Proceedings

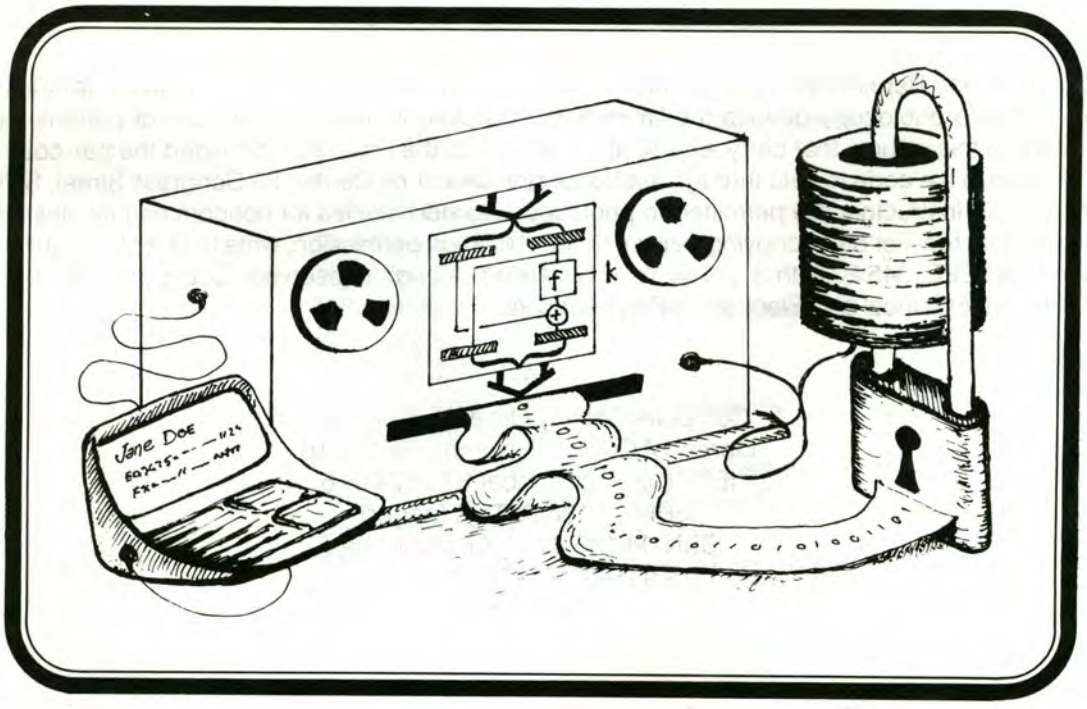
1987 IEEE Symposium on

Security and Privacy

April 27–29, 1987 Oakland, California

Sponsored by the
IEEE Technical Committee on Security and Privacy
in cooperation with the
International Association for Cryptologic Research

Computer Society Order Number 771
Library of Congress Number 86-83316
IEEE Catalog Number 87CH2416-6
ISBN 0-8186-0771-8
SAN 264-620X



THE COMPUTER SOCIETY OF THE IEEE

IEEE THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

IEEE COMPUTER SOCIETY PRESS

Published by Computer Society Press of the IEEE
1730 Massachusetts Avenue, N.W.
Washington, D.C. 20036-1903

Cover designed by Jack I. Ballestero

Computer Society Order Number 771
Library of Congress Number 86-83316
IEEE Catalog Number 87CH2416-6
ISBN 0-8186-0771-8 (paper)
ISBN 0-8186-4771-X (microfiche)
ISBN 0-8186-8771-1 (case)
SAN 264-620X

Order from: Computer Society of the IEEE
Post Office Box 80452
Worldway Postal Center
Los Angeles, CA 90080

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331

Computer Society of the IEEE
Avenue de la Tanche, 2
B-1160 Brussels
BELGIUM

IEEE

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

Physical Security for the μABYSS System

Steve H. Weingart

IBM Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598

Abstract

Open systems, now common in many small computers, have given the user logical access to all parts of his or her system. At the same time, the computing environment is moving out of the computing center and into the office and home, giving users physical access to their systems. This movement of the computing environment necessitates a mechanism to prevent the user from physically accessing certain parts of his or her system if logical security (of the type which limits the user's ability to make copies, change code, etc.) is to be reliable. This paper describes the development of a physical security system for protecting electronic circuits from unauthorized access. This system can be used to ensure that logical security mechanisms will remain uncompromised. The requirements, design criteria, and implementation of the system are discussed with an orientation towards practicality and manufacturing.

