DESIGN CONCEPTS FOR TAMPER RESPONDING SYSTEMS

David Chaum

Department of Computer Science
University of California
Santa Barbara, CA 93106

INTRODUCTION

If cryptography is to be used to provide trustworthy information processing systems for society, the important problems of shielding and tamper-safing must be effectively solved by non-secret designs[1]. Shielding techniques for protecting mechanisms against analysis of their radiated signal energy seem to be rather well understood, and are not discussed here. Tamper-safing systems can be divided between those which merely indicate tampering to an inspector, and those systems which can detect tampering and can respond by, for example, destroying some secret information. In some cases it may be desirable to augment a tamper-responding system with tamper-indicating techniques and periodic inspections, in order to place an upper bound on the amount of time available for compromise of the tamper-responding system. The present work, however, focuses on design concepts for tamper-responding systems.

A small shielded object, say less than one cubic foot, is to be protected from an adversary by a tamper-responding container. The adversary's objective is to penetrate the shielding within the container, in a reasonable amount of time, without initiating a successful response, so that the adversary may obtain the secret information within the shielding. The system designers objectives are to design a system that can keep adversarys from obtaining their goals, that can be publically constructed and verified, that has a reasonable cost, that allows power to be supplied to and communication with the shielded device, that is not likely to be subject to rapid unanticipated modes of attack, and that will be reliable in an office building environment.

Security systems pose unique design problems because they assume an adversary. While estimation of adversarys involves uncertainties and possible

change in many dimensions, there may be reasonable bounds, such as, the amount of time available to an adversary. It is often considered sound practice to design security systems assuming that the adversary has complete knowledge of the general system design (though some designs may call for random choices among a great many alternative values for some parameters). Baran[2] presents convincing arguments for making the general design public, which include the advantage of input from a much wider community, and the fact that intelligence techniques are bound to reveal the details of most large undertakings to a determined adversary. Many organizations seem to take the view that designs should be closely guarded. Computer systems that are to be widely trusted can't afford the luxury (whether advantageous or dangerous) of secret designs, since their construction must be verified by a wide range of observers.

MODEL

A tamper-responding container may be thought of as a series of layers. Each layer will have a set of known attacks that can be perpetrated against it with associated times, possibly other requirements, and likelyhoods of success. One design approach is to bring sensor systems to bear on a single layer that are sufficient to detect all known attacks with reasonable associated times and likelyhoods of success.

Such a single layer approach may not always be possible, and multi-layer approaches may be more economical. If the sensor systems for a particular layer can be disabled when that layer is penetrated, then the security provided by multiple layers is merely additive, and probably a comparatively expensive way to increase penetration time. If there are independent probabilities of success for attempts to penetrate each layer, however, the probability of success for a series of layers is the product of the independent probabilities for each layer. Also, it may be difficult to penetrate one layer of material without exposing the penetration mechanism to the next layer, particularly if the exact location and contour of the boundary is a random parameter.

If sensor systems for one layer can not be compromised until a deeper layer is penetrated, powerful advantages may result. For example, no known attack scenarios exist for a system comprising an inner layer that is secured against all fast attacks, and an outer layer that is effectively protected against all but fast attacks by sensor systems secured within the inner layer. In general, when a sensor system's view extends through a series of enclosing layers, it limits the kinds of attacks that can be employed against each layer of the series much as if it were embedded immediately within that layer, and it limits the kinds of attacks that can be brought to the internal layers of the series.

SENSOR SYSTEMS

Sensor systems may be divided between the passive, which merely monitor energy coming from a layer, and the active, which monitor the return of energy that they transmit into a layer.

Passive sensor systems can be triggered by thresholds, rates of change, and more sophisticated pattern analysis. They may be divided between those which monitor a kind of energy that will only exist in significant quantities or increase dramatically under attack, or they can monitor a level for relatively small suspicious fluctuations. Clearly the former is to be preferred. Examples include mechanical vibration, strain, pressure, electromagnetic and other forms of radiation. Randomness may be exploited by, for example, pressurizing a layer to a random pressure. Significant advantage may be taken of materials, such as chemically stressed glass or glass ceramic[3], which contain stored energy that is released by some attacks and will propagate through the material, or ideally cause a chain reaction and thus be amplified by the material itself. Such materials may be regarded as both the constituents of a layer and as part of the sensor system, even though the kind of energy emitted by the material is not the same as that of the ultimate output of the sensor system. Joints between parts of such materials may be subject to special attacks.

Active sensor systems may be divided between those which propagate energy through a fixed path in some layer, and those which do not use fixed paths. Path based systems must protect the area between the paths or exploit path overlap unless the path gap or minimum sensitive part of a path are below some acceptable size threshold. Also, they can provide resistance to straight line attack. Time domain, interference, capacitive and inductive techniques may indicate movement of paths, indicate changes in path length, and provide protection between paths or even of adjacent layers. Path systems may be comparatively slow to respond. Non-path systems may rely on the doppler effect, standing wave patterns, or even phased array techniques. They may also include such techniques as directed beams of energy, and sophisticated analysis of the reflected energy. Random values may be used to influence parameters of the transmitted energy, such as timing, direction and spectral composition, and they may also be used to determine parameters relevant to evaluation of the sensed energy, such as the sample and hold delay in a time domain system, so that probabilities of detection may be introduced and certain countermeasures made ineffective. While active techniques may require more power than passive techniques, path techniques appear to be potentially cost effective, and directional techniques appear to have the potential for extreme sensitivity, though they may be relatively expensive.

