2017 Anti-Tamper Conference
Call for Papers

11-13 April 2017
Johns Hopkins University/Applied Physics Laboratory
Kossiakoff Center - Laurel, MD 20723

The 2017 Anti-Tamper Conference is sponsored by the DoD Anti-Tamper Executive Agent in collaboration with the DoD Anti-Tamper Executive Agent Program Office.
2017 Anti-Tamper Conference Theme

Anti-Tamper Implementation: The Good, The Bad, and The Ugly of Systems Engineering

The theme for this year’s Conference is Anti-Tamper Implementation: The Good, The Bad, and The Ugly of Systems Engineering. Anti-Tamper (AT) continues to grow and mature as a systems engineering discipline in the defense industry. Now is a good time to review lessons that have been learned over the last 15 years of Anti-Tamper Systems Engineering. This Conference will focus on the practice of systems engineering for Anti-Tamper and its role in the broader Systems Security Engineering (SSE) world. The Good: what has been successful and why; the Bad: overly prescriptive requirements that limit new technology leverage; the Ugly: performance shortfalls causing unexpected impacts on schedule and cost.

AT Systems Engineering is a unique competency, however our designs exist as part of larger systems that must address a range of protection requirements across the SSE sub-disciplines (AT, Cyber, Supply Chain Risk Management (SCRM), Trust, etc.). As part of this Conference, we will explore the generation and resolution of conflicting requirements across the SSE spectrum.

Ultimately, AT robustness depends on the experience of the designers and the quality of information on threats, electronic component capability, and awareness of recent technology advances at their disposal. This Conference will also focus on Government and Industry plans and recent results in component assessment/acquisition, threat education, and AT system integration training in order to advance the standards of AT and make AT a mission effective part of Department of Defense (DoD) systems development.
We are currently seeking abstracts on, but not limited to, the following topics:

1. **Protecting Open Architectures/Commercial Hardware**  
   Designs to protect sensitive application code running on high-performance Commercial Off the Shelf (COTS) processors so that the open architecture, or COTS, will be protected against tamper attacks.

2. **Utilizing Commercial Intellectual Property (IP) for DoD Capabilities and Lowering DoD/Commercial Barriers**  
   How are exposure risks mitigated to enable application of commercial anti-tamper technology in DoD systems? (Better Buying Power (BBP) 3.0: “Remove barriers to commercial technology utilization.”)

3. **Technology Selection/Readiness**  
   After a program has identified the Critical Program Information (CPI) that needs to be protected, it is now faced with multiple questions, such as: How do programs identify new available AT technologies? What is the maturity for the new AT technology? How viable is the solution? When is an AT technology ready for DoD program insertion?

4. **From TRL 1 to Fielding**  
   Taking an AT technology from a basic principle to a technology that has been proven successful does not come easy. How successful or unsuccessful have projects been? What succeeded/failed and why? Describe technology moving from an idea to a fully assessed product and why some make it and some don’t. What is the “valley of death” and how do you get across it?

5. **Morphing from AT to AT with Information Assurance (IA)/Cyber**  
   How similar are these two disciplines? What is the IA/Cyber community doing that the AT community can leverage to help programs? Are there examples of designs that meet AT and cyber requirements?

6. **Repair Methodologies of AT-Enabled Systems**  
   When broken parts are returned to depot for repair, how do programs provide the correct requirements to properly test and repair the system and return it to the field without accidentally triggering the AT on the system? Provide examples of programs that are successful or unsuccessful with depot level repairs.

7. **Benchmarking**  
   How is the private sector protecting its critical technology? Is the AT community ahead, the same as, or behind the private sector? If the private sector is successful against a certain attack, is there a way that the AT community can leverage these technologies? How can the AT community safely bring in hackers, the private sector, and academia, to discuss AT strategies?