Introduction

Computer security can be loosely separated into two parts. The first is logical security, security that deals with access to, and use of, data and programs in the conventional computing environment. The second is physical security. Physical security deals with access to data and programs outside of the normal environment by physical means (accessing the operator's console, removing a tape or disk, probing the circuits). Logical security is usually implemented in the design of the operating system and system software, while physical security has usually been implemented using walls and doors. Classically the problem of physical security has been addressed by limiting physical access to the machine room, the tape library, etc. However, as personal and other small computers have come into common use, this approach has become impractical. Open systems, now common in many small computers, have given the user logical access to all parts of his or her system. At the same time, the computing environment is moving out of the computing center and into the office and home, giving users physical access to their systems. This movement of the computing environment necessitates a mechanism to prevent the user from physically accessing certain parts of his or her system if logical security (of the type which limits the user's ability to make copies, change code, etc.) is to be reliable.

These changes in computing environment bring with them a wide range of security problems. Users now have both the place and time, in privacy, to attempt to defeat the security mechanisms that may have been installed by the author/vendor of data/software used on their system. As an example, examine the effectiveness of the copy protection systems that have been employed to prevent illegal copying and distribution of software. Almost every copy protection scheme employed to prevent unauthorized duplication has been circumvented within a matter of days (if not hours) upon the release of a new software package. This has resulted in the development of a sub-industry: the development and sale of programs that bypass the copy protection of other programs. The reason why these attempts at logical security fail is twofold. First, the user has complete access to all operating system and system software. The system can be used as a tool to inspect, and modify, itself or any other program (or data). A program can be written to "watch" another program, report the sequence of events in progress, and then change the program so its copy protection (or other logical restriction) is removed. The machine state can be "frozen" and a "snapshot" taken of the memory contents, so conditions not normally revealed are displayed. Second, the system can be probed, by means of a logic analyzer or other electronic tool. Programs that hide their efforts at logical security by convoluting, or otherwise obscuring their software execution, can be monitored by a device which looks for the exact condition in question and captures it when it occurs. This capture can be performed invisibly to the system being probed.

For these reasons physical security must be employed to enclose and protect the implementation of logical security. If system integrity is to be maintained, the physical security mechanism must be able to stand up to rigorous attempts by individuals who have unlimited private access to these systems.

Some individuals have begun to address the problem of physical security. However, there are presently few descriptions of practical systems which can be implemented.

Price [1] describes some approaches to physical security. He discusses the concepts of potting the circuit in a medium that has been filled with substances to make cutting, drilling, etc. more difficult. He goes on to describe the use of wires embedded in the potting medium as an intrusion sensor, and discusses the concept of intentionally imparting differences in individual units to make sacrificing one unit to gain information for use in attacking another less useful. Price's article takes the form of a

survey of concepts and possibilities from a theoretical standpoint, so implementation and manufacturing are not discussed. The concepts discussed here are intended to be practical, and manufacturable.

Multiply-layered physical security systems such as described by Chaum [2] will give a high level of security. These systems can tend to be very complex, and quite expensive. After investigation, our decision was to develop a single layer system, using a very dense sensing element to obtain good security, cost/performance, and manufacturability.

The physical security design discussed here was developed for the μABYSS implementation of the ABYSS architecture. For a description of the security, other than physical, of the μABYSS system see White and Comerford [3].

μABYSS is a co-processor system designed to be used for software and data protection in the personal computer environment. Software and/or data is distributed with critical portions encrypted. When execution or access is required the encrypted portions are loaded into the co-processor unit, decrypted for use, and executed or used (in plaintext) only within the co-processor. The co-processor must be kept physically secure if the integrity of the data/code used within it is to be maintained.

It is required to be a low cost, high reliability addition to a personal computer for use in the common environment. The physical security implementation must meet the system needs for unobtrusiveness, while maintaining an effective barrier against intrusion.

Overview

The physical security system under consideration is a package which houses electronic circuitry containing information to be protected. Its responsibility is to make it difficult to gain access to parts which contain sensitive information. If an attempt is made to invade the protected region, the security system will sense this condition and render the contents unusable. In its simplest form, the circuitry to be protected may be a single RAM. In larger systems, such as the μABYSS security system, the circuitry to be protected is a microcomputer system which includes two microprocessors, RAM, ROM, and a real-time clock.

The physical security package for the μABYSS system is a necessity for the protection of the data within the co-processor unit. Its battery-backed RAM contains the system's encryption/decryption keys. In addition, parts of applications which are stored on disk in encrypted form are loaded into the processor unit, decrypted, and executed within the unit. These application parts are not intended for viewing or modification by the user. To prevent unauthorized individuals from gaining access to sensitive data, the physical security system, upon detection of an attempted intrusion, interrupts power to the volatile storage, and grounds the V_{cc} pin of the CMOS RAM, thereby erasing the contents.

