Potential Chemical Attacks on Coatings and Tamper Evident Seal Adhesives

Carol Cantlon, B.E. (Chemical Engineering)
EWA-Canada IT Security Evaluation & Test Facility

6 September 2005

Summary

FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* requires the use of an encapsulation material (e.g. a hard epoxy material) for multiple-chip embedded cryptographic modules at Physical Security Level 3. This requirement is reduced at Physical Security Level 2 to a bleeding paint or etch-resistant coating. If the multiple-chip embedded or multiple-chip standalone cryptographic module is relying on an enclosure for protecting its components from observation, tamper evident seals or pick-resistant locks for removable covers and doors are required at Physical Security Level 2.

This paper provides an analysis of chemical attack approaches on coating and tamper evident seal security mechanisms. The investigation will be based upon the chemical composition of epoxy resins, conformal coatings, or bleeding paints used for circuit board physical security and the properties of tamper evident seals used to provide tamper evidence for the opening of a door or the removal of a cover in an enclosure. The attacks postulated in this paper are restricted to those that will not damage the electronic circuitry of the cryptographic module or leave tamper evidence on a commercially available enclosure.

Coatings

Coatings are one mechanism for providing physical security protection for a cryptographic module. Coatings include epoxies, conformal coatings, and bleeding paint. Coatings need to be able to adhere to the circuit board.

Epoxy resins are made from the chemical reaction of two compounds, bisphenol A - Bis A - (or bisphenol F -Bis F- and/or 'Novolac') and epichlorohydrin. Bisphenol A is the chemical product of combining one acetone unit with two phenol groups. Phenol contains a benzene ring with an attached hydroxyl (OH). Conformal coatings are acrylics, epoxies, urethanes, parxylenes or silicones. Paints are polymer emulsions.

Most coatings are thus a type of polymer. Polymers are long chain hydrocarbons composed of many repeating chemical bond units each of which is referred to as a monomer.

Some potential attacks on coatings are those common to polymers. Applying a shear force to a polymer may break some of the polymer bonds allowing the coating to be removed, but this approach is not practical for a circuit board coating.

By their nature, polymers resist decomposition. The atoms on the ends of the monomer that combine together to form the polymers have a valence such that they are highly reactive encouraging the lengthening of the polymers. Strong acids such as sulphuric acid, or strong bases such as sodium hydroxide, could dissolve the coatings or break their polymeric bonds but these chemicals will also likely damage the circuitry of the cryptographic module. Some epoxies are even resistant to sulphuric acid. A solvent like acetone may be effective on an epoxy since acetone is used in the making of epoxies. Acetone is an organic ketone containing a carbonyl C=O group surrounded on both sides by a methyl group (CH_2).

One polymer attack that potentially could work on a coating is the breaking of the polymer chemical bonds with an ultraviolet light source. For this ultraviolet light source to remove some of the board coating in a timely manner, it would need to be a concentrated ultraviolet light source. To prevent the decomposition of the coating in sunlight, some coatings have included in them a UV stabilizer.

Tamper Evident Seals or Labels

Tamper evident seals or labels may be used to provide evidence of the unauthorized opening of a door, or the removal of a cover, on an enclosure. Tamper evident seals are comprised of a paper, which is the tamper evident seal's surface, and an adhesive.

An attack on a tamper evident label security mechanism can be considered successful if all, or just a necessary part, of the tamper evident label or labels affixed to the cover can be lifted to allow the cover to be opened without the paper of the labels showing signs of damage. Damage must occur to the label paper for the label to provide tamper evidence because damage to the label's adhesive can be counteracted by reaffixing the label with household glue. If adhesive is left behind on the enclosure's surface potentially providing evidence of a tamper attempt, the enclosure can easily be cleaned with a solvent such as acetone or alcohol.

Signs of paper damage include obvious breaks in the paper such as tears or scores, deformation of the paper through stretching, discolouration of the paper through the designing of colour changes to the paper when the seal is removed or through the paper's soaking in a liquid of some type, and the appearance of words such as "VOID" if the seal is designed for these words to be appear when it is removed from a surface. These words are punched in the paper such that they will more easily stay bonded to the adhesive when the rest of the paper is pulled away from the adhesive when the seal is removed.

Another sign of tamper that could be exhibited by a tamper evident label is the paper dye running off the paper and staining an enclosure. This evidence of tamper, although not a

common one, should also be considered to fall in the category of paper damage since the dye is not in the adhesive, but in the paper.

All these types of paper damage rely on the efficacy of the adhesive bond between the label's paper surface and the surface of the enclosure. This adhesive bond is a mechanical bond wherein the adhesive has flown into microscopic holes of the enclosure, or adherend, and hardens holding the seal to the enclosure. Tamper evident seal bonding is not chemical bonding whereby a chemical change is made to the enclosure's surface to allow the seal to adhere to it.

