

MALINTENT DETECTION

the technology and its governance

The DHS is developing a system, called Future Attributes Screening Technology or FAST, to help detect from a stream of people those with hidden malevolent intentions. Israeli companies WeCU and SDS already have such systems available.

The presentation features a brief overview of the technology, a comparison with polygraph systems, an examination of security trade-offs, the consequences to our privacy, and the governance required to avoid abuse and misuse of these systems.

Vincent Poirier, cissp – security transcends technology : (isc)²

Vincent Poirier consults on information security, business continuity planning, and IT management & governance.

He came to Japan in 1989 and has worked for Ricoh, ANZ Bank, Citibank, Depfa Bank, and TÜV Rheinland. He has taught information technology management at Sophia University and he currently represents security technology products in Japan.

Mr. Poirier was born in Montreal, Canada and attended McGill University, obtaining a B.Sc. in Mathematics in 1988. In 2007 he received from ISC2 the CISSP designation (Certified Information Systems Security Professional) the information security industry's gold standard certification. He lives in Tokyo with his family.



Malintent detection

some available systems

- **Future Attributes Screening Technology or F.A.S.T.**

Department of Homeland Security (DHS)

- **Screening and investigative systems**

WeCU

- **More in-depth interrogation screening systems**

Suspect Detection Systems (SDS)

