IMPROVED SECURITY VIA "TOWN CRIER" MONITORING

R.G. Johnston, A.R.E. Garcia, and A.N. Pacheco
Vulnerability Assessment Team
Los Alamos National Laboratory
MS J565, Los Alamos, NM 87545

ABSTRACT

Waste managers are increasingly expected to provide good security for the hazardous materials they marshal. Good security requires, among other things, effective tamper and intrusion detection. We have developed and demonstrated a new method for tamper and intrusion detection which we call the "town crier" method. It avoids many of the problems and vulnerabilities associated with traditional approaches, and has significant advantages for hazardous waste transport. We constructed two rudimentary town crier prototype systems, and tested them for monitoring cargo inside a truck. Preliminary results are encouraging.

INTRODUCTION

Hazardous wastes and waste management programs represent tempting targets for terrorists, criminals, radical activists, disturbed individuals, and disgruntled current or former employees. Countering these threats requires effective security. Effective security, in turn, requires (among other things) reliable methods for tamper and intrusion detection. Tampering can be thought of as gaining unauthorized entry or access, i.e., engaging in intrusion, for nefarious purposes such as theft, diversion, espionage, sabotage, vandalism, or unscrupulously hiding high-level wastes inside containers previously certified to hold only low-level wastes.

Tamper-indicating devices ("seals") are often used for tamper detection [1-3], especially for individual containers, or for truck, railcar, transportainer, or room doors. Seals are designed to detect tampering after the fact. Intrusion detectors, on the other hand, are meant to work in real-time: they report unauthorized access or entry as it happens. There are advantages and disadvantages to each approach.

It is difficult under the best of circumstances to provide reliable, unspoofable, cost-effective tamper or intrusion detection. In fact, it may not even be totally possible [4,5]. Hazardous wastes represent particular security challenges because of the health, safety, environmental, legal, bureaucratic, and financial issues associated with waste management. When hazardous wastes are under transport, the problem is even more complex because of their mobility, as well as constraints on the space, weight, personnel, and electrical power available to provide security.

Detecting tampering or intrusion for international safeguards purposes adds even more challenges [5]. This is because the "adversary" is a nation (treaty signatory) with world-class resources that can be used to try to defeat the monitoring systems should it desire to cheat on the treaty or arms control agreement. Moreover, the adversary (not the protagonist) owns the assets of interest, the facility or transport vehicle that contains them, and must approve and have

complete knowledge of all details of the monitoring hardware. This is backwards from conventional security applications such as domestic nuclear safeguards [5].

Given the difficulty of providing effective tamper or intrusion detection in general, and particularly for waste management applications, it is useful to consider unconventional approaches to security. This paper concerns an alternate approach to tamper and intrusion detection: continuous, unidirectional, real-time, low-bandwidth, anti-alarm monitoring. This approach, which we call the "town crier" method, is meant to overcome the problems associated with conventional tamper and intrusion detection, including for transport applications. The town crier method can be applied to complete monitoring systems, or to sub-components such as tamper-indicating seals or intrusion sensors.

THE PROBLEMS WITH CONVENTIONAL TAMPER & INTRUSION DETECTION

A tamper-indicating seal is a device for detecting tampering or unauthorized entry [1]. The most familiar everyday example of seals is probably that of the tamper-evident packaging found on over-the-counter pharmaceuticals. Unlike locks, seals do not attempt to delay or impede unauthorized access. Instead, they record that it took place.

With seals, the fact that tampering has occurred is stored until such time that the seal can be inspected. This fact can be exploited by an adversary [6]. Many of the most effective attacks on seals involve an adversary letting the seal detect the unauthorized access, but then erasing or removing the stored information, i.e., the alarm condition, prior to inspection. Indeed, most seals, including high-tech seals, can be easily and quickly defeated using low-tech methods, tools, and supplies [3, 5]. (To "defeat" a seal means to open it, then reseal using either the original seal or a counterfeit, without being detected.)

