

Authenticating and Monitoring Shipping Containers and Cargo to Detect Weapons of Mass Destruction

Fred Hewitt Smith
ANGEL Secure Networks™, Inc.
127 Washington Street
Belmont, MA 02478
617 489 7304

fredsmith@angelsecurenetworks.com

Benjamin Smith
Columbia University
910 Riverside Drive, 4C
New York, NY 10032
(917) 575 1298
bhs16@columbia.edu

ABSTRACT

Application of Angel system to prevent enemy use of shipping containers or truck bodies to deliver nuclear weapons (or other weapons of mass destruction) into US ports or cities. Extends existing technology of embedding wireless temperature sensors inside shipping containers to securely install and embed nuclear etc. sensors attached to wireless intelligent agents inside containers and harden them against attack by a sophisticated enemy working possibly in concert with insider moles. Embedded sensors can more thoroughly examine container cargo over long time periods. Guards against sophisticated reverse engineering, detects tampering, and automatically detects containers lacking sensors. Military monitors sensors via satellite.

1. INTRODUCTION

This is a systemic approach to the problem of preventing the use of shipping containers as vehicles for delivery of weapons of mass destruction into US ports. New system components, such as orthogonal authentication, strobed encryption, orthogonal sensors, and random confusion are described [1][2][3][4]. The availability of these technologies makes the system design feasible. The system could be extended to detect and prevent weapon delivery via trucks.

The proposed system involves introducing sensors inside containers and monitoring the containers as the containers move through world commerce. The use of sensors to monitor temperature in shipping containers is already well known [5]. However, the existing technology operates in an environment where the persons placing the sensors in the containers want them to be there.

The new elements in the problem which we address are (a) how to introduce sensors into containers against an enemy who does not want them there; (b) how to prevent the enemy from tampering with the sensors and/or data collected by the sensors and how to detect tampering; (c) how to prevent the sensors from being reverse engineered; (d) how to be certain that all arriving containers are equipped with the required sensors; and (e) how to integrate data collected from sensors in containers and present it in real time to the military to facilitate timely intervention [6].

Approximately 95% of US annual commerce comes by ship through US ports [7]. Maritime industries contribute \$742 billion per year to the US GNP [7]. Approximately 10,000

© Angel Secure Networks, 2002, All rights reserved

vessels enter the US each year, and make approximately 68,000 port calls [7]. Although more than 2,000 vessels have been boarded since September 11, 2001, by the Coast Guard in New York Harbor alone [7], only 2% of the roughly 6 million containers that arrive on cargo ships each year are actually inspected by US officials [8]. The facilities for inspecting the contents of containers from outside the container are large and expensive and their effectiveness has not yet been proven. Practically speaking, it is hard to see how thousands of containers could be inspected daily without creating huge bottlenecks in maritime commerce. At best, spot checks would be possible. In any case, most US ports have no such facilities at all.

Sensors located inside the container might have advantages over the procedure of scanning a container from the outside, in that the sensors would not have to penetrate the container itself and could collect data over a much longer period of time, i.e. the duration of the voyage as opposed to a few seconds or minutes. Their use would not require the construction of costly scanning equipment at each port, or persons to run the scanning equipment. (The addition of scanning equipment and personnel at US ports could also provoke a labor dispute with the dockworkers' union). By comparison, wireless processors are cheap and can be easily and inexpensively replaced as sensor and wireless technology evolves. Sensor technology is highly sophisticated [9]. Sensors appropriate for the use described in this paper can reasonably be expected to become available in the near future.

2. SYSTEMIC APPROACH

The stated goal of preventing the delivery of weapons through the use of shipping containers requires an examination of the total problem space. The enemy is presumed to be determined, technologically sophisticated, well financed, and to be working with insider moles who have been bribed, coerced, or recruited by ideological commitment. The enemy has time, and can choose the time and place of an attack. The enemy may mount numerous attacks simultaneously. The enemy has agents available for suicide missions.

The defenders, who are broadly defined as the US military, can control the containers, even though they will be briefly in the custody of the enemy while being loaded. The defenders can configure the container sensors just in time before

delivery and can present the enemy with a randomly generated configuration. The defenders can choose which sensors to use and can conceal which sensors are operating from the enemy. The defenders have the time required for an ocean voyage in which to conduct their inspection of the container's contents. The defenders can mandate conditions for entry of containers into US ports.

