IFIP 10.4 Winter Meeting 2005

Security in Autonomic Web Computing

Bob Blakley

Chief Scientist, Security and Privacy, IBM

blakley@us.ibm.com

This Morning’s Headline

- Lexus Landcruiser 100 models LX470 and LS430 have been discovered with virus-infected operating systems.
- It is understood the virus could affect the navigation system of the Lexus models
- It transfers onto them via a Bluetooth mobile phone connection.

Challenges

- Accountability
  - Driven by compliance mandates
- Availability
  - Driven by shift from “hard asset value” to “information value” to “process value”
- Privacy
  - Driven by customer perceptions

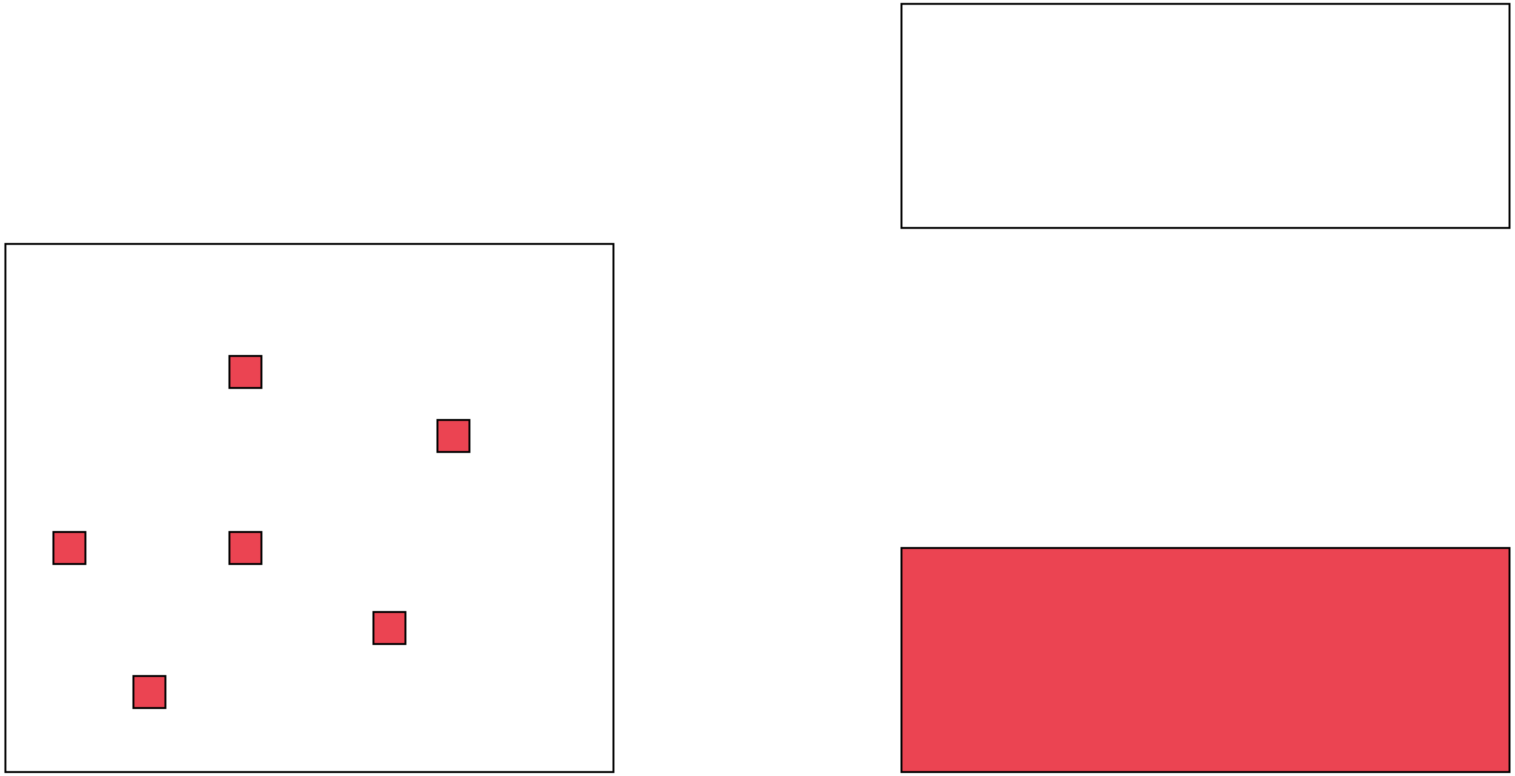
More Challenges

- Breakdown of the TCB
  - Where is the boundary?
  - Drives the requirement for vulnerabillity management
- Introductions
  - Identity of strangers
- Risk aggregation and Risk Diffusion
  - Single points of failure
  - No single point of incentive or responsibility

