Security Economics

Matthew Edwards

Focus: Security Economics

November 15, 2020

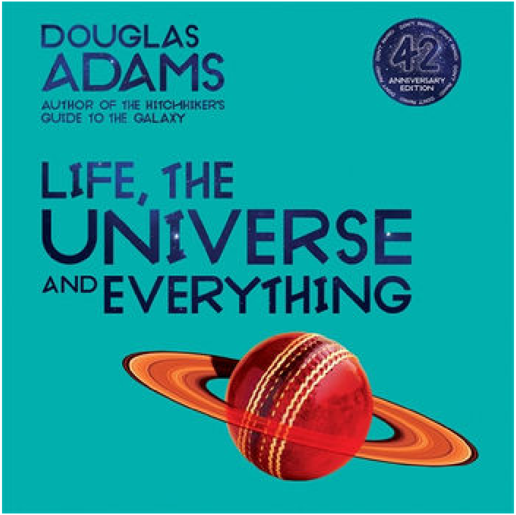
Economics in security

One use is to analyse cybercriminal economies, design interventions that disrupt them.

Not all cybercriminals are motivated by money – what then?

Another use of economics is to examine the *incentives* for or against security in other areas. Tools of economic analysis allow us to find and alter incentives.

Somebody else's problem


DOUGLAS ADAMS
AUTHOR OF THE HITCHHIKER'S GUIDE TO THE GALAXY
42
ANNIVERSARY EDITION
LIFE, THE UNIVERSE AND EVERYTHING

Example: ATM fraud

Legal precedent in the US: *A bank customer's word that they have not made a withdrawal is found to outweigh the bank experts' word that they must have done.*

At the time, no corresponding precedent in the UK.

In the US
Onus was on banks to prove customer defrauded them. Systems were better protected against fraud.

In the UK
Onus was on customer to prove bank was wrong – basically impossible. Banks were careless, poor fraud security.

Examples

> *"In general, where the party who is in a position to protect a system is not the party who would suffer the results of security failure, then problems may be expected."*

Medical payment privacy If systems are paid for by insurers rather than hospitals, patient privacy is not protected whenever this conflicts with insurers wanting data.

Digital signatures Risk from a signature being forged is transferred from the bank (building the system) to the customer.

Tragedy of the Commons

Grazing extra cattle on the commons means healthier cattle at no cost to you.

Everyone grazes their cattle on the commons, the commons is over-grazed and dies, nobody can graze on the commons.

Ignoring security patches and weaknesses saves time and money. . .

Adverse selection

The market for lemons

Where buyers don't know the quality of the product, there is severe downward pressure on both price and quality.

"Plum": \$3000
"Lemon": \$1000
Equal-odds pricing: \$2000

Application to information security. . . ?

Cost asymmetry

Why do attackers find bugs first?

Bugs to find: 1,000,000
Mean time-to-find 1,000 hours.

Attacker investment: 1,000 hours/year.
Defender investment: 10,000,000 hours/year.

In one year, the attacker might find 1 bug, while the defender has found 10,000. Yet the probability the defender has found the attacker's bug is low.

Security economics

- Reason about human (security) behaviour at scale;
- Implement policies that create or align with incentives;
- Update understanding of human behaviour based on data.