CE879 - Information Security Mng. & Eng.

Lecture 8: Supply Chain Security

Seyedeh Atefeh Musavi / Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology
Spring 1404

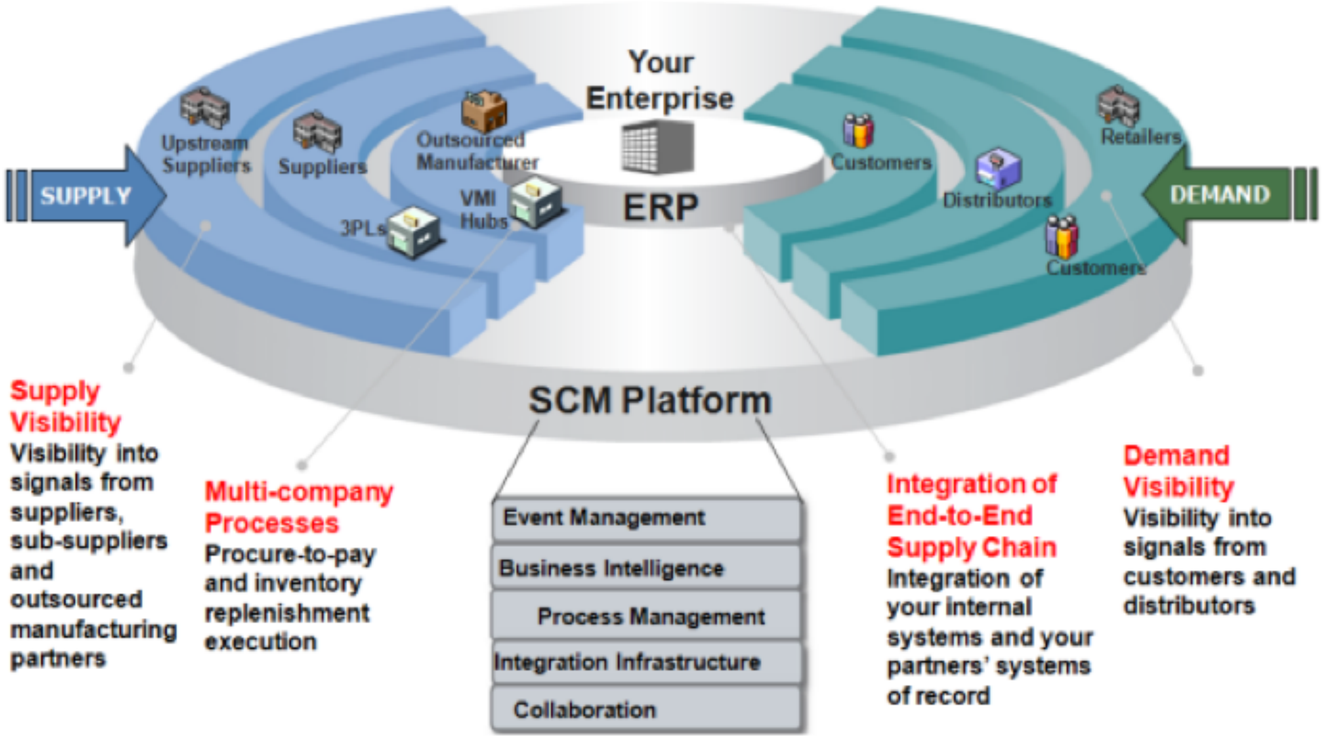
S4Lab

Acknowledgments: Some of the slides are fully or partially obtained from other sources. A reference is noted on the bottom of each slide to acknowledge the full slide or partial slide content.

What is supply chain ?

S4Lab

- A supply chain is traditionally understood as a system of organizations, people, technology, activities, information and resources involved in moving a product or service from supplier (producer) to customer.
- Only for industry sectors with physical good?
  - No, is also a concern for non-industrial organizations.



[Image:http://blog.wallix.com/supply-chain-security]

[Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses, Demidov O. & Persi Paoli G., 2019]

Why digitize the supply chain?

S4Lab

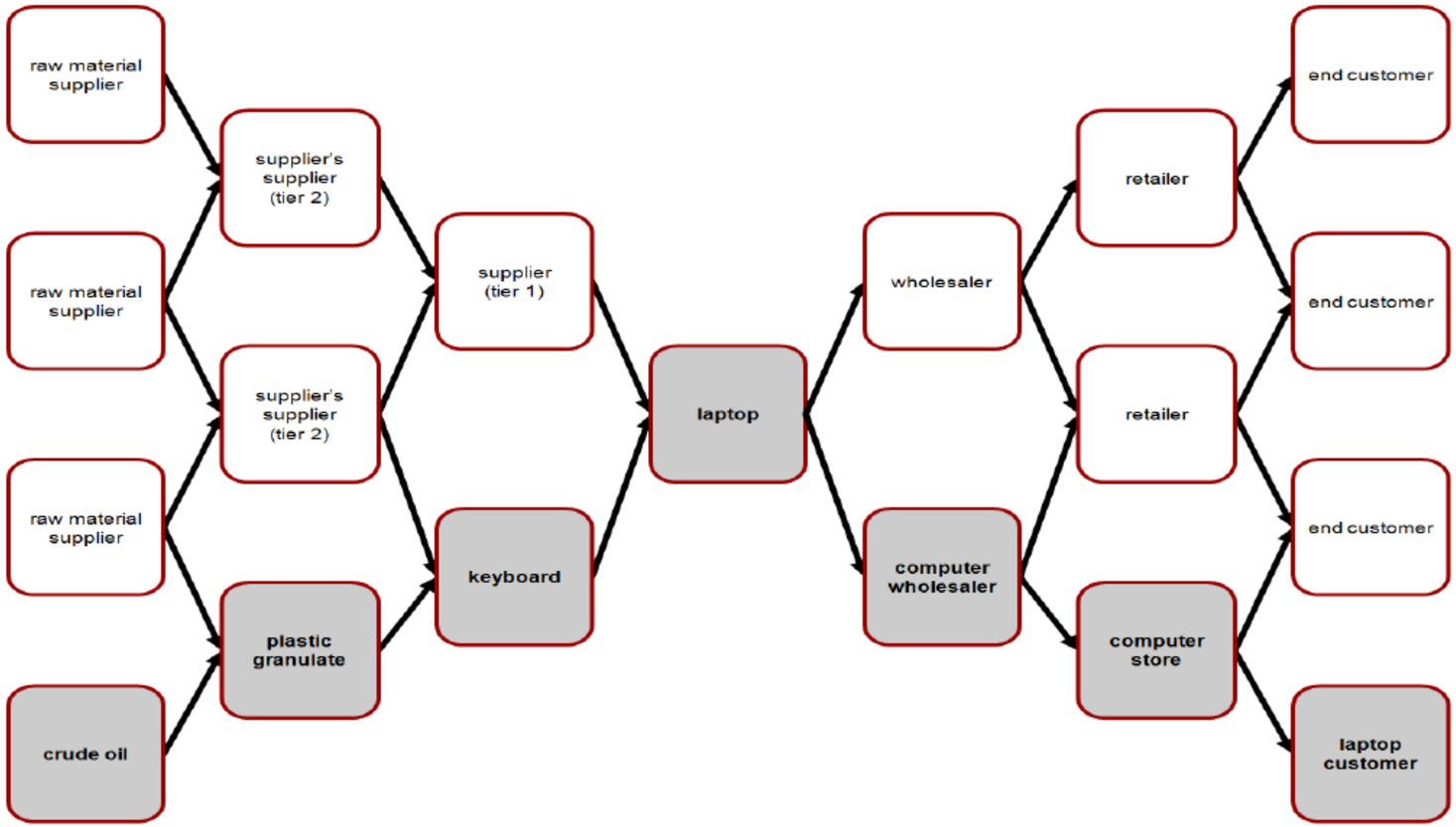
- Today’s supply chains are complex.
- Not only for critical industries:
  - KFC!
- So they hope the existing problems can be mitigated by using digital technologies.
- New technologies may extend the attack surface, too.