Intrusion detectors [7], in contrast to seals, typically attempt to overcome the problem of storing the alarm condition by instead immediately sending a real-time alarm to some distant location when unauthorized access has been detected. The usual weakness in this approach is that the alarm signal can be blocked, leaving the intrusion undetected. It is common to attempt to overcome this vulnerability by using encryption, authentication, or sensor polling methods involving two-way communication. Such approaches, however, tend to create serious problems including complexity, high cost, and difficulty in hardware installation and use. The need to maintain continuous, often two-way and/or high-bandwidth communication is also a challenge, especially for moving cargo.

Other common problems with conventional intrusion detectors include inadvertent and deliberate false alarming, and a wide variety of security vulnerabilities and real-world reliability problems, aggravated by hardware and software complexity. Moreover, the encryption or authentication cipher used by some intrusion detector systems is computationally intensive, and can be compromised, broken, or bypassed any number of different ways, sometimes by even relatively unsophisticated adversaries [4, 8]. There are also serious challenges associated with protecting the sensors, the encryption or authentication electronics, the network, and any cipher keys.

THE "TOWN CRIER" APPROACH TO INTRUSION DETECTION

Our alternate approach to intrusion detection, the "town crier" method, relies on continuous, unidirectional, real-time monitoring. Rather than storing information about intrusion (which can be erased), or sounding a real-time alarm (which can be blocked), or maintaining complex two-way communications, or needing to process continuous high-bandwidth data at a distant location, or dealing with the problems and vulnerabilities of computational ciphers, this approach involves a simple, very low bandwidth "anti-alarm". The anti-alarm is a frequent and periodic "All OK" signal that indicates the *absence* of intrusion. Under this approach, the failure of the "All OK" signals to arrive, at least for any significant amount of time, must be taken to mean there has been intrusion.

For most applications, the bandwidth required for the anti-alarm will be between 1 bit and 1 byte per second. Even lower transmission rates, however, are possible, especially if it takes more than 1 second to attack the assets being monitored. Because of this low bandwidth, the "All OK" signal is ideal for encryption using a one-time keypad. A "one-time keypad", also called a "one-time pad" or "Vernam cipher", uses a random key having the same length as the message to be encrypted [9]. This key can never be reused. One-time keypads are not practical for encrypting large amounts of data because the key is so long. One-time keypads, however, are practical for low bandwidth data. A one-time keypad has the advantage of being the only encryption algorithm that can be shown mathematically to be unbreakable. It is also quite simple in that it uses a lookup table, instead of the massive computation required by other encryption schemes. This is a definite advantage for hardware simplicity and cost effectiveness. The size of the lookup table is fairly modest by today's standards: 4 MB for a year of monitoring at 1 bit/sec, and 32 MB at 1 byte/sec (less with data compression). Moreover, unlike certain other ciphers, use of a one-time keypad does not introduce proprietary or international export control issues, nor does it compromise domestic security by giving away domestic security hardware and approaches.

The anti-alarm approach considered here is analogous to the town crier concept used in the past by soldiers and medieval towns for security [10]. The town crier would call out each hour (sometimes in code) that, for example, "10 o'clock and All's Well!". If invaders should overpower him before he could sound an alarm, the absence of the "All OK" signal (and the crier's familiar voice) at the appointed time would indicate trouble.

Receiving the "All OK" signal at Headquarters (HQ), or at a security or inspector's station, can be fully automated. A computer can easily check the incoming data against its copy of the one-time keypad to verify that the correct "All OK" signals continue to be sent. The computer can alert HQ personnel if the expected "All OK" signal fails to appear on time.

The major advantages of the "town crier" approach to intrusion detection include:

- It permits continuous monitoring.
- It operates in real-time, and can alarm in real-time, allowing immediate response.
- It is simple, open, and transparent, yet offers very high levels of security.

- For reasons of security and simplicity, no sensor data or other information (other than the low-bandwidth "All OK" signal) is released from the monitoring system during the monitoring process. This provides little opportunity to sneak classified or sensitive data out of a facility or transport vehicle being monitored.

- Because of this low bandwidth, it should be possible to monitor large numbers of moving vehicles, ships, or cargo containers simultaneously.