In general, a good physical security system must meet the following requirements:

1. The system must be sensitive to attack from any casual or expert probing.
2. The incidence of "false alarms" must approach zero.
3. The system must cost as little as possible.
4. The protection circuitry must take as little space as possible.
5. The protection circuitry must use very little power.

Approach

For a security system to be competent, it must require greater effort to breach the system than the value of the protected asset warrants. In the pursuit of this goal the system cannot be made so sensitive that false alarms will become common, representing an unacceptable inconvenience to the user. If the system requires expensive parts, or changes the way a user interacts with his or her system this is also unacceptable. Since the cryptographic keys are kept in CMOS storage, which must be powered at all times, power consumption must be consistent with limited available battery power. The user should not have to perform routine maintenance often (changing the battery), and the cost and time required for this maintenance should be minimal.

A design has been developed which meets the above requirements. This design functions without the need for close tolerance or specially selected parts, and it covers the avenues of entry thoroughly. A single error at any time during a break-in attempt can be sufficient to cause the erasure of the protected data. This design also meets the goal of being relatively insensitive to environmental conditions. This is important considering that the protection circuitry must keep operating correctly regardless of the conditions encountered during use, handling, transport, etc.

The first consideration in this system was the design of an intrusion sensor that would completely cover the surface area of the volume being protected. To open a single hole on the order of 1 millimeter in diameter would allow the intruder access to enough of the system (the CMOS RAM's power pin, or the controlling signal in the protection circuitry for example) to defeat it. Therefore a sensor was needed that left no holes in the surface of the package, and which resisted the creation of such holes by an attacker.

A number of sensing arrangements were studied. Prime considerations for the sensor included:

- Fragility of the sensing element so that attempts to manipulate it would cause breakage.
- High density of the element so no holes would be left open.
- High reliability
- Ruggedness of the assembled system
- Low environmental sensitivity
- Ease of assembly and automation of assembly

The first sensor tested utilized a dense pattern of lines on a conventional printed circuit board. This was rejected because the lines could not be made narrow enough nor spaced closely enough to meet requirements. Another version used deposited

SnO_2 lines on glass. This method was rejected as being too fragile. The next attempt used a frame wound with fine wire, and top and bottom covers also wound with fine wire. Two basic problems arose from all of the designs which used a number of flat panels assembled to form a box. First, in almost all of the above cases the edges allowed a line of entry where a panel could be carefully cut loose and then bent or removed, or a small slot could be opened to gain access to the inside of the package. The second problem began as an attempted solution to the first. Elastomeric or light spring contacts, which had a very small positioning range, were substituted for wires and conventional insertion type connectors to protect against bending or lifting the edge of a panel. These connectors proved to be unreliable because of sensitivity to impact, vibration or environmental conditions. These connectors also define a single point which, if accessed, would allow bypassing of an entire panel. Various pouch type containers were examined (layered plastic/conductor bags, piezo-electric sheets, etc.), and none of them met the requirements.

After examining a large number of sensing arrangements, a multiple layer wrapping of very fine wire, completely surrounding the package, emerged as the most reliable, manufacturable, and lowest cost sensor design. An additional benefit of the chosen design is that by the nature of the winding process, individual units are slightly different from each other, even though they are made by the same production process. This makes attacking the system more difficult, because sacrificing one unit to work out a strategy for attacking another will be of limited use.

Package/Sensor Implementation for the μABYSS Prototype

To meet system requirements the prototype had to be readily portable. Approximately forty square inches of card space are required to accommodate the processor and support circuity. A three inch by eight inch package using two cards sandwiched back to back was chosen. The cards will be supported by two ramps (Fig. 1) which are constructed out of plastic or epoxy/glass board material. These ramps allow the smooth, continuous winding of a wire "cocoon" which surrounds the package, forming the intrusion sensor.

The wire winding is applied to cover the entire package with four layers of 40 ga. (0.0035 in., or finer) thinly insulated nichrome wire which serves as a resistance element in the protection circuitry. Nichrome wire was chosen because it is difficult to attach to, and its high resistance lowers the power requirements. The wire covering is then potted in a hard, opaque epoxy, such that the wire is not visible from the surface of the potting. This increases the likelihood of breaking a wire during a mechanical attempt to remove the potting material. The epoxy is also chemically "harder" than the insulation on the wire so attempts to dissolve the potting will dissolve the insulation (and possibly the wire), causing shorts or opens. Also, the potting material is filled with alumina or silica. The presence of either of these materials makes the package more difficult to machine. The fillers also make UV laser ablation more difficult due to heating effects caused by the inorganic fillers. Generation of heat causes mechanical stress in the epoxy which could crack the package, thereby breaking one or more wires. If the wrapping is broken, or wraps are shorted together, or if the resistance changes due to an attempt to "jump out" segments, the protection circuit will detect it and erase the contents of the protected RAM.

