CONF-890736--20

TRACE - TAMPER RESISTANT AUTHENTICATED CAMERA ENCLOSURE

DAVID SKOGMO SANDIA NATIONAL LABORATORIES ALBUQUERQUE,NM 87185-5800

SAND--89-1587C

DE89 014186

ABSTRACT

To protect a security instrument such as a television camera from subversion by signal substitution, the data from the instrument are digitized and submitted to an authenticator. The digital data may then be transmitted in the clear over a non-secure medium. Appended to the data is a 10-bit authentication value based on the values of the data and a random authentication number. At the receiving end, the data are submitted to an identical authenticator. If it produces the same authentication value, the data are authentic. Such a scheme can only work if the instrument, the authenticator, and the link between them can be protected from tampering. This paper describes a tamper resistant container designed to protect a data authenticator and television camera against an adversary having sophisticated resources and complete design information. The container's design includes active elements to detect and report intrusion attempts in real time. It also includes passive elements to indicate upon later inspection that the container had been violated.

AUTHENTICATION

Having decided to use television cameras to view a scene, one wishes to be sure that the images viewed are indeed those produced by their camera and not bogus images substituted by an adversary. For an adversary with limited resources, simply transmitting the image through optical fiber would be a sufficient deterrent. However, for an adversary having more substantial resources, signal substitution becomes quite possible. One needs some means of positively identifying an image as coming from a certain camera. Authentication is a possible technique.

Although one can do much toward authentication of analog video information[1], within the TRACE, a digital authenticator is used. Regardless of which authentication scheme is used, the link between the camera and the authenticator must be kept from tampering. If a bogus signal may be inserted before the authenticator, it becomes the authenticated signal and the camera is defeated. The TRACE must protect this link while the camera is in service and also while it is being transported and stored. A block diagram of the TRACE system is shown in Figure 1.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

TRACE

TAMPER RESISTANT AUTHENTICATED CAMERA ENCLOSURE

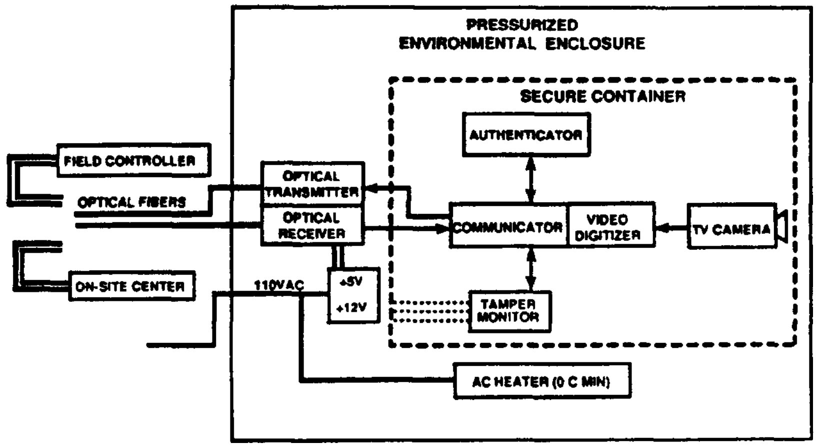

FIGURE 1

TAMPER PROTECTION SYSTEM

The system is housed in a pressurized environmental enclosure that is penetrated by the connectors for two optical fibers and AC/DC power. Via the optical fibers, the TRACE may communicate with a central computer or a field controller. Within the environmental enclosure are the optical communication components, power supplies, and a heater to keep the insulated interior above 0 degrees C. This provides the home for the secure container. Within the secure container are the four principal elements of the system: the Camera, the Authenticator, the Communicator, and the Tamper Monitor. Upon external command, the Communicator will digitize one field of video from the Camera. As each picture element is serially communicated to the outside, it is submitted to the Authenticator. When the last picture element has been processed, the Tamper Monitor is consulted for the container's security status. This status is authenticated and transmitted. Finally, the Authenticator's result is obtained and transmitted. On the outside, the data have been presented to an identical Authenticator. If it produces the same result, the image is accepted as authentic.

