Security Analysis of a Full-Body Scanner

Keaton Mowery, *University of California, San Diego;* Eric Wustrow, *University of Michigan;* Tom Wypych, Corey Singleton, Chris Comfort, and Eric Rescorla, *University of California, San Diego;* Stephen Checkoway, *Johns Hopkins University;* J. Alex Halderman, *University of Michigan;* Hovav Shacham, *University of California, San Diego*

https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/mowery

This paper is included in the Proceedings of the
23rd USENIX Security Symposium.

August 20–22, 2014 • San Diego, CA

ISBN 978-1-931971-15-7

Security Analysis of a Full-Body Scanner

Keaton Mowery,[*] Eric Wustrow,[†] Tom Wypych,[*] Corey Singleton,[*] Chris Comfort,[*]
Eric Rescorla,[*] Stephen Checkoway,[‡] J. Alex Halderman,[†] Hovav Shacham[*]
[*] *UC San Diego,* [†] *University of Michigan,* [‡] *Johns Hopkins University*

Abstract

Advanced imaging technologies are a new class of people screening systems used at airports and other sensitive environments to detect metallic as well as nonmetallic contraband. We present the first independent security evaluation of such a system, the Rapiscan Secure 1000 full-body scanner, which was widely deployed at airport checkpoints in the U.S. from 2009 until 2013. We find that the system provides weak protection against adaptive adversaries: It is possible to conceal knives, guns, and explosives from detection by exploiting properties of the device's backscatter X-ray technology. We also investigate cyberphysical threats and propose novel attacks that use malicious software and hardware to compromise the the effectiveness, safety, and privacy of the device. Overall, our findings paint a mixed picture of the Secure 1000 that carries lessons for the design, evaluation, and operation of advanced imaging technologies, for the ongoing public debate concerning their use, and for cyberphysical security more broadly.

1 Introduction

In response to evolving terrorist threats, including nonmetallic explosive devices and weapons, the U.S. Transportation Security Administration (TSA) has adopted advanced imaging technology (AIT), also known as whole-body imaging, as the primary passenger screening method at nearly 160 airports nationwide [50]. Introduced in 2009 and gradually deployed at a cost exceeding $1 billion, AIT provides, according to the TSA, "the best opportunity to detect metallic and non-metallic anomalies concealed under clothing without the need to touch the passenger" [48].

AIT plays a critical role in transportation security, and decisions about its use are a matter of public interest. The technology has generated considerable controversy, including claims that the devices are unsafe [40], violate privacy and civil liberties [27, 41], and are ineffective [8, 21]. Furthermore, AIT devices are complex cyberphysical systems — much like cars [23] and implantable medical devices [13] — that raise novel computer security issues. Despite such concerns, neither the manufacturers nor the government agencies that deploy these machines have disclosed sufficient technical details to facilitate rigorous independent evaluation [40], on the grounds that such information could benefit attackers [48]. This lack of transparency has limited the ability of policymakers, experts, and the public to assess contradicting claims.

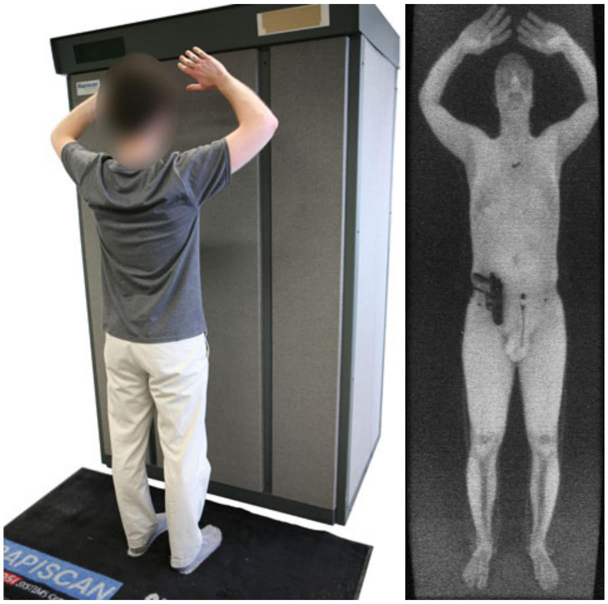


Figure 1: The Rapiscan Secure 1000 full-body scanner uses backscattered X-rays to construct an image through clothing. Naïvely hidden contraband, such as the handgun tucked into this subject's waistband, is readily visible to the device operator.

To help advance the public debate, we present the first experimental analysis of an AIT conducted independently of the manufacturer and its customers. We obtained a Rapiscan Secure 1000 full-body scanner — one of two AITs widely deployed by the TSA [32] — and performed a detailed security evaluation of its hardware and software. Our analysis provides both retrospective insights into the adequacy of the testing and evaluation procedures that led up to TSA use of the system, and prospective lessons about broader security concerns, including cyberphysical threats, that apply to both current and future AITs.

The Secure 1000 provides a unique opportunity to investigate the security implications of AITs in a manner that allows robust yet responsible public disclosure. Although it was used by the TSA from 2009 until 2013, it has recently been removed from U.S. airports due to changing functional requirements [34]. Moreover, while the Secure 1000 uses backscatter X-ray imaging, current TSA systems are based on a different technology, millimeter waves [11], so many of the attacks we present are not directly applicable to current TSA checkpoints, thus reducing the risk that our technical disclosures will inadvertently facilitate mass terrorism. However, while Secure 1000 units are no longer used in airports, they still are in use at other government facilities, such as courthouses and prisons (see, e.g., [15, 29]). In addition, other backscatter X-ray devices manufactured by American Science and Engineering are currently under consideration for use at airports [34]. To mitigate any residual risk, we have redacted a small number of sensitive details from our attacks in order to avoid providing recipes that would allow an attacker to reliably defeat the screening process without having access to a machine for testing.

In the first part of our study (Section 3), we test the Secure 1000's effectiveness as a physical security system by experimenting with different methods of concealing contraband. While the device performs well against naïve adversaries, fundamental limitations of backscatter imaging allow more clever attackers to defeat it. We show that an adaptive adversary, with the ability to refine his techniques based on experiment, can confidently smuggle contraband past the scanner by carefully arranging it on his body, obscuring it with other materials, or properly shaping it. Using these techniques, we are able to hide firearms, knives, plastic explosive simulants, and detonators in our tests. These attacks are surprisingly robust, and they suggest a failure on the part of the Secure 1000's designers and the TSA to adequately anticipate adaptive attackers. Fortunately, there are simple procedural changes that can reduce (though not eliminate) these threats, such as performing supplemental scans from the sides or additional screening with a magnetometer.

Next, we evaluate the security of the Secure 1000 as a cyberphysical system (Section 4) and experiment with three novel kinds of attacks against AITs that target their effectiveness, safety features, and privacy protections. We demonstrate how malware infecting the operator's console could selectively render contraband invisible upon receiving a "secret knock" from the attacker. We also attempt (with limited success) to use software-based attacks to bypass the scanner's safety interlocks and deliver an elevated radiation dose. Lastly, we show how an external device carried by the attacker with no access to the console can exploit a physical side-channel to capture naked images of the subject being scanned. These attacks are, in general, less practical than the techniques we demonstrate for hiding contraband, and their limitations highlight a series of conservative engineering choices by the system designers that should serve as positive examples for future AITs.

Finally, we attempt to draw broader lessons from these findings (Section 5). Our results suggest that while the Secure 1000 is effective against naïve attackers, it is not able to guarantee either efficacy or privacy when subject to attack by an attacker who is knowledgeable about its inner workings. While some of the detailed issues we describe are specific to the scanner model we tested, the root cause seems to be the failure of the system designers and deployers to think adversarially. This pattern is familiar to security researchers: past studies of voting machines [4], cars [23] and medical devices [13] have all revealed cyberphysical systems that functioned well under normal circumstances but were not secure in the face of attack. Thus, we believe this study reinforces the message that security systems must be subject to adversarial testing before they can be deemed adequate for widespread deployment.

Research safety and ethics. Since the Secure 1000 emits ionizing radiation, it poses a potential danger to the health of scan subjects, researchers, and passers by. Our institutional review board determined that our study did not require IRB approval; however, we worked closely with research affairs and radiation safety staff at the university that hosted our device to minimize any dangers and assure regulatory compliance. To protect passers by, our device was sited in a locked lab, far from the hallway, and facing a thick concrete wall. To protect researchers, we marked a 2 m region around the machine with tape; no one except the scan subject was allowed inside this region while high voltage was applied to the X-ray tube. We obtained a RANDO torso phantom [33], made from a material radiologically equivalent to soft tissue cast over a human skeleton, and used it in place of a human subject for all but the final confirmatory scans. For these final scans we decided, through consultation with our IRB, that only a PI would be used as a scan subject. Experiments involving weapons were conducted with university approval and in coordination with the campus police department and all firearms were unloaded and disabled. We disclosed our security-relevant findings and suggested procedural mitigations to Rapiscan and the Department of Homeland Security ahead of publication.

Online material. Additional resources and the most recent version of this report are available online at `https://radsec.org/`.

2 The Rapiscan Secure 1000

The Secure 1000 was initially developed in the early 1990s by inventor Steven W. Smith [42, 44]. In 1997, Rapiscan Systems acquired the technology [43] and began to produce the Rapiscan Secure 1000. In 2007, the TSA signed a contract with Rapiscan to procure a customized version of the Secure 1000 for deployment in airport passenger screening [47].

We purchased a Rapiscan Secure 1000 from an eBay seller who had acquired it in 2012 at a surplus auction from a U.S. Government facility located in Europe [17]. The system was in unused condition. It came with operating and maintenance manuals as well as detailed schematics, which were a significant aid to reverse engineering. The system consists of two separate components: the scanner unit, a large enclosure that handles X-ray generation and detection under the control of a special purpose embedded system, and the user console, a freestanding cabinet that contains a PC with a keyboard and screen. The two components are connected by a 12 m cable.

