PNNL-25612

AiR2: Asymmetry in Resilience

Report on the Second Meeting on Asymmetry in Resilience for Complex Cyber Systems

July 2016

CS Oehmen
NJ Multari

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov


This document was printed on recycled paper.
(8/2010)

PNNL-25612

AiR2: Second Meeting on Asymmetry in Resilience

Report on the Second Meeting on Asymmetry in Resilience for Complex Cyber Systems

CS Oehmen
NJ Multari

July 2016

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Acknowledgments

Second Meeting on Asymmetry in Resilience (AiR2)

Crystal City, VA (September 16-17, 2015)

Authors/Hosts:

Christopher Oehmen, PhD
Nicholas Multari, PhD

Participants:

Dan Adams, Defense Advanced Research Projects Agency
Ehab Al-Shaer, University of North Carolina, Charlotte
Daniel Best, Pacific Northwest National Laboratory
Thomas Carroll, Pacific Northwest National Laboratory
Tom Clark, Air Force Research Laboratory
Ann Cox, U.S. Department of Homeland Security
Anurag Dwivedi, Johns Hopkins University Applied Physics Laboratory
Michael Farmer, Pacific Northwest National Laboratory
Scott Godwin, Pacific Northwest National Laboratory
Charles Gunzel, Pacific Northwest National Laboratory
Arlette Hart, Federal Bureau Investigation
Craig Jackson, Indiana University
Yasir Khan, University of North Carolina, Charlotte
Kimberly King, MITRE
Patrick Mackey, Pacific Northwest National Laboratory
David Manz, Pacific Northwest National Laboratory
Cori Mejia, Pacific Northwest National Laboratory
Richard Metzger, Air Force Research Laboratory
Nicholas Multari, Pacific Northwest National Laboratory
Brian O'Donnel, Boeing
Christopher Oehmen, Pacific Northwest National Laboratory
Jeffrey Picciotto, MITRE
Frank Prautzsh, Velocity Technology Partners
Pradeep Ramuhalli, Pacific Northwest National Laboratory
Sokwoo Rhee, National Institute of Standards and Technology
Craig Rieger, Idaho National Laboratory
Greg Shannon, Office of Science and Technology Policy
John Sullivan, SAP

Contents

1.0 Purpose and Major Outcomes

Currently, a worldwide collection of actors has free reign to probe, attack, monitor, and manipulate networks, including those crucial for supporting U.S. critical infrastructure. While many research efforts are already underway to develop resilient cyber systems, few address a key component of making systems truly resilient—the need to measure and shift the cost balance that currently favors the attacker. Asymmetry in Resilience **(AiR)2** was a two-day meeting for leaders from universities, government institutions, Federally Funded Research & Development Centers, and industry to expand upon the successes from the initial AiR meeting held in 2014. In that meeting, the participants agreed upon a definition of asymmetry, some of its human and non-human dimensions, and a research agenda for the future. In the second year, the group expanded upon the results achieved in 2014 by examining several case studies using recent and high-impact cyber-attacks. In each case, the participants examined the attack, the impact of the attack, and how that impact and cost differential could have been altered in a resilient environment.

The primary outcome of this exploration was the initial establishment of an empirical foundation for the study of the potential effect of resilient technologies on the asymmetric imbalances between attacker and defender in cyber conflict. The participants examined the effects on asymmetry in terms of cost and level of effort, action/reaction, and final impacts. A secondary outcome of the meeting was the establishment of provisional collaborative (multidisciplinary, multi-institutional) teams to begin refining these concepts and creating advocacy in the wider cyber resilience community.

Specific issues addressed include

1. re-examination of the working definition and the attributes of asymmetry;
2. identification of the asymmetric imbalances resulting from several example cyber-attacks;
3. identification of resiliency techniques that may reduce the attacker advantages;
4. definition of the key research challenges identified by the case studies;
5. identification of the research domains and directions that can be applied to address these research challenges; and
6. refinement of the research roadmap originally discussed at AiR1.

2.0 Meeting Participants

The hosts of the AiR2 meeting selected the participants based on two criteria. The first was to ensure a broad representation of institution types. The group spanned U.S. Department of Energy Laboratories and other Federally Funded Research and Development Centers, industry, government, and academia. The second criterion ensured the representation of a broad range of relevant expertise spanning measures/metrics, risk management and models, economics of cybersecurity, high availability systems, and behavioral models as related to cyber resiliency.