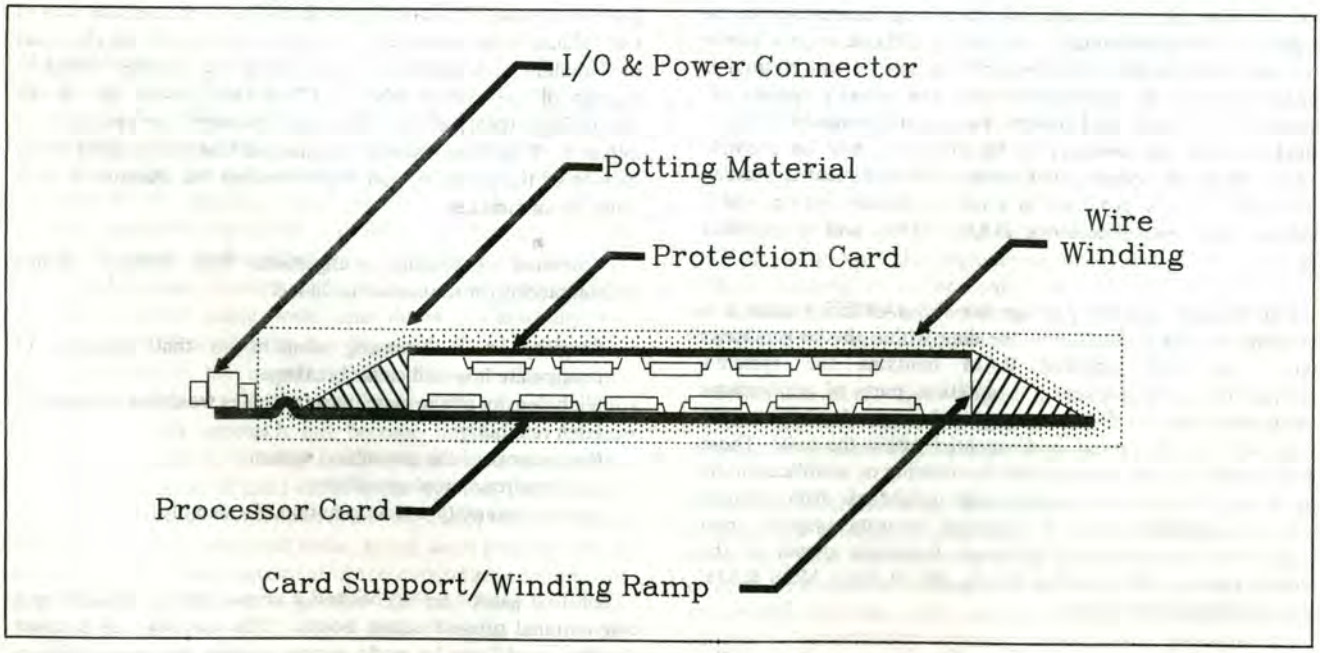


Figure 1. A Physical Security Package

To increase sensitivity, the wire is not applied as one strand. It is applied as four to eight mechanically parallel wires, which are connected in different configurations. The inside ends of the wires can be connected to the circuit in different combinations, and the outside ends of the wires can be connected in different pairings, while maintaining the same electrical configuration. This permits differences between units. It also increases the sensitivity of the system by making adjacent wires farther apart on the distributed resistance (Fig 2). Shorting two adjacent wires will cause a larger signal change than if they were two adjacent turns in a single strand wrap.

At the start of the winding, the wires are attached to connection points on the outside surface of the package. These contact points are then covered by the winding. At the outside end the wires are connected together, then the connections are tucked under the surface of the winding. To add protection to the edges of the board, the winding is extended beyond the end of the board and crushed if no connector is needed. The board can be bent or warped to prevent a straight line entrance if a connector is needed. To make an entrance at a connector edge even more difficult it can be covered by "stitching" rows of vias, which are part of the protection circuit, through the board at the border of the wound and potted area.

To allow additional variation in location of the wires, they are wrapped at a very low tension. This causes the wire to float somewhat above the surface of the package, so the exact depth from the surface of the potting material to wires varies between individual units. This adds an additional element of randomness.

The finished package is then molded in the potting material. The cured potting is too hard to allow the unwinding of the wire. If the wire breaks, the circuit will detect it.

The windings are effectively bi-filar. This is a result of the simultaneous winding of both segments and the way they are connected. This makes the circuit relatively insensitive to electrical interference by cancellation of induced signals.

The thermal properties of the wrapped, potted package have been calculated and experimentally verified. The package can be used at normal room temperatures, with standard commercial parts, while dissipating up to 2.5 W internally. This is due to the excellent thermal properties of both the potting material and the wrapping wire. This is consistent with the power dissipation requirements of the circuitry in use.

