2 - Probably True
3 - Possibly True
4 - Doubtful
5 - Improbable
6 - Truth cannot be judged

Reliability

A source is assessed for reliability based on a technical assessment of its capability, or in the case of human intelligence sources, their history. Notation uses alpha coding, A-F:

Reliability of Source

A - Completely reliable
B - Usually reliable
C - Fairly reliable
D - Not usually reliable
E - Unreliable
F - Reliability cannot be judged

Credibility

An item is assessed for credibility based on likelihood and levels of corroboration by other sources. Notation uses a numeric code, 1-6:

Figure 3 – Admiralty Code
organization to help your program move forward. You may believe you know your company but knowing your professor ensures an “A.”

Tenth, give your organization time to implement an intelligence function. Determine what makes sense for your organization as to what that time frame is. Institutionalize lesson-learning as a process of performance improvement, not assessing blame [4]. Give your intelligence organization time to learn. Making mistakes in the early stages of maturity is expected. Just do not make the same mistakes repeatedly. Give your intelligence organization the authority to make decisions and the access to stakeholders to learn requirements and communicate capabilities. Establish goals and objectives that are actually reachable and practical. Stretching goals when first building a function can lead to unnecessary failures. Leadership—and the right level of leadership—is required to manage analysts. Find the right level for your organization. When you add an intelligence function to an organization that has never had one, manage expectations. Eventually, a properly staffed, trained, and led group can deliver significant value to the organization.

Lastly, although non-inclusively, prepare your organization for the next steps. Those next steps involve counterintelligence. Although now seen as a high-risk area for organizations, my belief is that we will eventually adopt certain principles associated with this tradecraft. In fact, several organizations already employ methods associated with counterintelligence, both passive and active.

Figure 4 – National Intelligence Council confidence levels

Make note that many vendor report subscriptions provide generalized and generic data and information. Periodically, intelligence is part of the report. Occasionally, something relevant to your organization is included. Most time the reports are of a create once, distribute many format.

To drive industry change, work with vendors. Request and require source credibility ratings, citations with confidence levels, explanations of analytic methods, and resumes of staff working your contracts.

What are confidence levels?

Confidence levels relate to evidence helping intelligence staff state not just how confident they are as analysts but why they are confident [11]. This helps intelligence functions define why they believe something (the because) at what level, based upon high, moderate, and low as defined in figure 4.

Sixth, create a model of your adversaries and their capabilities that are target centric. Expand your collection to include all areas concerning your adversary. The only way to fully understand what threatens your organization is to fully understand the enemy, their motivations, their competence, and their skills. Otherwise, organizations will continue to play a basketball game on defense, never crossing the half-court line—a recipe for assured loss.

Seventh, write in intelligence analysis format. Stakeholders have little time. Making them hunt for the answers ensures failure. Use the guide in figure 5 to assist in your writing.

Eighth, create a strategic plan followed by a program plan for intelligence in your organization. Define what it is and is not. Author a vision and mission along with guiding principles. Develop a series of goals with three to four objectives, each determining how to achieve those goals. Gain acceptance and follow the plans.

Ninth, set up a listening tour of your lines of business and corporate stakeholders. Gain permission to attend their meetings with the understanding that you are there to listen and learn. Do not offer your services. Listen to digest and gain knowledge of your stakeholders. Do not listen to prepare a response. Gather this information and take it back to your organization to help your program move forward. You may believe you know your company but knowing your professor ensures an “A.”
In 2011, we adapted the Ten Commandments of Counterintelligence into a list focused on cyber. They are:

1. **Be offensive**
   a. Do not be afraid to anonymously collect information on your adversaries. In many cases, they are hiding in plain sight. You just need to know where to look.
   b. Cyber intelligence is the basis for cyber counterintelligence. Learning your adversary prepares an organization for counter denial and counter deception.

2. **Honor your profession**
   a. Learn about intelligence analysis. Leave your security comfort zone.
   b. Take classes in critical thinking. It is never too late.