The system we tested is a dual pose model, which means that the subject must turn around in order to be scanned from the front and back in two passes. TSA screening checkpoints used the Secure 1000 single pose model [32], which avoids this inconvenience by scanning from the front and back using a pair of scanner units. Our system was manufactured in about September 2006 and includes EPROM software version 2.1. Documents obtained under the Freedom of Information Act suggest that more recent versions of the hardware and software were used for airport screening [45, 52], and we highlight some of the known differences below. Consequently, we focus our analysis on fundamental weaknesses in the Secure 1000 design that we suspect also affect newer versions. A detailed analysis of TSA models might reveal additional vulnerabilities.

2.1 Backscatter Imaging

X-ray backscatter imaging exploits the unique properties of ionizing radiation to penetrate visual concealment and detect hidden contraband. The physical process which generates backscatter is Compton scattering, in which a photon interacts with a loosely bound or free electron and scatters in an unpredictable direction [7]. Other interactions, such as the photoelectric effect, are possible, and the fraction of photons that interact and which particular effect occurs depends on each photon's energy and the atomic composition of the mass. For a single-element material, the determining factor is its atomic number *Z*, while a compound material can be modeled by producing an "effective *Z*," or Z_{eff} [46].

Under constant-spectrum X-ray illumination, the backscattered intensity of a given point is largely determined by the atomic composition of matter at that location, and to a lesser extent its density. Thus, organic materials, like flesh, can be easily differentiated from materials such as steel or aluminum that are made from heavier elements.

The Secure 1000 harnesses these effects for contraband screening by operating as a "reverse camera," as illustrated in Figure 2. X-ray output from a centrally-located tube (operating at 50 kVp and 5 mA) passes through slits in shielding material: a fixed horizontal slit directly in front of a "chopper wheel," a rapidly spinning disk with four radial slits. This results in a narrow, collimated X-ray beam, repeatedly sweeping across the imaging field. During a scan, which takes about 5.7 s, the entire X-ray assembly moves vertically within the cabinet, such that the beam passes over every point of the scene in a series of scan lines.

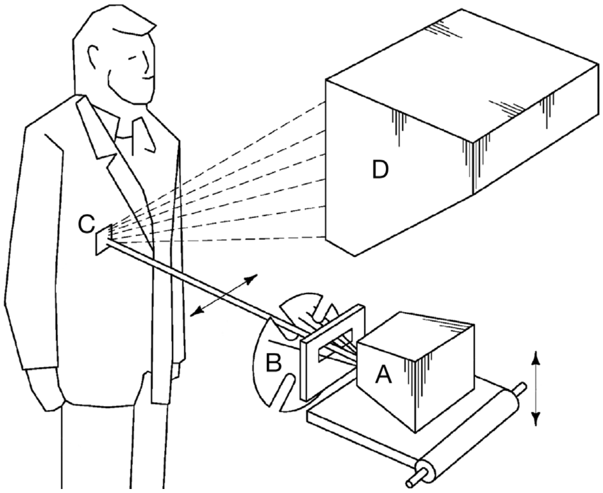


Figure 2: Backscatter Imaging — An X-ray tube (A) mounted on a platform travels vertically within the scanner. The X-rays pass through a spinning disk (B) that shapes them into a horizontally scanning beam. Some photons that strike the target (C) are backscattered toward detectors (D) that measure the reflected energy over time. Adapted from U.S. Patent 8,199,996 [16].

As the beam sweeps across the scene, a set of 8 large X-ray detectors measures the intensity of the backscattered radiation at each point, by means of internal photomultiplier tubes (PMTs). The Secure 1000 combines the output of all 8 detectors, and sends the resulting image signal to the user console, which converts the time-varying signal into a 160×480 pixel monochrome image, with the intensity of each pixel determined by the Z_{eff} value of the surface of the scan subject represented by that pixel location.

2.2 Subsystems

Operator interface. The operator interacts with the Secure 1000 through the user console, a commodity x86 PC housed within a lockable metal cabinet. With our system, the user console is connected to the scanner unit via a serial link and an analog data cable. Documents released by the TSA indicate that airport checkpoint models were configured differently, with an embedded PC inside the scanner unit linked to a remote operator workstation via a dedicated Ethernet network [45, 52].

On our unit, the operator software is an MS-DOS application called SECURE65.EXE that launches automatically when the console boots. (TSA models are apparently Windows-based and use different operator software [45, 47].) This software is written in a BASIC vari-

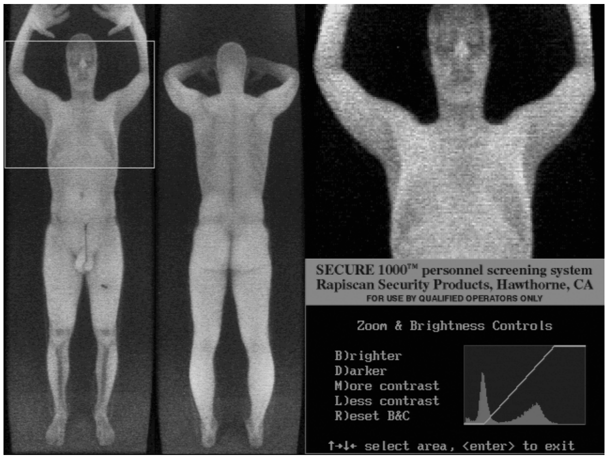

SECURE 1000™ personnel screening system
Rapiscan Security Products, Hawthorne, CA
FOR USE BY QUALIFIED OPERATORS ONLY
Zoom & Brightness Controls
B)righter
D)arker
M)ore contrast
L)ess contrast
R)eset B&C
↑→↓← select area, <enter> to exit

Figure 3: Operator View — The user console displays front and back images and offers basic enhancements and 2 × zoom. It also allows the operator to print images or save them to disk.

ant, and the main user interface is a 640 × 480 pixel, 4-bit grayscale screen, as shown in Figure 3. The operator invokes a scan by pressing a hand switch. After image acquisition, the operator can inspect the scan by means of a 2× zoom and interactive brightness and contrast controls. The image can also be saved to disk or printed. Further, the software contains several calibration functions that can only be accessed by entering a 4 digit numeric password. The password is hard-coded and is printed in the maintenance manual.

Scanner unit. The scanner unit contains an assortment of electrical and mechanical systems under the control of an embedded computer called the System Control Board (SCB). The SCB houses an Intel N80C196KB12 microcontroller, executing software contained on a 32 KiB socketed ROM. It interacts with the user console PC over a bidirectional RS-232 serial link using simple ASCII commands such as `SU` for "scan up" and `SD` for "scan down." In turn, the SCB uses digital and analog interfaces to direct and monitor other components, including the X-ray tube, PMTs, and chopper wheel. It also implements hardware-based safety interlocks on the production of X-rays, which we discuss further in Section 4.2.

To control vertical movement of the X-ray tube, the scanner unit uses an off-the-shelf reprogrammable servo motor controller, the Parker Gemini GV6. In normal operation, the servo controller allows the SCB to trigger a movement of the X-ray tube, initially to a "home" position and subsequently to scan up and down at predefined rates. There is no command to move the tube to a specific intermediate position.

3 Contraband Detection

As the Secure 1000 is intended to detect prohibited or dangerous items concealed on the body of an attacker, the first and most obvious question to ask is how effectively the Secure 1000 detects contraband.

To make the discussion concrete, we consider the machine as it was typically used by the TSA for airport passenger screening. Under TSA procedures, subjects were imaged from the front and back, but not from the sides. A trained operator inspected the images and, if an anomaly was detected, the passenger was given a manual pat down to determine whether it was a threat [45]. The Secure 1000 was used in place of a walk-through metal detector, rather than both screening methods being employed sequentially [48]. We focus our analysis on threats relevant to an airport security context, such as weapons and explosives, as opposed to other contraband such as illicit drugs or bulk currency.