Package Winding

A strong point in favor of using the described technique for producing the sensor/package is that it draws upon very well known methodology. Wire winding technology, in the form of transformer and coil production, is a well known art. Materials of many varieties are available off-the-shelf, and documentation on the properties of these materials is readily available.

While materials were readily available, a commercial machine capable of winding the package was not. Some time was spent looking for a suitable coil winder which could hold and wind the package. All of the winders that were examined could not hold a package as large as the one described, or would not run slowly enough with sufficiently light tension. This turned out to be only a small problem. A winder was designed using standard laboratory mechanical apparatus (0.5 in. round aluminum rods and off-the-shelf fittings). One variable speed D.C. motor was used to turn the package, and another was used to drive a level

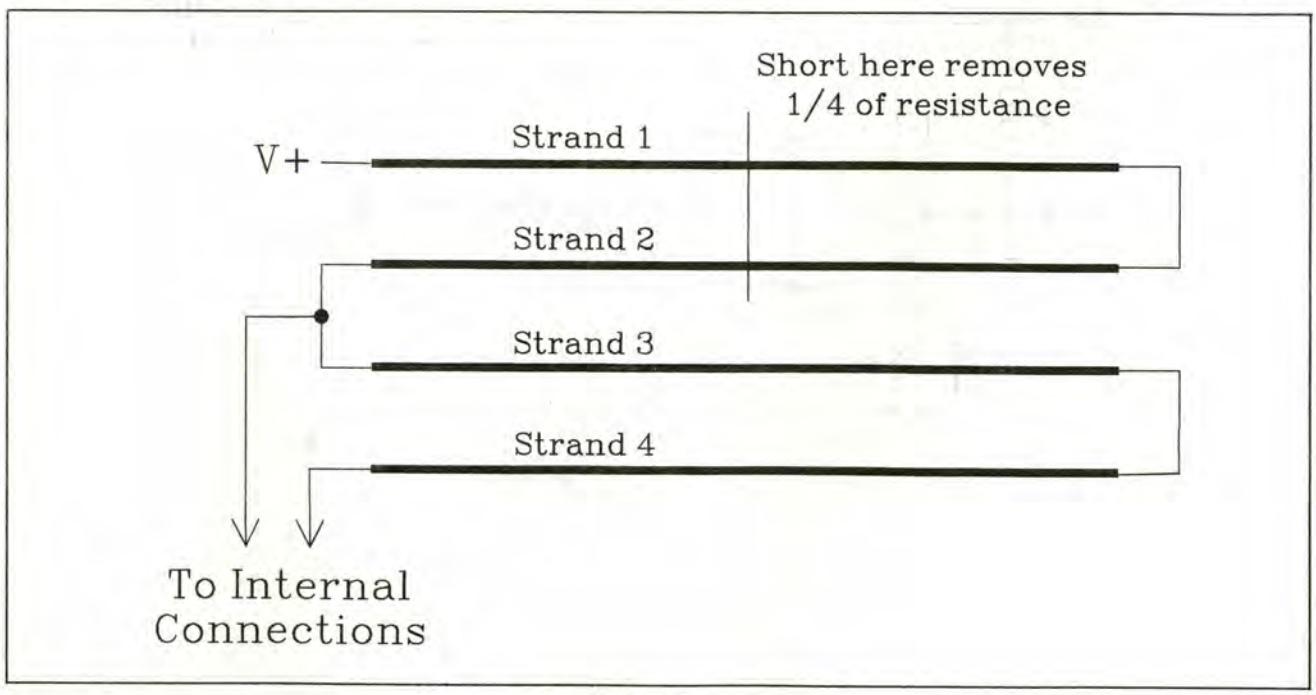


Figure 2. An Example of Multi-Strand Winding

winding device (a device to smoothly move the wire across the package as it turned). Once the winder was functional, tension controllers were added to the wire spool holders. The unit functioned in this fashion for a number of months and produced quite usable test samples. At that time the D.C. motors were replaced with stepper motors, and the winder was automated using a personal computer. The packages produced in this manner were uniformly covered with no gaps whatsoever. Overall resistance variation between strands is typically 0.5% or less. This is very good considering no special efforts are taken to ensure the equality of strand lengths, except for passing all strands through one winding guide.

Producing machines commercially for wrapping this type of package would present no real technical difficulties. The requirements are satisfied by simple extensions of currently available technology. The machine that was constructed as part of the package development process is a usable model for further development.