[Image: https://www.cips.org/]

Visibility complexity

S4Lab

- One major concern among security experts and government regulators has been the inability to effectively map and trace the complete supply chain beyond tier 1 vendors.
- This has been considered a principal challenge to SCRM in both private and public sectors.
- Once a tainted or tampered product or component enters the upstream supply chain, it can compromise the supply chains of customer organizations in any tier.

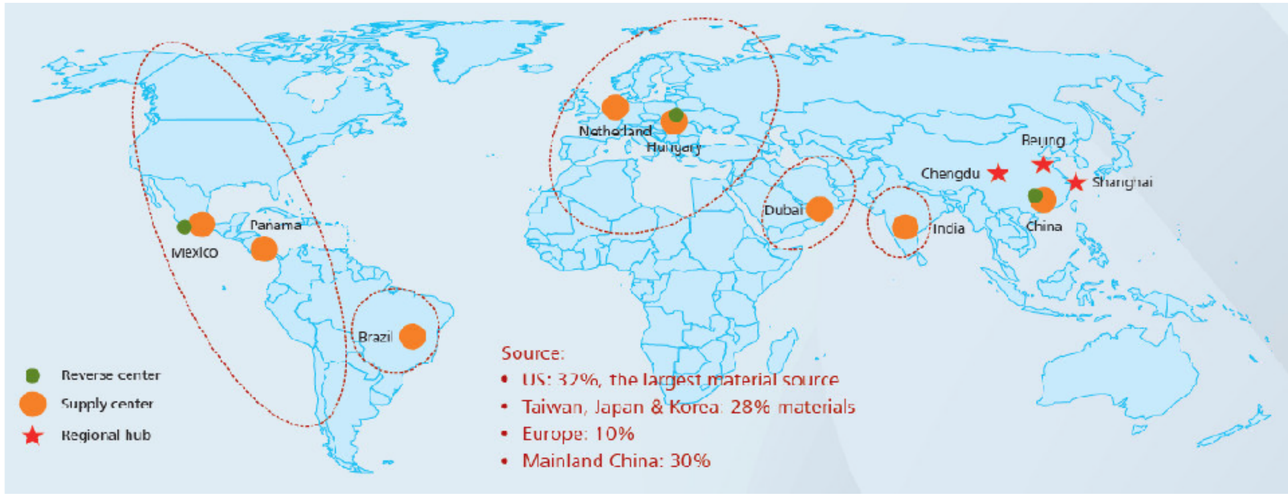


[Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses, Demidov O. & Persi Paoli G., 2019]

Cross border complexity

S4Lab

- In many cases, these third-party suppliers of software development services are be based in a different jurisdiction or a different region.
- India and, more recently, South- East Asian and Latin American countries have become known as global software outsourcing factories for companies from the United States and other North-East Eurasian and Western European countries.
- The reliance on foreign suppliers has, in some cases, sparked security concerns ranging from cybersecurity to national security.



[Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses, Demidov O. & Persi Paoli G., 2019]

Other complexities can be managed by digitization?

S4Lab

- Prevent/detect counterfeiting,
  - Every thing can be tracked in transit.
- Knowing about customer demand/behavior is having all the cards.
  - In addition, informing about the product lifecycle is important.
  - Improve demand planning.
  - The nearer to the customer, the better.
- Identifying delays/bottlenecks.
- Checking desired conditions in delivery process (temperature/humidity and shock levels).

Other complexities can be managed by digitization? (con't)

S4Lab

- No need to trust other nodes in supply chain, but having the ability to monitor/verify.
- The ability to define policies, monitor the flow in an end-to-end manner.
- So why not use:
  - Sensors on the products
  - Fleet tracking hardware
  - Machine learning
  - Block-chain
  - …

An example of digitization: RF technology

S4Lab

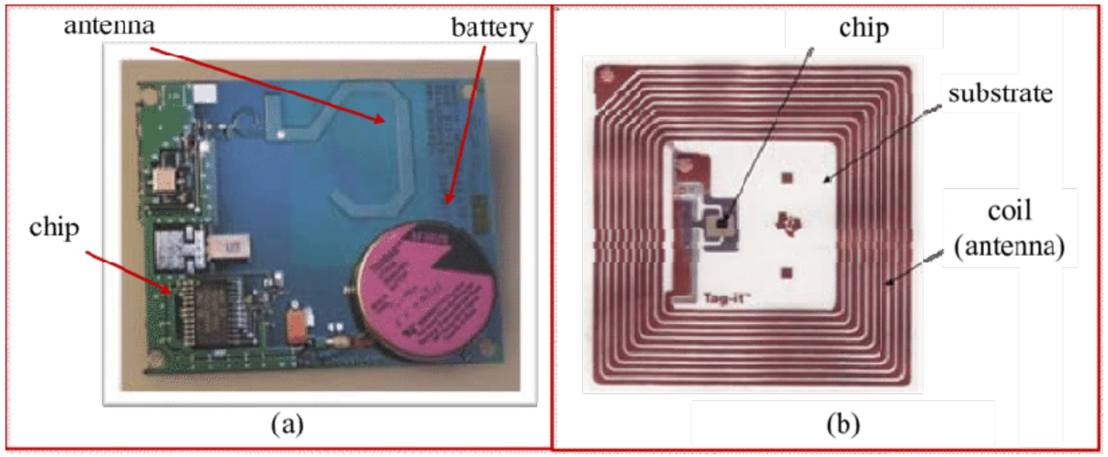
- Advantageous for:
  - Augmented Enterprise Resource Planning (ERP).
  - Automated inventory tracking.
- Not only the goods, but also employee monitoring to reduce idle times.
- The existing delay for the quality control can be decreased.
  - Process can be checked in real-time by implanting wearable sensors in product lines.
  - Increasing/checking the speed and efficiency in workflows

[Image: http://rfidinventorysystem.blogspot.com/]

RF-IDs

S4Lab

- Why RFIDs? Why not barcodes?
- What is the power source of an RFID?
- Does RFID require a direct line of sight?
- How fast are the RFID readers?
- How to disable a tag?
- What is the operable range for a RFID?



[Image: https://www.researchgate.net/]

Another example of digitization: Block-Chain Technology —> Blockverify

S4Lab

- General access to manufacturers' details and distribution history.
  - Since every record added to the blockchain is unchangeable and timestamped, it is easy to track products, confirm their origins, and diminish risks to sell counterfeit goods in the end.
- NFC tags for package verification and tracking.
  - Every product at all stages of the supply chain keeps a label with a unique NFC tag.
  - Record the history of transfers, ownership, locations, and other significant distribution data.
  - Intermediary stations and distribution centers staff open mobile apps, scan the tags, and verify goods authenticity.
- Public and private blockchain options for supply chain data storage.
  - Both public and private storage options with limited access to specific groups and third-party providers are enabled.

BLOCKVERIFY

[PR: PixelPlex developed an anti-counterfeiting solution called Blockverify, Securing Industry, 2020]

Digitized communication through the Supply Chain

S4Lab

- In past all communications were manual.
- Regardless of paper-based or electronic, e.g. by an email.
- EDI (Electronic Data Interchange) is a choice to automate B2B comm.
  - Often include exchange format, as well as communication protocol.
- Suppose you sell your product to a big factory/web shop. It would have a special EDI system which determine the exchange format of different kinds of documents and you should comply with.

[Image:https://www.infinite-b2b.com/ir/solutions/edi]

EDI management models

S4Lab

- Common standard EDI formats? UN/EDIFACT, TRADACOMS, ANSI x12
- EDI system choices:
  - Direct Connect
  - On-premises B2B software: B2B gateway, e.g. BizManager.
  - Value-Added Network (VAN): Single unified integration cloud network, e.g. “document mailbox” service which all parties connect to.
  - Managed Services: Software as a Service (SaaS) solutions receives your business documents directly from your ERP system.
- So as a security manager did you think about security at the company’s EDI system?