The 30 meeting participants divided into three working groups of 10 participants each. Each working group was assigned one recent cyber intrusion event to consider. The goal of the working groups was to discuss the weakness exploited and the potential impact of resilience technologies on their cyber intrusion

in an environment conducive for open discussion. Each working group consisted of a balanced representation from across the five areas of host institutions and a balance of technical backgrounds. Intrusions considered by each breakout team were selected in advance of the meeting to focus the conversations on recent, impactful intrusions for which many of the relevant facts were known. In each breakout session, all participants were encouraged to share their points of view and collectively work toward assimilating these various perspectives into cohesive summaries for presentation to the plenary group.

The intrusions selected for consideration at the AiR2 meeting were

- HAVEX – an intrusion that affected control systems via weakness in trusted vendor systems;
- U.S. Office of Personnel Management (OPM) Breach – during which sensitive data was stolen via a breach that originated from trusted contractor; and
- Shamoon – an apparently targeted virus that infected thousands of machines within a critical infrastructure sector and rendered the systems useless.

Each working group was tasked with

a. identifying the asymmetric issues that favored the attacker in the environment current at the time of the attack, and
b. identifying the potential resilience technologies or practices that may shift the balance back in favor of the defender.

Insight from briefings and discussions from all of the intrusion groups were assimilated to identify major findings and recommendations of the meeting. These findings are discussed in the following sections.

3.0 Breakout Team Results

3.1 HAVEX

HAVEX was a control-systems focused intrusion that operated by exploiting a weakness in a trusted and widely used industrial vendor that interfaced with many other systems (Desso 2014; Team 2014; Walker 2014; Sullivan 2015). This is a likely model for many attacks due to the many interdependencies found in most complex systems. Understanding and predicting the possible interactions between these components/networks is nearly impossible and in fact, most are not even known. In the control systems world, and specifically in the supervisory control and data acquisition systems arenas, safety is understandably the first consideration, making security often secondary. Furthermore, the ability of these systems to continue functioning is typically their measure of success, which does not always incentivize security. Recently, there has been a groundswell of new functionality in control systems via wireless technologies; however, such functionality increases not only their capabilities but also their attack surface and the associated threat space. Future and emerging technologies such as the Internet of Things threaten to make this problem worse through the introduction of billions of additional threats into this landscape.

Key Finding 1: The conflict landscape, not the technology, is driving much of the asymmetry. The key asymmetric attribute that favors attackers in the HAVEX example is time. Not only do attackers have the time to explore and search for vulnerabilities, but also when an attack happens, the system only has so

much capacity to respond in real time. Attackers can have a variety of motivations including causing death, financial gain, a desire to destabilize or disrupt infrastructure, political leverage, ideology, or vengeance. Instead of thinking about technologies, the goal is to think more philosophically about resilience and asymmetry; once a foundational understanding is developed, move on to considering technologies.

Methods by which attackers can exploit an asymmetric advantage can be broadly categorized as *advantages of opportunity* and *advantages of environment*. Examples of advantages of opportunity include the fact that attackers have the ability to overwhelm a defender, as well as the fact that the target is more visible than the attackers, even though not all of the attack surface is critical for correct functioning. Also, a successful cyber-attack on, for example, the power grid would disrupt not only the delivery of power but many other systems as well, including the power grid defensive mechanisms. Potentially the greatest advantage of opportunity for the attacker is the difficulty of modeling human behaviors, providing a creative attacker many opportunities to do the unexpected.

Advantages of environment include a preference for homogeneous systems by system owners, resulting in a single vulnerability being pervasive throughout the environment. In addition, control systems (and other cyber systems) have very complex chains of interdependency that are crucial for their operation, but which are not completely understood or even known. Such misunderstood or unknown interdependencies provide adversaries with a means to exploit their target. An advantage for the defender is they are on "home turf" and, as a result, can know the system's state at any point in time. However, they may not always know of or monitor external dependencies. One confounding issue here is that any centralization of state information becomes a high-value target, providing a single source of information that could potentially make an adversary's job easier. Configuration management addresses one aspect of security surrounding the state of a system, but it also reveals the highly complex interdependencies between systems' states.

To approach questions of asymmetry in this example, there are several relevant aspects to measure. These include the breadth of assets an attacker could control, the size of a system's attack surface, discoverability of attack surface, recovery time, time to degrade availability, consequences of an attack, and the cost of attacking in terms of resources, time, and knowledge.