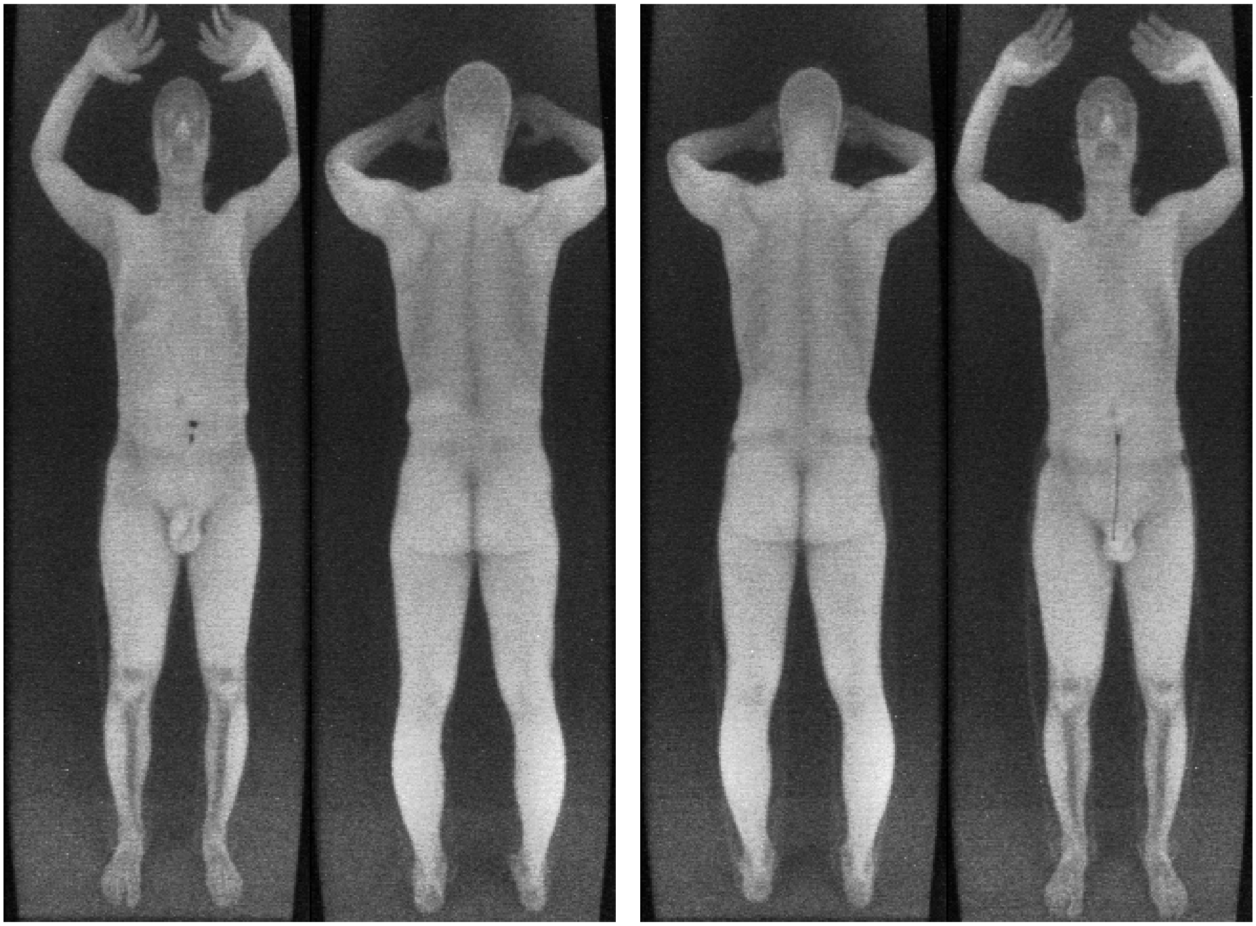
To replicate a realistic screening environment, we situated our Secure 1000 in an open area, oriented 2.5 m from a concrete wall sufficient to backstop X-ray radiation. This distance accords with the manufacturer's recommendation of at least 2 m of open area "for producing the best possible images" [35]. For typical tests, we arranged the subject at a distance of about 38 cm in front of the scanner using the foot position template provided with the machine.

Naïve adversary. First, we consider the scanner's effectiveness against a naïve adversary, an attacker whose tactics do not change in response to the introduction of the device. Although this is a weak attacker, it seems to correspond to the threat model under which the scanner was first tested by the government, in a 1991 study of a prototype of the Secure 1000 conducted by Sandia National Laboratories [22]. Our results under this threat model generally comport with theirs. Guns, knives, and blocks of explosives naïvely carried on the front or back of the subject's body are visible to the scanner operator.

Three effects contribute to the detectability of contraband. The first is *contrast*: human skin appears white as it backscatters most incident X-ray radiation, while metals, ceramics, and bone absorb X-rays and so appear dark gray or black. The second is *shadows* cast by three-dimensional objects as they block the X-ray beam, which accentuate their edges. The third is *distortion* of the subject's flesh as a result of the weight of the contraband or the mechanics of its attachment. The naïve adversary is unlikely to avoid all three effects by chance.

A successful detection of hidden contraband can be seen in Figure 1. The subject has concealed a .380 ACP pistol within his waistband. The X-ray beam interacts with the gun metal significantly differently than the surrounding flesh, and the sharp contrast in backscatter intensity is immediately noticeable.

Adaptive adversary. Of course, real attackers are not entirely ignorant of the scanner. The TSA announced



(a) Subject with .380 ACP pistol taped above knee.

(b) Subject with .380 ACP pistol sewn to pant leg.

Figure 4: Concealing a Pistol by Positioning — The Secure 1000 cannot distinguish between high Z_{eff} materials, such as a metal handgun, and the absence of a backscatter response. Carefully placed metallic objects can be invisible against the dark background.

that it would be used at screening checkpoints [12, 48], the backscatter imaging mechanism is documented in patents and manufacturer reports [16, 24, 36], images captured with the device have appeared in the media [12, 25], and the physics of backscatter X-rays are well understood [2, 7, 22]. We must assume that attackers have such information and adapt their tactics in response.

To simulate an adaptive adversary, we performed experiments in the style of white-box penetration testing commonly employed in the computer security field. We allowed ourselves complete knowledge of how the scanner operates as well as the ability to perform test scans, observed the resulting images, and used them to adjust our concealment methods.

Such interactive testing is not strictly necessary to develop clever attacks. Indeed, researchers with no access to the Secure 1000 have proposed a number of concealment strategies based only on published information [21], and we experimentally confirm that several of these attacks are viable. However, the ability to perform tests substantially increases the probability that an attack will succeed on the first attempt against a real deployment. A determined adversary might acquire this level of access in several ways: by buying a machine, as we did; by colluding with a dishonest operator; or by probing the security of real installations over time.

In the remainder of this section, we describe experiments with three adaptive concealment techniques and show that they can be used to defeat the Secure 1000. We successfully use them to smuggle firearms, knives, and explosive simulants past the scanner.

3.1 Concealment by Positioning

The first concealment technique makes use of a crucial observation about X-ray physics: backscatter screening machines emitting X-rays in the 50 keV range, such as the Secure 1000, cannot differentiate between the absence of matter and the existence of materials with high Z_{eff} (e.g., iron and lead). That is, when the scanner emits probing X-rays in a direction and receives no backscatter, it can either be because the beam interacted with nothing, i.e., traveled unimpeded past the screening subject, or because the beam shone directly upon a material which absorbed it entirely and thus did not backscatter. In either case, the resulting pixels will be dark.

These facts lead directly to a straightforward concealment attack for high Z_{eff} contraband: position the object such that it avoids occluding the carrier's body with respect to the X-ray beam. This technique was first suggested on theoretical grounds by Kaufman and Carlson [21]. In limited trials, a TSA critic used it to smuggle small metal objects through airport checkpoints equipped with the Secure 1000 and other AITs [8]. Note that this attack is not enabled by a poor choice of image background color; as discussed above, the scanner cannot differentiate between the metal objects and the absence of material.

To more fully investigate this attack, we obtained a set of weapons: both knives and firearms, ranging from a .380 ACP pistol to an AR-15 semi-automatic rifle. When we scanned the weapons against a dark backdrop, most of the firearms were readily visible due to the presence of nonmetallic parts. After testing a number of firearms, we settled on our .380 ACP pistol as the most suitable candidate for concealment.

We performed several trials to test different placement and attachment strategies. In the end, we achieved excellent results with two approaches: carefully affixing the pistol to the outside of the leg just above the knee using tape, and sewing it inside the pant leg near the same location. Front and back scans for both methods are shown in Figure 4. In each case, the pistol is invisible against the dark background, and the attachment method leaves no other indication of the weapon's presence.

In a similar test, we concealed an 11 cm metal folding knife, in its closed position, along our test subject's side. In this case, too, front and back scans were completely unable to detect the weapon.

Fortunately, simple procedural changes can thwart these attacks. Instead of performing only front and back scans, every subject could also be made to undergo scans from the left and right sides. Under these scans, a high Z_{eff} weapon positioned on the side of the body would be as obvious as the one in Figure 1. Unfortunately, these additional scans would nearly halve the maximum throughput of the checkpoint, as well as double each person's radiation dose. Another possible mitigation would be to screen each subject with a magnetometer, which would unequivocally find metallic contraband but would fail to uncover more exotic weapons, such as ceramic knives [50, 54]. We note that the attacker's gait or appearance might be compromised by the mass and bulk of the firearm or knife, and this might be noticeable to security personnel outside of the backscatter X-ray screening.

3.2 Concealment by Masking

The second object concealment techniques we attempted are similarly based on X-ray physics: the brightness of a material in the image is directly correlated to its backscatter intensity, which in turn is determined by the Z_{eff} and density of the matter in the path of the beam. Therefore, any combination of substances which scatter incoming X-rays at the same approximate intensity as human flesh will be indistinguishable from the rest of the human.

One consequence of this fact is that high-Z_{eff} contraband can be concealed by masking it with an appropriate thickness of low-Z_{eff} material. We experimented with several masking materials to find one with a Z_{eff} value close to that of flesh. We obtained good results with the common plastic PTFE (Teflon), although due to its low density a significant thickness is required to completely mask a metallic object.

To work around this issue, we took advantage of the Secure 1000's ability to see bones close to the skin. Figure 5 demonstrates this approach: an 18 cm knife is affixed to the spine and covered with 1.5 cm of PTFE. As the X-rays penetrate through the material, they backscatter so that the knife outline approximates our subject's spine. While this mask arrangement creates hard edges and shadows which render it noticeable to screening personnel these effects could be reduced by tapering the edges of the mask.

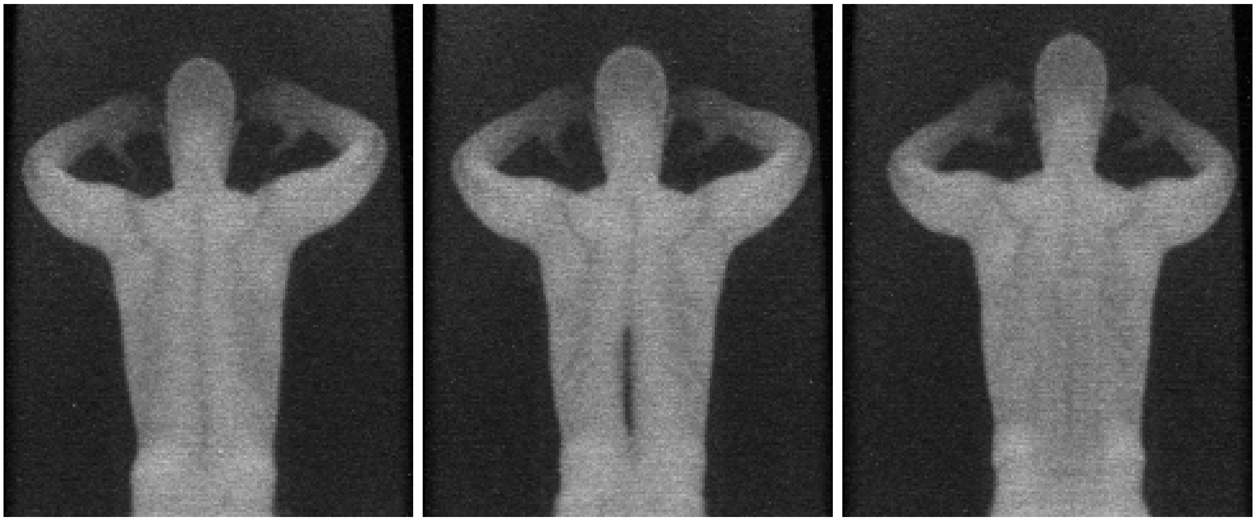
A more difficult challenge for the attacker is taking into account the anatomy of the specific person being imaged. Shallow bones and other dense tissue are visible to the scanner under normal conditions, and a poorly configured mask will stand out against these darker areas of the scan. We conclude that masking can be an effective concealment technique, but achieving high confidence of success would require access to a scanner for testing.

