SAE INTERNATIONAL

Counterfeiting, Supply Chain Security, and the Cyber Threat; Why Defending Against Counterfeit Electronics is No Longer Enough

2014-01-2125
Published 09/16/2014

Janice Meraglia and Mitchell Miller
Applied DNA Sciences Inc.

CITATION: Meraglia, J. and Miller, M., "Counterfeiting, Supply Chain Security, and the Cyber Threat; Why Defending Against Counterfeit Electronics is No Longer Enough," SAE Technical Paper 2014-01-2125, 2014, doi:10.4271/2014-01-2125.

Abstract

Counterfeit items can be viewed as the by-product of a supply chain which has been compromised. While many industries are impacted, certain types of products can mean the difference between life and death. Electronics are of special interest, however, mechanical parts can also have dire consequences. The point is that the counterfeiting community is very diverse. The business model is fluid and unrestricted. Electronics today…hardware tomorrow. All of this leads to the need for an authentication platform that is agnostic to product. Most supply chains would benefit from a technical way to have assurance of authenticity - a benefit that could be shared by all. A comprehensive marking program, such as SigNature DNA, offers value to all supply chain participants as outlined below:

- Manufacturers will have the ability to effectively monitor their legacy components
- Authorized distributors will have an absolute way to verify and accept returns
- Defense contractors and agencies will have forensically authentic and traceable inventory at their disposal
- End users will have the power to authenticate stock to the component level

Background

In August, 2008, with the Iraq and Afghanistan wars still raging, a squad of Kentucky National Guard engineers struggled as they worked on several OH-58 A/C Kiowa helicopters, bound for battle.1 The problem was a handful of aviation locknuts used to secure the main rotor shaft on the choppers, parts of an assembly so critical that chopper pilots sometimes call them, “Jesus Bolts”. As the official description put it later, “The locknuts were flight-critical because the failure of the main rotary assembly could be catastrophic, resulting in death or serious injury to military personnel.”

But the fit and finish of these critical parts were not right and the Guardsmen were suspicious. As it turned out, their skepticism was well-founded.

The locknuts were indeed defective - and they were counterfeit. More than that, the package of eight thumbnail-sized defective pieces was only the tip of a counterfeiting iceberg. By 2011, a US Department of Justice investigation had zeroed-in on the bad guys: a counterfeiting “laundering” operation known as Kustom Products, who were soon indicted for selling defective, counterfeit and non-conforming products on at least 392 Department of Defense contracts totaling more than $7.5 million. Aside from the aviation locknuts, Kustom sold 180,000 clamps for the engine thrust reverser on C-5 military transport jets, while the company also made substantial profits on 22 contracts with the Army to provide truck parts for combat and tactical vehicles.

Beyond Electronic Parts

Incidents like these have attracted some publicity, but for several years, the focus on counterfeits in the military supply chain has been squarely on electronics. There is surely good reason for this concern, which these authors and many others have documented thoroughly. All this is coming to a head with electronics as the target of a new DFARS Final Rule, D-055, published May 6, 2014.2

Yet the crisis of counterfeits infiltrating the supply chain has gone far beyond electronic components. Hi-rel parts like the locknuts in the Kustom Products case - which could mean life or death if they are defective - have come along with the tide. The US Defense Logistics Agency (DLA) has published a heat map of parts which are sensitive and vulnerable - a graphic which is truly stunning (see Figure 1).

Figure 1. Assess Supply Chain Risk, Source: DLA

The list ranges from fasteners, to fire control equipment, weapons, automotive axles, and brake parts. On the map also are piping, wiring, cables and certain industrial materials, all of which threaten military and aerospace infrastructure.

Recent Department of Defense (DOD) memos also pointedly broaden the target beyond electronics. April, 2013, DOD Instruction (DODI) No. 4140.67, the "DOD Counterfeit Prevention Policy," anticipating the DFARS Final Rule cited above, responded to the National Defense Authorization Act (NDAA) for Fiscal Year 2012, Section 818.3

The DODI, unlike the DFARS Rule, has as its target, DOD components, not their suppliers. Its aim is to establish policy and guide the internal DOD organizational response as the DFARS rule is implemented. To our present point, the DODI explicitly states that its anti-counterfeiting efforts apply to *"any form of at-risk materiel and at any level of the DOD supply chain"* (our emphasis). The memo goes far beyond electronics, mentioning weapon systems, communications systems, and other areas of high-reliability.

The new DFARS Final Rule is only the beginning of a sweeping government effort to clean house against counterfeits, across the board. This effort, which we believe is not perfunctory and will gain traction, is driven both by the vulnerability of infrastructure and materiel and perhaps especially because of the connection between preventing counterfeits and cyber security, a subject to which we will return and which deserves attention.

Any technologies now being considered and adopted against electronics, should also in a broad way, be capable of preventing a much broader swath of counterfeited materiel.

