Why Airport Security Can't Be Done FAST

Semon Rezchikov, Joshua Engelman, Morgan Wang

Hi, DEFCON 19!

Here, we've compiled an outline of a small portion of the information we found and a detailed list of our sources in case you're interested in reading more about the FAST program. (Or about MALINTENT or Hostile Intent or SPOT or whatever else.) We thought you'd find this more useful than the slides to our presentation, as (if you recall) we presented most of the information verbally, using the slides only as a visual counterpoint. In fact, our slides are mostly cute pictures of bunnies and puppies and trailers and TSA agents, which works great during DEFCON but isn't so great if you want to continue research outside of it.

Our sources are broken up as follows: The articles on SPOT, Criticism of FAST, the legality of FAST, base rate fallacy, articles on FAST, Government Documents, and Information on SDS, the Israeli version of FAST. All of the documents are in the public domain and can be found using some creative Googling.

- Semon, Morgan and Josh

Outline

FAST - Future Attribute Screening Technology

Run by DoD's Behavioral Research Unit

A series of rooms that use biometric scanners analyze your physiological signs while someone questions you try to detect whether someone passing through the FAST system intends to blow something up - Pretty much a polygraph test on steroids

People: Check out http://www.dhs.gov/files/programs/gc_1218480185439.shtm

It seems that FAST is being developed at Draper Labs (so the trailers indicate)

Relations of various projects to each other:

Project MALINTENT: the overarching project to detect malintent

Hostile Intent: The actual technology that can detect malintent

FAST: a trailer with a packaged, practically usable form of malintent detection technology

History:

Paul Ekman did a lot of research into faces and is known for his work on microexpressions. (He's the guy the TV show Lie to Me is based on) He believes that things like detecting deception through face-reading can be made reliable through proper training.

SPOT (Screening of Passengers by Observational Training) is a program largely based on Ekman's research (he did a lot of the initial training for the program himself!) which trains some TSA agents in Ekman's face-reading curriculum. These "Behavioral Detection Officers" can then be called in to interrogate people. There seems to be no evidence that the program has ever led to the conviction of a terrorist; all of it's convictions seem to be related to other crimes like drug dealing. They may also be simply chance; they process quite a few people. The program has cost more than $212 million PER YEAR since it's inception, and the Obama administration wants to raise this to $232 million for 2011.

How FAST works:

A person enters a FAST trailer, say, in the airport.

While they are being scanned by the following sensors:

"BioLIDAR" for cardiovascular/respiratory data; infrared camera for stress; normal camera for pupil dilation, reddening, and facial expressions; motion detectors for gait analysis

they are asked a set of questions (like "Are you planning to detonate a bomb in this airport?"). If the machine flags them as suspicious, they have to go through it again. If they are flagged again, they may be taken away for questioning, or even arrested.

Issues:

False positives:

Because this is a system that processes large numbers of people it must have a VERY LOW FALSE POSITIVE RATE. Even a rate of 0.1% is terrible because of the tremendous amount of travelers; the system would arrest many, many, many innocent people because terrorists are so incredibly rare. The FAST false positive rates seem to between 1% and 17%, depending on which source you look at.

Research methodology:

Subjects were told to act "shifty and evasive" - not a great way of calibrating your instruments when you are trying to detect fine biometric differences. Essentially, the subjects are being told something like “Pretend you are a terrorist when you go through this apparatus.”

We do not know what sort of populations they have been calibrating baseline biometric measurements to. People who are sick can have very abnormal baselines.

Hacks:

Get someone who is normally sick to commit the crime. Certain types of heart arrhythmia and similar illnesses that screw up biometrics may pose an issue to the system.

Beta-blockers can artificially baseline you - they bring people to an emotional midline.

Legal -- Fast and the Fourth Amendment:

In 2010 Lindsey Gil wrote an article for the Boston University Journal of Science and Technology Law. In this article, Gil presents the main types justifications for searches without a warrant. http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume162/documents/Gil_WEB.pdf

The Plain View Doctrine

Eyes, Smell, and “sense enhancing tools” (like aerial surveillance and drug sniffing dogs, are acceptable (Coolidge v. New Hampshire, Cupp v. Murphy, and Horton v. California)

Thermal imaging cameras to see what’s happening in your home are not acceptable. (Kylio v. The US)

Administrative Search Exception

A search which is “conducted as part of a regulatory scheme with a defined adminstrative goal, rather than targeted at a specific individual.” (United States v. Davis)

Current airport security falls under this exception.