- For reasons of security and simplicity, there is no communication into the monitoring system during the monitoring process. In other words, the town crier approach is unidirectional.

- HQ remains passive and silent throughout the monitoring (as long as no intrusion is detected). As a result, any failures or deficiencies of hardware or personnel inside HQ—and perhaps even HQ's location—can remain unknown to the adversary.

- Decisions about whether intrusion has occurred are automatically made locally by the monitoring system, rather than at a distant HQ. The decision-making process is protected by the monitoring system itself in that it monitors itself for evidence of attempted spoofing.

- The data coming from the system ("All OK" signals) can be publicly broadcast. There is no need to keep the signals secret, or to secure the transmission channel, even when the signals emanate from a high security nuclear facility.

- It may be desirable for security and counterterrorism purposes not to advertise to the general public know that a given truck, railcar, or ship is carrying hazardous materials. It is relatively easy to hide a byte/second (or lower bandwidth) transmission in amongst general communications traffic. This is in contrast to a blatant high-bandwidth signal (often considered for conventional transport intrusion detection) that might call undue attention to the transport vehicle and its contents.

- For treaty monitoring, this approach is well suited to having 100% host-provided and host-controlled monitoring hardware, with the one-time keypad provided by the inspectors at monitoring startup time. There is little need for troublesome dual control of monitoring hardware.

- The simplicity of the approach permits the use of low-cost, commercial off the shelf (COTS) hardware.

A major disadvantage of the town crier approach is the need for continuous, highly reliable transmission of the (low-bandwidth) "All-OK" signals. (This not an issue for tamper detection, discussed below.) Indeed, the inadvertent loss of signal for longer than the time reasonably needed by an adversary to surreptitiously execute an attack must be taken to mean that intrusion has occurred. If the waste storage area, or transport vehicle is properly designed, however, any attack should be far from instantaneous. Moreover, communication reliability can, if necessary,

be enhanced by using redundant, dissimilar channels of low-bandwidth communication to send the same "All OK" signal. Only one of the channels needs to get through at any given time. Depending on whether the monitored assets are stationary or under transport, some possible communication channels include an electrical wire, fiber optics, radio signals (including short-wave), cell phones, the Internet, acoustic/infrasound/ ultrasonic signals, flashing lights or displays, laser beams, and mechanical signs.

Another significant disadvantage of the town crier approach is that it does not provide security personnel with an immediate indication of what specific event or activity led to intrusion being reported. On the other hand, they can eventually gain such information when allowed final access to the monitoring system to observe the recorded sensor data. This sensor data is for diagnostic purposes only, however, because its veracity is not guaranteed, given that intrusion has been reported.

A third, largely theoretical disadvantage of the town crier method is that the one-time keypad, unlike modern asymmetric (private/public key) ciphers needs—for the best security—to be physically exchanged between personnel at the monitoring location (or vehicle) and HQ prior to monitoring. This is in contrast to modern asymmetric (private/public key) ciphers where the encryption key can be openly published [8,9]. As a practical matter, however, this is not a serious limitation. Monitoring of critical assets cannot be done reliably by proxy; good security requires that trusted personnel be on hand to at least initiate the monitoring process and verify that the actual assets (hazardous waste) of interest are the ones truly being monitored. Moreover, a single exchange of computer media can provide many years' worth of one-time keypads for multiple containers, facilities, or transport vehicles.

THE "TOWN CRIER" APPROACH TO TAMPER DETECTION

Instead of using the town crier monitoring system as a (real-time) intrusion detector, it can also be used as a (delayed response) tamper detector. Unlike conventional seals, however, this approach does not try to store the alarm (tampering) condition, which is the chief vulnerability for most seals. Instead, the equivalent of an anti-alarm is used. At startup time, security personnel (or treaty inspectors) input a single, short random number known only to them. Should tampering be detected, the system immediately erases this number. When security personnel (or inspectors) return to re-examine the system, the absence of the correct random number means that tampering has occurred. The monitoring system can recognize authorized security personnel or inspectors through a password sent remotely via a radio frequency or infrared signal, or by a hard-wired external keypad. An adversary using the wrong password causes the stored random number to be immediately erased.