3. **Own the street**
   a. Establish a presence on the same sites of your adversaries.
   b. Create multiple personas when doing so.

4. **Know your history**
   a. The old adage of “know your history or be destined to repeat it” is in effect.
   b. Know what your adversaries have done in order to determine what they may do.

5. **Do not ignore analysis**
   a. Analysis is not grown from a server but resides in human skill.
   b. Until such time as artificial intelligence is truly with us, the human mind serves as the best solution for intelligence analysis (if properly trained).

6. **Do not be parochial**
   a. Share data even if you must do this via back channels. We do not advocate breaking corporate rules by sharing sensitive data.
   b. Quid pro quo sharing is required.

7. **Train your people**
   a. Understand your needs, understand the timing of those needs, and drive for increased training budgets.
   b. The best investment you can make is in yourselves.

8. **Do not be shoved aside**
   a. Gently push your way into business meetings establishing a “listening tour.”
   b. Clarify what intelligence is and is not.

9. **Do not stay too long**
   a. Fully document your actions while periodically shifting targeting assignments to stay fresh.
   b. Rotate assignments to learn every facet of the intelligence game.

    a. Perseverance and patience are required.
    b. Our adversaries do not operate under the same rules of engagement that hampers our actions.

Much like information security a short 15 years ago, cyber intelligence is in its infancy and largely misunderstood. We are rife with fallacies and inaccurate definitions and terminology usage. The profession of intelligence should not be confused with security and should not be clouded by poor and biased reporting. The only way to change the problems inherent in intelligence today is to drive that change internally while forcing the market to shift. The CIA realized this years ago, striving to create the “profession of intelligence analysis.” The framework of intelligence can and should be the underlying standard for intelligence planning and program builds.

This comes with frequent constructive criticism of vendor-delivered products and services. I have always said the best investment you can make in life is in yourself. Organizations should consider doing the same. Educate your staff. Plan your program. Drive the change from the inside.

For a summary of this article, see the conclusion at the beginning.
tive for a security architect. The security architect needs to be able to function similarly to the enterprise architect, seeing the big picture in order to provide appropriate security solutions.

Organizations need security engineers and security architects. Most security professionals function better when they are focused exclusively on one role. Security programs may struggle when a single person is asked to perform both roles; essential elements of either role may be neglected due to lack of skill or interest. The key is to identify and staff each role appropriately and then to continue to provide support for professional growth in each role to help the business and the individual succeed.

NOTE: this article is partly based on a blog post by Stephen Northcutt.

Resources
8. Hames, Jacqueline. Strategic Trickery: The U.S. Army’s Use of Tactical Deception. Soldiers, September 2014. http://soldiers.dodlive.mil/2014/09 стратегический-манипуляция-%d1%83%d0%b6%d0%b5%d0%bd%d1%81%d0%ba%d0%b8%d0%b9-use-of-tactical-deception/.

About the Author
Jeff Bardin: Chief Intelligence Officer, Treadstone 71. He may be contacted at jbardin@treadstone71.com.

The Security Architect and the Security Engineer
Continued from page 7

Since 2007 he has conducted over 40 in-depth interviews with leaders in the security industry in order to research the competencies required to be a successful leader in the security field.

Polluting the Privacy Debate
Continued from page 9

Even if this means law enforcement and intelligence agencies can’t bypass it? Look beyond phones. What about PGP encryption software? How about cars? Does the public have a right to effective security products or not? Some proponents of surveillance have done a poor job of advancing their argument. But that doesn’t mean they’re wrong.

Security professionals have an important role in this debate. To speak up. To educate. To criticize nonsense when we hear it and help clear the smog. This issue is too important to give up on, and isn’t going away any time soon.

About the Author
Geordie Stewart, MSc, CISSP, is the Principle Security Consultant at Risk Intelligence and is a regular speaker and writer on the topic of security awareness. His blog is available at www.risk-intelligence.co.uk/blog, and he may be reached at geordie@risk-intelligence.co.uk.