Medical Privacy Laws

The US has very strict medical patient confidentiality laws. As FAST consists of many aspects of a medical exam, one could argue that the gathering of such personal medical information is a violation of medical privacy laws.

In conclusion, it is highly likely that FAST would make it through any initial government legality check. (this is the Government we’re talking about), however a team of good lawyers could easily put up a strong case against it.

Suspect Detection Systems: a private Israeli outfit that is developing a biometrics system similar in goal if not in size and scope called Cogito. They have published their results.

Sources

SPOT: Links

Weinberger, S. (2010, May 26). Airport Security: Intent to Deceive?. Nature, 456, 412-415. http://www.nature.com/news/2010/100526/full/465412a.html

Malkin, M. (2011, April 8). See SPOT FAIL. The National Review Online. Harwood, M. (2010, May 21). http://www.nationalreview.com/articles/264214/see-spot-fail-michelle-malkin

Terrorists Slip Past TSA's Scientifically Untested Behavioral Threat Detection Program. Security Management. Retrieved from http://www.securitymanagement.com/print/7158

Harwood M. (2010, December 23). $385 Million TSA Program Fails to Detect Terrorists. Truthout, Retrieved from http://archive.truthout.org/385-million-tsa-program-fails-detect-terrorists66213

CBS News. (2009, October 8). TSA Screening is Security Theater. 60 Minutes. Retrieved from http://www.cbsnews.com/stories/2008/12/18/60minutes/main4675524_page4.shtml?tag=contentMain;contentBody

Keteyian, Armen. (2010, May 20). TSA's Program to SPOT Terrorists a $200M Sham? CBS News. Retrieved from http://www.cbsnews.com/stories/2010/05/19/eveningnews/main6500349.shtml

Criticism:

Protecting Individual Privacy in the Struggle Against Terrorists: a framework for program assessment. (2008). Washington, DC.: National Academic Press. epic.org/misc/nrc_rept_100708.pdf

Meijer, E. (2009). A Call for Evidence-Based Security Tools. Open Access Journal of Forensic Psychology, 1(1) 1-4. http://web.me.com/gregdeclue/Site/Volume_1__2009_files/Meijer%202009.pdf

BBC. (2009, July 6). Go Figure: Different Ways of seeing stats. BBC Magazine. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/magazine/8153539.stm

Appelbaum, P. S., M.D. (2007) Law & Psychiatry: The New Lie Detectors: Neuroscience, Deception and the Courts. Psychiatric Services, 58, 460-462. http://ps.psychiatryonline.org/cgi/reprint/58/4/460.pdf

Greenwald, H., & Heckman, K. (2010). Deception: The Quest for Detection. MITRE's Envision, 2, 6-7. http://www.mitre.org/news/envision/winter_10/greenwald_heckman.html

Aikins, D.E., Martin, D.J., & Morgan, C. A. III. (2010) Decreased Respiratory Sinus Arrhythmia in Individuals with Deceptive Intent., Psychophysiology, 47(4), 663-6 http://www.ncbi.nlm.nih.gov/pubmed/20230501

Legality

Gill, L. (2010). Bad Intent of Just a Bad Day? Fourth Amendment Implications Raised by Technological Advances in Security Screening. B.U. J. SCI & TECH Law, 16(2). http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume162/documents/Gil_WEB.pdf

Base Rate Fallacy

Heuer, R. J, (1999). Psychology of Intelligence Analysis. Washington, D.C: Center for the Study of Intelligence, Central Intelligence Agency. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/index.html

FAST

Barrie, A. (2008, September 23). Homeland Security Detects Terrorist Threats by Reading Your Mind. Foxnews.com, Retrieved from http://www.foxnews.com/printer_friendly_story/0,3566,426485,00.html

Eaton, K. (2008, September 24). Homeland Security's 'Hostile Thoughts' Detection System Dubbed FAST, Not Pre-Crime. Gizmodo. Retrieved from http://gizmodo.com/5054119/homeland-securitys-hostile-thoughts-detection-system-dubbed-fast-not-pre+crime

