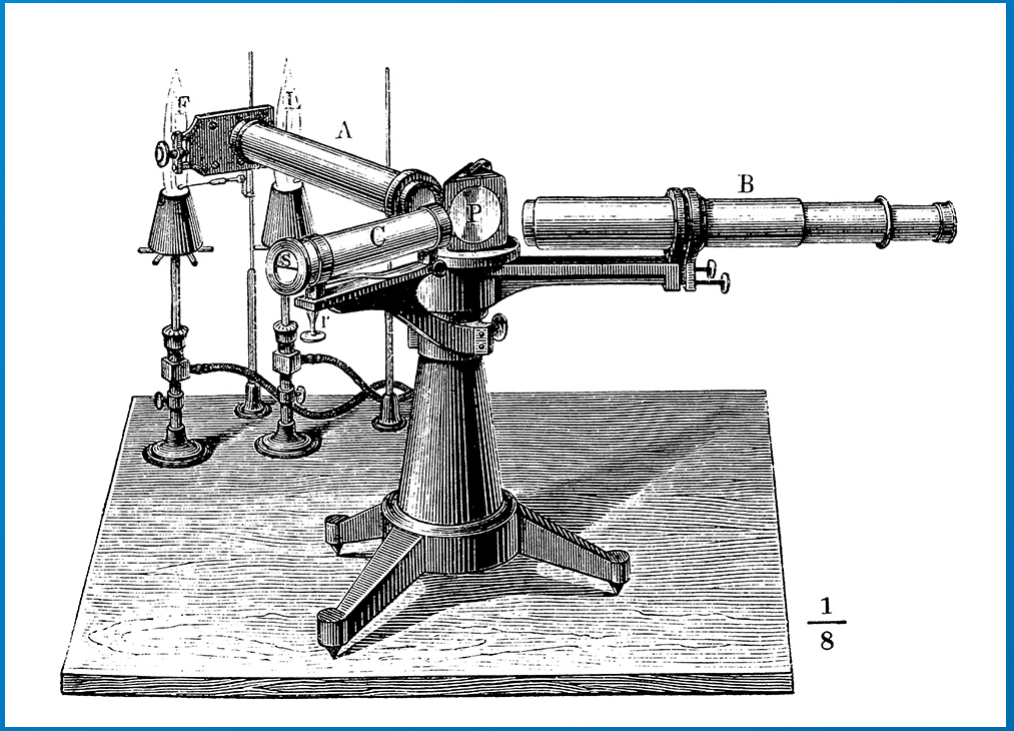

2 May 2017
Macro Security
Matthew Merzbacher
smiths detection
bringing technology to life

Overview

- Big advances in detection are increasingly rare
  - Perhaps no longer possible
  - Even if possible, take a long time to enable
- Current situation is not sustainable
  - Passenger volumes continue to rise
  - Passenger expectations continue to rise
  - Terrorists haven’t given up and change tactics
  - Budgets are under scrutiny
- What can we do?
  - Look at the bigger (macro) picture!

Hypothetical Premise: No more big leaps in detection technology

- Why?
  - None available
  - No need
  - Cost
  - Bad timing
- Does this matter?
  - To security industry
  - To aviation industry
  - To academia
  - To public
  - To regulators
  - To politicians



- Can we draw general conclusions about whether it matters to each of these groups?
- **What big security improvements can be achieved if there are no technological silver bullets (or even lead bullets) left, and how do we achieve them?**
  - Oh, and what if the premise is wrong?

Macro Security

- End-to-end architecture to capture the security process from ticket purchase to arrival at final destination
  - Passenger info (Meta-Data)
  - Threat info
    - Rapid change & deployment
  - ConOps (including screener)
  - Updated hardware and, more importantly, software
    - Support both transformational and incremental changes
  - Performance Model for decision making
    - Connects policy and implementation
  - Assessment & Reporting
  - Testing
  - Validation of all components
    - Including Data and Meta-Data
  - Enable and practice regular gap analysis

Some examples

- Manage threat envelope upward, downward, sideways
  - Remove / Replace / Add material
  - Increase / Decrease mass thresholds
  - Change detection expectations
  - Allow holes, argue about the size and location of the holes
- Increase use of meta-data to clear more passengers
  - How many times do I need to fly before I'm accepted as "safe"?
  - How many times do I need to be cleared?
  - How about my Mom?
  - Is screening me (or my Mom) effective use of funds?

