LLNL-PRES-752916

Summary and Next Steps

Carl Crawford, Suriyun Whitehead
and Harry Martz

ADSA 18 May 15-16, 2018

This research was funded by the Science & Technology Directorate of the Department of Homeland Security (DHS).

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

Was ADSA18 Successful?

- It depends on the metrics you choose, examples include
  - Audience learning about where TSA is headed
  - TSA learning about new technologies/capabilities
  - Number of
    - Attendees
    - Forming partnerships
    - Developed products
    - People working together
    - Enabled DHS sponsorship
  - Increase of stakeholders' participation
  - Spin off of other ADSAs
  - Number of side bar conversations

What Did We Hear?

- Introductions:
  - Emphasis on transition….
  - Security model is outdated; needs to be updated
  - Will the no-fly list be adaptable
  - Need to be careful to think metadata is a panacea
- DHS/TSA Perspectives
  - Guiding docs: TSA Strategy; Administrator's Intent; Capital Investment Plan
  - TSA has a security but not a business plan
  - Need to balance security and passengers experience
  - Government needs to provide a unified front to the public
- DHS/EXD Perspectives
  - Apex screening at speed
  - Engaging industry in new innovative ways
  - Have a list of problems not being addressed
  - Funding portfolio is balanced mix of low to high risk efforts
  - Hacking for Defense (H4D)

What Did We Hear?

- DHS/TSA Initiatives
  - Deployment of AIT resulted in long lines and poor traveler's experiences
  - Firearms discoveries have increased over the last several years
  - Need to reach out to all stakeholders' before deploying new CONOPS: e.g., all small-knives
  - TSA is creating a method like DISARM for prohibited items; list will be prioritized; reduce what is on the list … but air rage (policy).
  - New machine learning projects will be awarded in June/July 2018
  - Advancing Countermeasures Architecture is anew organization at TSA
  - Systems o systems who will architect it
  - New reorg at TSA…4 new deputy administrators
  - How do we architect intelligence, information, etc. to inform our national decisions, systems of systems, etc.
  - We need to disaggregate the current TSEs to do this.
  - Need to accelerate emerging threats to detect in field
  - Disaggregate to have higher functionalities
  - Countermeasures is more than metadata, but metadata is a key component
- Funding Opportunities
  - TSIC BAA, Targeted BAAs, SVIP, SBIR

What Did We Hear?

- DHS/TSA Initiatives (continued)
  - The architecture of a systems of systems will require privacy issues and we need to address it head-on
  - Need to show that the gov't can appropriately handle passenger privacy metadata
  - Concerned that 3rd Parties will need to go through large integrator
  - MOSSA—Modular Screening System Architecture
  - TSA is developing system engineering approaches
  - Adaptable ATRs need to back end to push metadata out, etc.
  - Who owns the data
  - Others open architecture systems:
    - DICOM
    - DoD MOSA
    - DoD FACE
    - DNDO ROSA
    - VA ViSTA
  - DHS's is MoSSA
  - How do we address IP issues, protect it, etc.
  - Voluntary vs. Mandatory DICOM on a volunteer bases did not work so well when VA made it mandatory it developed much quicker

What Did We Hear?

- DHS/TSA Initiatives (continued)
  - When the US develops it strategy does it involve other stakeholders' outside the US? We non-US countries may neve go to open architectures, TBD
  - TSA does consider other countries
  - TSA Biometrics analysis
- Identification of Malicious Intent
  - Technology vs. Human: guns vs. mental health
  - Lone terrorist coming out of nowhere
  - Reaction and trauma and inoculation and resiliency
  - Violence did not help, kindness and compassionate helps turn radicals around…
  - Social media is good and bad
- Deterrence vs. Chatty TSOs
- Security should be without intel.
  - Overreliance on meta-data is dangerous.
  - Focus on physical inspection, not identity inspection.

What Did We Hear?