The secure container consists of a fiberglass cylinder that is wrapped with four optical fibers in four layers. These fibers are each about 1.5 km long and are embedded in an opaque epoxy. Both ends of the four fibers are brought inside the container where they are optically monitored for continuity. This forms a penetration detecting membrane along the sides of the cylinder. At each end of the cylinder are two panes of stressed glass. The presence of the glass panes are electronically monitored from within the cylinder and form a penetration detecting membrane over the ends of the cylinder. Although these membranes and numerous sensors provide active tamper indications, the membranes also provide passive evidence of tampering.

Passive indicators

When polarized light is passed through the stressed glass panes and viewed through another polarizing filter, stress patterns in the glass are apparent. These patterns are made varied by preconditioning the glass in a random manner just before the pane in immersed in an ion exchange bath. These patterns are photographically recorded for each pane before assembly. Since one needs access to both sides of the pane to view this pattern, it is not available once the container has been assembled. An adversary breaking the glass for entry will not be able to replace it with a pane that produces the same stress pattern and his tampering will be detected.

Either through production accidents or intensionally, some of the optical fibers used to wrap the cylinder's sides will be broken at random locations. A cylinder that had only two intact fibers would be considered useful and would be deployed. Since both ends of all fibers are inside the cylinder, the condition of the fibers can only be determined from there. Before assembly, the location of any breaks in each of the fibers will be measured using an optical time domain reflectometer. Any intrusion attempt through the sides of the cylinder would alter the condition of the wrapping fibers. Since the adversary did not know the initial condition, he could not replace the windings with ones producing the same conditions and his tampering would be detected.

Active tamper indicators

Figure 2 shows a block diagram of the Tamper Monitor.

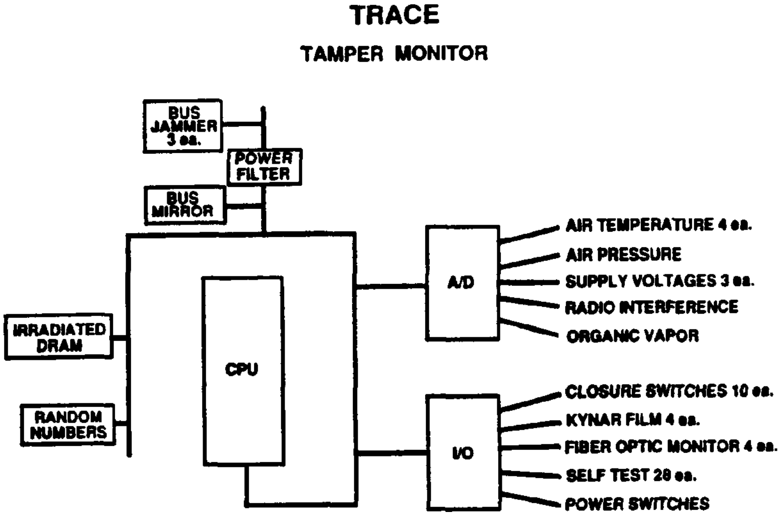

FIGURE 2

The Tamper Monitor is controlled by a CDP6805E2 microprocessor. Via a 12-bit analog-to-digital converter, the processor can monitor the outputs of several analog sensors.

Temperature - There is one electronic thermometer on the Tamper Monitor's circuit board and three off-board thermometers connected by cables. The thermometers (as all analog sensors) are monitored about 6 times a second. If any thermometer is found below 0 degrees C or above 70 degrees C, the Tamper Monitor declares an alarm state. In the alarm state, the Tamper Monitor evokes its penalty (discussed later) and will respond as being non-secure to any status queries by the Communicator . The Tamper Monitor controls the power to several devices within the secure container. Among these are the Camera, and the Authenticator. Generally these are only turned on as needed. However, below 10 degrees C, they will be left on to provide supplementary heat.

Air Pressure - An air pressure transducer is mounted on the Tamper Monitor board next to the thermometer. Since the air pressure in the secure container is the same as that in the interior of the environmental container, a change in this pressure is an indication that the environmental container has been breached. To accommodate the fact that air pressure will change benignly with temperature, the allowable limits on air pressure are computed based on a convolution of the four thermometers using the ideal gas law. Each pressure transducer has been calibrated over temperature. The processor's program contains the transducer's temperature correction data and uses the on board thermometer to compensate it. Since the interior would probably have been pressurized with dry nitrogen to provide a good environment for the Camera, this security indication comes at little extra cost.