There is no easy way for an intruder to erase the evidence of tampering, because the unauthorized access itself causes an erasure of the stored random number before the intruder can determine what it is. Note that this approach is different than the idea of a security monitoring system deleting the encryption or authentication key when tampering is detected; such a strategy is sometimes used by conventional electronic seals and monitoring systems that transmit encrypted data to the outside world. Their encryption/authentication key is not as secure to begin with because the hardware has been telling the outside world bits of information (through its data transmissions) that can be exploited by cryptanalysts to try to break the cipher. With town crier

tamper detection, in contrast, no hints are provided to the outside world about the random number stored within.

THE "TOWN CRIER" PROTOTYPES

We constructed two generations of rudimentary town crier prototypes and briefly tested their performance for both tamper and intrusion detection. The prototypes were installed in a delivery truck, shown in figure 1. The truck was a salvaged, 1989 K30 Chevrolet truck with a somewhat light-tight cargo area.

Fig. 1. The truck used for tests of the town crier prototype.

The two prototypes, Generation 1 and 2, differed primarily in their means of communication. The earlier Generation 1 prototype relied on use of Apple Airport radio frequency (rf) cards. No antennas were used. The Generation 2 prototype used an inexpensive consumer cell phone and digital modem to transport the "All OK" signals. Two, 33-cm tall, passive repeater antennas (BCT, Inc) were used to increase the cell phone signal strength. While not mandatory, these antennas improved the reliability of the cell phone connection.

With the Airport cards, the maximum rf transmission range was only 50 meters for our "All OK" signals. This is far too limited for most intrusion detection applications, though not impractical if an escort vehicle is intended to closely follow a transport truck. For tamper detection, however, a range of 50 meters is more than adequate since the cargo can come to rest in front of security personnel or inspectors at its final destination before they check for tampering.

The transmission range of the cell phone used for Generation 2 was not a limitation, since it can cover most of the United States, but the reliability of the cell phone connection can be a significant problem for a moving vehicle, especially in the mountains of Northern New Mexico where this work was undertaken.

While either the Airport cards or the inexpensive digital cell phone are satisfactory for "town crier" tamper detection, they are inadequate in terms of range and/or reliability for real-world, real-time intrusion detection. Nevertheless, we found them useful for testing the town crier concept. Either method of communication is probably acceptable as a backup, rather than primary, means of continuous communication back to HQ.

There are a number of other serious problems and constraints with our prototypes. Because of the very limited funding available for this project, they were assembled with the assistance of relatively inexperienced undergraduate students, and was constructed from surplus and borrowed inexpensive hardware. Much of the hardware, including most of the sensors, are not intended for security applications. Indeed, we used several devices made by Vernier Software and Technology, Inc. that are actually low-cost science lab equipment meant for high school students. Another serious constraint is that the amount of time available for testing our prototypes was severely limited.

Given these problems and constraints, we do not consider our prototypes to be ready for practical use, anywhere near robust and reliable enough for real-world applications, or even developed enough to merit extensive testing. Nevertheless, we believe that the performance of our prototypes, crude as they are, does suggest that the town crier concept may indeed be feasible for real-world applications.

Our prototype system was built around two Apple iBook notebook computers. The software for both computers was written in REALbasic 3.5 and 4.5.1 (Real Software, Inc.), a cross-platform, object-oriented BASIC development environment and compiler with extensive graphical user interface (GUI) tools.

One of the iBook computers, called the "Sender" computer, is located inside the truck to monitor the security sensors and transmit wireless Airport or digital cell phone signals to the "Receiver" computer. The Receiver computer remains outside the truck to receive signals from the Sender computer.