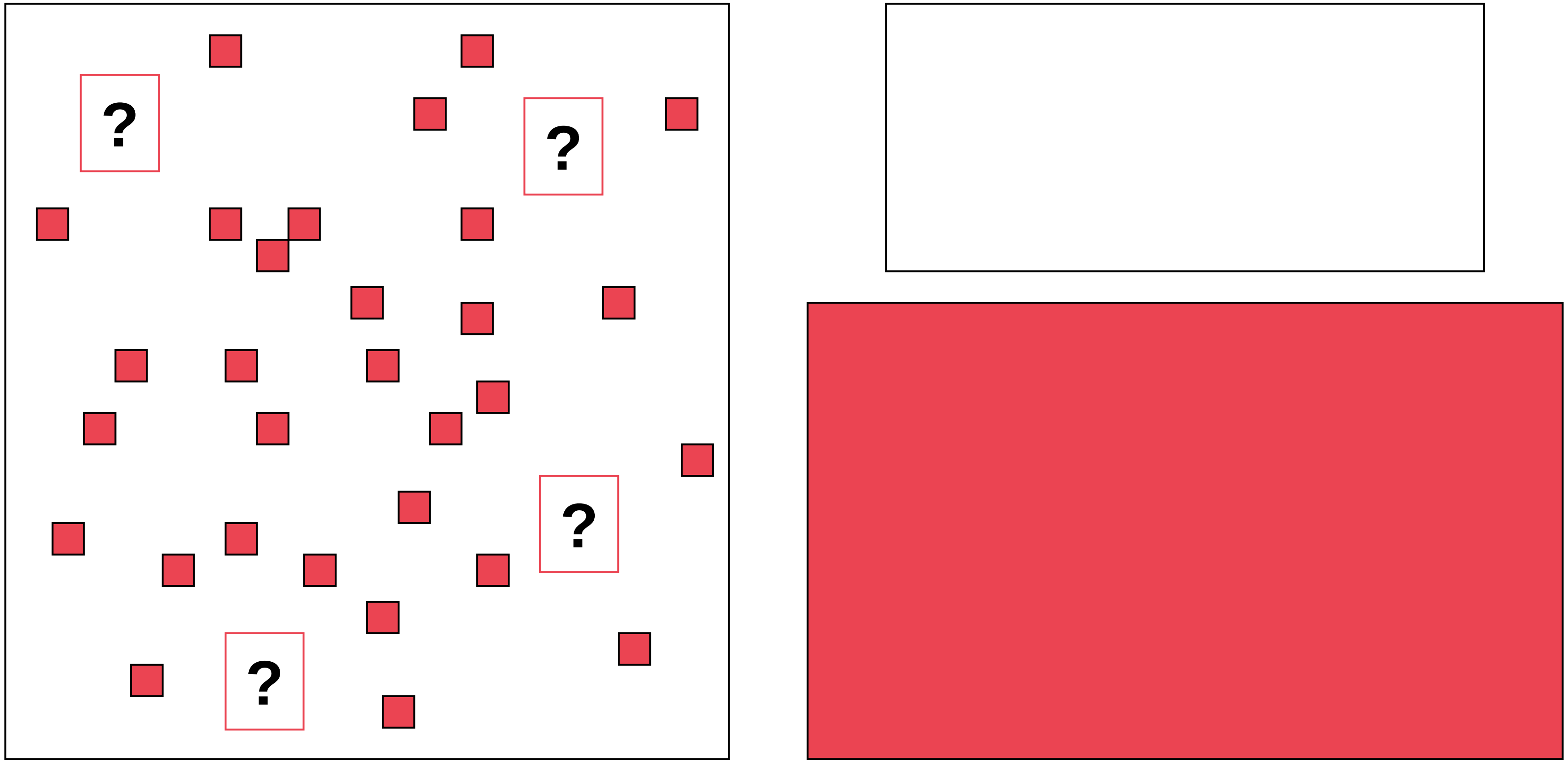
What’s Available?

- Traditional Security Technology
  - Wrong model, not well executed

TCB: Two Options



TCB: One Outcome



What’s Available?

- Assurance
  - EAL 4 down are useful
  - But mainly improve documentation and catch obvious flaws
  - EAL 7 would be great…
- Tools
  - It’s great that we’re gradually phasing out the dumb stuff we’ve always known was bad for us

What’s Available?