Supply voltages - Three of the internal supply voltages are monitored. An attempt to degrade the system's performance by tampering with the power provided will result in an alarm.

Radio Interference - One way to defeat this system is to discredit it by causing frequent false alarms by disturbing operation with radio energy beamed at the TRACE. Circuitry has been included to indicate this activity is taking place.

Organic vapor - A solid state organic vapor sensor is included. The device is insensitive to low vapor concentrations but provides a robust response to high concentrations. The purpose of the device is to block the use of solvents to manipulate the interior of the container. The container's wall materials have been selected to produce fumes when subjected to laser beams or solvents that might be used to modify an interior device.

The processor is connected by input/output expanders to a number of digital sensors.

Switches - The processor monitors the state of ten switches. Presently, four of these are used to monitor the presence of the stressed glass panes. These switches are mounted to the case and have their actuation rods depressed by the glass. A mix of complimentary action switches are used so that an adversary will not know if he should move the actuation rod in or allow it to move out to keep it safe. A fifth switch rests in a groove milled inside the cylinder. This switch detects motion of the interior electronics relative to the cylinder. Some of the remaining five switches are used for monitoring magnetic reed relays to detect the use of magnetic fields to manipulate the interior. The remaining switches are spares. Because the state of the switches is only sampled (alarm not latched), they are checked three times more frequently than other sensors.

Kynar film monitors - Kynar films are attached to each of the four stressed glass panes. These are piezoelectric polymers that produce an electrical signal if the glass panes break. The response of these films is so robust that the monitor circuitry must protect itself from the high voltage signal. Signals over 100 volts are typical. To guard against the metallization of these films being etched away, each electrode has two conductors attached at opposite sides. Continuity of the metal between conductors is frequently tested. Since application of an electrical signal to test continuity produces an audible sound in the piezoelectric film, decoy applications are made to prevent the adversary's using this sound to deduce interior operations.

Optical fiber monitors - Mounted on each side of the Camera are circuit boards containing optical transmitters and receivers. These are connected to each of the four optical fibers. A simple on/off light signal is sent into each fiber. All fibers are monitored to assure that the fibers are dark when they should be dark. At reset, the processor determines which of the fibers are continuous and configures the monitoring hardware to assure that these fibers have light when there should be light. The optical components produce substantial heat in operation. When the interior temperature rises above 50 degrees C, the optical fiber monitors are placed in sparse coverage mode where their power is cycled on for one second at random intervals of up to 20 seconds.

Sensor supervision - An adversary can short circuit conductors by merely introducing a puddle of mercury. Open circuits may be created with a strategically placed puddle of acid. To force the task of internal tampering beyond simply cutting or shorting wires, each of the 28 sensors is supervised. Via a separate conductor the sensor is forced to impose the alarm condition on its signal wires. Signal wires are tested each time the sensor is checked.

ADDITIONAL FEATURES

To keep the internal workings of the Tamper Processor private, several other features are used. The least significant bit of the 12-bit analog-to-digital converter is used to construct random numbers. These random numbers are used to alter the Tamper Monitor's route through its tasks each time through its surveillance loop.

Since the Tamper Processor has so many wires connected to it, it was deemed unrealistic to silence it in a TEMPEST sense. To block adversaries from deducing internal operations from monitoring electrical noise on the TRACE external power line, a bus mirror was employed. A bus inverter was connected to the internal Tamper Monitor system bus. The inverter drives a capacitor bank with the same capacitance as the system bus. Thus for every bus transaction, the compliment of the value written on the bus is written into an equivalent capacitance. Thus, noise produced on the power lines should be somewhat independent of the bus contents. All Tamper Monitor activity takes place inside of a noise filter. Connected outside of this noise filter is a jamming gate driving a large capacitor at the same frequency as the bus transactions. The two optical fiber monitor cards have their own independent oscillators to clock their activities. Outputs derived from these independent oscillators drive jamming capacitors at the same frequency as the Tamper Monitor bus transactions. The information related to the internal bus has been quieted and then covered with noise at the same frequency that bears no information.