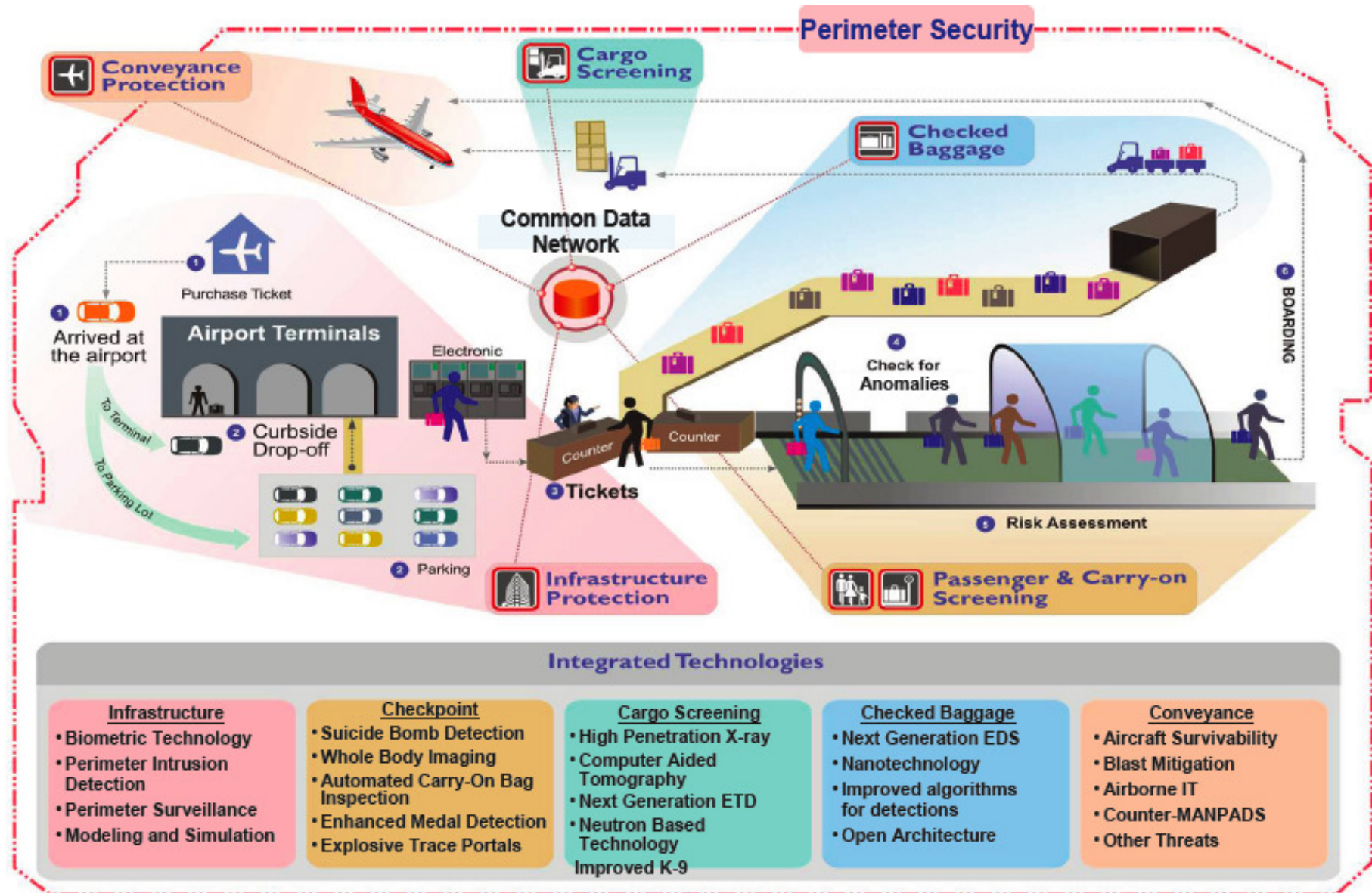
Malintent detection

application examples

- **Anti terrorist detection measures**
- **Drug smuggling detection**
- **Employee screening**
- **Out-of-hours building access**
- **Investigative tool**