3.3 Concealment by Shaping

Our third and final concealment technique applies a strategy first theorized in [21] to hide malleable, low-Z_{eff} contraband, such as plastic explosives. These materials produce low contrast against human flesh, and, unlike rigid weapons, the attacker can reshape them so that they match the contours of the body.

To experiment with this technique, we acquired radiological simulants for both Composition C-4 [56] and Semtex [57], two common plastic high explosives. These simulants are designed to emulate the plastic explosives with respect to X-ray interactions, and both are composed of moldable putty, similar to the actual explosive materials. We imaged both C-4 and Semtex simulants with the Secure 1000, and found that they appear very similar. We selected the C-4 simulant for subsequent tests.

Our initial plan was to modify the simulants' Z_{eff} to better match that of flesh, by thoroughly mixing in fine metallic powder. To our surprise, however, a thin pancake



(a) No contraband **(b)** 18 cm knife taped to spine **(c)** Knife behind 1.5 cm plastic block

Figure 5: Concealing a Knife by Masking — We find that high-Z_{eff} materials can be hidden by covering them with lower Z_{eff} materials, such as the common plastic PTFE (Teflon). For example, a metal knife is clearly visible when naïvely concealed, but when covered with a thin plastic block it approximates the color of the spine. Tapering the block's edges would reduce the visible outline.

(about 1 cm) of unmodified C-4 simulant almost perfectly approximated the backscatter intensity of our subject's abdomen.

We affixed the pancake with tape (which is invisible to the Secure 1000), and faced two further problems. First, the pancake covered our subject's navel, which is normally clearly visible as a small black area in the scans. Second, by design, plastic explosives are almost completely inert without a matching detonator. These problems neatly solve each other: we attached a detonator, consisting of a small explosive charge in a metal shell, directly over our subject's navel. Since the detonator is coated in metal, it absorbs X-rays quite well and mimics the look of the navel in the final image.

Figure 6 shows a side-by-side comparison of our test subject both carrying no contraband and carrying 200 g of C-4 explosive and attached detonator. To put this amount in perspective, "Shoe Bomber" Richard Reid reportedly carried about 280 g of explosive material [6], and the bomb that destroyed Pan Am Flight 103 is thought to have contained 350 g of Semtex [55].

These scans indicate that plastic explosives can be smuggled through a Secure 1000 screening, since thin pancakes of these materials do not contrast strongly with flesh. While a metal detector would have been sufficient to detect the detonator we used, not all detonators have significant metal components.

In summary, an adaptive adversary can use several attack techniques to carry knives, guns, and plastic explosives past the Secure 1000. However, we also find that multiple iterations of experimentation and adjustment are likely necessary to achieve consistent success. The security of the Secure 1000, then, rests strongly on the adversary's inability to acquire access to the device for testing. However, since we were able to purchase a Secure 1000, it is reasonable to assume that determined attackers and well-financed terrorist groups can do so as well. We emphasize that procedural changes — specifically, performing side scans and supplementing the scanner with a magnetometer — would defeat some, though not all, of the demonstrated attacks.

4 Cyberphysical Attacks

The Secure 1000, like other AITs, is a complex cyberphysical system. It ties together X-ray emitters, detectors, and analog circuitry under the control of embedded computer systems, and feeds the resulting image data to a traditional desktop system in the user console. In this section, we investigate computer security threats against AITs. We demonstrate a series of novel software- and hardware-based attacks that undermine the Secure 1000's efficacy, safety features, and privacy protections.

4.1 User Console Malware

The first threat we consider is malware infecting the user console. On our version of the Secure 1000, the user console is an MS-DOS–based PC attached to the scanner unit via a proprietary cable; TSA models apparently used Windows and a dedicated Ethernet switch [47, 49]. Although neither configuration is connected to an external network, there are several possible infection vectors. If the operators or maintenance personnel are malicious, they could abuse their access in order to manually install malware.

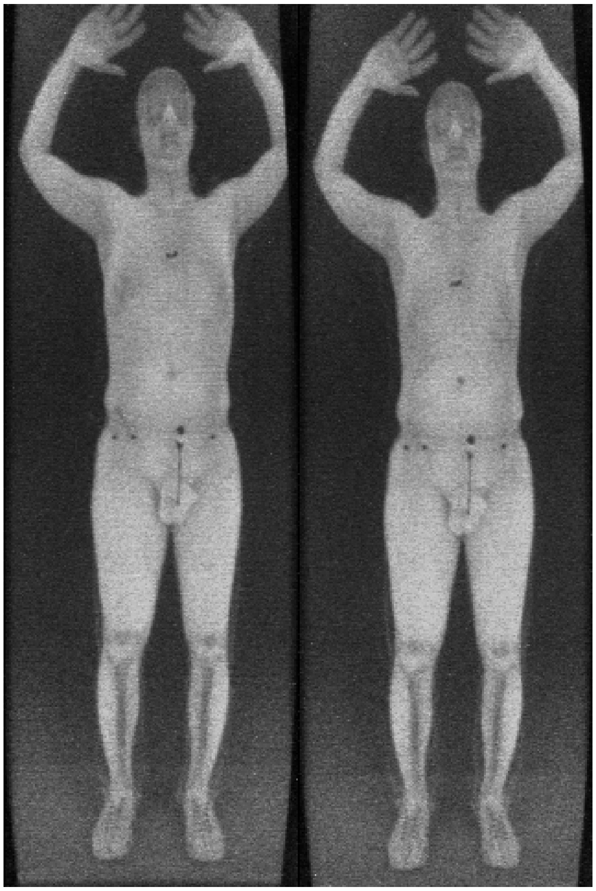


Figure 6: Concealing Explosives by Shaping — *Left:* Subject with no contraband. *Right:* Subject with more than 200 g of C-4 plastic explosive simulant plus detonator, molded to stomach.

The software on our machine lacks any sort of electronic access controls (e.g., passwords) or software verification. While the PC is mounted in a lockable cabinet, we were able to pick the lock in under 10 seconds with a commercially available tool. Therefore, even an outsider with temporary physical access could easily introduce malicious code. TSA systems may be better locked down, but sophisticated adversaries have a track record of infecting even highly secured, airgapped systems [26, 31].

We implemented a form of user console malware by reverse engineering SECURE65.EXE, the front-end software package used by the Secure 1000, and creating a malicious clone. Our version, INSECURE.EXE, is a functional, pixel-accurate reimplementation of the original program and required approximately one man-month to create.

In addition to enabling basic scanning operations, INSECURE.EXE has two malicious features. First, every scan image is saved to a hidden location on disk for later exfiltration. This is a straightforward attack, and it demonstrates one of many ways that software-based privacy protections can be bypassed. Of course, the user could also take a picture of the screen using a camera or smartphone — although operators are forbidden to have such devices in the screening room [39].

Second, INSECURE.EXE selectively subverts the scanner's ability to detect contraband. Before displaying each scan, it applies a pattern recognition algorithm to look for a "secret knock" from the attacker: the concentric squares of a QR code position block. If this pattern occurs, INSECURE.EXE replaces the real scan with a preprogrammed innocuous image. The actual scan, containing the trigger pattern and any other concealed contraband, is entirely hidden.

To trigger this malicious substitution, the subject simply wears the appropriate pattern, made out of any material with a sufficiently different Z_{eff} than human tissue. In our experiments, we arranged lead tape in the target shape, attached to an undershirt, as shown in Figure 7. When worn under other clothing, the target is easily detected by the malware but hidden from visual inspection.