[https://blogs.opentext.com/electronic-data-interchange-edi/]

API's – An Emerging Player in Supply Chain

S4Lab

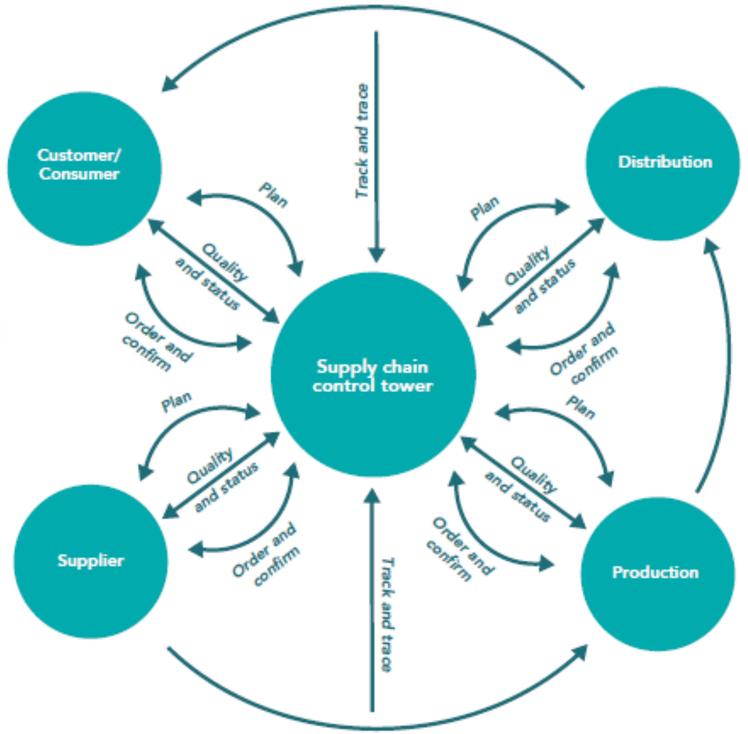
- Today, an estimated 90% of global supply chain relies on legacy EDI (Electronic Data Interchange) systems.
- APIs are poised to completely replace EDIs.
- The biggest value-add APIs provide is the ability for business users with non-technical backgrounds to access data and assets.
- Users don't need to understand how back-end systems function, or even how they communicate with the interface. Simply self-serve according to the data needs.
- Implementing an API is less costly and complex than implementing an EDI, but currently there is some industrial Inertia.
- What are the API threats?
  - Have you seen the OWASP API Security Top 10?

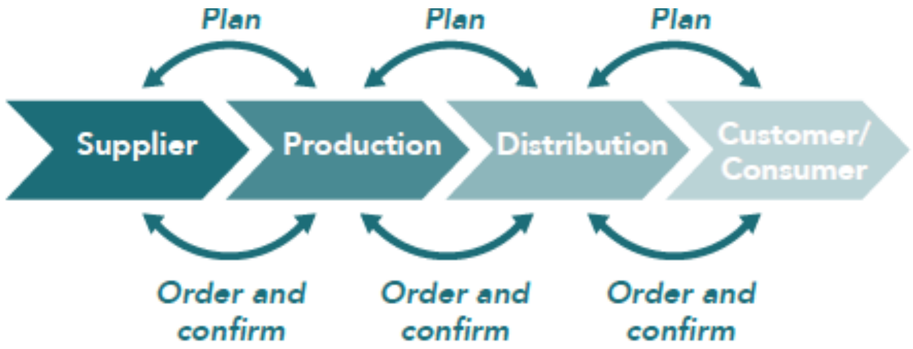
[https://connxus.com/tech-forward-apis-emerging-player-supply-chain/]

Supply Chain 4.0

S4Lab

- Digital technologies are transforming supply chain management:
  - From a linear model
    - Delays in the processing of information
    - One actor doesn't know every thing
    - Requirements change when feedback arrives from the end of the chain
  - To a more integrated model
    - Referred to as Supply Chain 4.0.
- How such an integrated model is possible?





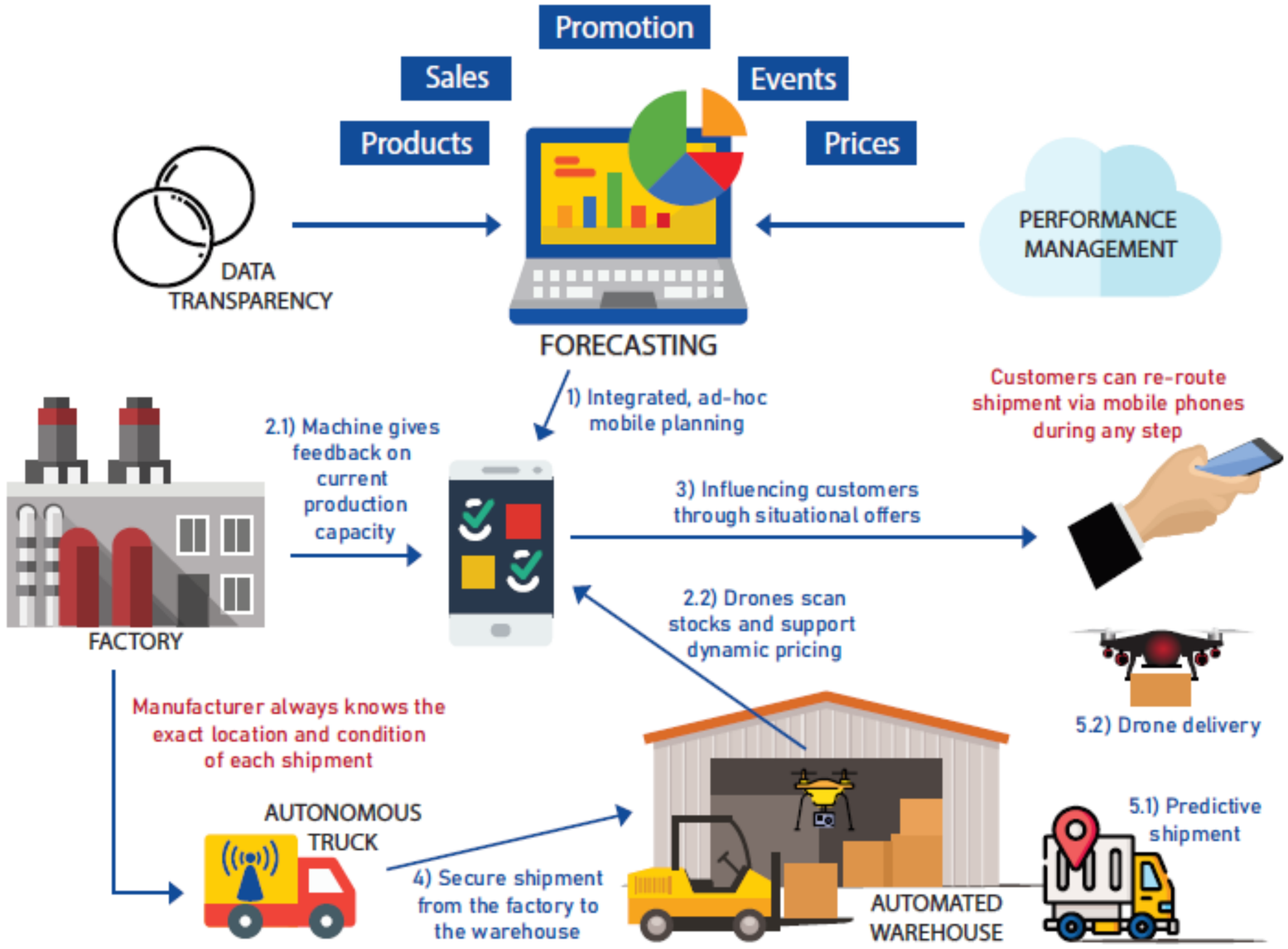
[Understanding Supply Chain 4.0 and its potential impact on global value chains, Ferrantino, M. J., et al., Global Value Chain Development Report, 2019]

Supply chain control towers

S4Lab

- In supply chain 4 we use industry 4 technologies.
  - E.g. IoT
  - Availability of fine grained data.
- Supply chain control towers are designed to provide deeper end-to-end (E2E) visibility across the supply chain.
- They often include a central dashboard of data with views into key business metrics and events.
- Control towers are a constantly evolving concept and technology.