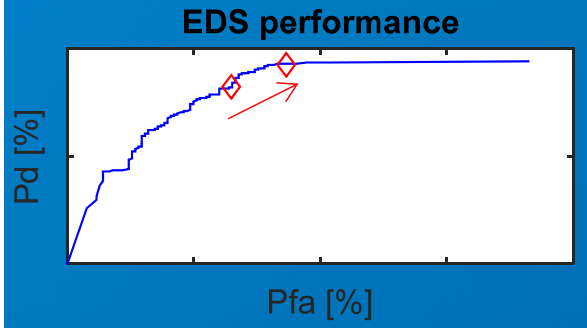
More examples

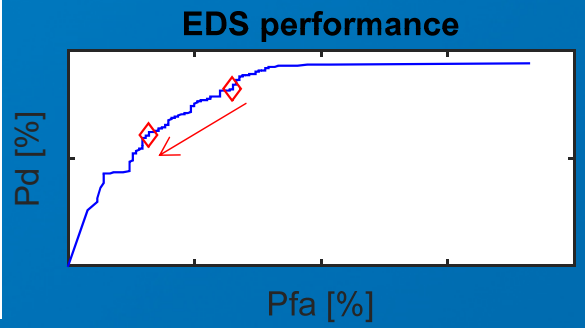
- Replace screener with algorithm
- Less rigid ConOps
- Deterrence
  - Randomized tactics (Algorithms / Devices / ConOps)
- Passenger green teams
- Predict (through meta-data) what a passenger is carrying, so that the problem becomes quick look validation instead of generalized detection
- Identify “creative” ways to extend existing tools (possibly locally sub-optimally)
- Revise testing methodologies
- Ban luggage (or send through alternate means)

One more example

- Use Risk to manage decision

Sensor/Action	Characteristics
Passenger Classification (Low/High)	P(High Threat Class Assigned|Threat Passenger) = [redacted] P(High Threat Class Assigned|No Threat Passenger) = [redacted]
Passenger Classification (Low/Mid/High)	P(High Threat Class Assigned|Threat Passenger) = [redacted] P(High Threat Class Assigned|No Threat Passenger) = [redacted] P(Med Threat Class Assigned|Threat Passenger) = [redacted] P(Med Threat Class Assigned|No Threat Passenger) = [redacted]
Attack Prior	P_0(Threat) = [redacted]
Level 2 (OSR)	PD = [redacted] PF = [redacted] $/bag = [redacted]
Level 3 (ETD)	PD = [redacted] PF = [redacted] $/bag = [redacted]
Post-Level 3 Inspection	PD = [redacted] PF = [redacted] $/bag = [redacted]
Clearing a Bag	PD = [redacted] PF = [redacted] $/bag (Stream of Commerce) = [redacted] $/bag (Threat) = [redacted]





Risk-Based Screening Architecture with Partially Observable Markov Decision Process (POMPD)

DHS, S&T Directorate, Explosives Division, Contract HSHQDC-14-C-B0042 (BAA 1305)

smiths detection

Where can we focus?

- Everyone wants sufficient detection
- If we have sufficient detection, why bother improving?
  - Gaps will surface
  - Things change
  - The status quo may not be sustainable
  - “Sufficient” could vary by situation
- What else is needed, beyond detection?
  - Passengers: Quicker and more seamless experience, Understanding of the tactical process
  - Regulator/Operator: Lower cost (overall and per PAX), Understanding of the strategic process
  - Industry: Continued opportunities, Low-overhead processes
  - Academia: Problems to be solved, Transition partners
- Macro Security: Extend the solution domain to enable transformational change

Requirements

- Acceptance that security is not perfect
  - Public
  - Politicians
- Model to sustain makers of boxes and/or brains
- Language to describe problems and support collaboration
- Get it right
  - Or at least, don’t get it wrong

- **Need a Hippocratic Oath for Security**

A thought that had no better place

- Can we learn from self-driving cars?
  - Question: Will we see self-driving cars during our lifetime?
  - Meta-Question: Has your answer to that changed in the past five years?
  - How will Google make money?
  - Maybe there's more to be squeezed from X-Rays after all

Concluding remarks

- The tactics are critical, but off topic
  - Network support, DICOS, Cyber-security
- How do we handle problems without evident solutions?
  - Hide them / Admit them / Deny them
- If we tolerate imperfect detection, how should we design systems?
- Can Macro Security work?
  - Of course, but requires collaboration and will
- How do we have a continued conversation?
- How do you decompose the problem into pieces that can be attacked?
- How do we build a strategy to create a strategy?
- **Need a Hippocratic Oath for Security**
- How do we prepare for a disruptive solution?
  - Don’t try to predict the disruption, it won’t come from where we expect