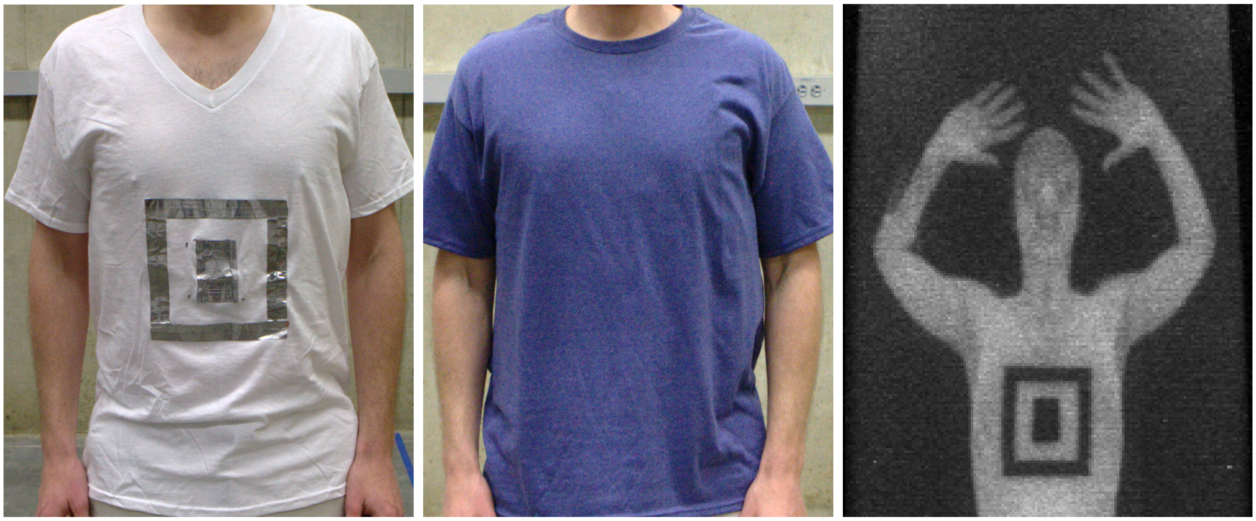
Recently, in response to privacy concerns, the TSA has replaced manual review of images with algorithmic image analysis software known as automated target recognition (ATR) [51]. Instead of displaying an image of the subject, this software displays a stylized figure, with graphical indicators showing any regions which the software considers suspect and needing manual resolution. (Delays in implementing this algorithm led the TSA to remove Secure 1000 machines from airports entirely [1].) If malware can compromise the ATR software or its output path, it can simply suppress these indicators — no image replacement needed.

4.2 Embedded Controller Attacks

The System Control Board (SCB) managing the physical scanner is a second possible point of attack. While the SCB lacks direct control over scan images, it does control the scanner's mechanical systems and X-ray tube. We investigated whether an attacker who subverts the SCB firmware could cause the Secure 1000 to deliver an elevated radiation dose to the scan subject.

This attack is complicated by the fact that the Secure 1000 includes a variety of safety interlocks that prevent operation under unexpected conditions. Circuits sense removal of the front panel, continuous motion of the chopper wheel and the vertical displacement servo, X-ray tube temperature and supply voltage, X-ray production level, key position ("Standby" vs. "On"), and the duration of the scan, among other parameters. If any anomalous state is detected, power to the X-ray tube is immediately disabled, ceasing X-ray emission.

While some of these sensors merely provide inputs to the SCB software, others are tied to hard-wired watchdog circuits that cut off X-ray power without software mediation. However, the firmware can *bypass* these hardware interlocks. At the beginning of each scan, operational


(a) Lead tape pattern

(b) Pattern concealed

(c) Scan as captured

Figure 7: A Secret Knock — We demonstrate how malware infecting the Secure 1000 user console could be used to defeat the scanner. The malware is triggered when it detects a specific pattern in a scan, as shown here. It then replaces the real image (c) of the attacker, which might reveal hidden contraband, with an innocuous image stored on disk. Pattern recognition occurs in real time.

characteristics such as tube voltage and servo motion fluctuate outside their nominal ranges. To prevent immediate termination of every scan, SCB software temporarily asserts a bypass signal, which disables the hardware interlocks. This signal feeds a "bypass watchdog" circuit of its own, meant to prevent continual interlock bypass, but the SCB can pet this watchdog by continuously toggling the bypass signal, and cause all hardware interlocks to be ignored. Thus, every safety interlock is either directly under software control or can be bypassed by software.

We developed replacement SCB firmware capable of disabling all of the software and hardware safety interlocks in the Secure 1000. With the interlocks disabled, corrupt firmware can, for instance, move the X-ray tube to a specific height, stop the chopper wheel, and activate X-ray power, causing the machine to deliver the radiation dose from an entire dose to a single point. Only the horizontal displacement of this point is not directly under firmware control — it depends on where the chopper wheel happens to come to rest.

Delivering malicious SCB firmware presents an additional challenge. The firmware is stored on a replaceable socketed EPROM inside the scanner unit, which is secured by an easily picked wafer tumbler lock. Although attackers with physical access could swap out the chip, they could cause greater harm by, say, hiding a bomb inside the scanner. For SCB attacks to pose a realistic safety threat, they would need to be remotely deployable.

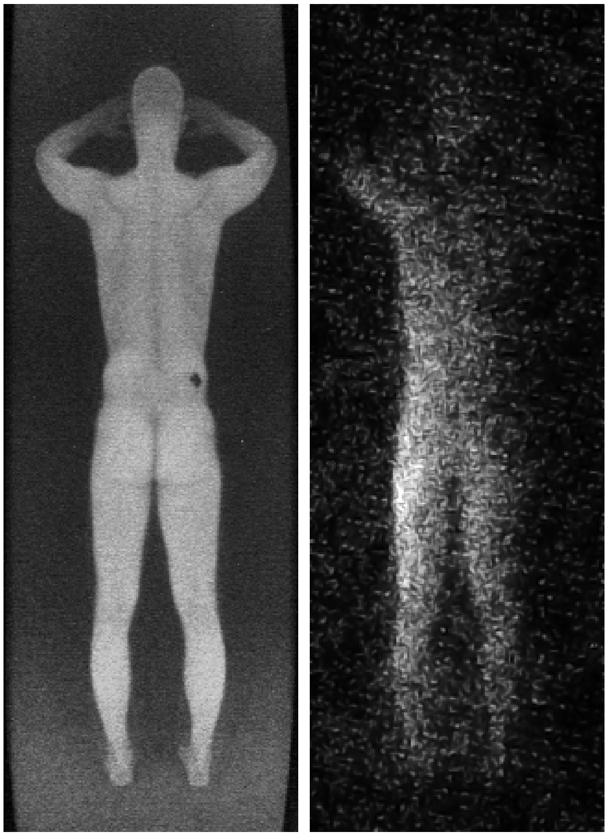
Due to the scanner's modular design, the only feasible vector for remote code execution is the serial link between the user console and the SCB. We reverse engineered the SCB firmware and extensively searched for vulnerabilities. The firmware is simple (<32 KiB) and appears to withstand attacks quite well. Input parsing uses a fixed length buffer, to which bytes are written from only one function. This function implements bounds checking correctly. Data in the buffer is always processed in place, rather than being copied to other locations that might result in memory corruption. We were unable to cause any of this code to malfunction in a vulnerable manner.

While we are unable to remotely exploit the SCB to deliver an elevated radiation dose, the margin of safety by which this attack fails is not reassuring. Hardware interlocks that can be bypassed from software represent a safety mechanism but not a security defense. Ultimately, the Secure 1000 is protected only by its modular, isolated design and by the simplicity of its firmware.

4.3 Privacy Side-Channel Attack

AIT screening raises significant privacy concerns because it creates a naked image of the subject. Scans can reveal sensitive information, including anatomical size and shape of body parts, location and quantity of fat, existence of medical conditions, and presence of medical devices such as ostomy pouches, implants, or prosthetics. As figures throughout the paper show, the resulting images are quite revealing.

Recognizing this issue, the TSA and scanner manufacturers have taken steps to limit access to raw scanned images. Rapiscan and DHS claim that the TSA machines had no capacity to save or store the images [27, 45]. The TSA also stated that the backscatter machines they used had a "privacy algorithm applied to blur the image" [50]. We are unable to verify these claims due to software dif-



(a) From scanner **(b)** From external detector

Figure 8: Attacking Privacy — An attacker could use a detector hidden in a suitcase to capture images of the subject during scanning. As a proof of concept, we used a small external PMT to capture images that are consistent with the scanner's output. A larger detector would produce more detailed images.

ferences between our machine and TSA models. Our Secure 1000 has documented save, recall (view saved images), and print features and does not appear to have a mechanism to disable them. In fact, using forensic analysis software on the user console's drive, we were able to recover a number of stored images from test scans that were incompletely deleted during manufacturing.

These software-based defenses aim to safeguard privacy in images that are constructed by the machine, but they do not address a second class of privacy attacks against AITs: an outsider observer could try to reconstruct scanned images by using their own external detector hardware. The most mechanically complex, dangerous, and energy intensive aspects of backscatter imaging are related to X-ray illumination; sensing the backscattered radiation is comparatively simple. Since X-rays scatter off the subject in a broad arc, they create a kind of physical side channel that potentially leaks a naked image of the subject to any nearby attacker. To the best of our knowledge, we are the first to propose such an attack; the privacy threat model for AITs appears to have been focused almost entirely on concerns about the behavior of screening personnel, rather than the general public.

In the scenario we envision, an attacker follows a target subject (for instance, a celebrity or politician) to a screening checkpoint while carrying an X-ray detector hidden in a suitcase. As the victim is scanned, the hardware records the backscattered X-rays for later reconstruction.

We experimented with the Secure 1000 to develop a proof-of-concept of such an attack. The major technical challenge is gathering enough radiation to have an acceptable signal/noise ratio. The Secure 1000 uses eight large photomultiplier tubes (PMTs) — four on either side of the X-ray generator — in order to capture as much signal as possible. For best results, an attacker should likewise maximize observing PMT surface area, and minimize distance from the subject, as radiation intensity falls off quadratically with distance. To avoid arousing suspicion, an attacker may be limited to only one PMT, and may also be restricted in placement.

To determine whether external image reconstruction is feasible, we used a small PMT, a 75 mm Canberra model BIF2996-2 operated at 900 V, with a 10 cm × 10 cm NaI crystal scintillator. We placed this detector adjacent to the scanner and fed the signal to a Canberra Model 1510 amplifier connected to a Tektronix DPO 3014 oscilloscope. After capturing the resulting signal, we converted the time varying intensity to an image and applied manual enhancements to adjust levels and remove noise.

Figure 8 shows the results from the scanner and from our corresponding reconstruction. While our proof-of-concept results are significantly less detailed than the scanner's output, they suggest that a determined attacker, equipped with a suitcase-sized PMT, might achieve satisfactory quality. A further concern is that changes in future backscatter imaging devices might make this attack even more practical. Since the PMTs in the Secure 1000 are close to the maximum size that can fit in the available space, further improvements to the scanner's performance — i.e., better resolution or reduced time per scan — would likely require increased X-ray output. This would also increase the amount of information leaked to an external detector.