Circuit Implementation for the μABYSS Prototype

Since the system could be made more sensitive by detecting changes in the resistance of the winding as well as simply checking for continuity, it was decided that an analog implementation would give better performance than a digital implementation. After investigation, two designs for the circuitry were able to meet the requirements. Both designs utilize CMOS integrated circuits to minimize power requirements. Needs for close tolerance or selected parts are minimal in both designs. The first design has the advantage of low cost with adequate sensitivity. The second design is much more sensitive, but costs more.

In the first design, the wrapped strands are connected as two equal resistors and used as a half bridge. This makes this design relatively immune to temperature effects, because the two legs of the winding are wound simultaneously, and are therefore similar in length and physical placement. Any changes in resistance due to temperature are seen equally in both segments so the signal, which is tapped from the electrical center of the element, does not change. The epoxy potting material also contributes to maintaining a homogeneous package temperature, due to its thermal conduction properties. The signal derived from the windings is then input to a window comparator, which continuously monitors its value. If continuity is lost or if the resistance of the winding changes (increases or decreases), indicating an intrusion, the comparator trips and disconnects the power to the battery backed RAM and shorts the V_{cc} pin to ground.

The second design is an adaptive implementation which compares the current condition of the winding to its condition at a previous time. This permits the system to drift with time, battery voltage and temperature, without tripping the comparator. If the change is larger than the set window in a given time period, the comparator will then trip and erase the RAM. The advantage of this implementation is that it can have a much smaller window, while not producing false alarms.