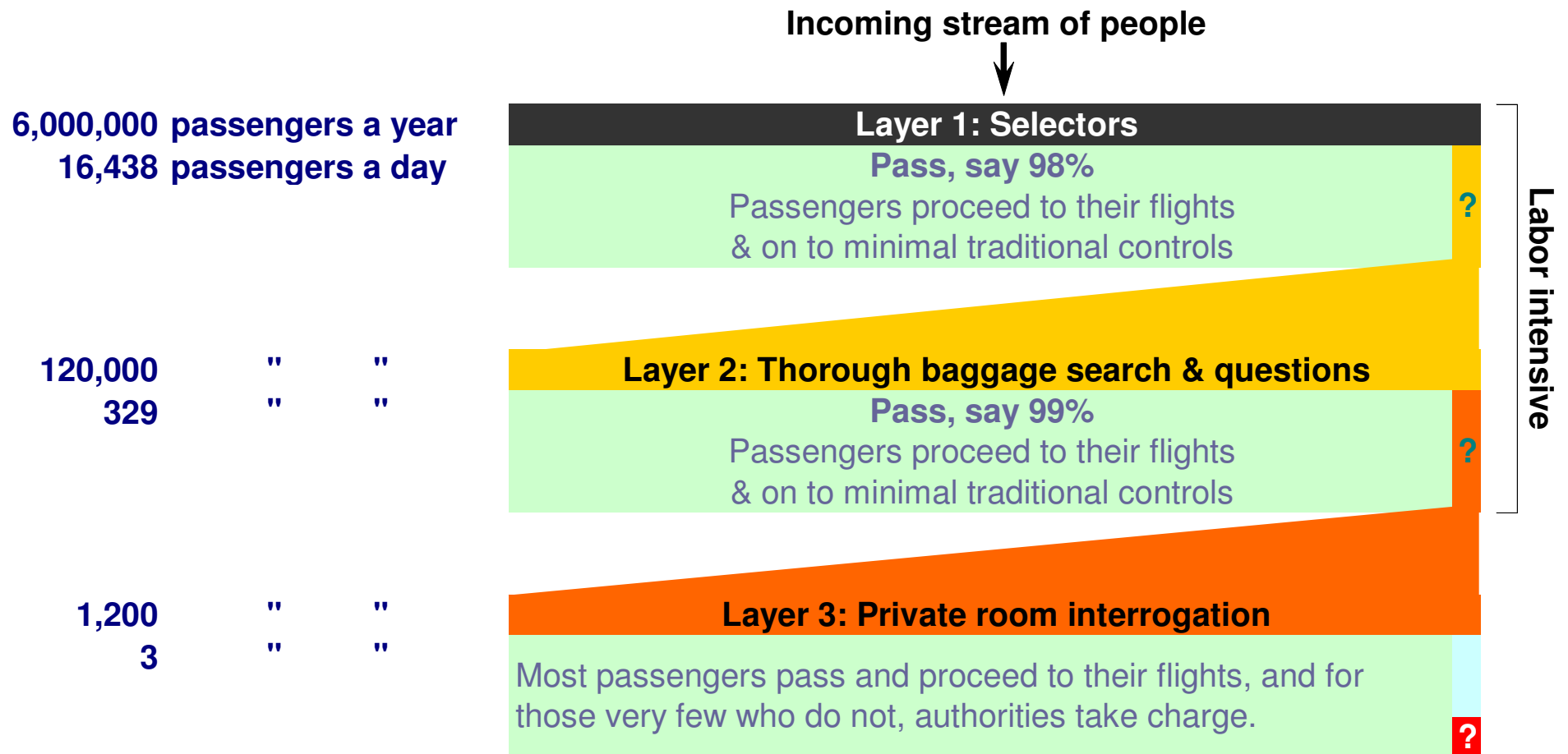
Airport security

traditional model – finding the bomb



Airport security

ben gurion airport model – finding the bomber, not the bomb



How it works

biometrics – the body reacts to simple questions & pictures – automation

STIMULUS

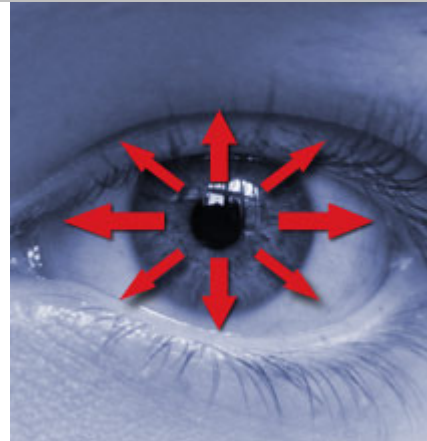


RESPONSE

Are you or are you not a terrorist?



Thank you for keeping this flight safe.



Are you smuggling drugs?



Responses are matched to a familiarity correlations database in 30 seconds.

ALL CLEAR

NO CONCLUSION

SUSPICIOUS

How it works

comparisons with the polygraph

Polygraph

Examinations are slow and laborious.

Targets a single individual who is aware of being examined.

Assesses the veracity of specific statements i.e. “Is the subject telling the truth?”

Requires professional operating skills.

Can be fooled by highly trained subjects.

Results are **indicative** and leave room for reasonable doubt.

Malintent Detection

Tests are quick, taking mere seconds.

Targets a stream of people who are unaware they are being scanned.

Assesses the subject’s familiarity with specific stimuli, i.e. “Is the subject reacting?”

Requires no operating skills.

Cannot be fooled.

Results are **indicative** and leave room for reasonable doubt.

How it works

advantages & limitations

+ **No profiling, no prejudice**

+ **Quick results**

+ **Non-intrusive**

+ **Results not stored**

- **Subversive**

- **Won't find bombs**

- **Storage *possible***

- **Hey, it's creepy...**

Descent Into the Maelström

Edgar Allan Poe, 1841



Descent Into the Maelström

Edgar Allan Poe, 1841

“...In all violent eddies at sea there is good fishing, at proper opportunities, if one has only the courage to attempt it; but among the whole of the Lofoden coastmen, we three were the only ones who made a regular business of going out to the islands, as I tell you.”

- ← 1. Fishing in dangerous waters is a risky but profitable business.

“.. It was just seven, by my watch , when we weighed and started for home, so as to make the worst of the Ström at slack water, which we knew would be at eight.”