8. **AT Systems Requirements Development (Operational, Contractual, or Program Requirements)**  
   A successful AT program can be traced to solid AT requirements and documentation. A program needs to understand the AT technology that will be added to a system and how that technology will change the requirements as well as how it is developed. What processes are being used across the AT community? How does a program create “good” requirements? What are examples of “bad” requirements that have been used on a program? What steps were taken, or process added, to ensure success of AT system requirements development?
9. **The Good in Anti-Tamper, for example:**
   a. IP integration success stories.
   b. Vulnerability mitigation using new technology development and system architecture.
   c. Examples of effective feedback from Anti-Tamper Executive Agent (ATEA) and why it was useful.

10. **The Bad in Anti-Tamper, for example:**
    a. Missing information I need from the ATEA, contract language, Service Leads, etc.
    b. Why am I doing this? Things programs do based on history that make no sense today.

11. **The Ugly in Anti-Tamper, for example:**
    a. How lack of timely feedback affects cost and schedule.
    b. How lack of an export decision is a decision.

Abstracts due by 11 November 2016
2017 Anti-Tamper Conference

The 2017 Anti-Tamper Conference solicits original, previously unpublished work on a wide range of AT topics of practical value to anyone developing, evaluating, or managing systems with AT requirements. Non-commercial papers from suppliers or universities dealing with new or unique technologies, tools, methodologies, applications and results are also welcome. Papers will be selected for inclusion in the technical program on the basis of relevance and quality of data, technical importance, and interpretation of results. As the audience for the 2017 AT Conference will be composed of Contractor and Government personnel, all papers and presentations must be non-proprietary. All abstracts will be considered for inclusion in the Conference proceedings regardless of whether or not they are selected for presentation. Acceptance is based entirely on the information included in the abstract. Presenters will be allocated 30 minutes at the 2017 AT Conference.

Security

All 2017 AT Conference registrants will be required to submit security clearance credentials to AFLCMC/XZZ. The venue will be at Johns Hopkins Kossiakoff Center. 2017 AT Conference Security will support presentations and discussion up to SECRET//COLLATERAL. All abstracts must be UNCLASSIFIED//FOR OFFICIAL USE ONLY (FOUO). The author should state in the abstract if the intent of the presentation will be at the SECRET//COLLATERAL level.

Abstract Submission

Abstract submissions should consist of a white paper with a maximum of three pages. The abstract can include representative images, figures, and references. Please include sufficient detail to allow for fair evaluation of the work discussed. Submissions must include the following information:

- Author’s complete name, title, and affiliation
- If multiple authors, list the individual that will be presenting the topic
- Complete mailing address
- Telephone number, fax number, email address

Any abstract that is missing any of the above information will be subject to disqualification. Submit your UNCLASSIFIED abstract to: AFLCMC.XZZ@us.af.mil. State “Abstract Submission for the 2017 AT Conference” as the subject email. Additionally, please be sure that the contact information for the person/organization submitting the abstract is included within the body of the email.

UNCLASSIFIED//FOUO Abstracts – Documents should be submitted as an encrypted attachment to an email using the Federal Information Processing Standard (FIPS) 140-2 validated version of Encryption Wizard. The program is available for download at https://at.dod.mil/content/security. An account is required to download Encryption Wizard.
If you don’t have an AT Website Account, please apply for one using the following information:

- Sponsor: 2017 AT Conference
- Sponsor Email: AFLCMC.XZZ@us.af.mil
- Sponsor Phone: 937-255-3520 or 937-255-3554
- Comments: Request an account to download Encryption Wizard in order to submit an UNCLASSIFIED//FOUO abstract for the 2017 AT Conference.

Once encrypted, send the email to the DoD ATEA Program Office at AFLCMC.XZZ@us.af.mil. State “Abstract Submission for the 2017 AT Conference” as the subject email. Additionally, please be sure that contact information for the person/organization submitting the abstract is included within the body of the email. Contact the AT Education and Outreach Office at 937-255-3520 or 937-255-3554, by phone with your encryption key.

**Timetable**

11 November 2016 3:00pm ET (firm) - Abstracts due
05 December 2016 - Notifications of acceptance
03 March 2017 – Presentations due

**Additional Information**

Additional information, including registration details, will be posted on https://at.dod.mil/content/conference as it becomes available. You are welcome to contact AFLCMC.XZZ@us.af.mil if you have any questions.