In a layer composed of multiple sub-layers, some of the sub-layers may be regarded as auxiliary sub-layers that form part of a sensor system, such as, reflective coatings, conductive coatings or piezoelectric coatings. These auxiliary sub-layers may be shared by several layers, and they may be regarded as layers themselves, though they may be subject to a relatively wide range of attacks. Also notice that a very thin boundary region of a layer, such as a reflective or conductive surface, may be providing substantial security.

ATTACK SCENARIOS

Attacks are divided here between probing, stealth, countermeasures, and disabling attacks. A complete attack scenario may include a sequence of combinations of these individual attacks on a series of layers and sensor systems.

Probing attacks seek to aid other attacks by finding out something about the particular values of random parameters, which may include static information about layer structure and dynamic information about sensor system operation. Appropriate techniques depend on the nature of the parameters, but radiography, ultrasonic scanning, and passive signal analysis are examples.

Stealth attacks attempt to penetrate through a layer without being detected. A physical barrier may be penetrated by applying mechanical cutting techniques, such as drills and abrasives; thermal techniques, such as oxygen lance, thermite, and shaped charges; energy beams, such as laser and electron discharge; chemical attacks, such as solvents and corrosives; and particle beams. The probability of detection of a layer penetration may be reduced by techniques, such as shoring, reconstruction, or introduction of counterbalancing elements, or by altering the material(s) of the layer, such as by by application of forces, energy or chemical reaction.

Countermeasures are techniques which introduce energy into a sensor system in such a way that the sensor system does not detect some other attack. Examples include, roughly in increasing order of difficulty, energy masking, such as by introducing static or interference; energy introduced to maintain a level decreased by another attack; energy introduced to null, at the sensor(s), energy generated by another attack; and energy introduced to restore at sensor(s) a pattern of energy disturbed by another attack.

Disabling attacks seek to completely destroy, reduce the effectiveness of, or influence a sensor system so that other attacks may be perpetrated with decreased risk of detection. Such attacks might employ the layer penetration techniques already discussed, or they might include such things as manipulation of power level, temperature, magnetic field, radiation level, etc. The following lists types of sensor system components, roughly in increasing order of difficulty of their corresponding disabling attack: those components that if disabled or destroyed would end the ability of the sensor system to initiate a response (a quick attack on these might be detected too late by the sensor system); those that if disabled could diminish the likelyhood of the sensor system to respond; and those that could be influenced during an attack to compensate for the exact changes caused by the attack.

NEW PROPOSAL

The above considerations suggest an approach that will be presented here as an illustration of a high-level design. The heart of the proposal is a layer formed from a plurality of small, irregularly-shaped particles of materials that may be roughly categorized as either detectors, protectors, or barriers. Detectors are materials that emit stored energy when subject to particular types of attack. For example, contact explosives may explode when some modes of physical penetration are attempted. A protector gives off stored energy when a nearby detector or protector is subject to a disabling attack, such as an explosive that is responsive to a solvent that could disable a contact explosive. Barrier particles, such as diamond or ceramic dust, may force

certain kinds of attack for which detectors are provided. Some particles may play more than one role.

Such an aggregate layer may be formed in a hardening matrix which will transmit energy released by the detector and protector particles. The construction of the layer may be readily verified by observers who may sample the various types of particles, and watch as the aggregate is prepared and the shielded container is potted within it. Power transmission and communication may be accomplished by inductive techniques, for example. The transducers and electronics of the detector system within the aggregate layer should be protected against disabling attacks, including very fast attacks. It may be desirable to include active sensor systems, such as time domain reflectometry paths, that are protected by the aggregate layer and whose protection extends for a ways beyond that layer, so that the attacks which can be brought to the aggregate are limited. Confidence in the unlikelyhood of a rapid and unanticipated mode of attack may be increased due to the variety of barriers, detectors and interfaces that may be provided. A variety of design concepts that appeared attractive from earlier discussions have been included in this design, including the use of what is in effect a great many layers, exploitation of random boundaries, stored energy mediums, and sensors protected within an inner layer.

APPENDIX

Several related points are worth mentioning:

(1) Some locations for a device may greatly ease the problem of providing a sufficient tamper-safing system. For example, a device within a satellite may be protected by the difficulty of reaching it, and by being observable by other satellites. A device which contains sophisticated seismic sensors and is at the bottom of a back-filled drill hole in several hundred feet of bedrock may be very difficult to reach, especially without being detected.

(2) Accelerometers can do a good job of detecting attempts to transport a secured device. Mechanical accelerometers have appeared in the literature which seem to provide adequate sensitivity and yet are self leveling, and resistant to shock such as might be caused by an earthquake[4]. Much more sophisticated, sensative and miniature devices may now be practical.

(3) Combinations of materials are often used in sophisticated barriers. Examples include, steel rebar or mesh in concrete, tungsten carbide chips in steel hard plate, and steel and ceramic balls in an epoxy matrix[5].

REFERENCES

(1) Chaum, David, Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups, Memorandum UCB/ERL M79/10, UC Berkeley, February 1979. Also as dissertation.

(2) Baran, Paul, On Distributed Communications: IX Security Secrecy and Tamper-Free Considerations, Memo RRM-3765-pr, Rand Corp., Santa Monica CA, August 1964.

(3) Miska, Herbert, Command-Break Glass and Glass Ceramics, Corning Glass Works, Corning NY.

(4) McManus, J., and Engel, A., Tamper Resistant Unattended Safeguards Techniques, IAEA Symposium on Progress in Safeguards Techniques, Karlsruhe Germany, July 1970.

(5) Ney, J., Surveillance and Containment Instrumentation for International Safegaurds, Annual Meeting of the Institute of Nuclear Materials Management, Washington DC, June 1977.