- ← 2. The protagonist’s pocket watch, i.e. time tracking technology, is a tool that mitigates the risk.

(As we progressed home, we hit upon the maelström in its full fury. How could we have missed it?)

“..soon a hideous thought flashed upon me. I dragged my watch from its fob. It was not going. I glanced at its face by the moonlight, and then burst into tears as I flung it far away into the ocean. It had run down at seven o'clock ! We were behind the time of the slack, and the whirl of the Ström was in full fury !”

- ← 3. Disaster struck because the protagonist gave no thought to the technology failing.

Descent Into the Maelström

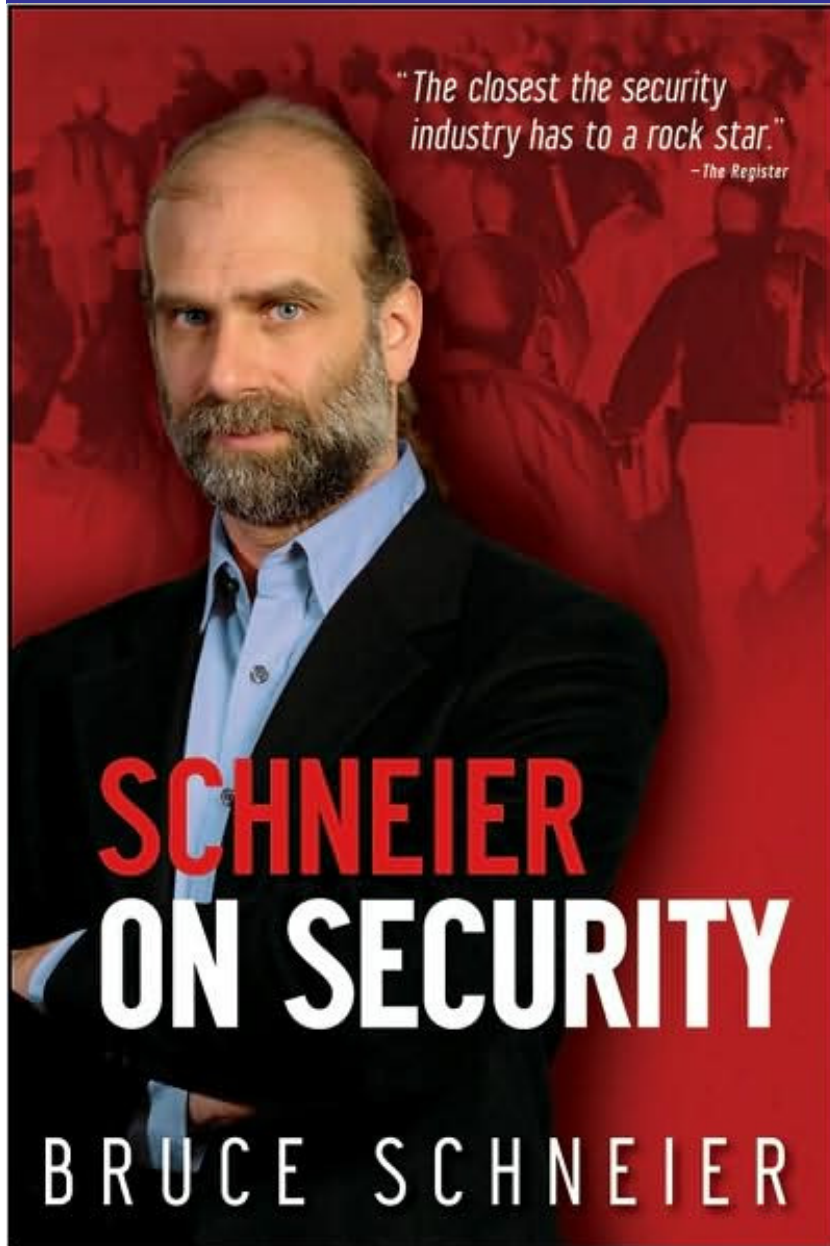
Edgar Allan Poe, 1841

Poe's tale illustrates that there is nothing new in our unfortunate habit of over relying on technology.