5 Discussion and Lessons

The Secure 1000 appears to perform largely as advertised in the non-adversarial setting. It readily detected a variety of naïvely concealed contraband materials. Our preliminary measurements of the radiation exposure delivered during normal scanning (Appendix A) seem consistent with public statements by the manufacturer, TSA, and the FDA [5, 18, 38, 54]. Moreover, it seems clear that the manufacturer took significant care to ensure that predictable equipment malfunctions would not result in unsafe radiation doses; in order for this to happen a number of independent failures would be required, including failures of safety interlocks specifically designed to prevent unsafe conditions.

However, the Secure 1000 performs less well against clever and adaptive adversaries, who can use a number of techniques to bypass its detection capabilities and to attempt to subvert it by cyberphysical means. In this section, we use the device's strengths and weaknesses to draw lessons that may help improve the security of other AITs and cyberphysical security systems more generally.

The effectiveness of the device is constrained by facts of X-ray physics . . . As discussed in Section 2.1, Compton scattering is the physical phenomenon which enables backscatter imaging. As the tight beam of X-rays shines upon the scene, it interacts with the scene material. The intensity and energy spectrum of the backscattered radiation is a function of both the X-ray spectrum emitted by the imaging device and the atomic composition of the material in the scene.

The Secure 1000 emits a single constant X-ray spectrum, with a maximum energy of 50 keV, and detects the intensity of backscatter to produce its image. Any two materials, no matter their actual atomic composition, that backscatter the same approximate intensity of X-rays will appear the same under this technology. This physical process enables our results in Section 3.3. This issue extends beyond the Secure 1000: any backscatter imaging device based upon single-spectrum X-ray emission and detection will be vulnerable to such attacks.

By contrast, baggage screening devices (such as the recently studied Rapiscan 522B; see [37]) usually use transmissive, rather than backscatter, X-ray imaging. These devices also often apply dual-energy X-ray techniques that combine information from low-energy and high-energy scans into a single image. To avoid detection by such systems, contraband will need to resemble benign material under two spectra, a much harder proposition.

. . . but physics is irrelevant in the presence of software compromise. In the Secure 1000, as in other cyberphysical screening systems, the image of the object scanned is processed by software. If that software has been tampered with, it can modify the actual scan in arbitrary ways, faking or concealing threats. Indeed, the ability of device software to detect threats and bring them to the attention of the operator is presumed in the "Automated Target Recognition" software used in current TSA millimeter-wave scanners [51]. Automatic suppression of threats by malicious software is simply the (easier to implement) dual of automatic threat detection. As we show in Section 4.1, malware can be stealthy, activating only when it observes a "secret knock."

Software security, including firmware updates, networked access, and chain-of-custody for any physical media, must be considered in any cyberphysical scanning system. Even so, no publicly known study commissioned by TSA considers software security.

Procedures are critical, but procedural best practices are more easily lost than those embedded in software. As early as 1991, Sandia National Labs recommended the use of side scans to find some contraband:

> A metallic object on the side of a person would blend in with the background and be unobserved. However, a side scan would provide an image of the object. There are other means of addressing this which IRT is considering presently [22, page 14].

Yet TSA procedures appear to call for only front and back scans, and the device manual characterizes side scans as an unusual practice:

> The Secure 1000 can conduct scans in four subject positions, front, rear, left side and right side. Most users only conduct front and rear scans in routine operations and reserve the side scans for special circumstances [35, page 3-7].

Omitting side scans makes it possible to conceal firearms, as we discuss in Section 3.1.

Since side scans are necessary for good security, the device's design should encourage their use by default. Yet, if anything, the scanner user interface nudges operators away from performing side scans. It allows the display of only two images at a time, making it poorly suited to taking four scans of a subject. A better design would either scan from all sides automatically (the Secure 1000 is already sold in a configuration that scans from two sides without the subject's turning around) or encourage/require a four-angle scan.

Adversarial thinking, as usual, is crucial for security. The Sandia report concludes that both C-4 and Detasheet plastic explosives are detected by the Secure 1000. Attached to their report is an image from one C-4 test (Figure 9), wherein a 0.95 cm thick C-4 block is noticeable only by edge effects — it is outlined by its own shadow, while the intensity within the block almost exactly matches the surrounding flesh. This suggests a failure to think adversarially: since plastic explosives are, by design, moldable putty, the attacker can simply gradually thin and taper the edges of the mass, drastically reducing edge effects and rendering it much less noticeable under X-ray backscatter imaging. We describe precisely such an attack in Section 3.3.

The basic problem appears to be that the system, while well engineered, appears not to have been designed, documented, or deployed with adaptive attack in mind. For

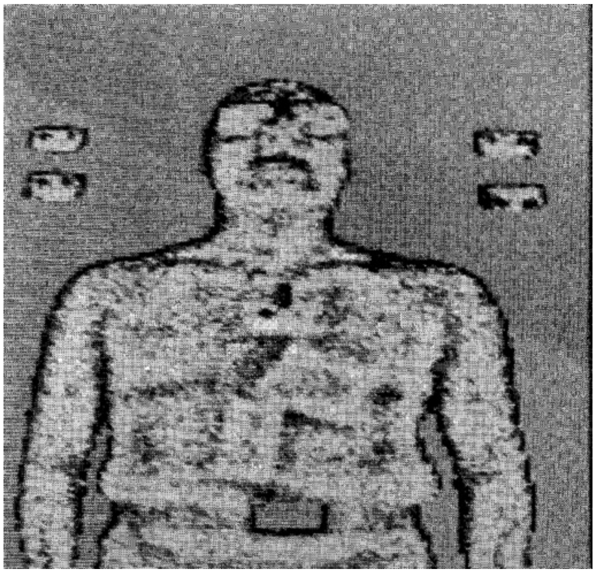


Figure 9: Naïve Evaluation — In an evaluation by Sandia National Labs, a Secure 1000 prototype successfully detects blocks of C-4 plastic explosive and Lucite attached to the subject's chest. Observe that the detection is based almost entirely on the X-ray shadow surrounding each rectangular block, which can be reduced or eliminated by an adaptive adversary through clever shaping and positioning of contraband. Reproduced from [22].

instance, attaching contraband to the side of the body as described in Section 3.1 is a straightforward attack that is enabled by scanning only straight-on rather than from all angles. However, the operator's manual shows only example images where the contraband is clearly at the front or the back.

The other attacks we describe in Sections 3 and 4, which allow us to circumvent or weaken the advertised efficacy, privacy, and security claims, again show that the system's designers failed to think adversarially.

Simplicity and modular design are also crucial for security. The system control board implements simple, well-defined functionality and communicates with the operator console by means of a simple protocol. We were unable to compromise the control board by abusing the communication protocol. This is in contrast to the scanner console, whose software runs on a general-purpose COTS operating system.

Simplicity and modular design prevented worse attacks, but do other AITs reflect these design principles? Modern embedded systems tend towards greater integration, increased software control, and remote network capabilities, which are anathema to security.

Components should be designed with separation of concerns in mind: each component should be responsible for controlling one aspect of the machine's operation. Communication between components should be constrained to narrow data interfaces. The Secure 1000 gets these principles right in many respects. For example, the PC software does not have the ability to command the X-ray tube to a particular height. Instead, it can only command the tube to return to its start position or to take a scan.

Our main suggestion for improving the Secure 1000's cyberphysical security is to remove the ability for the control board firmware to override the safety interlocks (something currently needed only briefly, at scan initialization). As long as this bypass functionality is in place, the interlocks can serve as safety mechanisms but not as a defense against software- or firmware-based attacks.

Keeping details of the machine's behavior secret didn't help... Published reports about the Secure 1000 have been heavily redacted, omitting even basic details about the machine's operation. This did not stop members of the public from speculating about ways to circumvent the machine, using only open-source information. In an incident widely reported in the press, Jonathan Corbett suggested that firearms hanging off the body might be invisible against the dark background [8], an attack we confirm and refine in Section 3.1. Two physicists, Leon Kaufman and Joseph Carlson, reverse engineered the Secure 1000's characteristics from published scans and concluded that "[i]t is very likely that a large (15–20 cm in diameter), irregularly-shaped, [one] cm-thick pancake [of plastic explosive] with beveled edges, taped to the abdomen, would be invisible to this technology" [21], an attack we confirm and refine in Section 3.3. Keeping basic information about the device secret made an informed public debate about its use at airports more difficult, but did not prevent dangerous attacks from being devised.

...but keeping attackers from testing attacks on the machine might. To a degree that surprised us, our attacks benefited from testing on the device itself. Our first attempts at implementing a new attack strategy were often visible to the scanner, and reliable concealment was made possible only by iteration and refinement. It goes without saying that software-replacement attacks on the console are practical only if one has a machine to reverse engineer. As a result, we conclude that, in the case of the Secure 1000, keeping the machine out of the hands of would-be attackers may well be an effective strategy for preventing reliable exploitation, even if the details of the machine's operation were disclosed.

The effectiveness of such a strategy depends critically on the difficulty of obtaining access to the machine. In addition to the device we purchased, at least one other Secure 1000 was available for sale on eBay for months after we obtained ours. We do not know whether it sold, or to whom. Also, front-line security personnel will always have some level of access to the device at each deployment installation (including at non-TSA facilities) as they are responsible for its continued operation. Given these facts, imposing stricter purchase controls on backscatter X-ray machines than those currently enacted may not be enough to keep determined adversaries from accessing, studying, and experimenting with them.

6 Related work

Cyberphysical devices must be evaluated not only for their safety but also for their security in the presence of an adversary [19]. This consideration is especially important for AITs, which are deployed to security checkpoints. Unfortunately, AIT manufacturers and TSA have not, to date, allowed an unfettered independent assessment of AITs. Security evaluators retained by a manufacturer or its customers may not have an incentive to find problems [30]. In the case of a backscatter X-ray AIT specifically, an evaluation team may be skilled in physics but lack the expertise to identify software vulnerabilities, or vice versa.