2.1 Strobed Encryption

Strobed encryption is a technology whereby two ends of a connection randomly generate and exchange keys and other data every 60 seconds. Strobed encryption, when combined with Orthogonality, can eliminate the need for digital certificates and certification authorities, that is, the PKI. The PKI maintains values that have a validity that extends into months, whereas with strobed encryption the life time of critical security values is a matter of seconds or minutes.

We have developed and tested strobed encryption over a period of several years [2][3][4].

2.2 Orthogonality

One of the most intractable problems in establishing secure networks is ensuring that the counter party, whether a person or a machine, located at a particular node, is in fact the authorized user and not some imposter. Orthogonal Authentication is a strategy for verifying that the party on the other end of the connection is who he, she, or it claims to be. "Orthogonal" in this context means that overlapping, different methods, systems, and chains of command are used to perform the authentication, and the overlap occurs both in the sense of different systems being in use at the same time and periodically. An enemy who could overcome one verification point will not have unlimited or continued access without surviving subsequent, periodic verification procedures. An example of how these different inputs come together and provide orthogonal authentication is shown in sections 3 and 4 below.

2.3 Preventing Reverse Engineering

In general, the enemy should not be able to determine how an executable operates; if the enemy could reverse engineer one executable, this should not help with another executable; attempts to reverse engineer should be detectable; the time the enemy has available to perform reverse engineering should be minimized. ANGEL provides techniques and strategies to address these issues.

2.3.1 Random Confusion

Random confusion is the general principle that random values should be generated just in time and introduced into software before it is installed. We extend the idea of diversity introduced by Wang and Knight [10] and attempt to overcome the techniques of reverse engineering described by Cifuentes and others [11].

One example is that network nodes are generated immediately before installation. The nodes are provided with keys that are used for the first key exchange. Each key pair begins with a unique set of randomly generated starting values. Immediately after the first connection, new key

values are randomly generated by the nodes themselves and securely exchanged using asymmetric encryption, that is, by strobing. We have developed network generators that randomly supply startup keys to network nodes.

However, the principle of random confusion can be taken beyond random key values. Each executable can be randomly different. The executable does not need to be a predictable derivative of its source code. All the executable has to do is run correctly. It does not have to be maintained. In fact it should not be maintained. It should be reinstalled.

When the executable first begins executing, there is no reason why, in the first second of life, it should not execute several billion instructions before it finally and unpredictably creates and loads into memory the instructions it will actually run.

2.3.2 Just In Time Installation

Software should be reinstalled as often as feasible, and critical software values should have periods of vulnerability that are as short as possible.

ANGEL applies just in time installation systematically throughout the system. Critical values have lifetimes that are measured in seconds or minutes.

2.3.4 Mutual Monitoring

As illustrated in SECTION 4.0 below, the ANGEL system can set up three or more nodes which each check on the others, and, if an attack is detected, can sound an alarm. This capability includes detection of man in the middle attacks.

2.4 Angel Installation

An Angel is a randomly generated agent which will install a network node one time only. The Angel's function is to install specific software in a specific target location one time only. The software for a particular node is generated with random start up values for connections to other nodes and random confusion. The executable and other files are delivered to an Angel server. The Angel then is delivered to the target site over a network. It checks that it is where it is supposed to be, contacts the Angel server, whose identify only it knows, installs the software and installs the node. The node then connects to a monitor server, whose identify only the node knows, exchanges key values and begins strobing. Each node is unique. If the ANGEL server detects the same node attempting more than one connection, something is wrong. The node is orthogonally audited immediately after installation. An orthogonal audit is a protocol that does not rely solely on the network between the target node and the Angel server. The military could place a telephone call to the remote location and ask the person on the other end to relay a code sent via the network to the target node. The military could require an employee previously known to be on the premises to identify himself through various biometric devices and to relay the code.

We would suggest that Angel installation be used throughout the proposed system.

2.5 Object Oriented Approach

The software described in this proposal is quite complex. Object oriented programming is important in allowing software development to occur in a controlled environment. We have developed package objects which turn themselves into streams and can be sent over networks. We have an item object from which other items can be derived to model any data format, including keys and one-time pads. Items can be inserted into and extracted from packages. Packages can be inserted into and extracted from packages and can be inserted into and extracted from warehouse objects, which are disk files. Packages are compressed and encrypted multiple ways. We can also implement dictionary compression at the data element level within an item.