[What is a supply chain control tower?, Katie Devlin, IBM, 2021]



[A survey on supply chain security: Application areas, security threats, and solution architectures, Hassija, V., et al., IEEE IoT Journal, 2020]

Global supply chain

S4Lab

- The term global supply chain management adds the dimension of international business into the mix.
- This raises issues of multinational operations, cross-cultural relationships, and a business space open to more risk (be it political or economic).
- Firms often find it necessary to expand their supply chain into other countries.
- This may be due to savings in labor cost, access to critical raw materials, or opening up new markets for goods and services.

[Global supply chain security and management: Appraising programs, preventing crimes, Prokop, D., Butterworth-Heinemann, 2017]

Fragmentary supply-chain visibility

S4Lab

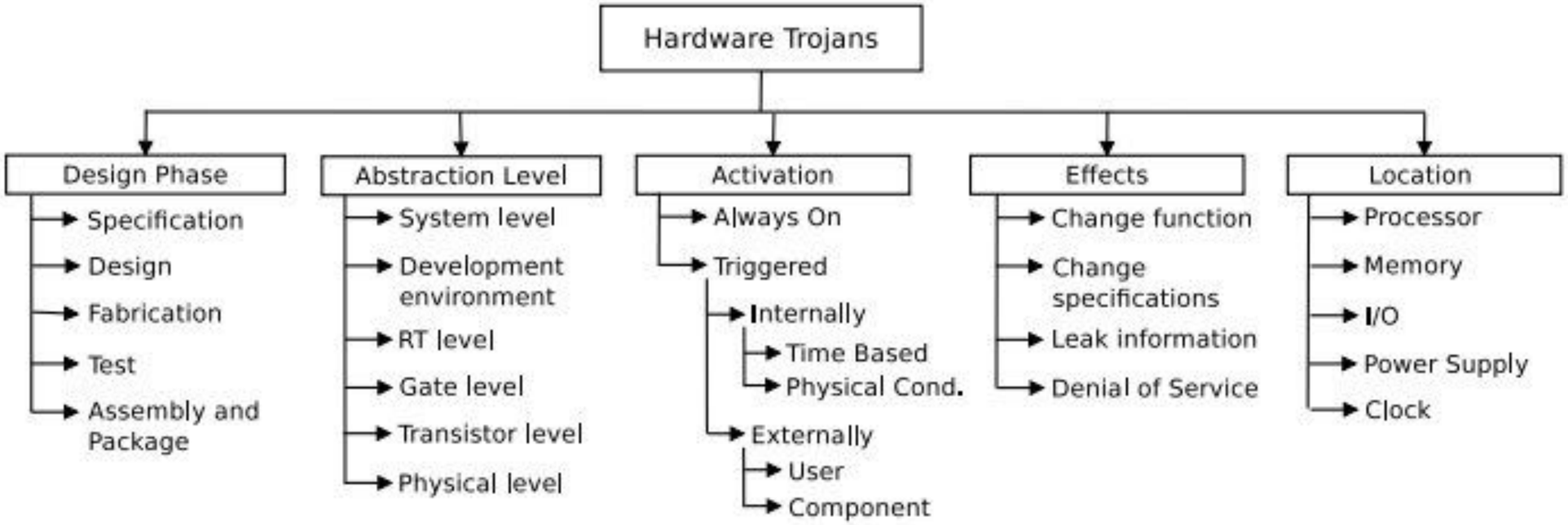
- Reader failure:
  - Due to factors such as tag orientation, tag placement, and nearby materials (e.g.,metal, water).
  - Large populations of tags are often scanned in a short time (like a pallet of tagged goods passing through an RFID-enabled gate), causing read failures.
- Some commercial partners cannot share supply-chain information or do not do so for fear of disclosing sensitive business intelligence.
  - Entire segments of a supply chain may be opaque to participating entities.
- Thus, real-world supply chains often have large “blind zones,” in which RFID tags scans do not happen or are not reported.
  - Very much like bgp blind spots.

[Tailing RFID Tags for Clone Detection, Zanetti, D., et al., NDSS, 2013]

ICT supply chain

S4Lab

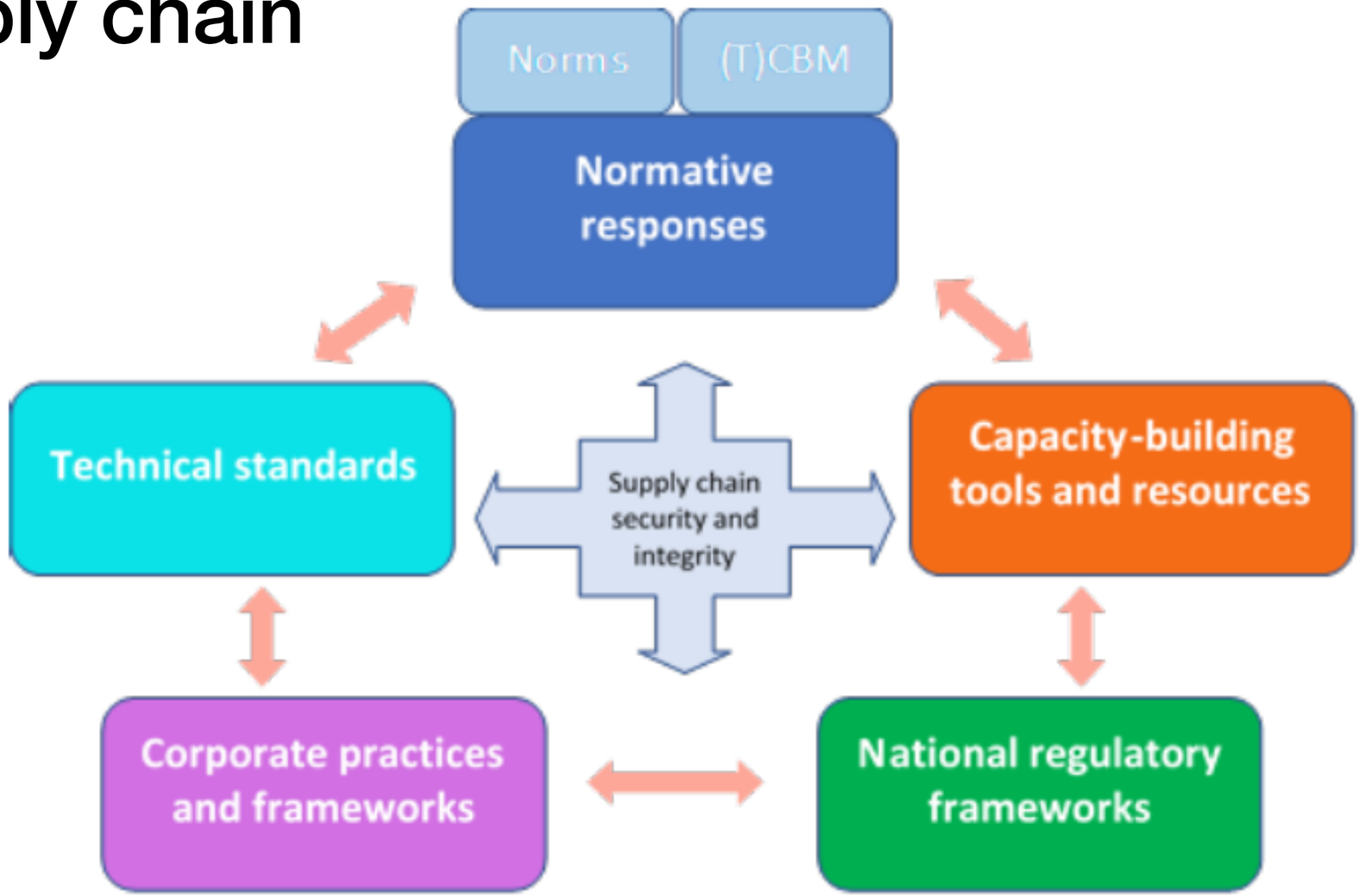
- A complex supply chain with so many entities involved around the world.
- Only the hardware supply chain consists of tens of entities which can increase the risk of an embed a Trojan inside the chip.