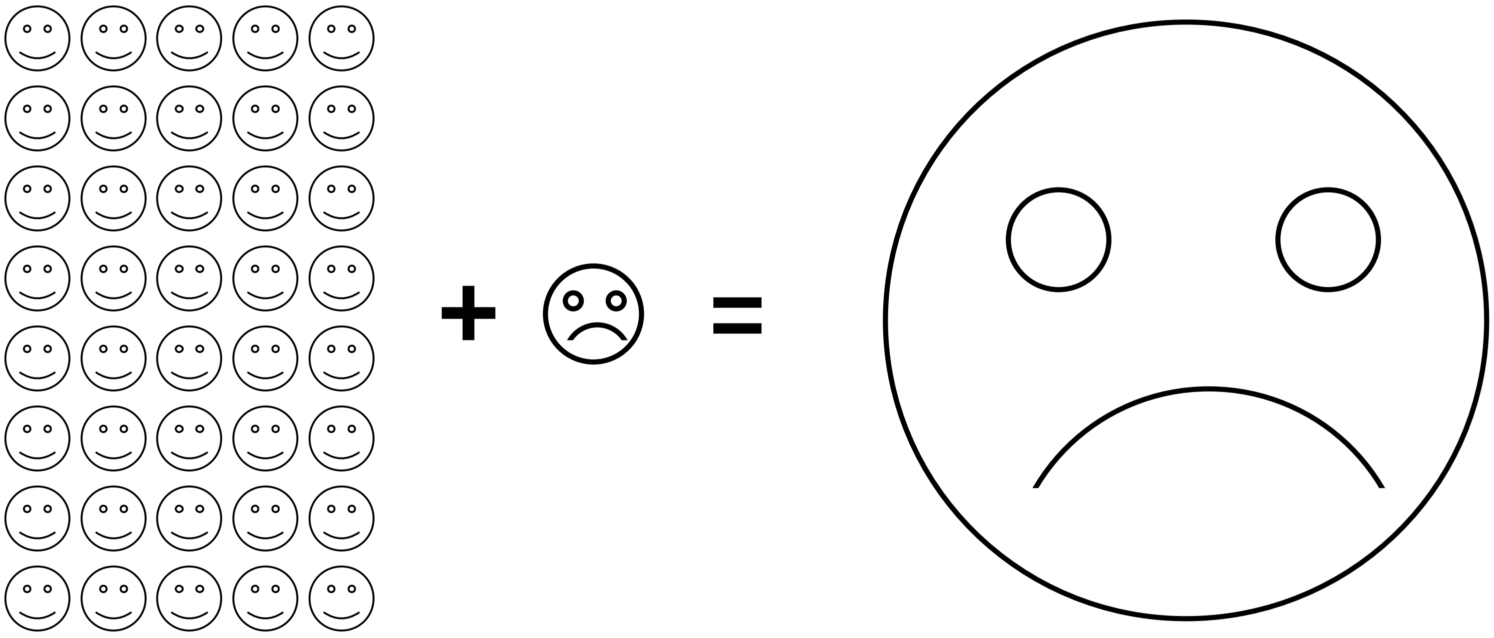
- Assurance
  - EAL 4 down are useful
  - But mainly improve documentation and catch obvious flaws
  - EAL 7 would be great…
- Tools
  - It’s great that we’re gradually phasing out the dumb stuff we’ve always known was bad for us
  - Like C++

What’s Available?

- New Security Technology
  - Intrusion Detection, Antivirus,
  - Vulnerability Management
  - Kinda like sprinkler systems, these are great if you already *have* a fire and don’t care about water damage…

Intrusion Detection

What detection?



Vulnerability Management

1,000,000 bugs
MBTF of each = 1,000,000,000 hours

Attacker has 1,000 hrs/yr available
Defender 100,000 hrs/yr plus expertise, source available

In 1 year, defender finds 100,000 bugs
Defender finds 1

Probability that defender finds attacker’s bug = 0.10

(Ross Anderson: Why Information Security is Hard)