Ours is the first study to consider computer security aspects of an AIT's design and operation, and the first truly independent assessment of an AIT's security, privacy, and efficacy implications informed by experimentation with an AIT device.

Efficacy and procedures. In 1991, soon after its initial development, the Secure 1000 was evaluated by Sandia National Laboratories on behalf of IRT Corp., the company then working to commercialize the device. The Sandia report [22] assessed the device's effectiveness in screening for firearms, explosives, nuclear materials, and drugs. The Sandia evaluators do not appear to have considered adaptive strategies for positioning and shaping contraband, nor did they consider attacks on the device's software. Nevertheless, they observed that side scans were sometimes necessary to detect firearms.

More recently, the Department of Homeland Security's Office of Inspector General released a report reviewing TSA's use of the Secure 1000 [10]. This report proposed improvements in TSA procedures surrounding the machines but again did not consider adversarial conditions or software vulnerabilities.

Working only from published descriptions of the device, researchers have hypothesized that firearms can be concealed hanging off the body [8] and that plastic explosives can be caked on the body [21]. We confirm these attacks are possible in Section 3 and refine them through access to the device for testing.

Health concerns. The ionizing radiation used by the Secure 1000 poses at least potential health risks. Studies performed on behalf of TSA by the Food and Drug Administration's Center for Devices and Radiological Health [5] and by the Johns Hopkins University Applied Physics Laboratory [18] attempted to quantify the overall radiation dose delivered by the device. Both studies saw public release only in heavily redacted form, going so far as to redact even the effective current of the X-ray tube.

In 2010, Professors at the University of California, San Francisco wrote an open letter to John P. Holdren, the Assistant to the President for Science and Technology, expressing their concern about potential health effects from the use of backscatter X-ray scanners at airports [40]. The letter writers drew on their radiological expertise, but did not have access to a Secure 1000 to study. The FDA published a response disputing the technical claims in the UCSF letter [28], as did the inventor of the Secure 1000, Steven W. Smith [43]. Under dispute was not just the total radiation dose but its distribution through the skin and body. In independent work concurrent with ours, a task group of the American Association of Physicists in Medicine [2] explicitly considered skin dose. The task group's measurements are within an order of magnitude of our own, presented in Appendix A.

7 Conclusion

We obtained a Rapiscan Secure 1000 and evaluated its effectiveness for people screening. Ours was the first analysis of an AIT that is independent of the device's manufacturer and its customers; the first to assume an adaptive adversary; and the first to consider software as well as hardware. By exploiting properties of the Secure 1000's backscatter X-ray technology, we were able to conceal knives, firearms, plastic explosive simulants, and detonators. We further demonstrated that malicious software running on the scanner console can manipulate rendered images to conceal contraband.

Our findings suggest that the Secure 1000 is ineffective as a contraband screening solution against an adaptive adversary who has access to a device to study and to use for testing and refining attacks. The flaws we identified could be partly remediated through changes to procedures: performing side scans in addition to front and back scans, and screening subjects with magnetometers as well as backscatter scanners; but these procedural changes will lengthen screening times.

Our findings concerning the Secure 1000 considered as a cyberphysical device are more mixed. Given physical access, we were able to replace the software running on the scanner console, again allowing attackers to smuggle contraband past the device. On the other hand, we were unable to compromise the firmware on the system control board, a fact we attribute to the separation of concerns embodied in, and to the simplicity of, the scanner design.

The root cause of many of the issues we describe seems to be failure of the system designers to think adversarially. That failure extends also to publicly available evaluations of the Secure 1000's effectiveness. Additionally, the secrecy surrounding AITs has sharply limited the ability of policymakers, experts, and the general public to assess the government's safety and security claims.

Despite the flaws we identified, we are not able to categorically reject TSA's claim that AITs represent the best available tradeoff for airport passenger screening. Hardened cockpit doors may mitigate the hijacking threat from firearms and knives; what is clearly needed, with or without AITs, is a robust means for detecting explosives. The millimeter-wave scanners currently deployed to airports will likely behave differently from the backscatter scanner we studied. We recommend that those scanners, as well as any future AITs — whether of the millimeter-wave or backscatter [34] variety — be subjected to independent, adversarial testing, and that this testing specifically consider software security.

Acknowledgments

We are grateful to the many people who contributed to the preparation of this report, including Michael Bailey, Nate Cardozo, Cindy Cohn, Prabal Dutta, Jennifer Granick, Nadia Heninger, Daniel Johnson, Daniel Kane, Brian Kantor, Falko Kuester, Sarah Meiklejohn, Kurt Opsahl, Stefan Savage, Daniel Scanderberg, Alex Snoeren, Geoff Voelker, Kai Wang, and the anonymous reviewers. We also thank the outstanding staff members at UCSD and the University of Michigan who helped us navigate the legal and regulatory landscape and made studying the device possible. This material is based in part upon work supported by the National Science Foundation Graduate Research Fellowship Program.

References

[1] M. M. Ahlers. TSA removing "virtual strip search" body scanners. CNN, Jan. 2013. http://www.cnn.com/2013/01/18/travel/tsa-body-scanners.

[2] American Association of Physicists in Medicine. Radiation dose from airport scanners. Technical Report 217, June 2013. http://www.aapm.org/pubs/reports/RPT_217.pdf.

[3] American National Standards Institute. Radiation safety for personnel security screening systems using X-ray or gamma radiation. ANSI/HPS N43.17-2009, Aug. 2009.

[4] D. Bowen et al. "Top-to-Bottom" Review of voting machines certified for use in California. Technical report, California Secretary of State, 2007. http://sos.ca.gov/elections/elections.vsr.htm.

[5] F. Cerra. Assessment of the Rapiscan Secure 1000 body scanner for conformance with radiological safety standards, July 2006. http://www.tsa.gov/sites/default/files/assets/pdf/research/rapiscan_secure_1000.pdf.

[6] CNN. Shoe bomb suspect to remain in custody. CNN, Dec. 2001. http://edition.cnn.com/2001/US/12/24/investigation.plane/.

[7] A. H. Compton. A quantum theory of the scattering of X-rays by light elements. *Physical Review*, 21(5):483, 1923.

[8] J. Corbett. $1B of TSA nude body scanners made worthless by blog: How anyone can get anything past the scanners, Mar. 2012. http://tsaoutofourpants.wordpress.com/2012/03/06/1b-of-nude-body-scanners-made-worthless-by-blog-how-anyone-can-get-anything-past-the-tsas-nude-body-scanners.

[9] J. Danzer, C. Dudney, R. Seibert, B. Robison, C. Harris, and C. Ramsey. Optically stimulated luminescence of aluminum oxide detectors for radiation therapy quality assurance. *Medical Physics*, 34(6):2628, July 2007.

[10] Department of Homeland Security, Office of Inspector General. Transportation Security Administration's use of backscatter units. Technical Report OIG-12-38, Feb. 2012. http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-38_Feb12.pdf.

[11] Department of Homeland Security, Science and Technology Directorate. Compilation of emission safety reports on the L3 Communications, Inc. ProVision 100 active millimeter wave advanced imaging technology (AIT) system. Technical Report DHS/ST/TSL-12/118, Sept. 2012. http://epic.org/foia/dhs/bodyscanner/appeal/Emission-Safety-Reports.pdf.

[12] EPIC. Transportation agency's plan to x-ray travelers should be stripped of funding, June 2005. http://epic.org/privacy/surveillance/spotlight/0605/.

[13] K. Fu. Trustworthy medical device software. In *Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report*, July 2011.

[14] M. E. Hoppe and T. G. Schmidt. Estimation of organ and effective dose due to Compton backscatter security scans. *Medical Physics*, 39(6):3396–3403, 2012.

[15] J. Hubbard. New jail to have x-ray scanner used for security at airport. Wilkes Journal-Patriot, Oct. 2013. http://www.journalpatriot.com/news/article_95a398bc-368d-11e3-99ec-0019bb30f31a.html.

[16] R. Hughes. Systems and methods for improving directed people screening, June 12 2012. US Patent 8,199,996.

[17] ivw-agne. Rapiscan Secure 1000 DP (Dual Pose) backscatter body scanner / nacktscanner. eBay listing, 2012. http://www.ebay.com/itm/Rapiscan-Secure-1000-DP-Dual-Pose-Backscatter-Body-Scanner-Nacktscanner-/110999548627.

[18] Johns Hopkins University Applied Physics Laboratory. Radiation safety engineering assessment report for the Rapiscan Secure 1000 in single pose configuration. Technical Report NSTD-09-1085, version 2, Aug. 2010. http://www.tsa.gov/sites/default/files/assets/pdf/research/jh_apl_v2.pdf.

[19] R. G. Johnston. Adversarial safety analysis: Borrowing the methods of security vulnerability assessments. *J. Safety Research*, 35(3):245–48, 2004.

[20] P. A. Jursinic and C. J. Yahnke. In vivo dosimetry with optically stimulated luminescent dosimeters, OSLDs, compared to diodes; the effects of buildup cap thickness and fabrication material. *Medical Physics*, 38(10):5432, 2011.

[21] L. Kaufman and J. W. Carlson. An evaluation of airport X-ray backscatter units based on image characteristics. *Journal of Transportation Security*, 4(1):73–94, 2011.

[22] B. Kenna and D. Murray. Evaluation tests of the SECURE 1000 scanning system. Technical Report SAND 91-2488, UC-830, Sandia National Laboratories, Apr. 1992.

[23] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *Proc. 31st IEEE Symposium on Security and Privacy*, pages 447–62, May 2010.

[24] A. Kotowski and S. Smith. X-ray imaging system with active detector, Dec. 16 2003. US Patent 6,665,373.