An industry consensus standard would establish the foundation from which any technologies adopted would provide a single authentication solution against counterfeits. Such technologies should support the new regulations and be capable of wide versatility, including but not limited to electronic parts. To ignore this need, and focus solely on electronics, would be short-sighted indeed, and could catch prime contractors behind the eight ball as the effort picks up steam. It has taken years to reach the point where laws, standards, regulations and technologies are finally at the ready against electronics; no one wants to repeat this long cycle again.

All that said, it is fair to ask why the new DFARS Final Rule D-055, is limited to electronics. Indeed, in one section - that which defines a counterfeit part - the Rule makes a point of narrowing the definition to electronic counterfeits, whereas in its first draft, the definition was not limited.

The answer, in our opinion, is that DOD is itself taking a risk-based approach to counterfeiting, just as the Final Rule encourages a risk-based approach to avoidance and detection of electronic parts. Counterfeiting in electronics is a clear and present danger; it must be attacked first. But it is, in the bigger picture, only a portion of the foreground.

Also, time has passed. The DFARS Final Rule D-055 is of course a partial implementation of NDAA legislation passed 2012 and 2013, and owes its lineage more fundamentally to a Senate Armed Services Committee hearing and investigation in 2011.4 Much has changed in the nearly three years since. Events both man-made and from natural causes have made the vulnerability of our infrastructure grossly apparent. Even more immediate has been a rapidly growing awareness of cyber threats. We learn about new cyber attacks seemingly by the month; and it is disconcerting to deduce the occurrence of attacks not disclosed due to national security.

Counterfeiting poses severe threats to both infrastructure and cyber security (two areas which are themselves closely related). A key document was issued in January, 2014, as a Joint Report between the Department of Defense and the General Services

Administration[5]. It emphasizes the "nexus" between counterfeiting and cyber threats, and goes on to make specific recommendations concerning protection of the supply chain, especially information- and communications-related equipment.

In one section, the Joint Report states: "This recommendation is intended to be harmonized with the ongoing DFARS rulemaking entitled 'Detection and Avoidance of Counterfeit Electronic parts'".[6]

Taken as a whole, the Joint Report moves considerably beyond electronics to the fundamentals of a holistic supply chain security outlook, where counterfeiting is one, albeit very dangerous, element.

What has changed, then, since 2011, is surely not the importance of mitigating the risk of counterfeit electronics, certainly more critical than ever, but first, the merging of counterfeit threat with cyber threat and second, greatly heightened awareness of counterfeiting as a part of supply chain security over a broad range of vulnerable materiel.

A Single Authentication Platform and the Role of a Standard Anti-Counterfeiting Mark

Some months after passage of NDAA for Fiscal Year 2012, Section 818, SAE published a paper by the present authors entitled "Traceability in the Age of Globalization, A proposal for a marking protocol to assure authenticity of electronic parts."[7] In the paper, we urge adoption of a standard anti-counterfeit marking protocol which would assure the authenticity of high-reliability electronics.

Today we would extend the proposal for a standard anti-counterfeiting mark - more urgent than ever - to cover high-reliability materiel, not only electronics.

We believe the details of the mark remain the same: we urged the application of a mark at the unit level, that is, on each electronic part at the point of manufacture. The mark would carry information detailing the origin of manufacture, a date range, and perhaps other identifying data, and would be robust enough to travel and survive the entire length of its intended supply chain. Marks would be optionally available to verify distributor nodes (including the ability to handle legacy parts), completion of testing protocols, parts integration and to verify end-of-life, the latter treating the disposal phase.

The standard should specify that any marking technology must be market ready and readily available. This standard also must be held to the performance standards of the item which it protects.

It is now clear that such a marking standard should apply to more than electronic parts, but to potentially any vulnerable element in a supply chain. It would be a single marking protocol to assure the authenticity of materiel.

The marking standard as we have stated, cannot specify any particular technology. But our views on this are of course informed by our own experience, with our SigNature® DNA technology, required since November 2012 by the Defense Logistics Agency for suppliers of Federal Supply Class 5962 (Microcircuits).[8]

Impact of SigNature DNA Marking

We believe that the need and appetite for such a mark is demonstrated by the impact of our SigNature DNA. As of May, 2014, the platform is in use by 30 defense contractors, and 3 Industrial Prime Vendors (Lockheed Martin, SAIC and Herndon). DNA marking was the only technology specifically referenced in the October 2013 Industrial Capabilities Report to Congress, published by the Department of Defense. Recently, the House of Representatives passed a version of the NDAA for Fiscal Year 2015 including language directing DOD to update Congress on its anti-counterfeiting efforts, specifically naming initiatives for marking with deoxyribonucleic acid (DNA). On June 12, 2014, the House of Representatives commended NASA for its proactive use of DNA Authentication Marking.