Each iBook in the Generation 1 prototype had an internal Apple AirPort card for transmitting or receiving 2.4 GHz spread spectrum rf signals at 15 dBm. No government communications license is required to operate the AirPort cards. They are capable of transmitting up to 11 Mbps, although our "ALL OK" signal requires only 1 byte per second. Maximum nominal transmission distance was found to be 50 meters. No antennas were used. The AirPort card on the Sender computer had to transmit through the metal encased cargo area of the truck, while the Receiver computer was typically located inside a building (when the truck was stationary), or inside an escort automobile (when the truck was in motion).

For the Generation 2 prototype, a Motorola StarTac 7868W digital cell phone (nominally 800 Mhz) with a digital modem was attached to the Sender iBook computer. The Receiver computer relied on its internal modem and a fixed phone connection to receive signals from the Sender computer.

All rf signals were sent without redundancy. Thus, the appropriate one-time "All OK" byte was transmitted only once each second. Presumably greater signal reliability would be possible if each "All OK" byte were to be broadcast dozens or hundreds of times during its one second lifetime.

The 120V, 60Hz AC power for the monitoring system was provided by a Galaxy 1500 Watt DC to AC Power converter that ran off the truck battery, although the nominal total power requirements for all the hardware used inside the truck (including the iBook computer) was less than 24 Watts, half of which are needed by the Infrared (IR) illuminator to provide lighting for the video camera.

The monitoring system inside the truck consisted of the following:

- the Sender iBook notebook computer to monitor the sensors, detect unauthorized access to the truck and act accordingly, plus transmit rf signals via either the Airport card or digital cell phone
- a Vernier Labpro Analog to Digital Converter & Computer Interface to read the sensors
- a Vernier MG-BTA Magnetic Sensor to detect the opening of the truck backdoor
- a Vernier LS-BTA Light Sensor to detect changes in ambient lighting (such as the appearance of daylight or flashlights) inside the cargo area
- a Vernier MB-BTD Ultrasonic Motion Detector to detect relative motion inside the truck
- a SuperCircuits PC-21XP2 monochrome pinhole camera to monitor the cargo, iBook computer, and sensors
- a ICU Security DVMD-1 Digital Video Motion Detector
- a SuperCircuits Infrared illuminator
- a Visonic DUET Combination Passive Infrared Detector and 10.525 GHz Microwave Motion Detector (PIR/MW) to detect movement and the presence of people

The various sensors are polled by the Sender computer in a random, constantly changing order, typically 5-10 sensor readings per second. Any sensor reading above the allowed threshold is interpreted by the monitoring program as intrusion or tampering, and the one-time pad or stored random number, respectively, is then quickly erased. Similarly, any attempt to move the computer cursor, click the mouse, depress keys on the keyboard, insert removable media, halt the

program, or shutdown/powerdown the computer is also interpreted almost immediately by the monitoring program as tampering or intrusion.

Other types of sensors such as magnetometers, force sensors, microphones, and photocells also appeared to work well with our prototype for monitoring stationary assets, but were found not to be reliable when the truck was in motion, primarily due to its worn suspension that made for a noisy and rough ride. One of the attractive attributes of the prototype systems is that they can readily accept different, or additional sensors without modifying or re-compiling the software.

Figures 2 and 3 show the monitoring hardware inside the truck. The labels in figure 3 identify the various components: PIR/MW=passive infrared/microwave motion sensor, IR=infrared illuminator, cam=pinhole video camera, VMD=video motion detector, ADC=analog to digital converter.

Fig 2. The cargo area, as viewed from the rear of the truck

The "cargo" used for our tests and demonstrations was an empty ALR8 container, typically used to store plutonium pits. (This isn't a common waste management container. On the other hand, it is not too dissimilar from a standard 55-gallon drum.) The ALR8 was strapped tightly into a holding pallet, which in turn was bolted to the floor of the truck. Preventing shifting of the cargo during monitoring is important—at least for the sensors used in these experiments—because major cargo movement could be misinterpreted as intrusion or tampering.

Most of the monitoring hardware, including the Sender computer, is closely mounted on the frame of the container pallet. This allows the video camera and other sensors to more easily

watch the ALR8 container, each other, and the Sender computer. Moreover, by rigidly attaching the IR illuminator and video camera to the frame of the pallet, jolts and vibrations experienced by the ALR8 due to truck motion and road bumps are not interpreted by the video motion detector (VMD) as a video scene change.