In addition to providing a controlled framework for software development, the object oriented approach and the package objects provide strategies and facilities for implementing randomly confused software.

3.0 INSTALLING SENSORS IN CONTAINERS

The goal is to securely introduce sensors into containers and to use these sensors to detect whether the containers are hiding weapons. Also, it is necessary to be able to detect whether a given container is equipped with working sensors.

3.1 Sensor Box

Our design is based around a sensor box, which is a tamper aware, tamper resistant container holding multiple processors connected to various sensors suitable for detecting weapons of mass destruction. The sensing devices should also include audio and video recorders suitable for intelligence acquisition [8][12]. One processor would manage communication, whereas others would manage sensing devices. Some sensor boxes would be capable of communicating with an external monitor via wireless technology. The sensor box is manufactured and sold to shipping companies by the military. Using an orthogonal procedure controlled from a remote military facility (operated probably by the Coast Guard and/or Navy), the shipping company installs some number of sensor boxes in each container immediately before delivery of the container to a shipper.

Once installed in a container, each sensor box becomes a network node. Each sensor box is installed with an Angel. When the Angel starts a sensor box, following a protocol discussed in section 3.6 below, the sensor box immediately begins communicating with other sensor boxes in the container and with an external node maintained by the military.

3.2 Shipping Container

The container should contain mounting brackets for the sensor boxes, which are reusable. The sensors would communicate with one another via wireless communication or over a wired network provided by the container. We do

not rely on a hard wired network provided by the container to provide security, since a sophisticated enemy could penetrate a hard wired connection. Sensor boxes would have batteries to operate for short periods of time. The container should have an outlet to supply power to the sensor boxes. Power should be supplied to the container by the shipper while being loaded and by the shipping company while in the company yards and while on board the container ship.

3.3 Sensor Box Tester

A sensor box tester consists of various processors inside a tamper aware, tamper resistant container connected to various devices which simulate inputs so that sensors inside sensor boxes can be tested to determine that they are operating properly. The sensor box tester would be placed inside the container after the sensor boxes were installed. The sensor box tester would be operated remotely by the US military.

3.4 Control Box

A control box consists of several processors inside a tamper aware, tamper resistant container which is used by the shipping company to communicate with the US military and to order and install software for sensor boxes. The control box would contain various biometric devices to identify authorized participants at the shipping company site. The control box would also contain audio and visual sensors and other sensors appropriate for control and intelligence gathering.

3.5 Installation Protocol for Shipping Company

(a) Identifying software for each sensor box, sensor box tester, and control box is installed at the factory by the military using orthogonal Angel installation. (b) A set of sensor boxes, at least one sensor tester, and one control box is delivered to the shipping company. (c) Software for use by the shipping company is remotely installed and audited at the shipping firm by the military using the orthogonal Angel installation. (d) The control box will now remain in constant contact with the US military. (e) The installation of the control box and the tester software could be repeated remotely, automatically, and frequently, perhaps once per week.

3.6 Installation Protocol for Preparing Container for Delivery to Shipper

(a) Using the control box, the shipping company orders software for sensor boxes for a container. (b) The US military randomly generates software for these sensor boxes. (c) Using Angels, the software is remotely installed in the sensor boxes and the tester by the US military and is audited using orthogonal procedures. The software running in each sensor box is unique and only seconds or minutes old. (d) The sensor boxes are installed in a container and they immediately connect with one another using previously installed keys and begin strobing keys and communicating with one another and with the US military. (e) The tester is placed in the container and, under control of the US military, verifies that the sensors and sensor boxes are operating

correctly.(f) The container is delivered to the shipper for loading.

4.0 SECURITY OF INSTALLED SENSOR BOXES

The sensors are in constant communication with one another and a remote monitor via wireless. An attack on one would be detected by the others and set off alarms. A network of nodes can detect man-in-the-middle attacks against other nodes. For example, suppose that M is a man in the middle between A and B. When A and B strobe with one another, then send a hash of their key values to C, C can compare these values. If they are not the same, there is a man in the middle. A can similarly check B and C, and B can check A and C [3] [13]. The sensor boxes will also return audio and video information to the remote monitors.

