Economic and Consumer Chain Analysis of Secure Hardware Adoption

Prof. Siraj Ahmed Shaikh

Professor in Systems Security

School of Maths and Computer Science
Swansea University
Swansea, Wales UK
Email: s.a.shaikh@swansea.ac.uk

Co-Founder and Chief Scientist
CyberOwl
London, United Kingdom
Email: siraj.shaikh@cyberowl.io

16th September 2022

Acknowledgment

Academic Collaborators

- Coventry and Aston Universities (UK), and TU Delft (NL)

Industrial Collaborators

- TechWorks/AESIN/IoTSF (UK) and SEMI Europe (DE)

Funding

- Funded by Discribe, the Digital Security by Design Social Science Hub+ (UKRI ESRC grant no. ES/V003666/1)

Publication

- Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac009, https://doi.org/10.1093/cybsec/tyac009

Securing Hardware: cybersecurity and sovereignty

Prifysgol Abertawe
Swansea University

theguardian
Winner of the Pulitzer prize

all opinion culture economy lifestyle fashion environment tech money travel ≡ browse all sections

Scientist banned from revealing codes used to start luxury cars

High court imposes injunction on Flavio Garcia, who has cra
of cars including Porsches and Bentleys

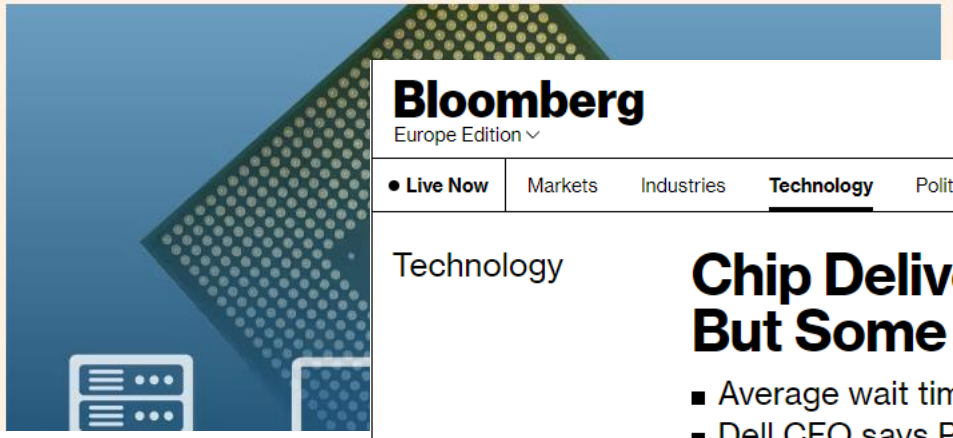
FINANCIAL TIMES

COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HTSI

Cyber Security + Add to myFT

Meltdown and Spectre: what we know so far

Chip design vulnerability could have serious implications for computer users



Bloomberg
Europe Edition

• Live Now | Markets | Industries | **Technology** | Politics | Wealth | Pu

Technology

Chip Delivery Tim
But Some Shorta

- Average wait times for semic
- Dell CFO says PC supply cha

Forbes

INNOVATION

The Connected Car Is The Next Attack Vector

Nic Surpatanu Brand Contributor
Tanium BRANDVOICE | Paid Program

Sep 7, 2022, 09:21am EDT

Automotive hacks represent a looming threat for corporate fleets and consumer privacy.

These days, cars are rolling computers. Modern vehicles contain dozen of computer chips that control everything from cabin temperature to braking systems. The software running on these chips features more code—some 100 million lines—than the U.S. Air Force's F-35 Joint Strike Fighter. But with so many hardware and software components involved in the complex automotive supply chain, connected vehicles c be difficult to secure.

Securing Hardware: securing the supply chains?

Complex Spread

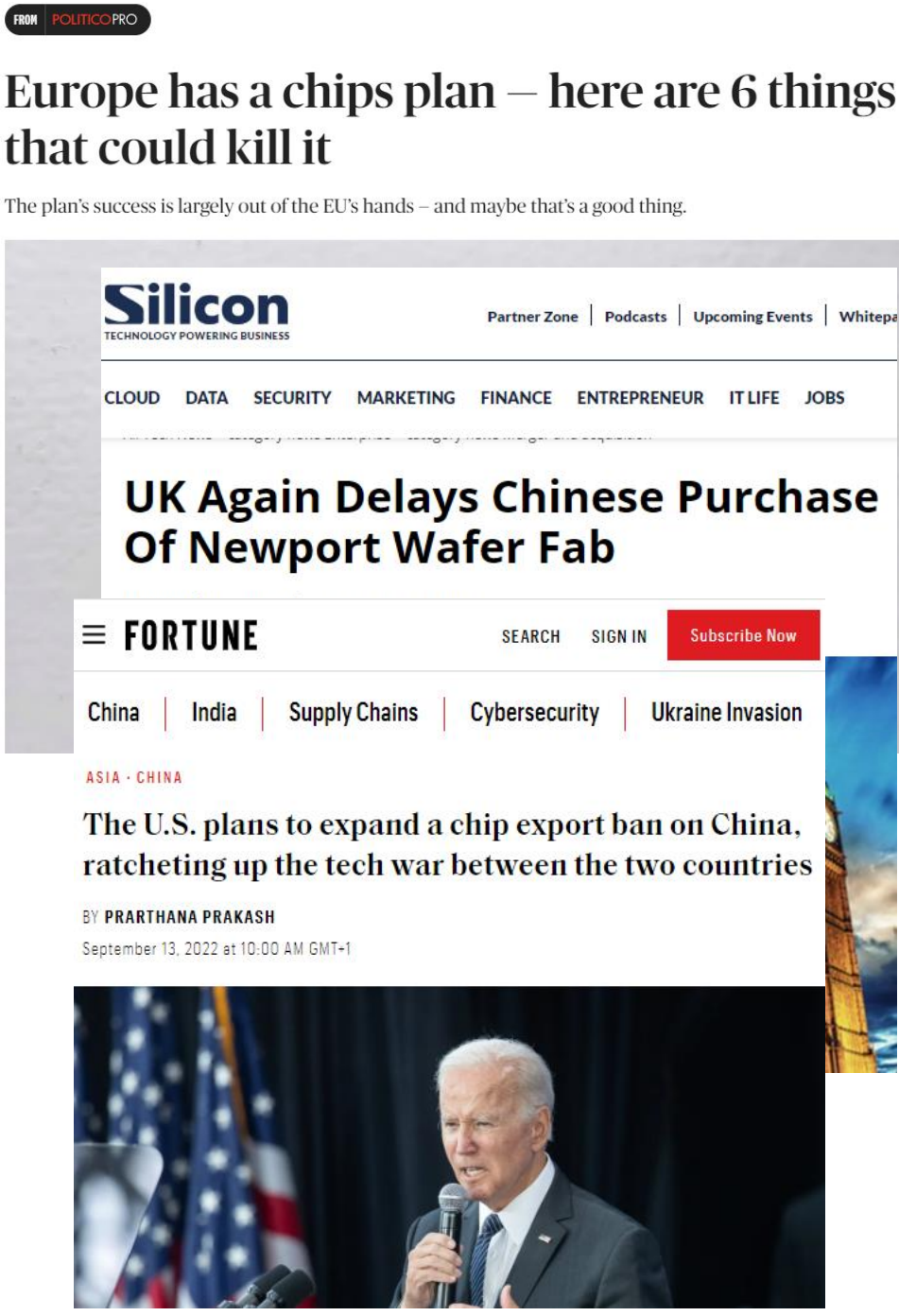
- Tiered supplier hierarchies can make it difficult to have visibility and traceability through the supply chain
- Offshoring and remote location of design, development and production is a challenge
- Geographic spread makes supply chain players vulnerable to
  - Geopolitics
  - Weather and climate change
  - Cultural perspectives, such as attitudes to IP and communication

Economic Trade-offs

- Cost pressures may lead to compromise on quality and ethics
- Just in time production possibly allowing for less of a buffer to recover from failures in the chain
- Monopolistic tendencies causing single point of failure

Assurance Challenge

- SW/HW is inherently difficult to assess for non-functional attributes



So the question is…

Research questions

1) What are the benefits of secure hardware adoption, and how are such benefits measured and perceived?

2) What are the costs of security failures arising out of lack of such practices, where losses are identifiable?

3) What are the value gains from software add-ons and developer platforms adding to enhanced security of hardware?

Key insights on

- Barriers to adoption include lack of a compelling economic case and awareness, uncertainty in the market, and complexity introduced; security risk reduction and compliance are key drivers for adoption.
- Choice of solution driven by clarity of security benefits, cost of failure, performance and scalability.
- Organisational factors include position of internal stakeholders, chip provision and indirect incentives.

Our study

Scope of secure hardware

- concepts and technologies that fall under physical, structural and behavioural domains of hardware abstraction layers. This covers enhanced hardware ISAs, TPMs, HSMs, TEEs, PUFs, RNGs, SoC analytics, physical quantum computers and tamper-resistance and proofing.

Participants

- 23 semi-structured (anonymised) interviews with senior decision-makers from companies spanning a range of sectors, sizes and supply-chain roles in the automotive industry (along with supporting industries including Tier-1/2s, electronics, semiconductors, system integrators, and firmware and hardware security evaluation players, from Europe, UK and US.

Ethics

- Menlo report guidance on disclosure on industry practices

Thematic focus

- **business decisions**; **adoption decisions; adoption criteria**; **integration activities; and technologies**.

Our findings: perceived drivers

Market forces

- Increasing demand, enabled partly by big players such as Samsung and the defence sector
- Early adopters in the deep tech acknowledging *"going above and beyond what the rest of the industry is doing"*

Standardisation

- Compliance, standards and regulation were raised by every participant in one way or another.
- Some also emphasising that compliance was the only significant driver:
- …"people don't tend to do things [in cybersecurity] unless they are actually required to, either by a supply chain requirement or via governmental certification"
- …"if we go back to HSMs, the answer is compliance, regulatory obligation. And you can almost trace the sales from when various regulatory things were introduced, and that led to adoption of hardware"

- Is compliance security? Or is security just compliance?
- …"the business says, 'as long as I'm compliant with regulations, I should be safe, or I should be secure".