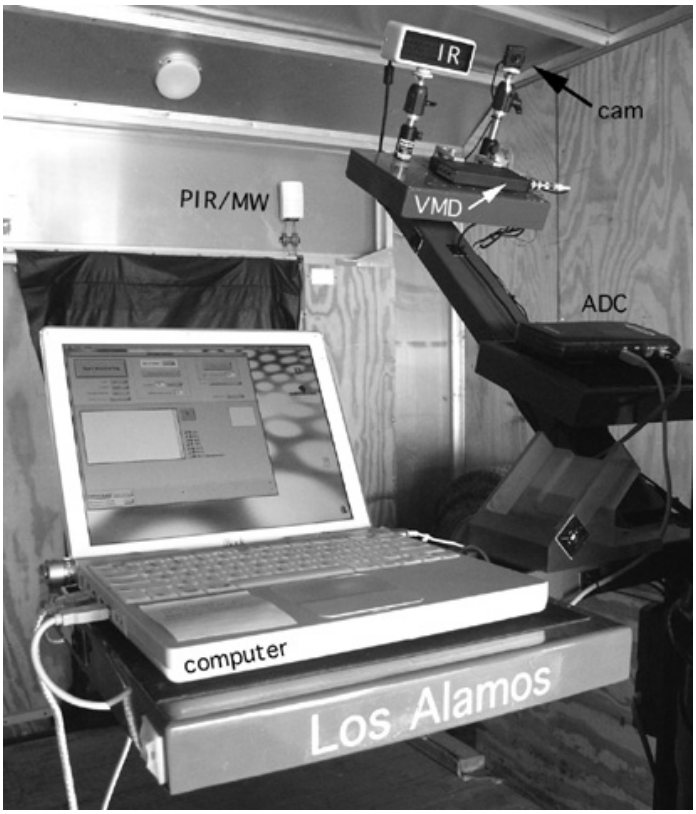

Fig. 3. A close-up of the Sender computer and some of the monitoring hardware.

Excluding the ALR8 and its pallet, the total cost of the monitoring hardware inside the truck was $3400 (in quantities of one). If the video motion detector is eliminated, the cost goes down to only $1800. The only hardware required at the receiving end of the town crier prototype is the Receiver iBook notebook computer ($1200), which could theoretically monitor signals from over 500 Sender computers simultaneously. Devoting an entire notebook computer to the Receiver task for a single truck is somewhat extravagant since the Receiver computer does little more than wait for signals from the Sender computer and compare them with what is expected. Both the Sender and Receive computers could be replaced with smaller and cheaper microprocessors.

The Generation 2 prototype has the additional security feature that it keeps track of time slippage. With town crier intrusion monitoring, one possible attack is to record the transmitted "All OK" signal, then immediately rebroadcast it with a delay of a few milliseconds. (The original, non-delayed broadcast is attenuated to reduce its range.) This delay, or "time slippage" is increased gradually over time until the adversary has accumulated enough of a lag to execute a surreptitious attack on the monitoring system. For monitoring periods greater than a few weeks, both the Sender and Receiver computers would need a more accurate internal clock to reliably detect time slippage attacks. External time signals, such as from (public) GPS or NIST radio broadcasts, should not be used because they are susceptible to spoofing.

The Generation 2 prototype, unlike the first generation system, is capable of doing both tamper and intrusion detection simultaneously.

EXPERIMENTAL RESULTS

Table I summarizes the preliminary test results on the Generation 1 and Generation 2 town crier prototypes operated in intrusion detection mode. Results are shown for when the truck was stationary, as well as for when it was driven on public roads at speeds up to 80 km/hour. Frequent turns and hills were encountered during the latter.

Table I. Experimental results for intrusion detection using the town crier prototypes.