5.0 DETECTING CONTAINERS THAT LACK SENSOR BOXES

The enemy could attempt to place a container on a container vessel that did not have sensor boxes, and in this container it could place a weapon of mass destruction. Consequently, a method is needed to examine containers on a ship to identify a container that does not have embedded sensor boxes.

The containers on a container ship that are equipped with sensor boxes can communicate with a shipboard monitor. Attendance can be taken. However, that will not identify a rouge container without sensor boxes that has been hidden among the containers equipped with sensor boxes.

For this purpose, a robot is needed which can scan for and identify large objects and, having identified the object, approach it and determine whether it contains sensor boxes. Laser scanners have been used to successfully scan huge buildings to obtain precise measurements [10] A further development of this technology might permit laser scanning of containers on board ship by robot controlled scanners and then eventually laser scanning of cars and trucks passing through tunnels and bridges.

6.0 PROVISION OF DATA TO US MILITARY

The sensor boxes in the container communicate with external monitors and through them with the US military via satellite networks. The communication is secure and continuous. Data is fused and analyzed to target containers that require manual inspection.

7.0 EXTERIOR INSPECTION OF SHIPPING CONTAINERS

A potential danger of an exterior inspection system is that the container could be altered or tampered with after inspection. If a container with sensor boxes is inspected by an exterior system, this information can be securely conveyed to the sensor boxes inside the container. The sensor boxes can be used to detect whether the container has been thereafter tampered with, opened, or substituted.

Thus the system presented herein is complementary to and can enhance container inspection systems using exterior sensors.

REFERENCES

- [1] B. Smith and F.H. Smith, co-inventors, US Patent No. 6,067,582, issued May 23, 2000, "System for Installing Information Related to a Software Application To A Remote Computer Over A Network". This patent describes a system for securely distributing software applications and other digital information over a network.
- [2] F. H. Smith and B. Smith, PCT/US99/27138, "System and Method for Installing an Auditable Secure Network", which received preliminary approval from the Examining Authority of the Patent Cooperation Treaty on April 13, 2001. This patent provides for strobed encryption, network security, counter-party authentication, automatic network generation, and further network auditing.
- [3] F.H. Smith and B. Smith, PCT/US01/03954, "System and Method for Installing An Auditable Secure Network", which received preliminary approval from the Examining Authority of the Patent Cooperation Treaty on August 12, 2002. This patent describes a method for preventing man-in-the-middle attacks on the system.
- [4] Patent pending on some aspects of these technologies..
- [5] www.sensitech.com.
- [6] For a discussion of some of the problems in data collection experienced by the Navy, see Admiral Vern Clark remarks, "Meeting the Homeland Defense Challenge: Maritime and Other Critical Dimensions", p. 10, Institute for Foreign Policy Analysis and Fletcher School of Law and Diplomacy, Royal Sonesta Hotel, Cambridge, MA (March 26, 2002).
<http://www.chinfo.navy.mil/navpalib/cno/speeches/clark-hdtran020326.txt>
- [7] *Coast Guard News and Events*,
http://www.uscg.mil/news/homeland_security/homeland_security.htm
- [8] N Boodhoo, *Reuters*, "Al Qaida not the only threat to U.S.", *The Miami Herald*, May 26, 2002.
- [9] www.ortec-online.com/papers/reprints.htm.
www.canberra.com/homeland.htm.
- [10] C. Wang and J. Knight, "Towards Survivable Intrusion Detection", Department of Computer Science, U. Va, <http://www.cert.org/research/isw/isw2000/papers/38.pdf>.
- [11] C. CiFuentes, T. Waddington, & M. Van Emmerik, "Computer Security Analysis through Decompilation and High-Level Debugging", Proceedings of the Eight Working Conference on Reverse Engineering (WCRE '01) IEEE, 2002.
- [12] DEBKA-Net-Weekly, "Container Stowaway Terrorists Steal into America", Vol. I, Issue 64, DEBKA, Jerusalem, June 14, 2002, www.debkafiles.com
- [13] Patent pending.
- [14] P.K. Allen, I. Stamos, A. Troccoli, B. Smith, M. Leordeanu, Y.C. Hsu, "3D Modeling of Historic Sites using Range and Image Data", 2002,
www.cs.columbia.edu/allen/PAPERS/ra03.pdf
<http://www.cert.org/research/isw/isw2000/papers/38.pdf>.