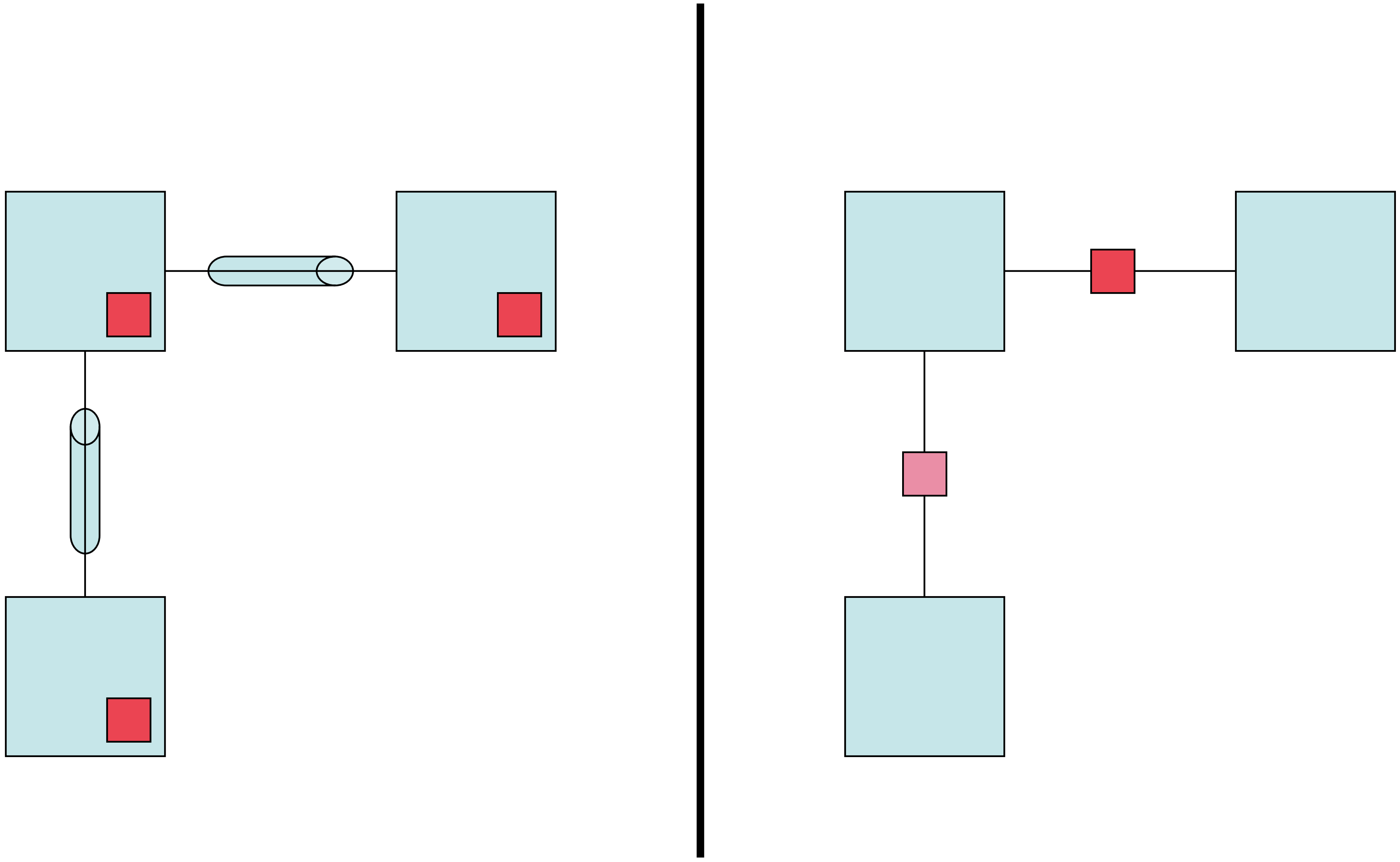
What’s Going To Happen?

- None of this stuff is going to work.
  - Traditional security technology assumes an infrastructure and an environment which don’t exist.
  - New security technologies lock the barn door after the horse is already gone.
  - Vulnerability management is a fool’s game.
- Periodic catastrophes will occur