Prototype generation	truck in motion?	longest continuous monitoring time	cumulative monitoring time	no. of "ALL OK" signals not received	no. of false alarms (wrong bingo numbers)	no. of intrusions detected
1 (Airport)	no	100 hours	181 hours (652600 secs)	1 out of 652600	0 out of 652600	20 of 20
1 (Airport)	yes	2 hours	3.2 hours (11522 secs)	0 out of 11522	0 out of 11522	4 of 4
2 (cell phone)	no	1.2 hours	5.1 hours (18438 secs)	0 out of 18438	0 out of 18438	6 of 6
2 (cell phone)	yes	1.3 hours	4.1 hours (14637 secs)	0 out of 14637	0 out of 14637	6 of 6

We focused primarily on intrusion detection, rather than tamper detection. This is because the reliability of the continuous rf "All OK" transmissions used for intrusion detection was a significant unknown. Otherwise, the two modes are virtually identical in how they interact with the sensors, plus they share 90% of the same software code.

For the intrusion monitoring of table I, we were able to acquire much more Generation 1 data with the truck stationary than when it was in motion because the latter required continually following the truck with an escort vehicle (containing the Receiver computer) at a distance of less than 50 meters to stay within the Airport range. For intrusion monitoring using the Generation 2 prototype, however, the truck ranged from a distance of 0 to 15 km from the Receiver computer.

Combining all rows in the table, it can be seen that no false alarms, i.e., no "wrong" bingo numbers were ever received that could be misinterpreted as intrusion. Moreover, there was only one missing "All OK" signal, lasting but 1 second, out of 697197 total seconds (194 hours) of monitoring. It is doubtful that an adversary could easily attack the monitoring system, fool the sensors and Sender computer, gain access to the one-time keypad, copy it, and begin counterfeiting the "All OK" signals during this one second of lost signal.

All 36 intrusion attempts listed in Table I were detected. For those in the second row, the truck was brought to a stop before entry was attempted in 3 of the 4 attempts. In the remaining

intrusion test, one of the passengers entered the cargo area of the truck from the passenger compartment while the truck was in motion, and his intrusion was also immediately detected.

In addition to the results summarized in the table, 60 more tampering or intrusion attempts were all also successfully detected for very short-term monitoring experiments. In fact, the prototypes have never failed to detect a person entering the truck's cargo area. While this is encouraging, it certainly cannot be considered a comprehensive test of security. No subtle attacks on the truck were attempted; all tampering/intrusion events involved a single individual entering the truck cargo area by either raising the rear truck door, or by entering from the driver's compartment. We believe attempts to cut a hole in the truck floor, wall, or ceiling would also be detected, but this has not been tested.

ONGOING WORK

Our town crier monitoring system is continuing to slowly evolve. We are in the process of miniaturizing the system, including replacing the iBook notebook computer inside the truck with a microprocessor. This new town crier system can be installed or removed from the truck in under 5 minutes.

We are also developing other sensors to be used with the truck monitoring system. As seen in figure 2, the prototype system discussed here was demonstrated with the truck cargo area largely empty. This makes it convenient to use line of sight sensors such as the video camera and the PIR/MW motion detector. For more conventional applications, however, the cargo area may be filled to capacity with containers or cargo. This necessitates the use of different kinds of sensors.

It is worth noting that the town crier approach can be applied both to complex, integrated, multi-component monitoring systems, as well as individual monitoring devices like seals or intrusion sensors. It is easy, for example, to imagine a storage vault or transport vehicle full of one-time keypad "seals" each monitoring a different waste container for tampering. The volume could be watched over by a single photosensor or video camera. As long as there is no tampering, each seal would flash its (LED) light at a random, unpredictable time (or with a characteristic modulation) given by the unique one-time keypad stored inside it. This light flash is the town crier "All OK" signal. Should tampering be detected by one of the seals, it will signal this fact by failing to send the correct "All OK" signal, and this will be noted by the computer that operates the photosensor or video camera watching the scene.

We had originally assumed that a town crier type of tamper-indicated device must be active, i.e., based on electronics or electrooptics. Surprisingly, however, it turns out that it is possible to design a fully passive, mechanical seal based on the town crier approach. We have constructed a working prototype of such an unconventional seal. It is inexpensive and completely reusable—something virtually unheard of in a passive seal.