Recommendations:

- Validate that the implementation of a network is consistent with its design
- Insist on good hygiene
- Develop a scrubbing procedure for networked components that can be measured
- Prohibit network connections until devices meet hygiene requirements
- Create proper financial incentives for proper cyber hygiene
- Start preparing now for the Internet of Things and how it will impact control systems
- Implement closed systems whenever possible, with configuration control
- Predict what will happen in cyberspace based on physical-world patterns
- Discover dependencies between systems, processes, data, among others, where possible
- Perform cyber-intent intelligence analysis via social network and deep web analysis
- Implement different configurations for training technology and operations

- Take advantage of physical defenses when possible. It is harder to penetrate walls.
- Spend effort on introspection to discover vulnerabilities and entryways and explore the attack surface
  - Automated
  - Red team
  - Network map
- Practice ongoing configuration management of the architecture once established
- Implement power system regulations requiring good cyber practices
- Design system to persist in the face of small attacks.

3.2 Shamoon

Shamoon was an intrusion that stole data from and destroyed computers in the corporate enterprise of energy delivery companies, primarily in Saudi Arabia (Industrial Control Systems - CyberEmergency Response Team 2012; Hilfiker 2013; Corvin 2015; Sullivan 2015). Attackers specifically targeted the energy delivery corporate information technology systems, while leaving the energy delivery infrastructure untouched.

There were three modular components to Shamoon attack—Dropper, Wiper and Reporter. Dropper was the initial infection that scanned the target. Wiper erased files in the Windows documents folder and sys32config and replaced them with .jpegs of a burning flag. Wiper prevented any chance of system restarts by destroying the system boot record. Reporter communicated back to the command and control systems to share information about progress. According to public records, Shamoon infected a privileged account at 11:08 on August 15, 2012 while a large number of employees were at home for a religious holiday. Within 24 hours of the initial infection, approximately three-quarters of the systems were infected. By August 16, announcements from various antivirus vendors were released describing the infection and a group claimed responsibility for the attack. It took until August 26 to restore the 30,000 workstations that had been affected by Shamoon. The next day a natural gas company was attacked using the same tools.

Shamoon was remarkably effective, in part because of its broad ability to target various Windows systems that are ubiquitous in corporate enterprises. The intent of Shamoon was to destroy, not steal for financial gain. This is the main difference between Shamoon and more common ransomware, where the intention is to gain money.

Key Finding 2: Attackers and defenders have important differences in perspective on the conflict environment. There are several attributes of Shamoon and its environment that provided an asymmetric advantage for attackers. First, the adversaries chose the time of attack and gave themselves plenty of time to gain information. Second, while the defenders must defend the entire attack surface, attackers only need to find one weakness. In the case of Shamoon, the attackers needed only to identify a single means to infect and move between systems. Homogeneity in the systems ensured that an exploit that works on one system would likely work on many systems. On the human element side, disgruntled staff or and other users can intentionally or unwittingly allow their systems to be compromised. Finally, adversaries have a large collection of collaboration and collusion tools and techniques. The cheap availability of root kits, third-party collaborators, and even computing resources such as public clouds, puts enormous capability into attackers' hands for potentially very little cost. One aspect in favor of the defender is that

attackers using or adapting previously known tools have a higher risk of detection, so avoiding this introduces an elevation in cost for developing new attack tools.

Recommendations:

Several identified technologies show promise in shifting the asymmetric balance back in favor of defenders in the context of the Shamoon intrusion. Better situational awareness and decision support might have alerted defenders to the occurrence of scanning and probing. Connecting this realization to any of several responses might have interfered with the adversaries' ability to maneuver. Such responses include partial quarantines, dynamic encryption of certain sensitive data or automated healing or regeneration of data using distributed approaches, moving target responses, deception, enforcing term limits on credentials, applications, or other system elements, or even providing challenge puzzles to systems performing certain operations on behalf of users. There are also several design or policy features that might have changed the asymmetric advantage, including proactive segmentation of systems or user communities, increasing the diversity in systems (either at the application, operating system, or hardware levels), or requiring multiple concurrent administrators for certain sensitive operations. Mission mapping, physical modeling, and applying other models may provide additional insight into deviations between expected and observed system behaviors.

3.3 Office of Personnel Management

According to reports, the OPM breach was a two-stage attack (Finklea et al. 2015). A first actor probed OPM infrastructure and found an old mainframe system. A different actor gained access and observed systems interacting with the mainframe. This actor exploited the fact that the mainframe system relied on supporting systems (like cloud infrastructure) having exploitable vulnerabilities, gained access to sensitive data, and exfiltrated the data using encrypted file transfer. The attack was introduced into the vulnerable system via a trusted contractor. The increasingly interconnected nature of complex cyber systems and their dependence on multiple other systems, contractors, and vendors will likely continue to provide attackers the means to access systems and data indirectly.