- Collection and Use of Metadata
  - Metadata is Data about Data
    - Descriptive (What is the data
    - Structural (how is it laid out?)
    - Administrative (when/where/who)
    - Context matters: what is "suspicious" activity?
  - Anomaly detection is used for AT since it is an easier problem
  - Need to solve data, knowledge and control representation
  - How do we protect/enhance civil liberties in a world of meta data?
  - How do we know when someone is radicalized after being accepted by the system
  - Spending too much time scanning everything and not focusing on a select few
  - "You can have my privacy data if everyone else also provides it"
  - Check ethnic bias by articulating TSO observations.
  - Incomplete and inaccurate sources; data volunteered for benefits.
- Legal and Civil Liberties
  - Privacy matters, and personal control
  - Civil consequences of China's Social Credit System
  - Wrt a terrorist's event of course after the fact it is easy to say we should have seen the signs. Not so easy to be predictive
  - Given the lack of aviation security events it is hard to determine how well our system works. How do you know we are reducing risks if you cannot measure it?
  - Does not like precheck. Never enough data to determine if TSAs predictions are correct
  - Airline security tends to permeate outwards, we see metal detectors at sports, concerts, etc. area

What Did We Hear?

- But never enough data, and some approaches… (rare events, machine learning).
- Cybersecurity
  - Commercial practices for cyber security trends
  - Prevent, detect and respond to advanced cyber-security events and protect critical components
  - Different domains Secret, Top Secret, etc. Air gap solutions…
  - IT and OT should be considered two different domains and should be treated differently but may be fused/mixed somehow
  - Use Guard technology…
  - Baseline Risk Mitigation Strategies by committee (e.g. NIST 800 and "Best Practices“) are not sufficient against zero-day threats.
  - Statistical analysis does not work for zero-day attacks
  - Asymmetric threats. Breaking in, subverting.
- Development Methods and Financial Implications
  - Used Battelle’s DICOS A-A interface for their Low Dose CT Challenge
  - Prize competitions; are bragging rights worth it?
  - Confidence-based predictions empower TSA’s risk-based Screening goal
  - How will this be shared with industry so they can learn what was done, results obtained, etc.
  - Bomb goes off on an aircraft and 2 people die plane was able to land. Indirect impacts: $13.1B over fist 2 years. 9x direct impacts
  - If we are concerned with protecting life then we need to look at tobacco use, diabetes, etc.

What Did We Hear?

- Development Methods and Financial Implications (continued)
  - We are more concerned with economic impacts than loss of life
  - Work on the mindset of the public…Pre-crisis inoculation risk communication may increase public resilience by accelerating recovery after attack
  - TSA has funded $900k for two CT at the checkpoint.
  - Large sums of funding for checkpoint CT over the next 5 years.
  - Estimated security market growth (facial recognition, checkpt CT, etc.) is ~5%/yr.
  - Recommend that TSA continue to have meetings where OEMs can meet 3rd party developers.

- Deep Learning & Other algos
  - Medical CNN methods may apply to security problem
  - Passengers walking, no divestiture, lower false alarms, automatic and adapting dynamically
  - May be able to distinguish explosives from other non-threat organic materials. Some questions were raised whether this is true.
  - Face recognition on the move in two cases: uncooperative (surveillance) and cooperative
  - Replace the boarding card with face recognition
  - ADSA has helped Marc ramp up in this area and make connections.
  - Only needed a few 100-1000 data sets for training
  - Used Universidada Catholica de Chile, Santiago open data sets and OPTA and TO4 and TO3 (segmentation) data sets.
  - YOLO-You Only Look Once—Approach (Joseph Redmon et al.)
  - Showed results for YOLO vs. holistic training approaches.

What Did We Hear?