[The Most Significant Cyberattack in History Prompts Questions About Supply Chain Security, Jake Hertz, 2020]

Existing regulations/standards for security of supply chain

S4Lab



[Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses, Demidov O. & Persi Paoli G., 2019]

Categorization of normative initiatives involving ICT-driven risks to supply chain

S4Lab

Initiatives or criteria	Stakeholders		Positive vs negative		Subject scope			
	IGO	Multi	Positive	Negative	Backdoors/ HHF	Tampering	Supply chain S&I	SC S&I + backdoors / HHF
GGE	✓		✓	✓				✓
G7	✓		✓	✓				✓
SCO	✓		✓	✓			✓	
Digital Geneva Convention		✓		✓	✓			
Cybersecurity Tech Accord		✓		✓		✓		
Cybersecurity Charter of Trust		✓	✓				✓	
GCSC		✓		✓		✓		
Paris Call for Trust and Security in Cyberspace		✓	✓			✓		

[Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses, Demidov O. & Persi Paoli G., 2019]

Supply chain security certificates

S4Lab

- TAPA (Transported Asset Protection Association) freight security certification.
- ISO 28000 certification - supply chain security management systems.
- CTPAT (Customs-Trade Partnership Against Terrorism) audit.

Software Supply Chain Security

What's the software supply chain

S4Lab

- Do you know any one writing his/her own … code?
  - OS
  - Cryptography
  - Http stack
  - Database
- As of August 2019, there are more than 100M repositories on Github.
- Programmer prefer not to re-invent the wheel, Why not?
- Most of the discussion is in the context of open source codes.
  - But also valid when you use closed source code.

[LibDX: A Cross-Platform and Accurate System to Detect Third-Party Libraries in Binary Code, Tang, W., et al., IEEE SANER, 2020.]

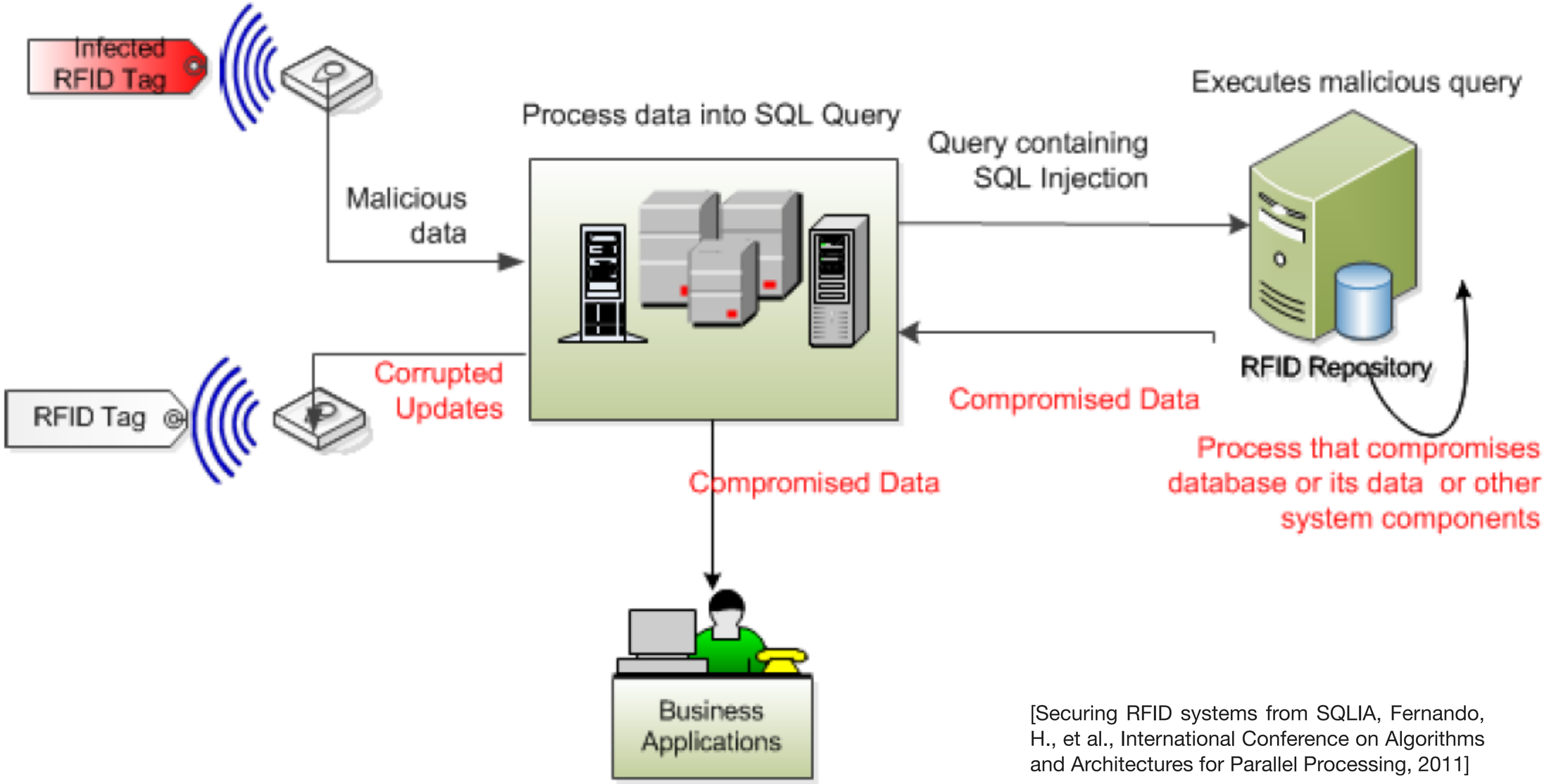
Importance of software security

S4Lab

- Information security concerns are valid in new supply chains since there are more usage of HW/SW technologies compared to the traditional supply chains.
- Let’s consider RFIDs, major attack vectors include:
  - Wireless attack
  - Software attack
  - Clone attack
  - Supply chain specific attack

SQL Injection in RFID

S4Lab



[Securing RFID systems from SQLIA, Fernando, H., et al., International Conference on Algorithms and Architectures for Parallel Processing, 2011]

Importance of software security

S4Lab

- Information security concerns are valid in new supply chains since there are more usage of HW/SW technologies compared to the traditional supply chains.
- Let’s consider RFIDs, major attack vectors include:
  - Wireless attack
  - Software attack
  - Clone attack
  - Supply chain specific attack
- But this is not the only important issue with respect to software security in the supply chain domain.

A paradigm shift in supply chain

S4Lab

Supply chains is getting more about the flow of information instead if flow of physical goods.

[From Physical Flows to Information Flows: An Evolving Concept of Supply Chain Management, Cragg T., McNamara T., SCMR, 2016]

Supply chain evolvement

S4Lab

- Because of digitalization and dematerialization:
  - Many of the leading companies today possess no stock (alibaba), own no taxis (uber) or property (airbnb), create no content (facebook), own no telecommunications infrastructure (skype) or own no cinemas (netflix).
  - Music industry, from CD era to download phenomenon.
  - 3D printing (i.E. Additive manufacturing)
    - “Download” anything you want, leading to the disruption of almost all industries.
- For leading companies in the digital sector, there are no physical products to be managed, only data to be controlled and a customer on-line experience to be constantly nurtured and nourished.
- A common refrain among supply chain experts is that in the future competition will be between supply chains, not firms.
- And for some, the future would be now by way of virtual businesses in which the supply chain really is the firm.

[From Physical Flows to Information Flows: An Evolving Concept of Supply Chain Management, Cragg T., McNamara T., SCMR, 2016]

Software security management of supply chains

S4Lab

Changes in the nature of firms mean that the focus of Supply Chain Management is changing too.
The priority switches away from physical flows between "lumpy-object purveyors" to those who manage data (encryption, data protection etc.)?