Key Finding 3: Shifting the asymmetric balance to defenders will require coordination between system owners/operators and the community of applications and vendors on which they depend, or the ability to operate in a completely untrusted environment. The trusted-environment approach will drive an ecosystem-like solution that will make it possible to measure and verify the level of trust in the trusted-partner systems. This means that all participants must have good basic cyber hygiene and a clear mapping of the relationships between their various missions. This ecosystem model should also it make possible to ascertain how organizations are protecting each other.

While the mathematical concept of cyber resilience is very important, both monetary and non-monetary value concepts will be required to get a real understanding of asymmetry. For instance, OPM's mission may not currently have a capital value, but achieving its national security mission is critical. That means any trusted partner must have it in their interest (whether they are driven by security mission or by profit motive) to keep the data safe. But these partners have other partners and dependencies that have their own motivations. Mission-based valuation must propagate all the way through the supply chain.

Recommendations:

The breakout group covering OPM's breach saw patch management as an essential component in pushing the asymmetric advantage in favor of defenders. Patches must be pushed without disruption, and should take into account third-party components and other complex interactions. Other essential technologies

include privilege access management, to include processes for discovering who has what level of privileged access. Understanding the "home turf" (in a constantly changing environment) is also important and should include automatic and regular mapping of network and data flows, tagging of data using identifiers, and a higher contextual view similar to a "cyber weather map." In addition, the working group identified several important organizational factors, including the need to create a culture of cyber accountability, methods for rapid communication of possible issues and status from end users. This "soft skill" can be significantly enhanced or supported using technologies.

4.0 Summary of Findings

Identified above are three aspects of resilience in cyber systems that are considered important components of asymmetry across all of the intrusions we studied. The following is a summary of those aspects that transcend intrusion particulars.

4.1 Key Finding 1

The conflict landscape, not the technologies, is driving much of the asymmetry.

4.1.1 Sub Finding 1

Sensing and response control should be active and out-of-band whenever responsible

When a system is compromised, control, sensing, and response are also compromised. Part of the current asymmetry adversary advantage is that once they breach a system, they can gain access to sensing and control. Preventing this with out-of-band sensing, control, and actuation systems may incur a large one-time cost but may still be worth the investment. Such an approach would provide continuity, awareness, and control even during an attack. Where out-of-band opportunities are not feasible, at the very least, sensing and control should be as orthogonal or independent as possible to the underlying system. This may lead to a broader definition of out-of-band that may include non-cyber options. The more creative the solution, the more advantageous it may be.

4.1.2 Sub Finding 2

Asymmetry can happen at many levels—we must get better at exploiting the ones that favor defenders

Participant analysis identified several types of asymmetry. These included (1) knowledge and situation awareness, (2) control, (3) agility, (4) technology, (5) efficiency, and (6) resources. *Knowledge* asymmetry comes from the ability to find ground truth about the system, including network details, infrastructure, health, and data flow. *Agility* asymmetry is a factor of one party in a cyber-conflict having more flexibility, timely adaptation and response, or pace of learning than the other. *Technology* asymmetry comes from software, hardware, quality, complexity, standards, protocols, and integrated assurance. *Efficiency* asymmetry comes from imbalance in cost between assailants and defenders. *Resource* asymmetry refers to capabilities, assets, components, intellect, culture, and other aspects such as time. In each of these cases, defenders have a unique perspective that is not fully exploited, but which could potentially shift the asymmetric balance in their favor. This is discussed in the following section.

4.2 Key Finding 2

Attackers and defenders have important differences in perspective on the conflict environment.

4.2.1 Sub Finding 1

Understanding the adversary's tools and attacks will help focus countermeasures, but resilience should not rely on this knowledge

Some advantages of asymmetry for the defender come from disrupting the adversarial process. For example, while there are multiple points in the kill chain where the defender can disrupt adversarial activity, the defender may select a time and type of disruption that is cost advantageous to them. Awareness of what is happening gives the time advantage back to defenders because they can choose when and where to defend, and they can focus their defenses on specific "locations" that are relevant to blocking the attack. Behavioral indicators may also be useful, since at some point, adversary behavior has to be inconsistent with the defender's mission. However, an adversary could be doing something completely unpredictable, including being irrational. Since models cannot typically predict irrational behavior, the defender should not completely rely on knowledge of adversaries.