Cheung, H. (2008, September 24). Homeland Security testing 'mind-reading' checkpoints. TG Daily, Retrieved from http://www.tgdaily.com/technology/39464-homeland-security-testing-‘mind-reading’-checkpoints

Marks, P. (2008, September 23). 'Pre-Crime' detector shows promise. New Scientist, Retrieved from http://www.newscientist.com/blogs/shortsharpscience/2008/09/precrime-detector-is-showing-p.html

Underhill, K. (2008, November 19). DHS Says Scanners Successfully Detect "Mal-Intent". Lowering the Bar. Retrieved from http://www.loweringthebar.net/2008/11/dhs-testing-hos.html

Segura, L. (2009, December 9). Homeland Security Embarks on Big Brother Programs to Red our Minds and Emotions. Alternet, Retrieved from http://www.alternet.org/story/144443/

Cherry, S., & Corley, A. (2010, January). Loser: Bad Vibes. IEEE Spectrum. Retrieved from http://spectrum.ieee.org/computing/embedded-systems/loser-bad-vibes

Kahn, M. (2009, October 12). How Things Work: Future Attribute System Technology. The Tartan, Retrieved from http://thetartan.org/2009/10/12/scitech/howthingswork

Government Documents:

Rubin, Philip E. Ph D. Interview by Subcommittee on Investigations and Oversight Committee on Science Space and Technology, U.S. House of Representatives. 2011, April 6. http://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/2011%2004%2001%20RubinTestimony.pdf

U.S. Homeland Security. DHS Privacy Office. (2009). Annual Report to Congress 2008-2009. Washington, DC: U.S. Government Printing Office. http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf

U.S. Homeland Security. Human Factors Division: Social-Behavioral Threat Analysis-EAST (2008). S&T Annual Stakeholders Conference. Washington, DC. http://www.dtic.mil/ndia/2008homest/hsre.pdf

U.S. Homeland Security. Human Factors Division: Social-Behavioral Threat Analysis-WEST (2008). S&T Annual Stakeholders Conference. Washington, DC. http://www.dtic.mil/ndia/2008hls/Breakouts/511AWed/breakout23HFDSocialBehavioralThreatAnalysisResearch_LAstakehold.pdf

U.S. Homeland Security. Office of Innovation/Human Factors Division. (2007). S&T Annual Stakeholders Conference. Washington, DC. http://www.homelandsecurity.org/StakeholdersMay07/Br40_Burns.pdf

Robert, B. P. (Science and Technology Directorate.). (2008, December 15). Privacy Impact Assessment for the FAST Project. Washington DC. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf

U.S. Homeland Security. Science and Technology. (2007, February 1). Broad Agency Announcement FAST Demonstration Laboratory. Washington, DC. http://www.wired.com/images_blogs/threatlevel/files/001_BAA07-03A_FutureAttributeScreeningTechnologyFASTDemonstrationLaboratory.pdf

Burgoon, J. K. Ed. D. (2004, March 19) Automated Detection of Deception and Intent. www.apa.org/about/gr/science/advocacy/2004/burgoon.ppt

Walker, Starnes. (Director of Research) U.S. Homeland Security. Science and Technology Directorate. (n.d.) DHS Science and Technology: Enabling Technology to Protect the Nation. Washington, DC.
www.ametsoc.org/boardpges/cwce/docs/2007-03/.../WalkerStarnes.pps

Department of Homeland Security. (2008, July 24). Department of Homeland Security Meeting: Implementing Privacy Protections in Government Data Mining. http://www.dhs.gov/xlibrary/assets/privacy/privacy_datamining_July24_2008_minutes.pdf

Suspect Detection Systems

Crane, D. Cogito1002 Terrorist Detection System: The Future of Airport Security Defense Review. Retrieved from http://www.suspectdetection.com/DefenseReview.html

Karp, J., & Meckler, L. (2006, August 14). Which Travelers Have 'Hostile Intent'? Biometric Device May Have the Answer. Wall Street Journal. Retrieved from http://online.wsj.com/public/article/SB115551793796934752-dM6lGSA11wU84eqSiLRwgCPR2ac_20060912.html?mod=tff_main_tff_top