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

How many people been through airport security in the USA?

TSA

- Transportation Security Administration
  - Created in response to 9/11
- From 2009, adopted non-invasive advanced imaging technology
- Controversial for a number of reasons

Paper motivations and objectives

- No prior private investigation of AIT devices
- Investigate from both cyber and physical scenarios
  - How does one impact the other?
- *Derive Lessons for future of cyberphysical systems*

A brief note about ethics and safety

Backscatter Imaging - Physics

- Traditional X-Ray machines detect variation in transmission through the target, backscatter detects radiation that *reflects* from the target
  - Useful for imaging organic material
- Utilizes a process called *Compton scattering*
  - Type of inelastic scattering, which does *not* preserve kinetic energy of incident particles
  - High energy photon hits electron and transfers energy; resulting in a decrease of energy of the photon that then scatters in an unpredictable direction
- Determining factor of scattering is a single element's atomic number, Z, and compound elements can be modeled with "effective Z", or Z_{eff}
- Key Takeaway: *Z is important in gaming backscatter systems*

Rapiscan Secure 1000

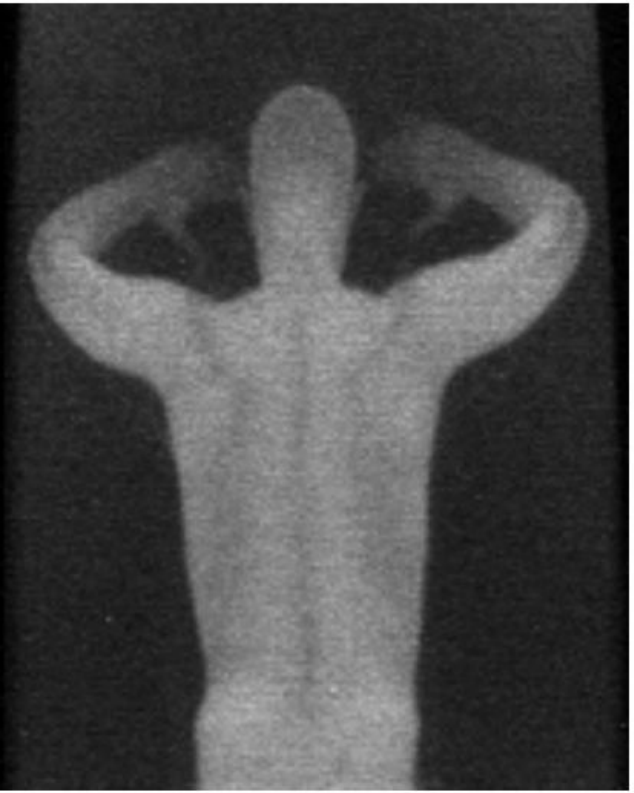
- Bought on eBay from a seller who had acquired it in an auction
- Used in airports widely between 2009 - 2013
- Utilizes backscatter technology discussed earlier
- Has two main subsystems
  - Operator interface
  - Scanner unit

Gaming the scanner: Concealment by Positioning

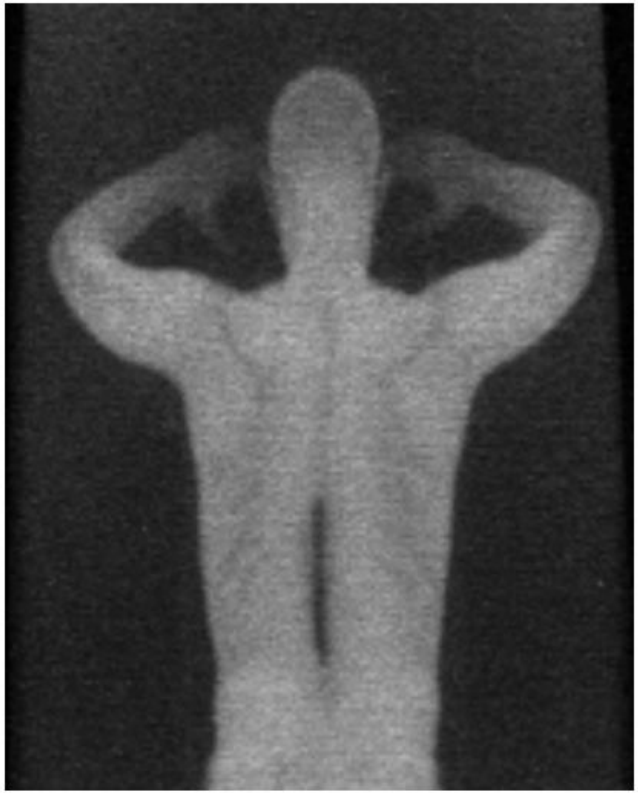
- Backscatter technologies emitting in 50 keV range have limitations
  - Cannot differentiate between absence of matter and high Zeff
- Concealed weapon in a way that does not block the person being scanned