To circumvent a tamper evident label, the adhesive bond between the paper of the tamper evident label and the enclosure's surface must be broken. One of the most effective ways of breaking this adhesive bond is through the application of heat with a hair dryer or heat gun. It is surmised that the heat warms the adhesive to allow it to flow and break the bond enough to pull the tamper evident label from the enclosure. This method is especially effective when the enclosure is metal since the enclosure expands slightly also breaking the adhesive bond. This attack is less effective if the enclosure is plastic, and thus less malleable. Adhesives become firmer with cold so putting the cryptographic module in a freezer will not work on tamper evident labels.

Another approach to removing tamper evident seals without leaving tamper evidence is the use of a solvent on the adhesive. The success of this approach depends on the type of paper utilized in the seal. Plasticized paper may not be affected by the moisture of the solvent. If the paper is actually paper, any solvent used would need to be applied directly to the adhesive, perhaps through the use of a syringe. This is difficult because the adhesive is completely underneath the paper of the seal.

Acids and bases may not be effective in removing tamper evident seals. Strong acids and bases will damage the enclosure and weaker acids and bases will only work to the extent they act as solvents.

Adhesives can be organic as well as synthetic, but in any event, adhesives are polymers and have the properties of polymers. Adhesives are even commonly epoxy resins similar in composition to epoxy resins utilized for coatings.

The alternative to tamper evident seals specified in FIPS 140-2 is pick-resistant locks. One advantage of pick-resistant locks over tamper evident seals is that they provide some prevention of an attack. Depending on the type of the lock, and how it is integrated with the enclosure, removing a lock without having the key to the lock, or knowing the lock's logical combination, requires a considerable amount of force. For example, ways of removing a lock include cutting of an external lock's shackle with a hacksaw or the drilling out of a lock incorporated into an enclosure. This type of attack of course could be performed but, if done in an office or in public, would certainly draw attention to the attacker.

Tamper evident seals do little or nothing to prevent an attacker's access to the circuitry of the cryptographic module; the seals can easily be removed through simply pulling them off. The advantage of tamper evident seals over pick-resistant locks is that they will provide indication of unauthorized access unless a sophisticated attack method is successful. With a pick-resistant lock, a simple attack method, such as the stealing of the lock's key or the discovery of the lock's combination through shoulder surfing, will allow an attacker to open the enclosure's door or remove its cover without detection.

Conclusions

Chemicals used in physical security, although composed of a variety of compounds, do have many properties in common. While research into chemical attack methods would never fully replace specific knowledge of the properties of the coating or tamper evident label, some directed research could provide generic information about the most effective attack methods. This information could then be provided to all Cryptographic Module Testing Laboratories allowing for a more standardized approach to physical security testing.

It is also suggested that more effective physical security could be provided through the implementation of multiple layers of physical mechanisms, i.e. tamper evident seals and pick-resistant locks or enclosures with tamper evidence security and epoxy coatings on internal circuit boards.

References

[1] Brown, David: "Clues to breaking down plastics", Science Notebook, washingtonpost.com, 4 April 2005.

[2] *Chameleon™ Electronic Hardware Tamper Evidence Marker*, Superior Tape & Label Incorporated, datasheet.

[3] "Chemistry of Epoxies, Novolacs, and Polyurethanes", URL: http://www.epoxyproducts.com/chemistry.html, viewed 5 September 2005.

[4] *Conformal Coatings Tutorial – What are Conformal Coatings?*, Dow Corning, http://www.dowcorning.com/content/etronics/etronicscoat/etronics_cc_tutorial.asp.

[5] "The elementary knowledge of adhesives:" [5th Installment] of the Viscosity Measurement "The Answer" Column, URL: http://www.tokisangyo.com/07_basic/clmn_05.html, viewed 2005 September 5.

[6] "Epoxy Resins", URL: http://sunilbhangale.tripod.com/epoxy.html, viewed 2005 September 5.

[7] FIPS 140-1, *Security Requirements for Cryptographic Modules*, U.S. Department of Commerce, 1994 January 11.

[8] FIPS 140-2, *Security Requirements for Cryptographic Modules*, U.S. Department of Commerce, 2001 May 25.

[9] http://sunilbhangale.tripod.com/epoxy.html web page viewed 2005 September 5.

[10] "Locks", Water and Wastewater Security Product Guide, U.S. Environmental Protection Agency, URL: http://www.epa.gov/safewater/watersecurity/guide/locks.html, 8 March 2005.

[11] Polylabel.com datasheet.