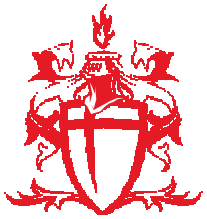


CITY UNIVERSITY
LONDON

Diversity for Safety and Security in Embedded Systems : decisions given supply chain risks

Lorenzo Strigini
Centre for Software Reliability, City University London, U.K.

reporting work with Andrey Povyakalo, Ilir Gashi

funded by
EU ARTEMIS SeSaMo (Security and Safety Modelling)
U.K. EPSRC D3S "Diversitry and Defecne in Dpeth for Security"
with thanks to
Martin Matschnig, Thomas Hinterstoisser, Bernhard Fischer, Peter Ryan

CSR Building confidence in a computerised world
www.csr.city.ac.uk

Background: the SESAMO project (2012-15)

Security and Safety Modelling

- *for embedded systems*
- *14 companies and 6 research institutes*
- *in Europe and the U.S.*

http://sesamo-project.eu/

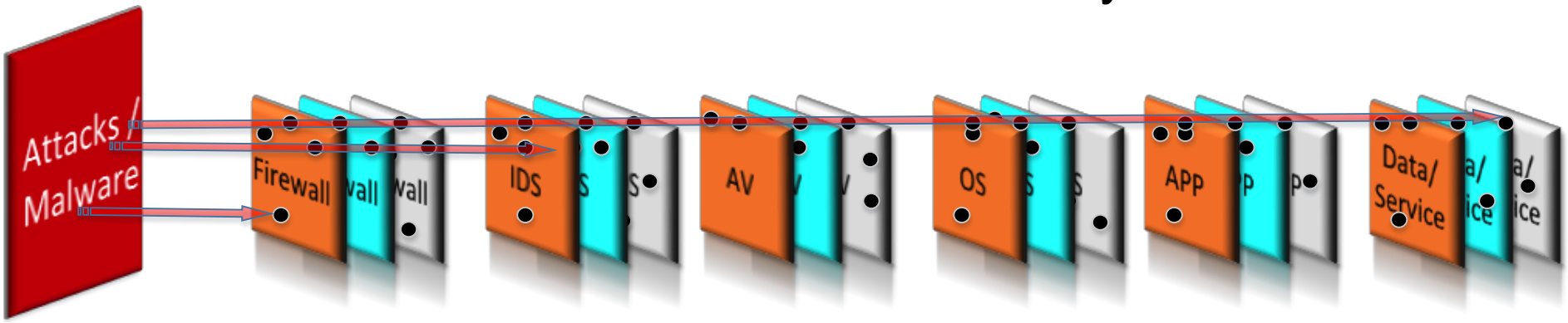
objectives include:

- joint reasoning about safety and security properties, their **conflicts and synergies**
- a model-based methodology and solutions for addressing safety and security within an integrated process, supported by an effective tool chain
- validation in use cases in multiple industrial domains (e.g. aerospace, energy management, automotive, ...)
  - also other CSR work here on
    + Impact of Cyber Attack in Critical Infrastructures
    + Safety-informed safety cases

Background: D3S project (2015-18)

Diversity and Defence in Depth for Security

- Security is a matter of diverse layers
- to which one can add intentional diversity

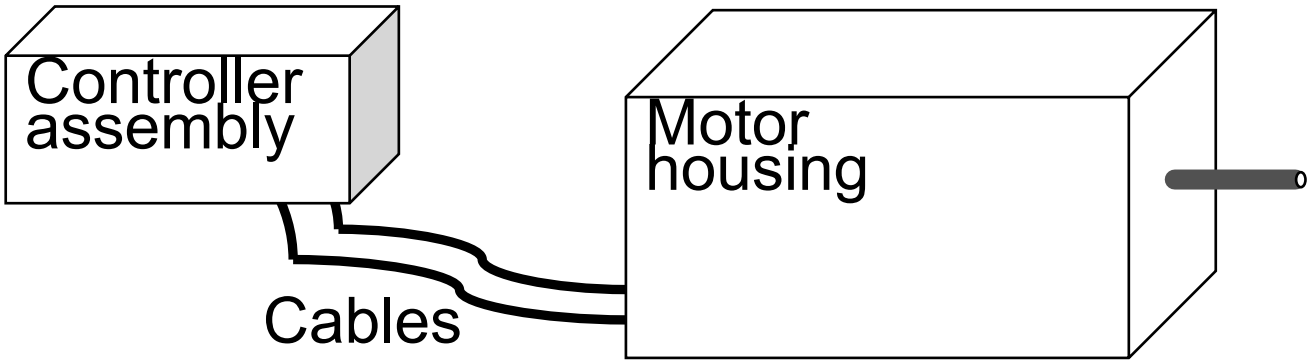


- ... to no end !?
- how do we decide how much is enough
  - or whether *this* architecture is better than *that* architecture?
  - in view of multiple requirements
- D3S directions
  - probabilistic modelling for insight
  - data collection to estimate joint effectiveness
  - studying how (how well) these measures support *prediction*

The example: industrial drive control

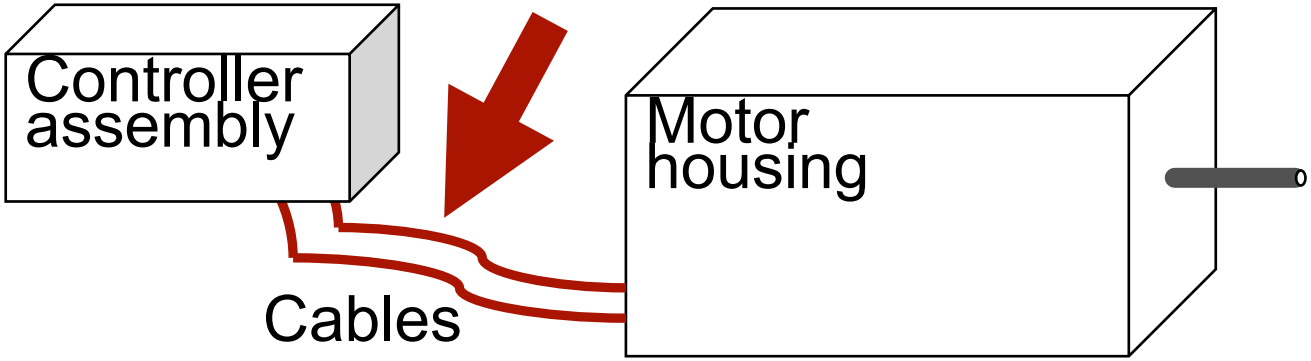
- inspired by aSeSaMo project "use case"
  http://sesamo-project.eu/content/industrial-drive

- electric motor under computer control
  - generic control unit; motor could be for any load...



The example: industrial drive control

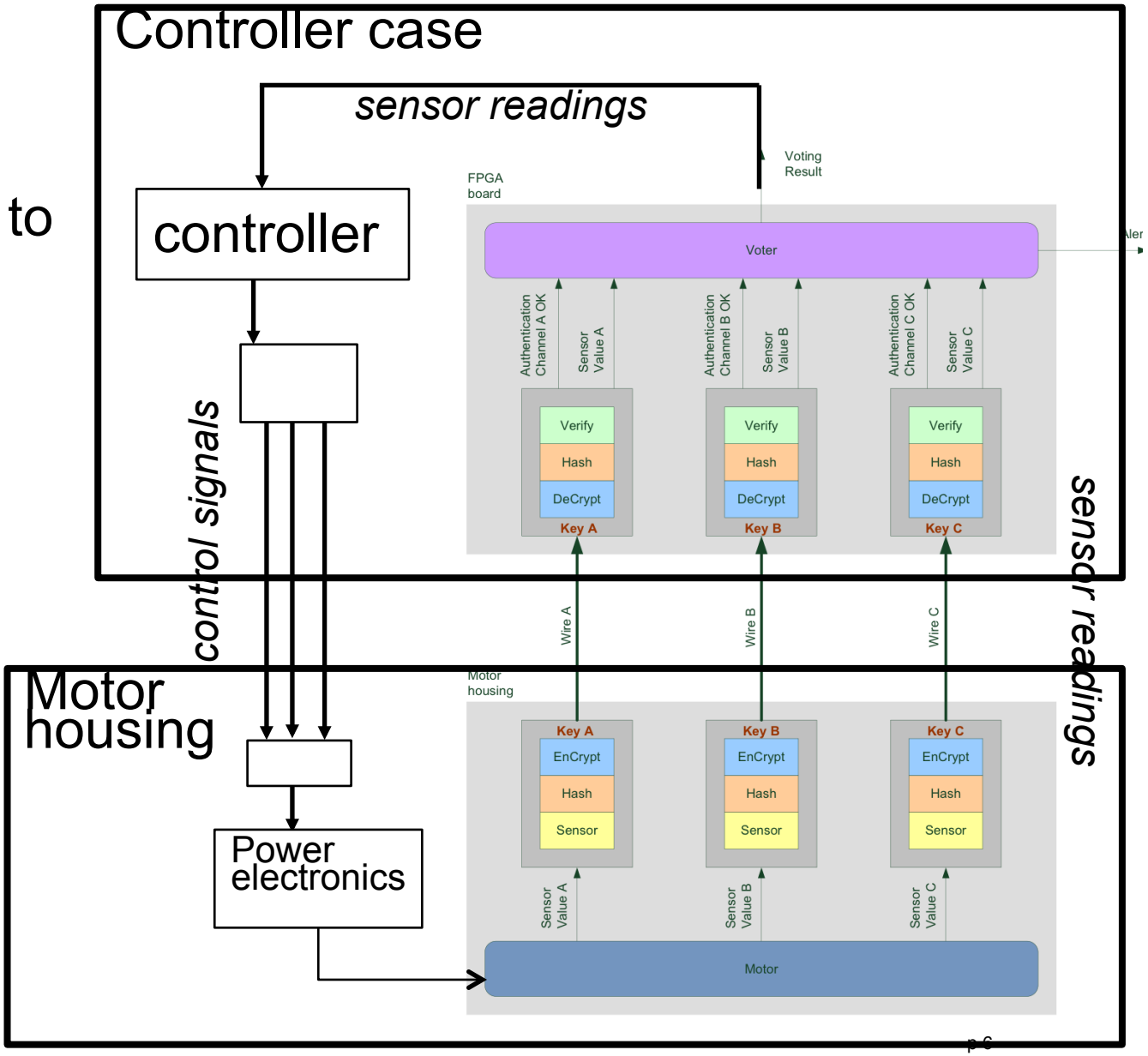
- electric motor under computer control
  - generic control unit; motor could be for any load...



- attackers may want to perturb motor operation
  - through access to *communication*
- for both safety and security, communications are *replicated* and *encrypted* – **diversely***? how, and with what gain?*

Our example... Industrial drive control

- to analyse: communication between the two parts
- adversary trying to *intercept* / *inject* messages
- communication *triplicated* & *encrypted*
- encryption for both confidentiality & authentication (here we study simplest design: "authentic" if it decrypts to a legal message)



The questions, the uncertainties

- communication is **replicated** for reliability, safety
  - against accidental faults
- and **encrypted** for integrity and confidentiality:
- prevent attacker from
  - reading real signal
  - crafting and inserting forged ones
- good encryption on each channel guarantees all this
- ....or maybe not!

What about crypto "**implementation errors**" in hardware, software, operation, management?

use ***diversity***!

But..

- *how much* will it help? (is it worth doing?)
- how will helping *integrity* harm *confidentiality*?

Security concerns studied

cryptography "implementation" flaws:

- flaws that make *cryptanalysis* affordable
  with decent chance of success
  – search of reduced key space
    + over days or years
  – how helpful is it to use *diverse keys ?*
- shortcut to penetration through *supply-chain* flaw
  – intentional chip design flaw, insider selling keys, ..
  – how helpful is it to diversify vendors, designs, algorithms..?

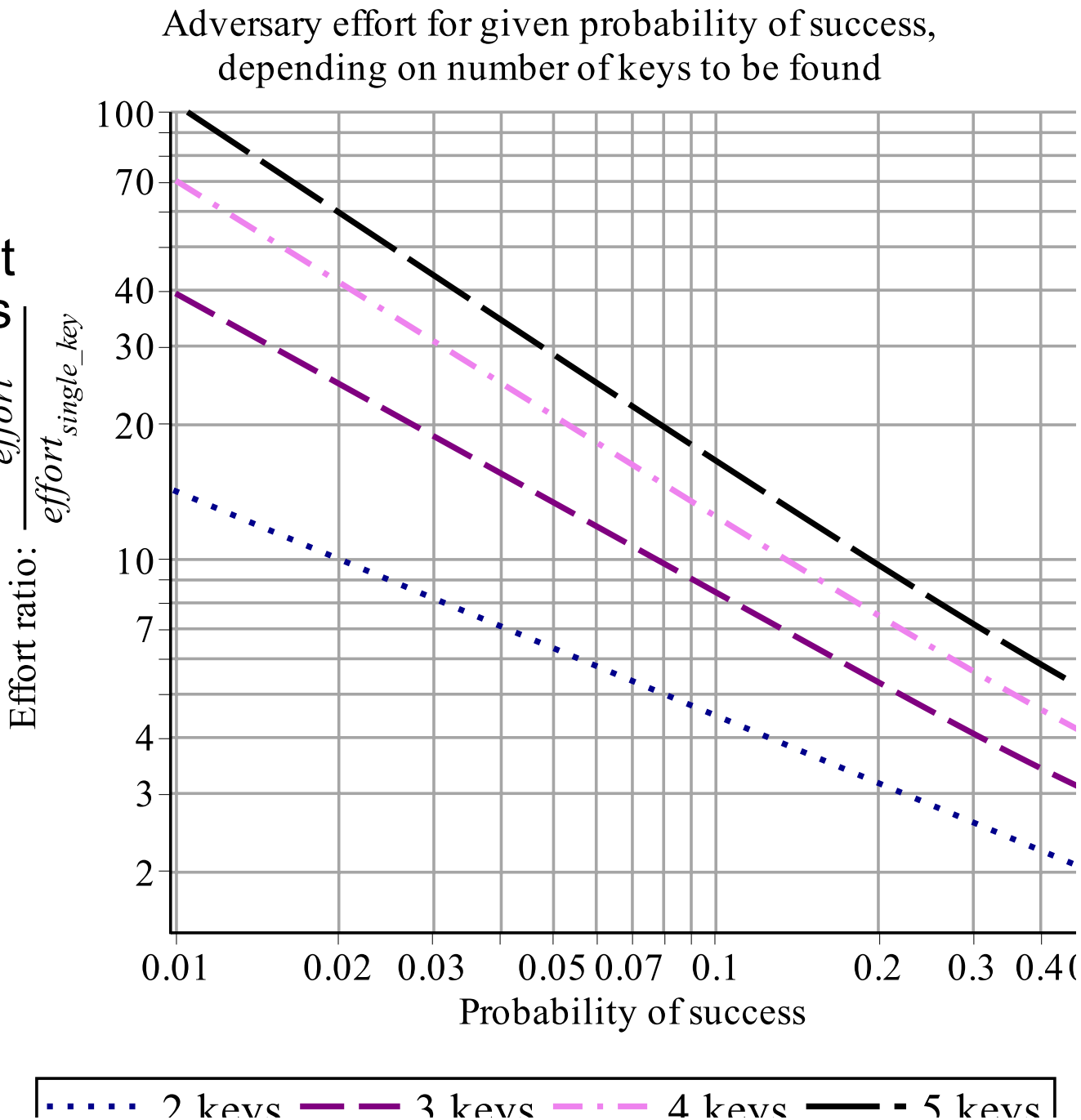
Adversary may want to

- highjack majority of control channels
  – to cause accident/loss
- spy on communication
  – to engineer better attacks
  – or to steal secrets

Example answers

"Affordable cryptanalysis" scenario

- *substantial* protection against *non*-ruinous flaws
- relevant for high-value targets
- if adversary is willing to attack for 5% chances of success.. diverse keys will cost 7 times the effort for same chances
- should he even try?



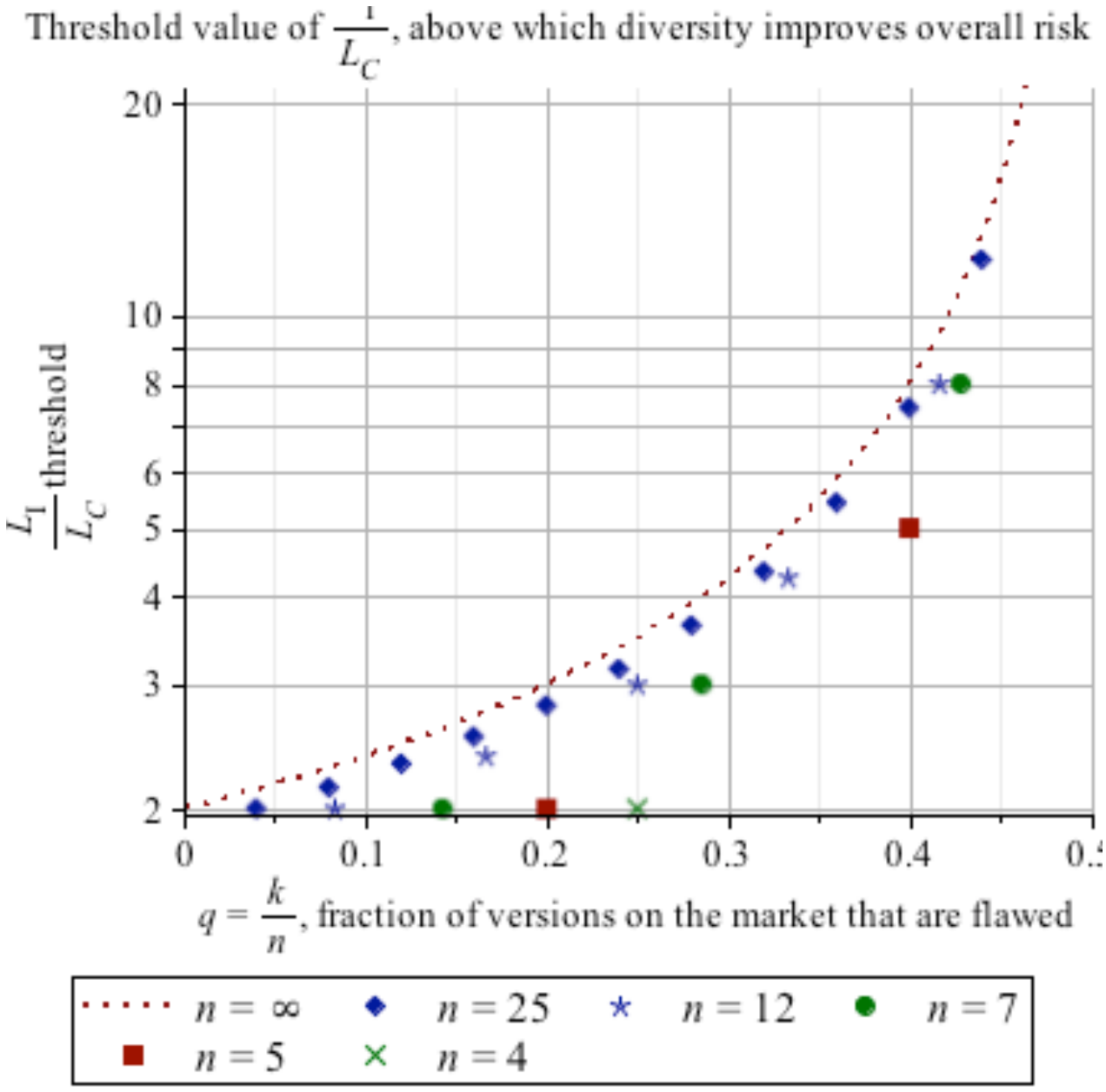
"Supply chain" flaws: when should we use diversity?

n implementations available,

for *k*, adversaries know holes

diversity buys *integrity at the cost of confidentiality*

use diversity if the *expected loss* from having an "integrity flaw" (2 flawed channels) exceeds this many times the expected loss from having a "confidentiality flaw" (1 flawed channel)



Some observations / conclusions

- useful insight from simple modelling
- simple, hence covering general classes of scenarios
  - attacks on safe shutdown ability of safety system
  - breaking into two user accounts
- results in paper at EDCC2016
- Extensions under way:
  - modelling more complex, realistic attack modes (the easy part)
  - dependencies between successes on two channels
    - causal and epistemic
  - guessing plausible model parameters from evidence