CONCLUDING REMARKS

Conventional approaches to tamper and intrusion detection have significant disadvantages and vulnerabilities. This paper presented an alternative approach, called the "town crier" method. For intrusion detection, it is based on the use of (1) an unbreakable one-time keypad, (2) continuous, real-time monitoring, (3) an "anti-alarm" or "ALL OK" signal that indicates the

absence of intrusion, and (4) very low bandwidth, one-way communication. As discussed in this paper, this approach is likely to be both simpler and fundamentally more secure for fixed and transport applications than traditional real-time monitoring concepts. It may also be better suited to simultaneously monitoring large numbers of vehicles or transportainers, due to attribute (4).

For tamper detection (not in real-time), the town crier monitoring requires no continuous communication with the outside world. Tampering is instead noted at inspection time when the stored, secret random number is found to have been erased. (In effect, the "town crier" tamper detection system waits until it is queried at the end before sounding or not sounding the "All OK" signal.) Intruders don't know how to spoof the system because their unauthorized access rapidly erases the random number known only to the owner of the hazardous waste. Unlike traditional truck or transportainer seals, moreover, this approach shows no evidence outside the truck or transportainer that tamper detection is underway. This is technically known as a Type 1 trap (covert seal).

For treaty monitoring applications, the town crier approach, whether in tamper or intrusion detection mode, permits the monitoring hardware to be provided and entirely controlled by the host (inspected) nation. Inspectors may nevertheless potentially have confidence in the veracity of the monitoring for reasons alluded to in this paper, but also discussed in more detail elsewhere [11].

ACKNOWLEDGEMENTS

The views expressed in this paper are those of the authors and should not necessarily be ascribed to Los Alamos National Laboratory or the United States Department of Energy. Eric Gerdes and Jim Doyle made important contributions to the development of these ideas. Sonia Trujillo, Jon Warner, Ron Martinez, and Sharon Seitz assisted with the experimental work. Morten Bremer Maerli and Harry Dewey provided useful comments and suggestions.

REFERENCES

1. R.G. JOHNSTON, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management," Science & Global Security 9, 105 (2002), http://lib-www.lanl.gov/la-pubs/00818333.pdf

2. R.G. JOHNSTON, "The Real Deal on Seals," Security Management, 41, 93 (1997), http://lib-www.lanl.gov/la-pubs/00418795.pdf

3. R.G. JOHNSTON, A.R.E. GARCIA , and A.N. PACHECO, "Efficacy of Tamper-Indicating Devices", Journal of Homeland Security, April 2002, http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=50

4. R.G. JOHNSTON, "Cryptography as a Model for Physical Security", Journal of Security Administration 24, 33 (2001).

5. R.G. JOHNSTON, "Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials," The Nonproliferation Review 8, 102 (2001), http://lib-www.lanl.gov/la-pubs/00367047.pdf

6. R.G. JOHNSTON and A.R.E. GARCIA, "An Annotated Taxonomy of Tag and Seal Vulnerabilities," Journal of Nuclear Materials Management 28, 23 (2000).

7. R.L. BARNARD, *Intrusion Detection Systems,* Butterworth-Heinemann, Boston, (1988).

8. B. SCHNEIER, *Secrets and Lies: Digital Security in a Networked World*, Wiley, New York, (2000).

9. D.R. STINSON, *Cryptography: Theory and Practice,* CRC Press, Boca Raton, FL, (1995).

10. A.J. PALMER, *48th Regiment NYS Volunteers In the War for the Union, 1861-1865*, Chapter IV, part 3. (1884), http://www.aint-that-cute.com/48th-4b.html

11. E.R. GERDES, R.G. JOHNSTON, and D.E. DOYLE, "A Proposed Approach for Monitoring Nuclear Warhead Dismantlement", Science and Global Security 9, 113 (2001), http://lib-www.lanl.gov/la-pubs/00818332.pdf