- The protagonist could have observed the sun.
- He could have checked his watch more often.
- He should have anticipated failure.

We must plan for the failure of the technology and also of the process.

What is security?



Some Schneier security mantras...

Security is about failure, not success.

Security is a trade off.

Security is about people, not technology.

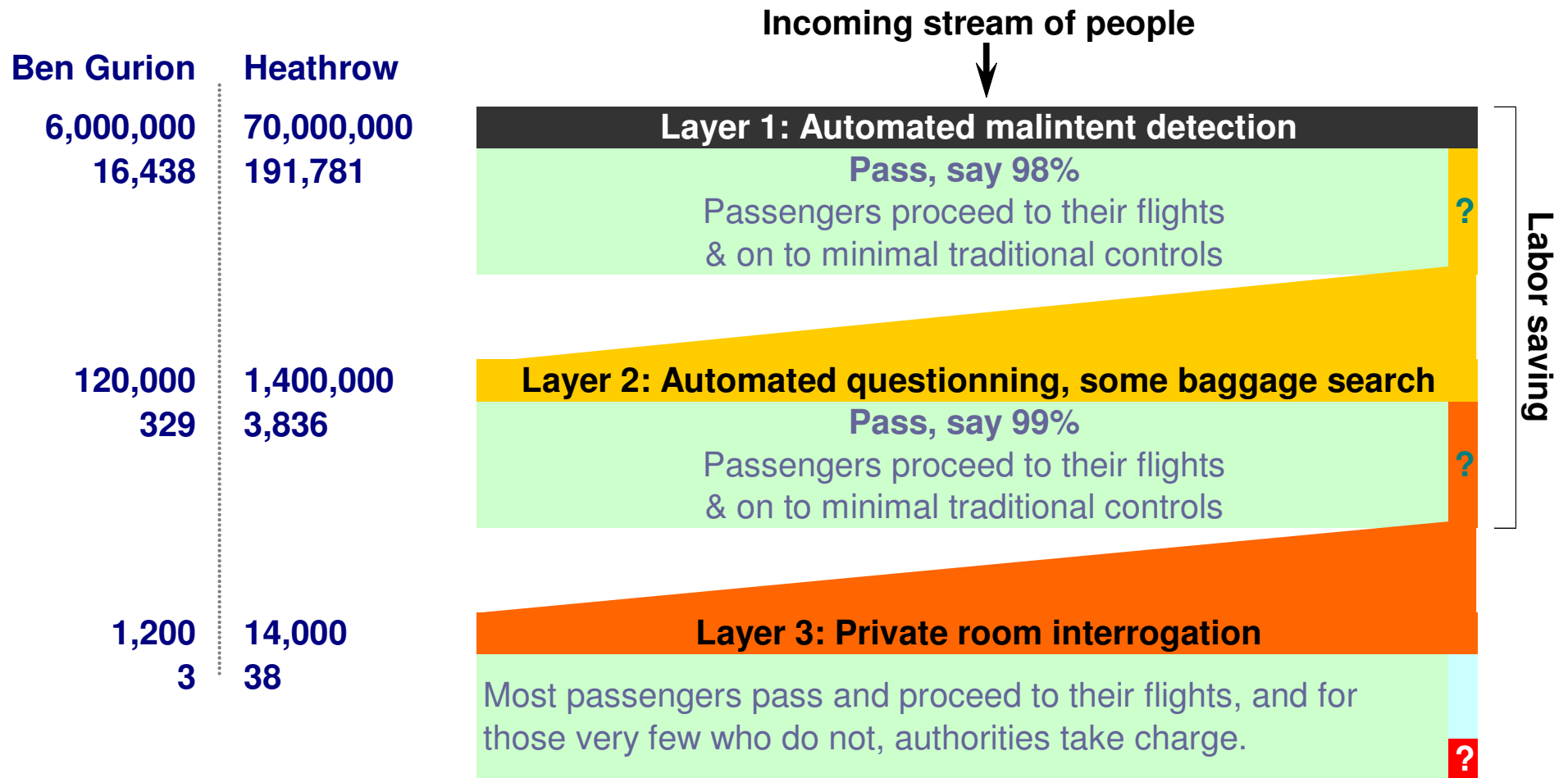
*Security is obtained by
skilled intelligence gathering.*