Also last year, the Defense Logistics Agency published a statement saying DLA was "…exploring [SigNature] DNA marking, along with other technologies as a possible solution to mitigate counterfeits in these high risk items:

- FSC 3110, Bearings (Aviation)
- FSC 4730, Fittings, Hoses, and Tubes (Land & Maritime or L&M)
- FSC 5325, Fasteners (Troop Support)
- FSC 5935, Electrical Connectors (L&M)
- FSC 5961, Semi-conductor Devices (L&M).[9]

Admittedly, calling for a marking standard that can handle much more than electronics is raising the bar significantly. The idea contrasts sharply with that underlying most proposals, which have been quite specific to electronics.

However, our experience with DNA marking shows that a marking platform can, in fact, be designed to protect a vast range of substrates, of varying footprints, and in highly differentiated thermal, radiation, and other ambient conditions.

Some examples:

1. We have demonstrated significant experience applying SigNature DNA authentication marks with polymeric inks on metal plating such as gold, electroless nickel, electrolytic nickel (in accordance with MIL-C-45204b, AMS-C-26074 and, AMS-QQ-N-290, respectively), alumina and epoxy surfaces for FSC 5962. Similar processes can be developed to mark on ceramic, metal, alloy and other plating surfaces on parts such as coaxial cable connectors, resistors, capacitors, and enclosures for electric and electronic equipment.
2. SigNature DNA is presently used by the Swedish National Railway, to mark copper in Sweden and the UK, protecting against copper theft at the national rail system. Similar processes can be developed to mark connectors, bare wires, waveguides, etc.[10]

3. We have demonstrated incorporating botanical DNA into polymeric coatings for guitars11, paper labels and other materials. Similar processes can be developed to tag coatings used on transformers, waveguides, wires, fasteners and fittings, etc.

Conclusion

It seems clear that a single authentication platform to obtain supply chain security is necessary and well within grasp. The federal government has been making it clear that its focus on counterfeit electronic parts, critically necessary, must be seen as a risk-based approach, and not an end in itself.

Not so far down the line, the focus must widen to supply chain security holistically, including mitigation of counterfeit risk on a wide variety of vulnerable items, with special focus on the vulnerabilities of cyber security.

A strategically-minded aerospace and defense community should adopt authentication technologies which handle this vast variety of vulnerabilities and can adequately enforce industry policies, protocols and procedures.

References

1. "Coos Bay defense contractor indicted in conspiracy to defraud military in truck and aviation parts," The Oregonian, December 18, 2011 http://www.oregonlive.com/pacific-northwest-news/index.ssf/2011/12/coos_bay_defense_contractor_in.html
2. Defense Federal Acquisition Regulation Supplement, Detection and Avoidance of Counterfeit Electronic Parts, (DFARS Case 2012 - D055), a Rule by the Defense Acquisition Regulations System, May 6, 2014
3. Department of Defense Instruction (DODI) No. 4140.67, "DOD Counterfeit Prevention Policy, http://www.dtic.mil/whs/directives/corres/pdf/414067p.pdf
4. Background Memo: Senate Armed Services Committee Hearing on Counterfeit Electronic Parts in the DOD Supply Chain, Monday, November 7, 2011 http://www.levin.senate.gov/newsroom/press/release/background-memo-senate-armed-services-committee-hearing-on-counterfeit-electronic-parts-in-the-dod-supply-chain
5. "Improving Cybersecurity and Resilience through Acquisition," Final Report of the Department of Defense and General Services Administration, November, 2013
6. Op cit p.9
7. Miller, M., Meraglia, J., and Hayward, J., "Traceability in the Age of Globalization: A Proposal for a Marking Protocol to Assure Authenticity of Electronic Parts," SAE Technical Paper 2012-01-2104, 2012, doi:10.4271/2012-01-2104.
8. "DNA Authentication marking on items in FSC 5962", Defense Logistics Agency Website, August 3, 2012 https://www.dibbs.bsm.dla.mil/notices/msgdspl.aspx?msgid=685
9. Defense Logistics Agency, 2013 Electrical and Electronics Industry Outreach Forum, October 11, 2013 http://www.landandmaritime.dla.mil/downloads/news/ElectricalElectronics.pdf
10. "Applied DNA Sciences smartDNA® system to protect against copper theft in Sweden," Applied DNA Sciences website, June 5, 2012 http://www.adnas.com/sites/default/files/sweden_railroad_smartdna_against_copper_theft.pdf
11. "Martin Guitar Fights Counterfeiting in Partnership with ADNAS," Applied DNA Sciences website, July 14, 2011 http://www.adnas.com/sites/default/files/adnas-martin-press_release.pdf

The Engineering Meetings Board has approved this paper for publication. It has successfully completed SAE's peer review process under the supervision of the session organizer. The process requires a minimum of three (3) reviews by industry experts.

ISSN 0148-7191

http://papers.sae.org/2014-01-2125