PENALTY EVOCATION

Detection of an intrusion is only part of the job. Things still have to be arranged so that an adversary can not:

1 open the container,

2 install signal substitution electronics on the Camera/Authenticator link,

3 close the container, and

4 offer it as the pristine product.

This situation becomes worse if the container must be stored away from supervision for an extended time. What was needed was a way for the Tamper Processor to record the fact of the intrusion in a way that could not be erased by the adversary, to whom is granted the ability to re-manufacture the entire TRACE. The mechanism of a Secure Storage Number (SSN) is used.

While it is known that the TRACE is still secure, a three-byte number is installed. The Tamper Monitor has the task of erasing the SSN if it detects intrusion. From time to time, the Tamper Monitor is asked to reproduce this number to demonstrate its fidelity. A Tamper Monitor that reports that it is secure but cannot correctly reproduce the SSN, has been tampered with. But suppose that the adversary employes a rapid attack. An adversary might use a high speed bullet or a laser beam that destroys or stops the processor before it can erase the SSN. For this reason, the SSN is stored in Dynamic Random Access Memory (DRAM).

DRAM is an inexpensive form of memory that has the property that data written to it exist there only tenuously. The data must be frequently refreshed or it is lost. This task is so complicated that many designers employ the more expensive static form of memory. However this shortcoming of DRAM makes it the ideal storage place for the SSN. The Tamper Monitor's processor is the only device keeping the SSN refreshed in the DRAM. If it is stopped, it will not be able to erase the SSN but it also will not be able to keep it refreshed. Either way, the SSN is erased. Or is it?

Commercial DRAM's were purchased. Their data sheets advised that the devices needed to be refreshed every 4 milliseconds. However when tested, it was discovered that the devices actually retained their contents for as long as 60 seconds without being refreshed. Reducing the temperature to 0 degrees C allowed them to retain data for several minutes. This was considered long enough for an adversary to open the container and install his own refreshing circuitry around the DRAM and thus save the SSN. Applying knowledge gained from radiation effects on weapon electronics, the DRAM's were irradiated with neutrons in the Sandia SPRIII reactor. After an integrated dose of $1x10^{13}$ nvt with energy greater than 1 Mev, the room temperature retention time was reduced to 3 seconds. The 0 degrees C retention time became 10 seconds.

ALARM RESPONSE

Upon detecting an intrusion, the Tamper Monitor erases the SSN. When next asked its status, it will report the intrusion. Of course, as with any alarm system, the alarm may be real, false, or caused by a malfunctioning sensor. If the TRACE is in service where the alarm may be promptly assessed, matters are simple. Indeed, to assure prompt assessment, it is recommended that TRACE's always be deployed in groups where each TRACE is in view of another TRACE that may be used for alarm assessment. If the alarm can be resolved as a false alarm, the external system need only instruct the Tamper Monitor to reset and then install a new SSN. The Tamper Monitor then resumes its business.

Upon being reset, the results of its first check of all sensors are recorded. Any faults detected at that time are noted as forgiven faults. Alarms will not be produced by a sensor being logged as having a forgiven fault. This philosophy allows the TRACE to "limp along" with a broken sensor and still be a useful security instrument.

If the intrusion detection takes place in storage or when it can not be promptly assessed, the TRACE will probably have to be disassembled and inspected for signal substitution electronics. At that time the TRACE would also be examined for passive evidence of intrusion.

CONCLUSIONS

A secure container to tamper protect the link between a television camera and a data authenticator has been described. This container provides both passive and active indications of tampering. An abundance of tamper sensors gives a high probability of intrusion detection and through the use of the Secure Storage Number concept, penalty evocation is guaranteed.

REFERENCES

1. C.S. Johnson et al, "Authentication Equipment for the Advanced C/S Systems." Proceedings of INMM, 1989.

ACKNOWLEDGMENTS

I acknowledge the help of the following individuals in the creation of TRACE. Bill Black, Robert Hogan, George Johnson, Howard Kimberly, Mark Lovell, Bill Payne, Mark Soo Hoo, Mark Vaughn, and Richard Vigil.