Bruce Schneier's Security Theater

Measures that make people feel more secure without doing anything to improve their security.



Security: what are the benefits?



Security: what's the trade-off?

As presented here, malintent detection systems are simply part of a screening process. They automate the initial task of sorting out those who are just trying to get on with their business from those who just might possibly be hiding something.

Our habit of relying on technology might lead to an attitude of relying on the machine. *“The machine flashed red, so who am I to contradict it?”* Operators with nothing to gain from questioning the results will therefore not question the results.

While we are assured these systems don't store response data, storage could very easily be implemented.

*If so, isn't there a danger
of the innocent being mislabeled
as guilty of something?*

What is privacy?



DANIEL SOLOVE

george washington university law school

We have yet to agree on a definition of privacy. Either definitions are too narrow and fail to include what most would consider private, or they are too broad and include what few would think as private. Solove proposes instead seeing privacy as a family of related concepts.

Information collection

surveillance
interrogation

Information dissemination

breach of confidentiality
disclosure
exposure
increased accessibility
blackmail
appropriation
distortion

Information processing

aggregation
identification
insecurity
secondary use

Invasion

intrusion
decisional interference

Oppression vs. Helplessness

problems with the “I’ve got nothing to hide” argument



Solove compares the traditional attack against the **“I’ve got nothing to hide argument”**, which focuses on the intrusive nature of surveillance, with a new approach which focuses on the unknown & uncontrolled use of innocuous information gathered by an anonymous bureaucracy.

Inspections intrude on our privacy and with them authorities project their power. We feel attacked and oppressed, as we can see from the outcries against body scanners and full body searches.



Gathering innocuous information lets authorities reach conclusions and act upon them without us having a say. We can't even defend ourselves in case of a mistake. There is no appeal procedure if we find ourselves on the no-fly list.

It's not mind reading!

Most media clips about this technology call it mind reading. WeCU itself has called it mind reading. Some news articles find the technology interesting but most journalists and bloggers react negatively. WeCU's own unfortunate choice of company name does nothing to quash our fears of Orwellian abuse. But the fact is, it's not mind reading at all.