Our findings: perceived drivers (2)

Standards as collaborative?

- Compliance and regulatory needs can motivate change, but also define a clear minimum standard to be met. Compliance was seen as impactful across industries and sectors, essentially having downstream impact.
- This is also framed as collaborative where *"the industry getting together, governments getting together and saying here are a set of standards, here are a set of kite marks or, you know, kind of quality marks to put on things"*

Automotive Standards

- UNECE Regulation 155, ISO 21434 and GDPR were cited as most important. UNECE Regulation 155 was noted as being a requirement to sell cars in some markets, and also cited as "really driving people" was ISO 21434.
- The role of GDPR was also cited as a likely push for automotive secure hardware since OEM revenue models are shifting towards service provision, implying processing more client data, which needs to be kept private.
- *"At the moment the current version of the UNECE regulations state that it's the OEMs that have to comply with that. [...] the OEMs are kind of pushing those requirements down into the supply chain"*

Our findings: perceived drivers (3)

…and yet other factors?

- *"Compliance is [...] not the only driver, and I wouldn't say if there wasn't compliance, they wouldn't bother. People do care about their reputation, they do care about their IP. [...] if you're dealing with a medical robot manufacturer, it's critical that they carry out the right operation on the right person [and] that any data associated around the records of that person is only accessed by the right consultant, or nurse or whoever. [...] Revenue protection is important as well. So there's multiple factors".*

Specific examples

- Emissions legislation was noted to be forcing the OEMs to ensure the secure preservation of in-vehicle data and the non-tampering of systems by third-party companies.
- Preserving the user experience of automotive infotainment interfaces through the prevention of aftermarket tampering and updates by third parties was also cited.

Our findings: perceived barriers

At what cost? For what return?

- Cost, complexity and lack of expertise were frequently cited by participants as disadvantages of secure hardware and key barriers to its adoption.
- *"horrible, massive, monumental task. [...] Almost 99.9% of the customers when it comes to security? The first question they ask is how complicated it is to get into".*
- Costs were cited as the hardware itself, changes to the design process and switching to the new solution, time to deliver and additional costs to the system through secure hardware adoption.
- The speed at which an application or product with secure hardware in it could be developed and deployed was seen by one participant as being especially problematical for small businesses, since *"they would probably argue that security hardware will be out of date in a year [when] a software solution they could upgrade over the internet, for example".*

Our findings: perceived barriers (2)

Prifysgol Abertawe
Swansea University

Challenge of integration

- Integration has been raised as a substantial challenge for adoption
- For one participant, the challenge was learning new APIs, which whilst *"not necessarily difficult [...] [was] another thing you got to learn. [...] It's another API, you got to learn and figure out how we're going to implement"*
- The lack of understanding and visibility of APIs is seen as restricting the optimal use of secure hardware features, as reasons why *"a lot of ARM chipsets have got trusted enclave, trusted execution process in the chipset that aren't actually particularly well used"*

Complexity of integration

- *Knowledge about the integration of secure hardware modules or functionality was seen as important. For example, "just because one module is plausibly secure, doesn't mean I can use it alongside another one in a secure way. That's a research issue [...], that virtually no one I think, in the outside world understands"*

Our findings: perceived barriers (3)

Prifysgol Abertawe
Swansea University

Communicating on return

- Measuring benefits from secure hardware, or indeed enhanced computer security in general, seemed challenging, or typically not attempted.
- *"The challenge is to be able to communicate the value proposition, not the technological advantage, [to] people at board level. [...] We try to quantify it from a cost perspective, engineering time, perspective, complexity perspective"*
- *"there is no methodology, scientific methodology that can quantify the cost of a breach, before the breach happens. Even when the breach happens, even then there isn't a reliable scientific methodology that can quantify this.[...] We don't have historic data of what happened when a breach happened on an IoT device, on a pipe for oil, for example"*

Skills gap

- A skills gap was discussed by some of the participants, and cited as a cause not only of lack of adoption of secure hardware, but also of failure to leverage the full potential of secure hardware. For example: *"Today there is [...] a lack of awareness of any of those kinds of systems. And so as a result, I just don't see them as being leveraged probably as much as they should be"*

Recommendations

Find opportunities for unified standards and common needs

- Compliance and standards were seen by our participants as a main driver for adoption of secure hardware, and development of standards ought to persist given that they are not yet mature. The activity of developing standards may also benefit from finding commonalities across emerging hardware standards, where secure hardware may find its way into various contexts (healthcare, IoT and so on).

Support the decision-maker in making adoption decisions

- Regarding the determinability of costs and benefits, it is not sufficient to focus on a small set of costs, as the drawbacks and benefits go beyond hardware.

Articulate switching costs and leverage existing skills

- It would aid the adoption of new hardware to find overlaps between existing and new skills in the development of solutions on top of the hardware, as developers also need to have sufficient support to leverage the features of new hardware.

Prifysgol Abertawe
Swansea University

Thank You