4.2.2 Sub Finding 2

Understanding how the system and users should behave gives insight into finding adversaries and limiting privileges

The defender typically has a good understanding of the mission of the organization and the cyber systems supporting it. Because the defender disproportionately cares about the mission, it is in their interest to ensure that it persists. The key is that it will be essential to measure the right attributes in order to have the understanding required to find normal and abnormal behaviors. Currently the data used to determine behaviors typically comes from available sources like login behaviors, applications used, network activity and others. But these are not necessarily the best measurements. Solving this measurement problem might lead to a more advantageous position for defenders, giving them the deep knowledge they need to understand their own systems and behaviors on that system. This would lead to a better model for encapsulating the privilege of users, systems, applications, and other system elements. This goes beyond just who has what access to what files. The key is to isolate and island segments of the system, limiting propagation and movement of adversaries. In some ways this is an extended form of hygiene and includes not only some measurements largely available today and easily implemented, but also the development of new functionality. This new functionality would have to be developed in conjunction with current technology providers and not require wholesale replacement of core technologies.

4.3 Key Finding 3

Shifting asymmetric balance to defenders will require coordination between system owners/operators, and the community of applications and vendors on which they depend, or the ability to operate in a completely untrusted environment.

4.3.1 Sub Finding 1

Cyber hygiene has to be improved at all levels through a cultural shift

Hygiene is the foundation of asymmetry. However, similarly to vaccines, its effectiveness depends upon the vast majority of people participating. When this communal protection breaks down, we all are at risk. One way to incentivize hygiene would be via third-party accreditation. Similar to crash-test ratings or credit ratings, a cyber-hygiene rating could itself produce a capital value. This would require some sort of independent assessment and verification about the presence of technologies and the following of procedures. Potentially, the insurance industry could be a driving force of this incentive system by requiring certain levels of hygiene to be attained for different levels of coverage.

To be clear, hygiene is more than just a compliance checklist. Ultimately, it should lead to a cultural change in the cyber realm. To be fair, attainable, and certifiable, hygiene standards need to be published. Hygiene practices that enhance resilience must accommodate the fact that cyber hygiene cannot be universally applied because of legacy systems and may take many forms in different contexts.

4.3.2 Sub Finding 2

Complex (often hidden) dependencies lead to easy targets that a provable chain of trust (potentially mediated by an independent third party) may mitigate

There are at least two types of dependencies—intended and unintended. Because unintended dependencies are typically unknown, they will be extremely difficult to discover, assuming they can be discovered. However, managing trust through these dependencies would provide an asymmetric advantage for defenders if combined with hygiene. It is not clear whether this is an algorithmically NP-hard problem, and is a good candidate for continued research.

4.3.3 Sub Finding 3

Integration of multiple technologies and human skills will lower response time for both human and system-mediated responses.

As cyber resilience technology becomes more common, purchase and maintenance costs for these technologies is likely to decrease. What is not clear yet is whether these technologies would introduce intolerable latencies or changes in productivity. Certainly, improved technology is not a one-size-fits-all opportunity; each institution would have its own peculiar needs and tolerance for cost. Integrating these technologies with human analysis and response may enable the mobilization of defensive actions, including alerting operators, before the human operators are aware of adversarial action. This combination affords the highest degree possible of effectiveness in cyber defense. An important consideration in a risk-based approach that balances cost and benefits will be the cost of *not* using these advanced technologies as they become more available.

5.0 Concluding Thoughts

In the first AiR meeting, participants discussed general properties of asymmetry as it pertains to resilience and the conflict between adversary and defender in complex cyber systems. In this second AiR meeting, the participants explored the details of asymmetry in the cyber conflict using real-world examples. Three key findings emerged with several nuanced facets described in the previous sections. Briefly, these findings are that

1. the cyber terrain itself is primarily responsible for the current asymmetry, so changing it requires changing the terrain itself;
2. this change will likely come from taking advantage of key elements in the defender's perspective; and
3. effective change in this terrain will likely come from a loosely coordinated community response rather than heroic individual cyber islands.

One important implication of this is that we can alter the asymmetric imbalance between defender and adversary through shifting the landscape by

- raising the barrier to entering a defended cyber terrain via collective, incentivized, ubiquitous hygiene;
- raising the cost of moving in this environment via enhanced situational awareness that comes from knowledge of the defender's environment and mission and from the understanding that adversaries must at some point exhibit behavior inconsistent with the mission, and
- reducing the value of success when possible.