[From Physical Flows to Information Flows: An Evolving Concept of Supply Chain Management, Cragg T., McNamara T., SCMR, 2016]

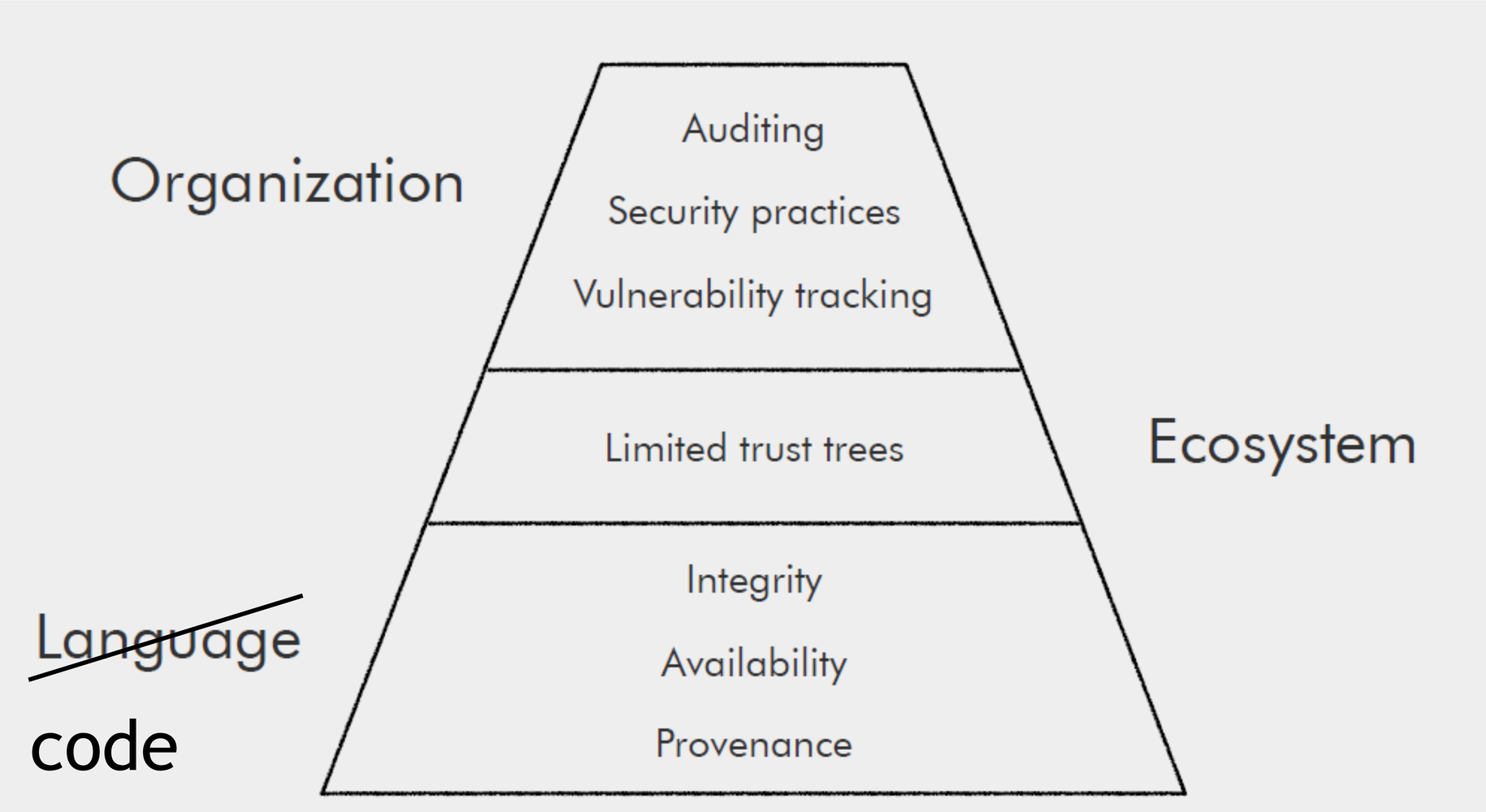
Why software supply chain security matters?

S4Lab

- New productive philosophies stemming from the shared economy
- Tapping into unused assets, they are forging new contacts across sectors and, in some cases, entirely re-configuring mature industries.
- Now, we are in the next shift in thinking: Can we not only look outside our company, but also outside our industries? Outside our normal trading relationships?
- New platforms such as
  - Goshare linking companies to unused transport capacity
  - Wework office space sharing platform
  - Flex, on demand warehousing
- This is the beauty of the shared economy: It uses technology to connect supply with demand irrespective of sector, industry or even past business relationships.
- The question is: Will these new ideas replace our old notions of a structured supply chain?

Three major players of software supply chain

S4Lab



[Securing The Software Supply Chain, Filippo Valsorda, Enigma. 2020]

Three supply chain security players

S4Lab

1. Language — enables trust
2. Ecosystem — propagates and limits trust
3. Organization — manages and mitigates trust

[Securing The Software Supply Chain, Filippo Valsorda, Enigma. 2020]

Language/code role in SW security of supply chain

S4Lab

- Enables trust
- Code policies:
  - A little copying is better than a little dependency.
  - Few and simple trusted components
- Provenance — what code do we depend on?
  - Trying to establish:
    - A universal name
    - A permanent version
- Availability — where do we get it?
  - Making sure the code is still available in the future.
- Integrity — has it been tampered with?
  - Protecting code from tampering.
  - The Go Checksum Database
- Dependency hell

[Insider Attack Resistancein the Android Ecosystem,René Mayrhofer, Enigma, 2019]

[Securing The Software Supply Chain, Filippo Valsorda, Enigma. 2020]

Ecosystem

S4Lab

- Importing a dependency delegates a degree of trust to it and to its transitive dependencies.
- A healthy ecosystem fights this like technical debt.

[Securing The Software Supply Chain, Filippo Valsorda, Enigma. 2020]

Example: Event-stream attack

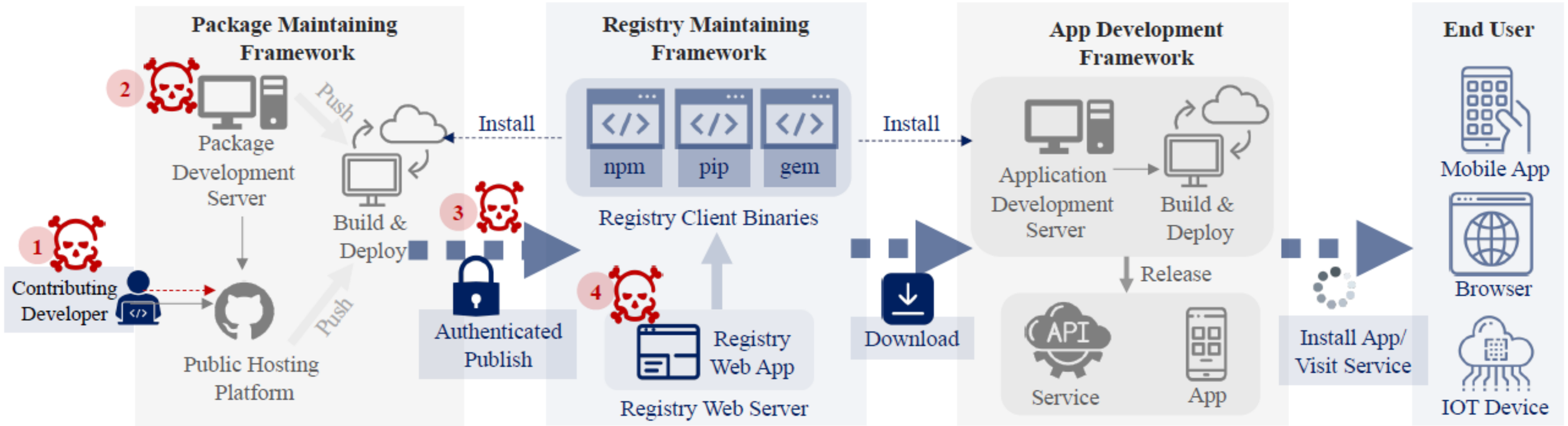
S4Lab

- Event-stream is a very popular npm package which exposes a number of helpers for working with streams inside a node application (over 1.9 million weekly downloads).
- Active maintenance was discontinued by original developers, and another user offered to take over maintenance duties.
- For about a week in September, event-stream included flatmap-stream as a dependency, as it was passed along to a new maintainer who added the dependency and removed it a week later.
- flatmap-stream had some code hiding at the end of its minified built output which attempts to decode and execute strings from its packaged test/data.js file, using the description of the top-level package as the AES256 key.
- For any other package, this produces a silently handled error (as the package description/ decryption key is wrong). But for copay-dash, this produces some valid JavaScript which runs another round of decryption and executes a malicious script that steals your bitcoin wallet.
- Innocent updates on Git., but an injected code uploaded to npm!