- Development Methods and Financial Implications (continued)
  - Possible Needs
    - ability to track passengers from the time they purchase tickets
    - Correlate passengers to bas
    - Risk based screening
    - Queue management and data analytics
  - Potential Solutions:
    - Have unique IDs; use GPS/Google; tie peoples objects to their IDs
    - Queue management based on peoples' cell phones
    - Create an app; smart cities initiative could apply this to airports
    - Create an ID that would avoid privacy issues
    - Notion of smart address used for other applications and bring it to the airport scenario.

- Airplane Cargo Panel
  - Shippers are responsible for their own Cargo screening; but it is qualified by the government, TSA
  - Printer and Australian scenarios were cargo issues
  - Metadata could be used for Cargo screening, automated targeting, etc.
  - CT can be used for skids 48" x 48" and pallets 109" x 109"
  - Cargo environments are nasty, they are very hot, very cold, dirty, humid, etc. Air cargo needs more rugged cargo screening machines
  - Have radiographic x-ray, ETD, etc. machines
  - Need to be able to see inside oil drums
  - If we can increase screening throughput then the cost is not so much of an issue

What Did We Hear?

- Deep learning & Other Applications (Part II)
  - BNNs for anomaly detection
  - Anomalies:
    - Appearance
    - Semantic
    - Appearance given Semantics
    - Relative
    - Passenger relative
  - Data in high dimensions all looks the same, such as pictures of faces
  - Anomaly detection has a role alongside threat detection
  - Transfer of representations
  - Build x-ray systems first responders systems
  - Single-energy for materials discrimination
  - Multi absorption plate (MAP) a structured filter enables materials discrimination
  - Look for the IBEX patent
  - Overlay materials image over the single energy image.
  - Shadow of MAP removed from the image.
  - Adapt a 3D piloted OSARP
  - Certify protocols; then fold into ATRs

What Did We Hear?

- DICOS Deployment and Open Architecture
  - To be constructed
  - We need real world implementations
  - Software innovation is a faster path than hardware iteration
  - Needs static or increase revenue streams.
  - Natural tension between the government's need for open system and industry's investment and need to protect IP.
  - Mandatory vs. voluntary participation, commitment and execution.
  - Need to be more adaptable instead of tearing out a box and not having the next box fit in right.
- Trace Detection and Meta Data
  - Temporal / Environmental / Sample / operator / Instrument metrics
  - Legally save meta data?

What we need to hear more about

- How meta data can
  - Enhance privacy
  - Invalid privacy
- How to exploit meta data to improve operations
  - Airport can use it, FSD can use it, resource allocation
  - Speed a passenger's journey – e.g. if I have a known hip replacement.
- How will the adversaries exploit meta data
- Business Models for 3rd parties
  - IP, etc.
- How do can algorithms find something that hasn't happened yet?
- How will Deep Learning be integrated and certified into security operations
- What are the risks or spectacular failures of Deep Learning in security?
- What are specific formulations of cargo screening problems that can be addressed by CT?
- How to manage disaggregation
  - Who takes responsibility for integration
- How to certify / test open architecture platform and solutions
- How DoD tools and approaches can align to TSA budgets and environments
- Where will the system fail spectacularly?
- What does be compliant with DICOS format mean?

What we did not hear?

- Not clear what DHS S&T and TSA needs are
- How 3rd parties, industry and TSA can dialog directly and participate in requirements development
- A cohesive vision from TSA – reimagining, redesigning and implementing security from a customer focus
- Filtering the metadata noise, errors, etc.
- Where is DICOS for wrt A-A
- How to fuse data, metadata.

ADSA19 – Oct. 16-17, 2018

Adaptability

- Adversary
- SOPs, OONOPS
- Training data
- Testing data
- Metrics
- Deterrence
- Red Team testing
- TSOs testing
- ATR: Deep learning data required
- AATRs
- Behavioral Detection Officer
- Limited data, statistics, etc.
- Fused systems
- Cyber security
- Random dynamic systems
- How do you test we are spending funds effectively
- Harmonization
- Others?