In the resilience mindset, defenders must frequently operate without specific knowledge of an adversary. This leads to an inward focus and realization that additional opportunities exist to shift the asymmetric balance. For example, reliance on fight through and achieving mission may make it possible to focus on functionality of the system as opposed to finding adversaries.

6.0 References

Corvin CM. 2015. *A Feasibility Study on the Application of the ScriptGenE Framework as an Anomaly Detection System in Industrial Control Systems*. Master's Degree Thesis, Air Force Institute Of Technology Graduate School of Engineering and Management, Wright-Patterson AFB, OH. Available at http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA622349.

Desso NH. 2014. *Designing a Machinery Control System (MCS) Security Testbed*. Master's Thesis, Naval Postraduate School, Monterey, CA. Available at http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA619487.

Finklea K, MD Christensen, EA Fischer, SV Lawrence and CA Theohary. 2015. *Cyber Intrusion into US Office of Personnel Management: In Brief*. Report No. R44111, Congressional Research Service, Washington, DC. http://digitalcommons.ilr.cornell.edu/key_workplace/1440/?utm_source=digitalcommons.ilr.cornell.edu%2Fkey_workplace%2F1440&utm_medium=PDF&utm_campaign=PDFCoverPages

Hilfiker JL. 2013. *Responding to Cyber Attacks and the Applicability of Existing International Law*. Report No. ADA589333, U.S. Army War College, Carlisle, PA. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA589333

Industrial Control Systems - CyberEmergency Response Team. 2012. "Alert (ICS-ALERT-14-176-02A)." *ICS-CERT Monthly Monitor* 2012(September):1-2. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2012.pdf

Sullivan DT. 2015. *Survey of Malware Threats and Recommendations to Improve Cybersecurity for Industrial Control Systems Version 1.0*. Report No. ARL-CR-0759, U.S. Army Research Laboratory, Dulles, Virginia. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA617910

Team ICS-CR. 2014. "Alert (ICS-ALERT-14-176-02A): ICS Focused Malware (Update A)." *ICS-CERT Monthly Monitor* 2014(July). https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A

Walker D. 2014. "'HAVEX' malware strikes industrial sector via watering hole attacks." *SC Magazine*. http://www.scmagazine.com/havex-malware-strikes-industrial-sector-via-watering-hole-attacks/article/357875/

Appendix A

Meeting Agenda

Appendix A

Meeting Agenda

September 16 (Wednesday)

8:00 – 8:30 a.m. Check in

8:30 – 9:00 a.m. Welcome and introductions Nick Multari

9:00 – 9:30 a.m. Summary of AiR1.0 (Sep 2014) Chris Oehmen

9:30 – 11:00 a.m. Level-setting presentations

Presenters: Ms. Arlette Hart

Dr. Craig Rieger (unconfirmed)

Dr. David Manz (unconfirmed)

11:00 – 11:30 a.m. Division into groups

11:30 – 3:00 p.m. Working lunch and breakout Session 1

Goal: Discuss the group's focused attack, identifying attributes and asymmetric issues. Specifically, discuss what about the attack provided the attacker with the asymmetric advantages and how the advantage could be measured.

3:00 – 4:00 p.m. Group reports and discussion

September 17 (Thursday)

8:00 – 8:30 a.m. Check in

8:30 – 11:00 a.m. Breakout Session 2

Goal: Discuss potential resilience techniques/technologies that could be invoked that would reduce the attacker's advantage. Specifically identify the technology, how it would work, why it would reduce the attacker's advantage, and how the resulting change in asymmetry could be measured.

11:00 – 11:15 a.m. Break

11:15 – 12:00 p.m. Group reports and discussion

12:00 – 3:00 p.m. Working lunch and group discussion

Goal: Discuss the results of the breakout discussions. Examine the technologies identified by multiple groups, why they worked in each scenario and what research is still needed to develop the concept, the effort to actually

develop it and barriers to potential acceptance. Examine technologies identified by only one of the groups and why it may/may not be applicable to the other scenarios.

3:00 – 4:00 p.m. Summary of results and next steps

Goal: Capture major findings and significant new insight that was attained by each participant. What are the key vision components of asymmetric resilience that we think are still viable? What do we think is now not attainable? How does this impact the research agenda that was developed in AiR1.0?

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

U.S. DEPARTMENT OF
ENERGY

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov