SECURITY ANALYSIS OF A FULL-BODY SCANNER
Warning: Nudity

talk shows unmodified scanner images to demonstrate the privacy implications of full body scanning
FULL BODY SCANNERS

IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS
Feb 2007: TSA introduces FBSs as ‘secondary screening’
FULL BODY SCANNER DEPLOYMENT

2007
Feb 2007: TSA introduces FBSs as ‘secondary screening’

2008

2009

2010
Dec 2009: Failed bombing of Transatlantic flight

2011

2012

2013

2014

IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS
FULL BODY SCANNER DEPLOYMENT

2007
Feb 2007: TSA introduces FBSs as ‘secondary screening’

2009
Dec 2009: TSA moves FBSs to primary screening

2010
Dec 2009: Failed bombing of Transatlantic flight

2011

2012

2013

2014

IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS
FULL BODY SCANNER DEPLOYMENT

- **Feb 2007:** TSA introduces FBSs as ‘secondary screening’
- **Dec 2009:** TSA moves FBSs to primary screening
- **Dec 2009:** Failed bombing of Transatlantic flight
- **Nov 2012:** Secure 1000 arrives at our lab

**Timeline:**
- 2007
- 2008
- 2009
- 2010
- 2011
- 2012
- 2013
- 2014

**Image:** Rapiscan Corp., L-3 Communications

**Logo:** Rapiscan Systems

**Logo:** L3
FULL BODY SCANNER DEPLOYMENT

Feb 2007: TSA introduces FBSs as ‘secondary screening’

Dec 2009: TSA moves FBSs to primary screening

Dec 2009: Failed bombing of Transatlantic flight

Nov 2012: Secure 1000 arrives at our lab

IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS
FULL BODY SCANNER DEPLOYMENT

Feb 2007: TSA introduces FBSs as ‘secondary screening’

Dec 2009: TSA moves FBSs to primary screening

Dec 2009: Failed bombing of Transatlantic flight

Nov 2012: Secure 1000 arrives at our lab

May 2013: TSA retires Secure 1000

IMAGE: RAPISCAN CORP., L-3 COMMUNICATIONS
Radiological Safety?

“... THE DOSE TO THE SKIN MAY BE DANGEROUSLY HIGH.”
PUBLIC DEBATE

Privacy?

"... THE DOSE TO THE SKIN MAY BE DANGEROUSLY HIGH."

Radiological Safety?
PUBLIC DEBATE

Privacy?

Contraband Detection?

Radiological Safety?

"... THE DOSE TO THE SKIN MAY BE DANGEROUSLY HIGH."

The TSO working the NoS said on his headset, "heads up, got a cutie for you."

"..."
Table 8-7 provides the exposure and background readings for the master unit and Table 8-8 provides the readings for the slave unit. Figure 8-10 provides the locations of the readings. As shown in Table 8-7 and 8-8, the dose above the units that occurs at the beginning of each scan. When the Single Pose system executes a scan, the start position (for the first scan) of the X-ray generator When the scan is initiated, the X-ray generator (and therefore x-ray beam) Therefore, the primary beam points toward During this phase are not monitored because as they are out of tolerance. At this time it is assumed that and these parameters are monitored. Therefore, there is approximately 0.5 seconds at the beginning of each scan where vertical motion has not reached peak velocity and may result in slightly higher doses at the position where the scan starts.
ACQUISITION
OUR CONTRIBUTION: THE FACTS

1. Is the Secure 1000 radiologically **safe**?

2. What **privacy** safeguards exist?

3. How **effective** is it at detecting contraband?

Cyberphysical systems use software!
INSIDE THE SECURE 1000
X-RAY PHYSICS 101

Photoelectric Effect

Incoming Photon -> Electron -> Photoelectron

Compton Scattering

Incoming Photon -> Electron -> Recoil electron

Scattered Photon

Low energy X-ray: 50 KeV at 5 mA
X-RAY PHYSICS 101

Photoelectric Effect

Dominant effect depends on material’s "effective atomic number"
SECURE 1000 X-RAY HARDWARE

FIGURE ADAPTED FROM U.S. PATENT 8,199,996
R. HUGHES, JUNE 2012
**SECURE 1000**

- Chopper spins
- Head assembly moves vertically
SECURE 1000

- Chopper spins
- Head assembly moves vertically
SECURE 1000 X-RAY HARDWARE
IMAGE PRODUCTION
OUR RESULTS
RADIATION SAFETY
RADIATION SAFETY

- X-ray energy: 50 KeV at 5 mA
- Dose per scan: 70-80 nSv
  - ~24 minutes of background exposure
- Similar results by AAPM (2013)
CYBERPHYSICAL RADIATION SAFETY

• Safety controls on radiological output
  • Not security controls!

• Simple, modular design
  • Cannot over-irradiate scan subject without ROM replacement
OPERATOR SOFTWARE

SECURE 1000™ personnel screening system
Rapiscan Security Products, Hawthorne, CA
FOR USE BY QUALIFIED OPERATORS ONLY

<table>
<thead>
<tr>
<th>scan</th>
<th>zoom</th>
<th>clear</th>
<th>redraw</th>
<th>save</th>
<th>recall</th>
<th>comments</th>
<th>options</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>→</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Press ENTER to save images to the harddisk.

Press the ↑↓ keys to select another action.

08-14-14  11:16
CONSOLE MALWARE

“Secret knock”  Visible light  X-ray
CONSOLE MALWARE

Operator’s View

“Secret knock”

X-ray
HANDS-OFF ATTACKS
ADVERSARIAL PHYSICS
ADVERSARIAL PHYSICS
FIREARMS

- Subject is carrying a .380 ACP pistol
Subject is carrying a .380 ACP pistol
FOLDING KNIFE

- Subject is carrying a folding knife
FOLDING KNIFE

Subject is carrying a folding knife.
PLASTIC EXPLOSIVES

After the failed Christmas Day “underwear bombing” attempt in 2009, Napolitano launched a worldwide and “historic” effort — in 190 countries — to enhance passenger screening and counter the threat of “nonmetallic devices” on aircraft, she said.

SANDIA: C4 DETECTION (1992)

SANDIA: C4 DETECTION (1992)

REPRODUCED FROM “EVALUATION TESTS OF THE SECURE 1000 SCANNING SYSTEM”
THINK ADVERSARially!
THINK ADVERSARially!

Plastic!
PLASTIC EXPLOSIVES

Subject carrying 200+ g of C-4 simulant

vs.

No contraband
PLASTIC EXPLOSIVES

Subject carrying 200+ g of C-4 simulant

vs.

No contraband
PLASTIC EXPLOSIVES

Subject carrying 200+ g of C-4 simulant

vs.

No contraband
EFFICACY RESULTS

• Our results imply adversaries can conceal:
  • Knives
  • Firearms
  • Plastic Explosive & Detonators

• Access to Secure 1000 allows attack refinement
DISCUSSION AND LESSONS
POLICY IMPLICATIONS

• Secure 1000 used at airports despite major flaws
  • Either TSA didn’t know (inadequate testing) or didn’t act

• Critical security infrastructure needs independent, rigorous, transparent testing
  • Including cyberphysical security testing!
  • Apply adaptive adversarial thinking
LESSONS FOR DEVELOPERS

• Simple, modular design
  • Remote malicious X-ray emittance not possible in Secure 1000

• Physics matters

• But only if software is safe!
  • Compromised software -> complete security failure
MITIGATIONS

- Disclosed results to DHS and Rapiscan in May 2014

- Procedural mitigations
  - Perform side scans
  - Pair with metal detectors
ADVANCED IMAGING TECHNOLOGY: TODAY & TOMORROW

- AIT deployed at nearly 160 U.S. airports
  - L-3 ProVision (millimeter wave)
  - Automated Threat Recognition
- TSA testing new X-ray backscatter AIT

IMAGE: L-3 COMMUNICATIONS, AMERICAN SCIENCE & ENGINEERING
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

Questions?

More information at https://radsec.org