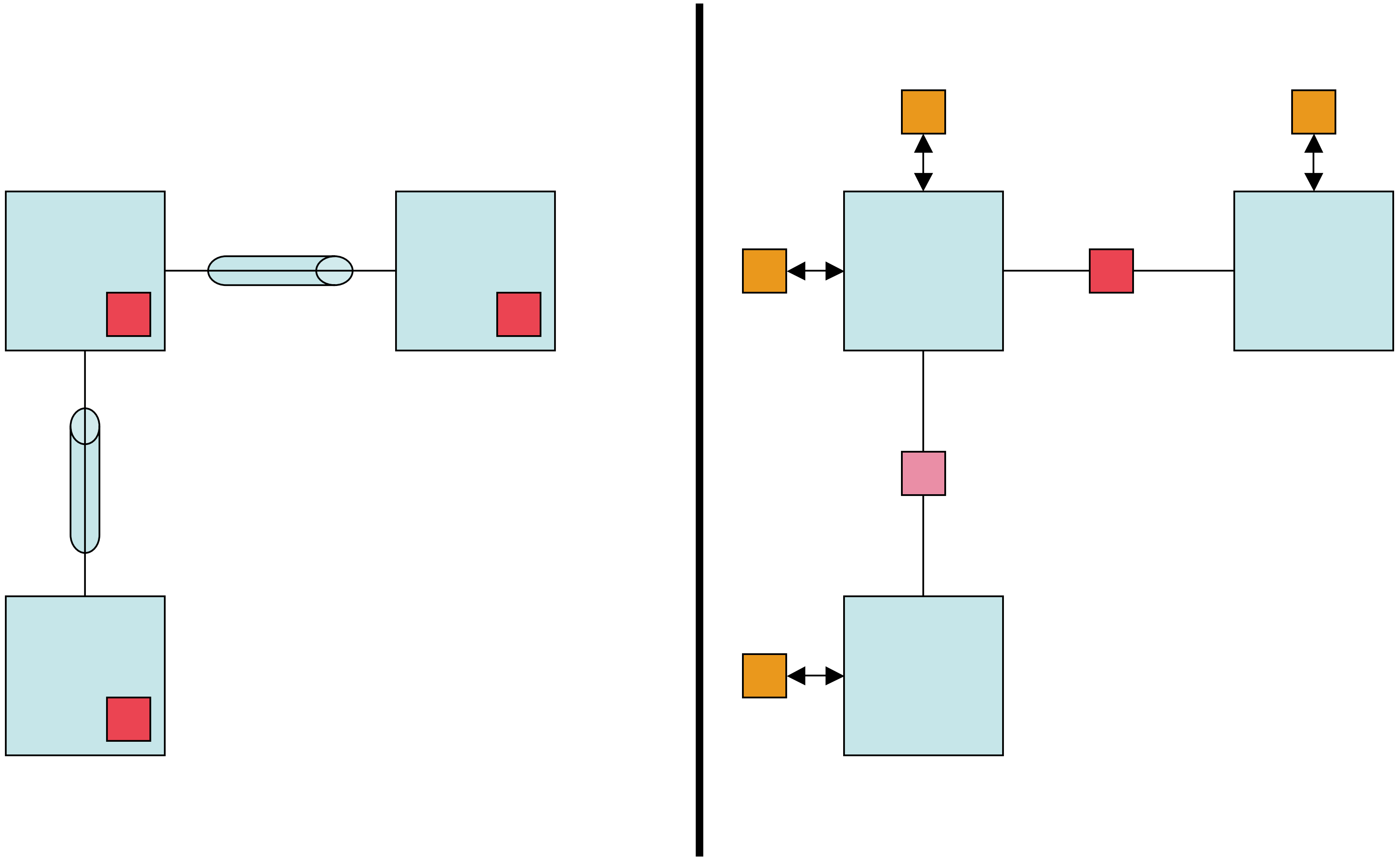
OK, What *Else* Is Available?

- Redundancy (hey, stuff is cheap now!)
- Diversity
- Use of time (need better way to say this…)
- Quick sense/analyze/respond loops
- Legislation/Regulation
  - HIPAA, GLB, etc…
  - Often diagnoses dyspepsia and prescribes leeches…
- New Models
  - Financial
  - Operational
  - Technical

Externalizing Security



Security Services



Y’all Got Questions?

Backup (covered by Brian)

What’s Out There?

- Hackers
  - Still lots
- Script Kiddies
  - Lots more
- Bots & Zombies
  - WAAAAY more
- Competitors
  - Hard to tell
- Terrorists
  - Definitely, but there are easier & more spectacular targets
- Nation-States
  - If you have to worry about these, you should be buying more specialized stuff

Why Is It Out There?

- Curiosity
- Fame (viruses)
- Fortune (trojans, spam, phishing)
- Malice (trojans)
  - Some people really hate Microsoft…
  - Which wouldn’t be quite so bad if they’d attack Microsoft’s servers instead of my client.

How Much Does It Cost?

- A lot
- But not as much as some folks want you to believe

How Bad Is It?

- Volume of attacks still doubles every year
- Time between discovery of vulnerability and release of automated exploit is asymptotically approaching zero
- Propagation of baddies is VERY fast
- Effectiveness of countermeasures against new exploits is pretty poor