Gaming the scanner: Concealment by Masking

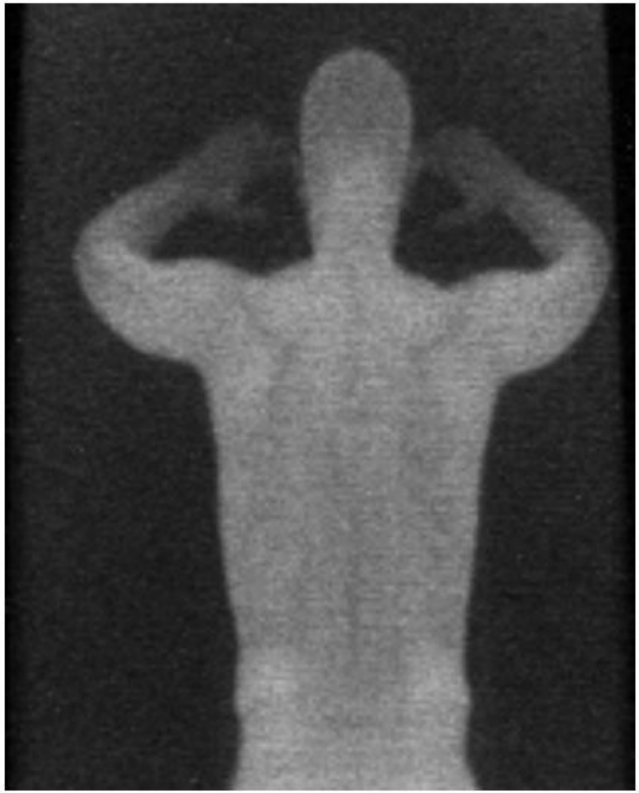
- Mask contraband with materials that have a Zeff value close to human flesh
  - Cannot differentiate between the two
- Heuristics of what the scanner can detect enable sneaky hiding in places on the body



(a) No contraband



(b) 18 cm knife taped to spine



(c) Knife behind 1.5 cm plastic block

Gaming the scanner: Concealment by Shaping

- Malleable contraband can be shaped to look like the body
  - C-4, Semtex
- Navel Engineering to solve “inhuman properties” of image

Cyberphysical Security: User Console Malware

- No passwords, no problems?
- If it's important enough for a physical lock, make the lock good
  - Lockpicked in ten seconds
- INSECURE.exe
  - Secret knocks

Cyberphysical Security: Embedded Controller Attacks

- System Control Board (SCB)
  - Controls mechanical systems
- Secure unless firmware is tampered with
  - Stored in EPROM inside scanner
  - Easy to access physically, remote attack much harder
- Many hardware safety mechanisms in place

Cyberphysical Security: Privacy Side Channel

- Motivated attacker can capture xray backscattering with their own device
  - What are possible attack vectors?

Lessons Learned from this Study

- X-ray physics bounds the realm of attacks on this particular set of devices
- X-ray physics does NOT bound the realm of software attacks
- Having procedures in place is good, but not *as good* as embedding rules in software
  - software is forever!
- Adversarial thinking is crucial for security, cyber or not
- Be *simple* when designing systems
- Security by obscurity is usually not the answer
- Tight restrictions on secure devices *may* keep attackers at bay

Discussion