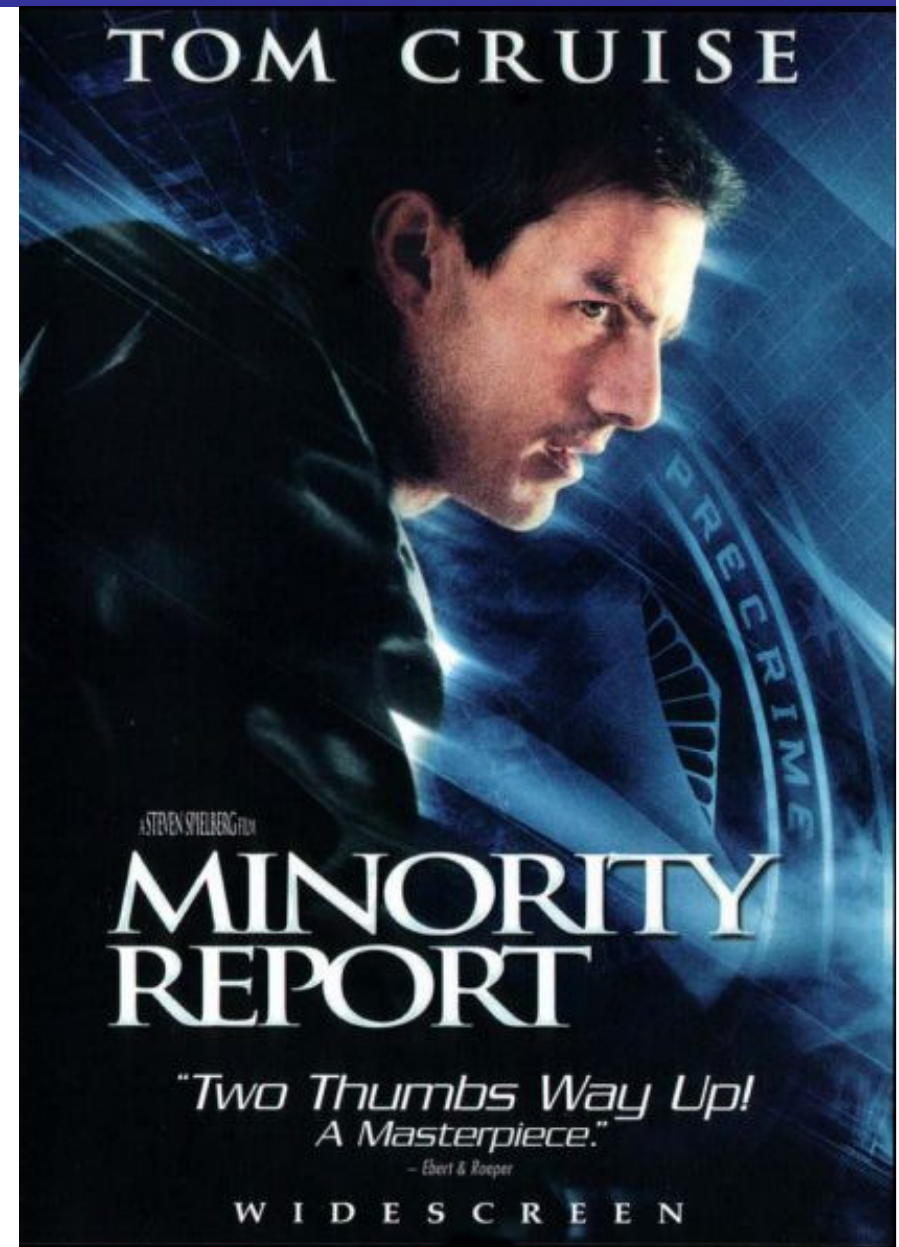
- Security agents can't read minds, neither can machines.
Good agents look for hinky behavior, machines look for fidgeting.
- The evidence jumps out of guilty subjects.
The systems don't dig inside our thoughts.
- Only what is sought is revealed.
Having naughty items for a bachelorette party won't set off the system.

Science Fiction? No.