[event-stream vulnerability explained, Schneider.dev, 2018]

How upstream stakeholders affect downstream?

S4Lab



[Towards Measuring Supply Chain Attacks on Package Managers for Interpreted Languages, Duan, R., et al., NDSS, 2021]

How to have a better ecosystem

S4Lab

Features				Registries		
				PyPI	Npm	RubyGems
Functional	For Package Maintainers	Access	Password	●	●	●
			Access Token	◑	●	●
			Public Key Auth	○	○	○
			Multi-Factor Auth	◑	◑	◑
		Publish	Upload	●	●	●
			Reference	○	○	○
			Signing	◑	◑	◑
			Typo Guard	○	●	●
			Namespace	○	◑	○
		Manage	Yank Package	◑	◑	◑
			Deprecate Package	○	◑	◑
			Add Collaborator	◑	◑	◑
			Transfer Ownership	◑	◑	◑
	For Developers	Select	Reputation	●	●	●
			Code Quality	○	○	○
			Security Practice	○	○	○
			Known Issue	○	○	○
			Typo Detection	○	○	●
		Install	Hook	●	◑	○
			Dependency Locking	○	◑	◑
			Native Extension	◑	◑	◑
			Embedded Binary	◑	◑	◑
Review†	For PMs and Devs	Metadata	Dependency Check	○	○	○
			Update Inspection	○	○	○
			Binary Inspection	○	○	○
			PM Account	○	○	○
		Static	Stylistic Lint	○	○	○
			Logical Lint	○	○	○
			Suspicious Logic	○	○	○
		Dynamic	Install	○	○	○
			Embedded Binary	○	○	○
			Import	○	○	○
			Functional	○	○	○
Remediation	PMs, Devs, Users	Remove	Package	●	●	●
			Publisher	●	●	●
			Installed Package	○	○	○
		Notify	PM	○	○	○
			Dependent PM	○	○	○
			Dev	○	○	○
			Advisory DB	○	●	●

unsupported - ○, optional - ◑, enforced - ●

[Towards Measuring Supply Chain Attacks on Package Managers for Interpreted Languages, Duan, R., et al., NDSS, 2021]

Organization

- Manages and mitigates trust
  - Vulnerability tracking — past vulnerabilities
  - Auditing — current vulnerabilities
  - Security practices — future vulnerabilities

[Securing The Software Supply Chain, Filippo Valsorda, Enigma. 2020]

Third Party Vendor Security Risks

S4Lab

- Almost all the organizations around the globe depend on one or more third-party vendors to successfully actualize their business strategies.
- In most cases, such parties have access to the company's private data, internal information, and technology systems.
- Third-party vendors often have inadequate cyber protection techniques against illegal access.
- "Target Corp." Breach of 2014
  - Attackers used malware to steal credentials from one of Target's less secure HVAC vendors, and consequently, the attackers gained access to Target's vendor-dedicated web services.
- One of the most overlooked attack vectors.

[A survey on supply chain security: Application areas, security threats, and solution architectures, Hassija, V., et al., IEEE IoT Journal, 2020]

Dependency confusion

S4Lab

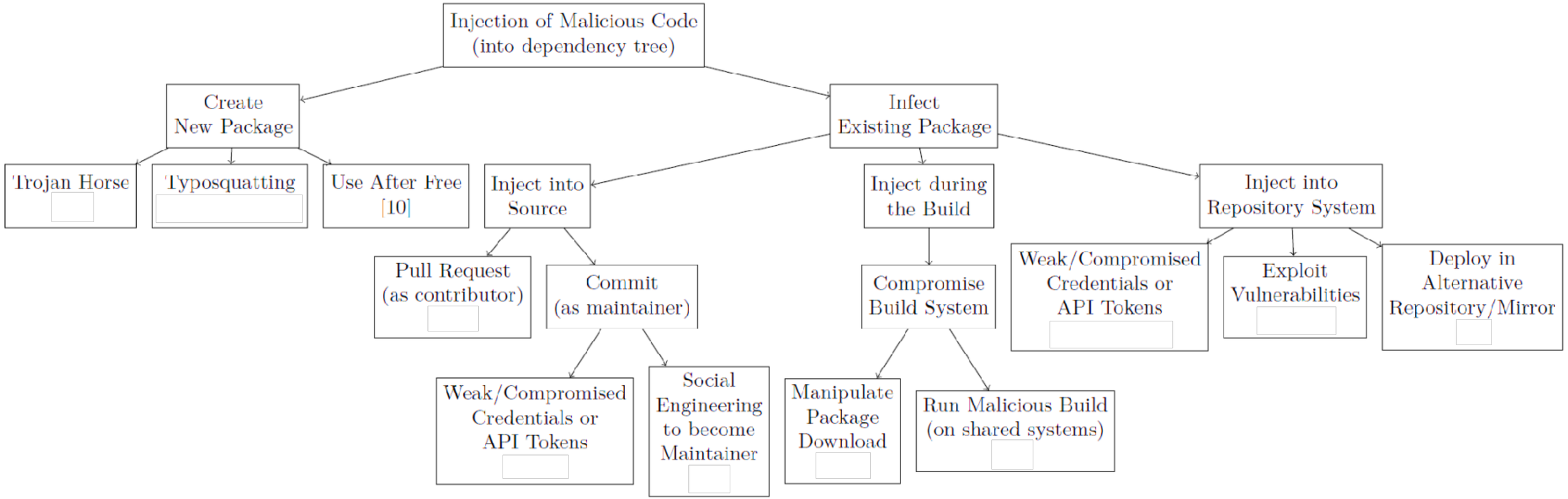
- Whenever you have separate sets of internal and external code in your chain, you are vulnerable!
  - Enterprise proprietary or highly-sensitive code, depending on their nature.
- For these codes, companies will often use private libraries that they store inside a private (internal) package repository, hosted inside the company's own network.
- If an attacker learns the names of private libraries used inside a company's app-building process, they could register these names on public package repositories and upload public libraries that contain malicious code.
  - How to learn internal names?
  - Why it will be preferred to the internal version?
  - How to prevent?

[Image:@alex.birsan]

[Microsoft warns enterprises of new 'dependency confusion' attack technique, Catalin Cimpanu, ZDNet, 2021]

Dependency threats should be handled

S4Lab



[Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies, Alex Birsan Alex Birsan, 2021]

Source code clone detection

S4Lab

- Want to check which libraries, which version are used in your project?
  - You should check the developers!
  - They may have not updates to the new library versions, e.g. Heartbleed
- If the source code of your program and libraries is available, it is relatively simple to detect reused libraries with mature techniques for source code clone detection.
- Source-to-Source Comparison.

[LibDX: A Cross-Platform and Accurate System to Detect Third-Party Libraries in Binary Code, Tang, W., et al., IEEE SANER, 2020.]

What about binary ?