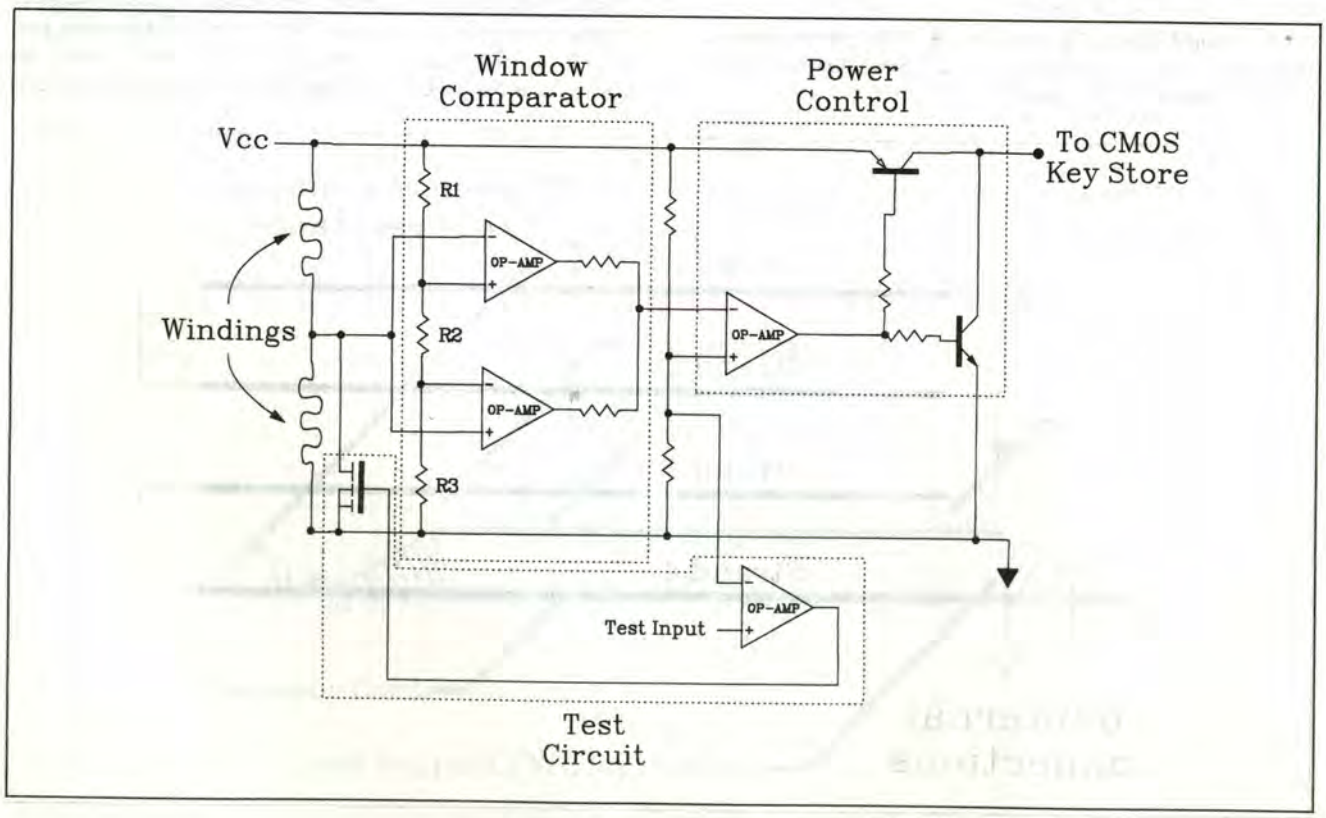


Figure 3. Intrusion Sensing Circuitry

Circuit Design for a Measurement Method

Referring to figure 3, the output of the divider, which is formed by the windings is used as input to a window comparator. The allowable change of the divider is set as a function of R1, R3 and the window setting resistor R2. The window setting resistors are in close physical proximity to each other inside the package, which minimizes window drift resulting from thermal effects. If the divider output is within limits, power is delivered to the CMOS key store RAM. If the wire is tampered with (broken or its resistance changed), the comparator trips, the power is removed and the V_{cc} pin of the RAM is shorted to ground. The fourth operational amplifier in the package is used as a manufacturing test port which can be used to deliberately trip the protection circuitry to verify its function after potting. This will prevent non-secure units from reaching the field.

This design fits into one CMOS I.C., one power/battery switching I.C., three discrete transistors, and 12 passive components. Power consumption is approximately 20 μA for the protection circuitry and 25 μA for the entire battery powered section. This circuit has proven to be quite reliable, and is presently in use. The window size is chosen as a cost/performance trade-off as a function of the operational amplifier drift and input bias current, resistor tolerance, and wire uniformity. Good performance has been obtained using 1% resistors, commercial grade operational amplifiers, off-the-shelf 40 ga. nichrome-c wire, and a 5% window size.

Circuitry for a Sample-to-Sample Comparison Method

To avoid the need for precision or close tolerance parts, while having a greater sensitivity, the protection circuitry in this design (Fig. 4) does not measure an absolute value, but instead measures the present relative value of the winding and compares it to the previous value. To accomplish this, the winding segments are connected in series and a voltage is applied to the series string. The resultant current is then integrated for fixed periods of time.

At the end of each integration period, the integrator output is compared to the previous value by a window comparator. The previous value has been stored in a sample-and-hold circuit. The window size is a function of the divider network R1, R2, R3, R4. The window's center is a function of the output of the sample-and-hold circuit (which is the value of the previous sample). Therefore the window is adaptive, and as a result can be made very small. The size of the window needs only to be large enough to allow for noise, drift, and sample-and-hold droop (in practice the window size in this design can be < 1%, while in the previous design > 5% is required). If the present value is within the the window set by the last reading, the circuit