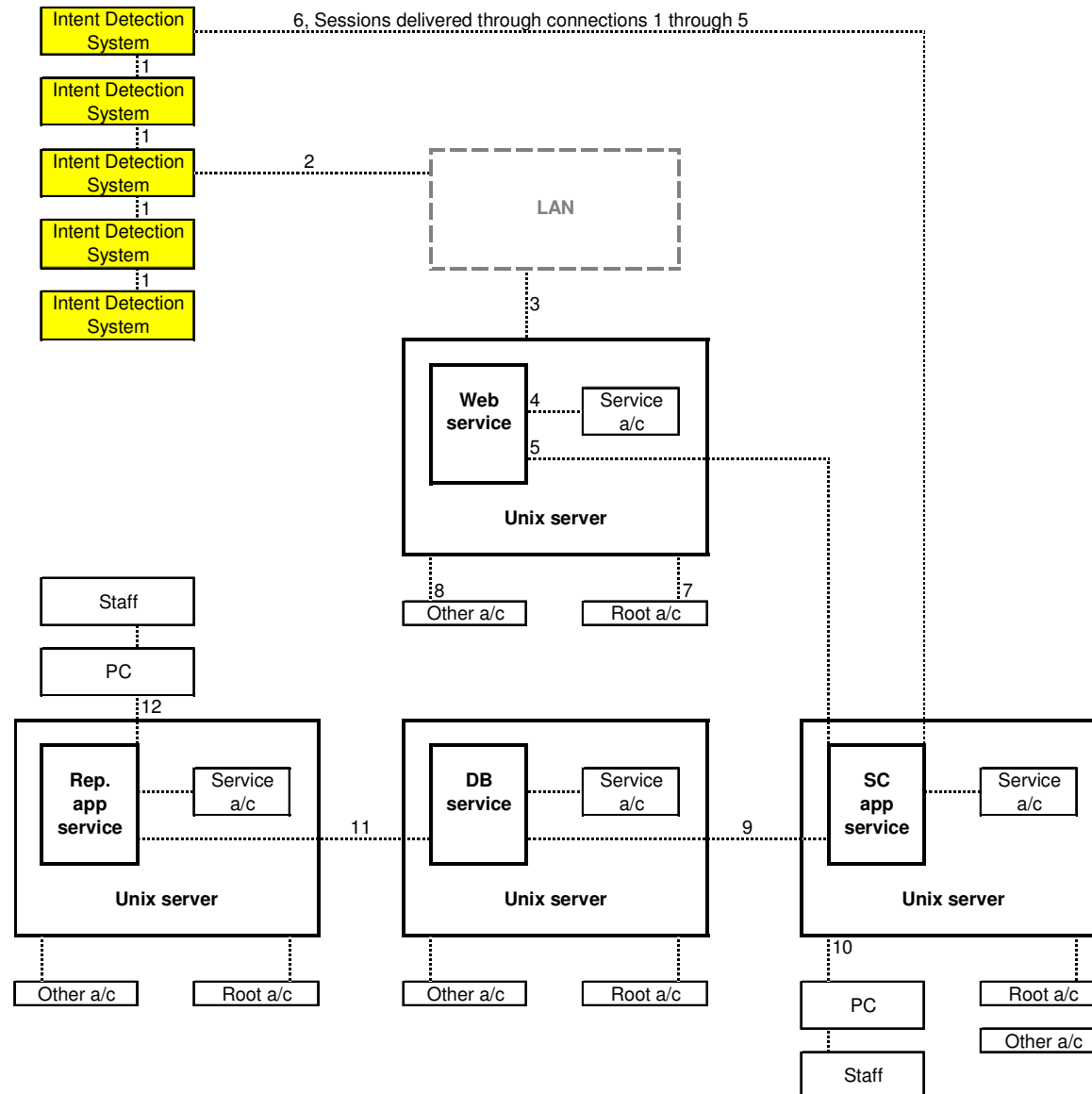
- Precognition technology? No.
- Punishing non-criminals? No.
- Assuming infallibility? No.
- These systems are not SF.

But their marketing leaves something to be desired...

(Interestingly the movie ends with the dismantling of the precrime division, while the short story by Philip K. Dick ends with the division saved from a plot to discredit it.)



Networked systems & potential security weaknesses



Networked systems have many weaknesses and vulnerabilities.

Each number stands for an interface, either between a person and a system or between two systems.

Even this simplified diagram reveals a dozen weak points.

Imagine the number we'd find in a nation wide system! And imagine this as one of many systems...

Stand-alone systems

Intent Detection
System

Intent Detection
System

Intent Detection
System

Intent Detection
System

Intent Detection
System

By contrast, stand-alone systems have no network vulnerabilities. The data would not be collected, so it cannot be stolen, unintentionally revealed, or misused.

What is IT governance?

The design & management of

IT policies,

frameworks,

regulations,

and controls

coupled with the allocation of authority among

users,

providers,

and auditors.

Why governance & oversight?

*“Give me six lines
written by
the most honorable of men,
and I will find
an excuse in them
to hang him.”*

*Armand Jean du Plessis
Duc de Richelieu*