[25] D. Kravets. Court oks airport body scanners, rejects constitutional challenge, July 2011. http://www.wired.com/threatlevel/2011/07/court-approves-body-scanners/.

[26] R. Langner. To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve. Online: http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, Nov. 2013.

[27] A. Lowrey. My visit to the offices of Rapiscan, which makes airport scanners. Slate, Nov. 2010. http://www.slate.com/articles/business/moneybox/2010/11/corporate_junket.html.

[28] J. L. McCrohan and K. R. Shelton Waters. Response to UCSF regarding their letter of concern [40], Oct. 2010. http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/SecuritySystems/ucm231857.htm.

[29] A. Medici. Guess where TSA's invasive scanners are now? Federal Times, May 2014. http://www.federaltimes.com/article/20140516/DHS/305160012/Guess-where-TSA-s-invasive-scanners-now-.

[30] S. J. Murdoch, M. Bond, and R. Anderson. How certification systems fail: Lessons from the Ware report. *IEEE Security & Privacy*, 10(6):40–44, Nov–Dec 2012.

[31] National Security Agency. Cottonmouth-iii. *Der Spiegel*, 2013. http://www.spiegel.de/international/world/a-941262.html, fetched 2014-02-27.

[32] OSI Systems. OSI Systems receives $25m order from U.S. Transportation Security Administration for advanced imaging technology. Press release, Oct. 2009. http://investors.osi-systems.com/releasedetail.cfm?ReleaseID=413032.

[33] Phantom Laboratory. The rando phantom, ran100 and ran110, 2006. http://www.phantomlab.com/library/pdf/rando_datasheet.pdf.

[34] J. Plungis. Naked-image scanners to be removed from U.S. airports. Bloomberg News, Jan. 2013. http://www.bloomberg.com/news/2013-01-18/naked-image-scanners-to-be-removed-from-u-s-airports.html.

[35] *Secure 1000 Personnel Scanner Operator's Manual*. Rapiscan Systems, Aug. 2005.

[36] Rapiscan Systems. Rapiscan secure 1000, 2005. http://epic.org/privacy/surveillance/spotlight/0605/rapiscan.pdf.

[37] Rapiscan Systems. Rapiscan 522b, 2006. http://www.wired.com/images_blogs/threatlevel/2014/02/RapiScan-522B.pdf, fetched 2014-02-27.

[38] Rapiscan Systems. Rapiscan Secure 1000 health and safety fact sheet, 2012. http://www.rapiscansystems.com/extranet/downloadFile/24_Rapiscan%20Secure%201000-Health%20and%20Safety-Fact%20Sheet.pdf.

[39] G. D. Rossides. TSA Reply to Rep. Bennie G. Thompson, Feb. 2010. http://epic.org/privacy/airtravel/backscatter/TSA_Reply_House.pdf.

[40] J. Sedat, D. Agard, M. Shuman, and R. Stroud. UCSF letter of concern, Apr. 2010. http://www.npr.org/assets/news/2010/05/17/concern.pdf.

[41] A. Shahid. Feds admit they stored body scanner images, despite TSA claim the images cannot be saved, Aug. 2010. http://www.nydailynews.com/news/national/feds-admit-stored-body-scanner-images-tsa-claim-images-saved-article-1.200279.

[42] S. W. Smith. Secure 1000, concealed weapon detection system, 1998. http://www.dspguide.com/secure.htm, fetched 2014-02-27.

[43] S. W. Smith. Re: Misinformation on airport body scanner radiation safety, Dec. 2010. http://tek84.com/downloads/radiation-bodyscanner.pdf.

[44] S. W. Smith. Resume, 2014. http://www.dspguide.com/resume.htm, fetched 2014-02-27.

[45] C. Tate. Privacy impact assessment for the Secret Service use of advanced imaging technology, Dec. 2011. http://epic.org/foia/dhs/usss/Secret-Service-Docs-1.pdf.

[46] M. Taylor, R. Smith, F. Dossing, and R. Franich. Robust calculation of effective atomic numbers: The Auto-Zeff software. *Medical Physics*, 39(4):1769, 2012.

[47] Transportation Security Administration. Contract with rapiscan security products, June 2007. IDV ID: HSTS04-07-D-DEP344, http://epic.org/open_gov/foia/TSA_Rapiscan_Contract.pdf.

[48] Transportation Security Administration. Passenger screening using advanced imaging technology: Notice of proposed rulemaking. *Federal Register*, 78(58):18287–302, Mar. 2013.

[49] Transportation Security Administration Office of Security Technology. Procurement specification for whole body imager devices for checkpoint operations. TSA, Sept. 2008. http://epic.org/open_gov/foia/TSA_Procurement_Specs.pdf.

[50] TSA. AIT: Frequently Asked Questions, May 2013. http://www.tsa.gov/ait-frequently-asked-questions. Fetched May 17, 2013: https://web.archive.org/web/20130517152631/http://www.tsa.gov/ait-frequently-asked-questions.

[51] TSA Press Office. TSA takes next steps to further enhance passenger privacy, July 2011. http://www.tsa.gov/press/releases/2011/07/20/tsa-takes-next-steps-further-enhance-passenger-privacy.

[52] TÜV SÜD America. EMC test report: Secure 1000 WBI, Feb. 2009. http://epic.org/privacy/body_scanners/EPIC_TSA_FOIA_Docs_09_09_11.pdf, pages 162–323.

[53] U.S. Army Institute of Public Health. Rapiscan Secure 1000 Single Pose dosimetry study. Technical report, Jan. 2012. http://www.tsa.gov/sites/default/files/assets/pdf/foia/final_ait_dosimetry_study_report_opa.pdf.

[54] U.S. Department of Homeland Security Office of Health Affairs. Fact sheet: Advanced imaging technology (ait) health & safety, 2010. http://www.oregon.gov/OBMI/docs/TSA-AIT_ScannerFactSheet.pdf.

[55] C. Wain. Lessons from lockerbie. BBC, Dec. 1998. http://news.bbc.co.uk/2/hi/special_report/1998/12/98/lockerbie/235632.stm.

[56] XM Materials. Material safety data sheet XM-03-X (Comp C-4 explosive simulant), Oct. 1999. http://www.xm-materials.com/MSDS/xray_msds/msdsxm_03_x.pdf.

[57] XM Materials. Material safety data sheet XM-04-X (Semtex explosive simulant), Oct. 1999. http://www.xm-materials.com/MSDS/xray_msds/msdsxm_04_x.pdf.

A Radiation Dose Assessment

The Secure 1000 generates low-energy X-rays (50 kVp at 5 mA tube accelerating potential) to construct its images. Although this output is low, the machine still produces ionizing radiation, and careful assessment is necessary to ensure public safety.

The imparted dose has been scrutinized recently by various agencies applying a number of experimental designs [2, 14, 53]. These findings have been consistent with manufacturer claims [38] that per-scan radiation exposure to subjects is nonzero, but is near natural background levels. Additionally, there have been claims and counterclaims surrounding the distribution of dose within the body, with some groups raising concerns that the scanner might impart a minimal deep dose but an overly large skin dose to the subject [5, 40, 43].

To shed light on this question, we executed a brief assessment of the radiological output of the scanner using Landauer Inc.'s InLight whole body dosimeters. These dosimeters give a shallow dose equivalent (SDE), a deep dose equivalent (DDE), and an eye lens dose equivalent. They are analyzed using optically stimulated luminescence (OSL), an established dosimeter technology [9, 20]. We read the results using Landauer's proprietary MicroStar dosimeter reader.

We used a simple experimental design to quantify the dose output: we arranged 21 dosimeters on a RANDO chest phantom positioned upright on a wooden table with a neck-to-floor distance of 144 cm and a source-to-detector distance of 66 cm, approximating the conditions of a normal scan. The dosimeters give a more accurate dose representation if the incident beam is perpendicular to the detector material. In this case, the dosimeters were attached to the chest phantom without regard for beam angle, and so no correction factors were implemented; geometry issues were expected in the results.

The InLight dosimeters require a total dose of at least 50 μSv to be accurate. To irradiate them sufficiently, we performed 4033 consecutive single scans in the machine's normal operating mode. (Each screening consists of at least two such scans: one front and one rear.) A scan was automatically triggered every 12 s and lasted 5.7 s, for a total beam-on time of 6 h 23 min.

We read the dosimeters the following day. A small loss of dose due to fade is expected, but for the purpose of this study we regard this decrease as negligible. We applied the standard low-dose Cs-137 calibration suggested by Landauer. Initially, we were concerned that the low energy output of the scanner (50 kVp tube potential emits an X-ray spectrum centered roughly in 16 keV–25 keV) would lead to inaccurate readings on the InLights, but since the dosimeters are equipped with filters, the dose equation algorithm in the MicroStar reader can deduce beam energy without a correction factor applied to the 662 keV energy from the original calibration.

The average DDE per scan for all the dosimeters was calculated to be 73.8 nSv. The average SDE per scan was 70.6 nSv, and the average eye-lens dose per scan was 77.9 nSv. The standard deviation (σ) and the coefficient of variation (CV) value of all the dosimeters for the DDE were 0.75 and 0.10 (generally low variance) respectively. For the SDE and lens dose, σ and the CV were 1.26 and 0.16, and 2.08 and 0.29, respectively.

An unexpected aspect of our results is that the measured DDE is higher than the SDE, and this occurrence is worth further examination. The irradiation geometry of the dosimeters could possibly explain this irregularity. It might be productive to conduct further experiments that account for this effect.

The doses we measured are several times higher than those found in the recent AAPM Task Group 217 report [2], but they still equate to only nominal exposure: approximately equal to 24 minutes of natural background radiation and below the recommendation of 250 nSv per screening established by the applicable ANSI/HPS standard [3]. A person would have to undergo approximately 3200 scans per year to exceed the standard's annual exposure limit of 250 μSv/year, a circumstance unlikely even for transportation workers and very frequent fliers.