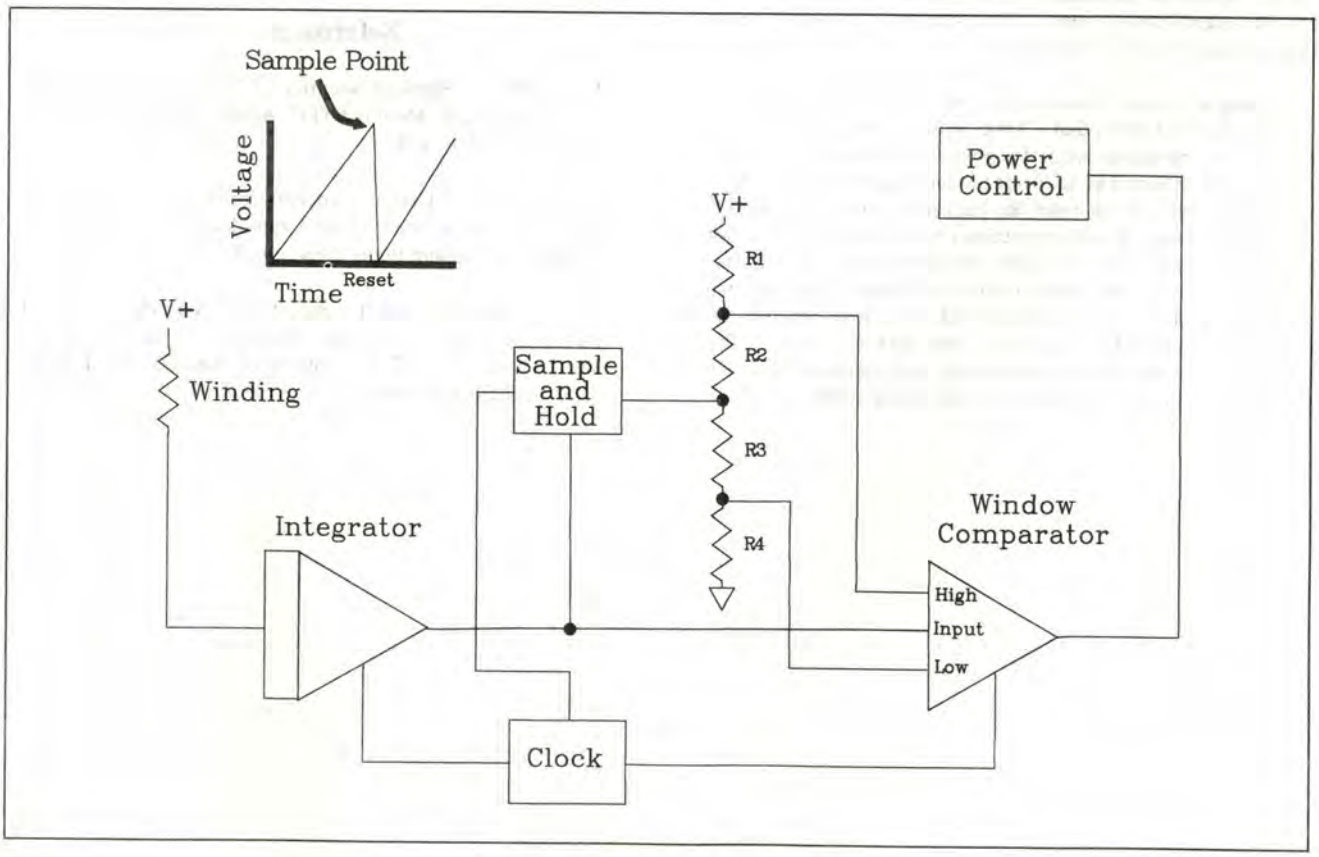


Figure 4. Adaptive Intrusion Sensing Circuitry

does nothing. If it is outside of the limit, the power is turned off and the V_{cc} pin grounded. At the end of each cycle the new value is loaded into the sample-and-hold circuit and the cycle repeats itself (driven by the clock).

If the circuit values change, over time or temperature, the circuit will not be affected (within limits). This produces a circuit in which the magnitude of the drift may be larger than the magnitude of the window without tripping the comparator.

This design fits into three CMOS I.C.s, one battery/power switching I.C., two discrete transistors, and 15 passive components. Power consumption is about 35 μA for the protection circuitry and about 40 μA total. This design, while greater in cost than the previous design, gives higher performance. There is one problem associated with this design. When the power is switched from line to battery or the reverse, the change in V_{cc} may move the window sufficiently during one sample interval to trip the comparator. The problem can be solved by using a voltage regulator to supply the winding and divider, but this adds to the cost. This design functioned very well during testing, with the integration contributing greatly to noise immunity.

Conclusion

Both circuit designs and the sensor have been implemented and have been tested. The measurement method circuit is now in use, because its performance is adequate for the task and its cost was significantly lower. The system is presently being tested against a variety of attacks.

Freezing is a form of attack that has not been addressed in this paper. It is known that CMOS memory can retain data at cryogenic temperatures with the power source removed. The attack approach would be to lower the temperature of the unit to the desired level and cut open the package. When the power is removed the data will still be retained for some time (It is not yet known if the crowbar circuit will be effective under these conditions). Next, the power control is disabled and external power is provided to the CMOS RAM. The unit can then be warmed to room temperature and the data extracted. The retention time/temperature relationship, and methods by which this attack can be prevented are currently being studied.

The approach taken for this design is not limited to the μABYSS data security project. A general view was taken towards the problem of physical security/tamper resistant packaging, with the resultant design being applicable to a range of problems. However, systems with different cost, performance, power, or environmental requirements may require different methods. Other winding materials, such as optical fiber, could prove to be more difficult to attack than the wire currently in use. However optical fiber would be more difficult to wrap. Additional layers of security, such as piezo-electric sheets or internal light sensors could be added to enhance performance.

Regardless of the application, each problem should be studied with respect to the type of adversary it will face. The setting, the amount of time, and the privacy of the location in which the adversary will work, have to be taken into consideration.

Acknowledgements

The author would like to thank L. D. Comerford, T. J. Nolan, W. D. Strohm, and Steve R. White of the ABYSS group for their contributions and help in the development of the physical security system. A special thanks to Stanley B. Green of Pollock, Vande Sande & Priddy, for preparing the patent docket. The author would also like to thank his wife, Pat, for infinite patience and excellent grammar.

References

[1] W. L. Price, "Physical Security of Transaction Devices", NPL Technical Memo DITC 4/86, National Physical Laboratory (Jan. 1986)

[2] David Chaum, "Design Concepts for Tamper Responding Systems", in Advances in Cryptology, Proceedings of Crypto '83, Plenum Press 1984, pp.387-392

[3] Steve R. White, Liam D. Comerford, "ABYSS: A Trusted Architecture for Software Protection", submitted to Proceedings of IEEE Symposium on Security and Privacy (1987), IEEE Publications