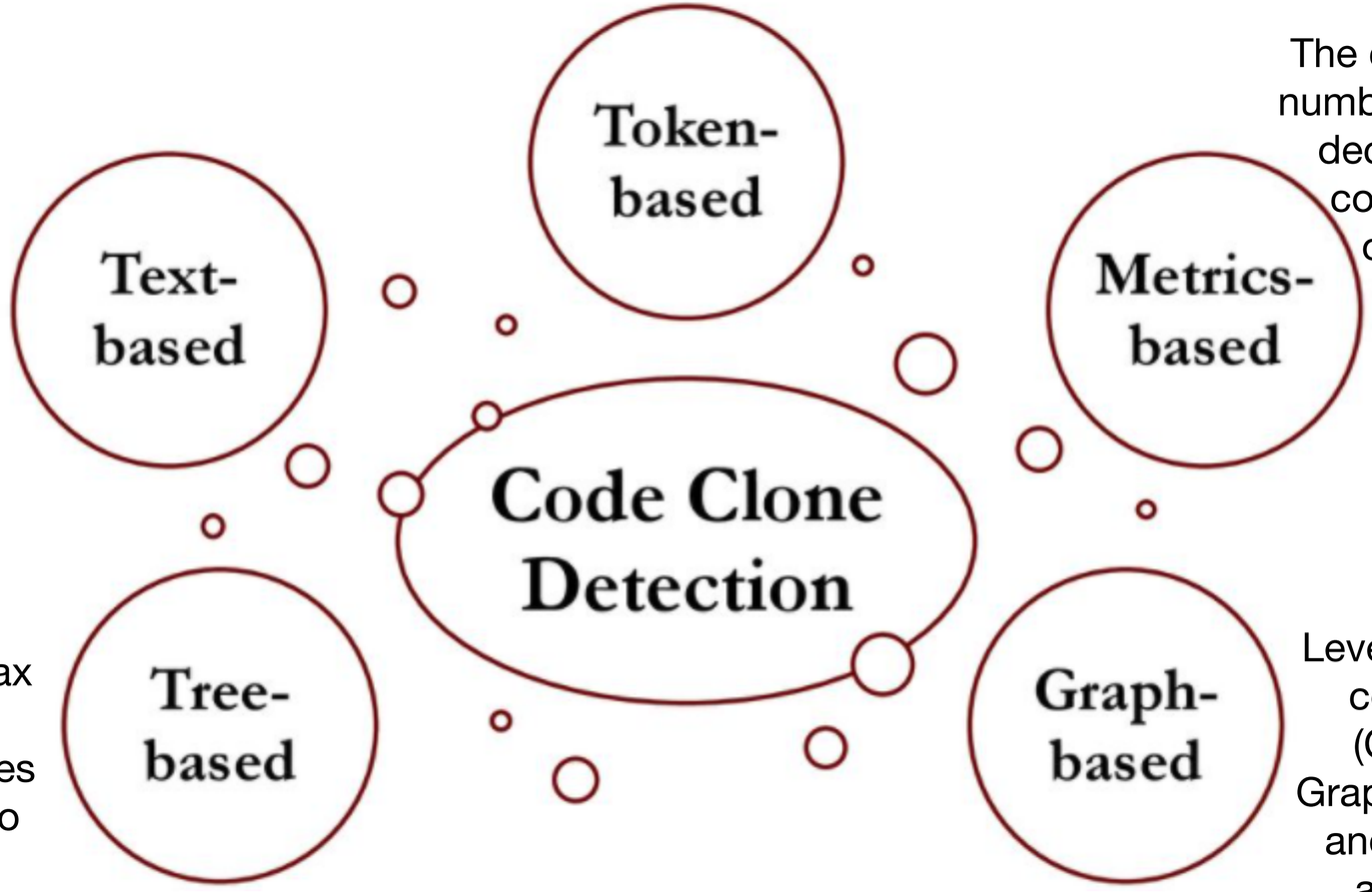
S4Lab

- Projects are released as executable files in binary format.
- Most features are stripped or changed to generate binary files such as function names, variable names and function call graphs.
- The same open-source package can be compiled into different binary code by different compilation processes.
- De-compilation is quite complex and usually unable to work perfectly and automatically
  - IDA is an expensive commercial product and it is not applicable to build a large-scale feature database containing thousands of libraries.
  - Binaries on different platforms have great differences with each other.
- Library (clone) detection by :
  - Binary-to-Source Comparison.
  - Binary-to-Binary Comparison

[LibDX: A Cross-Platform and Accurate System to Detect Third-Party Libraries in Binary Code, Tang, W., et al., IEEE SANER, 2020.]

First identify tokens and remove white spaces and comments from source code. Detect clones based on token comparison.

Line-based string matching algorithms to detect exact or near-duplication clones.



The collected metrics may include the number of function calls, the number of declaration statements, cyclomatic complexity, and the ratio of input/ output variables to the fanout.

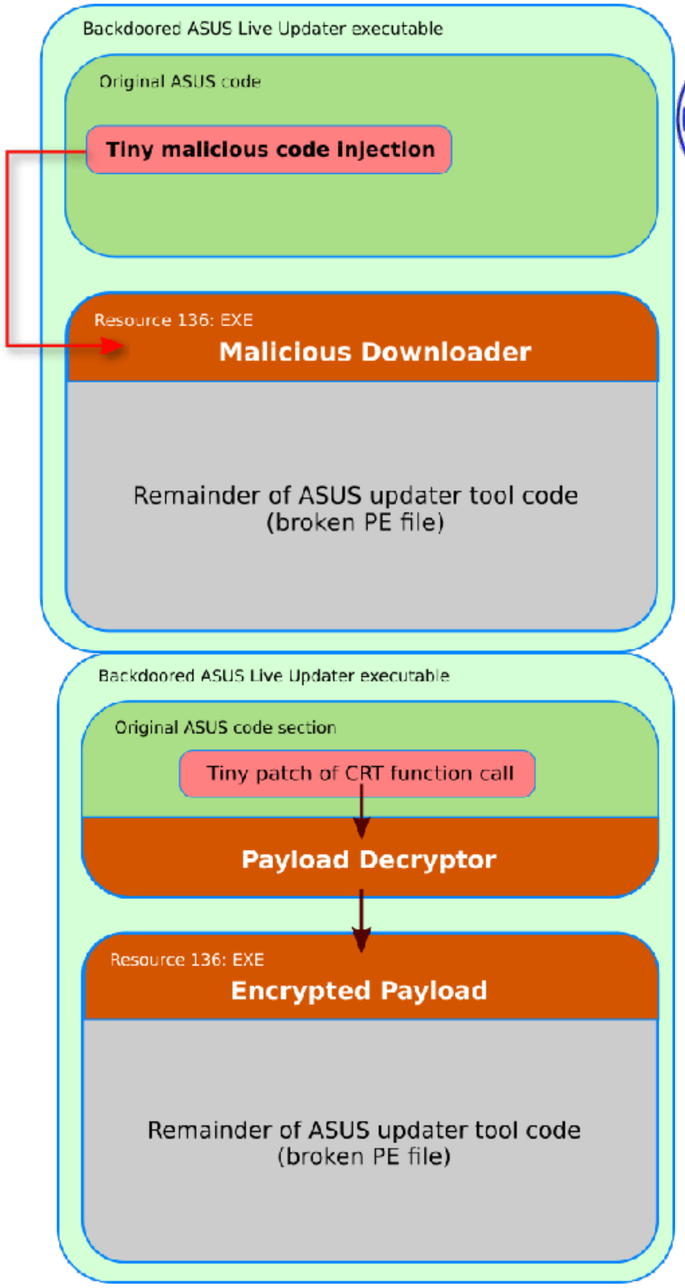
Generate an Abstract Syntax Tree (AST) for each code fragment, and then leverages tree matching algorithms to detect similar subtrees.

Leverages program static analysis to construct a Control Flow Graph (CFG) or Program Dependence Graph (PDG) for each code fragment, and then uses subgraph matching algorithms to find similar code.

[Cclearner: A deep learning-based clone detection approach, Li, L., et al., IEEE CSME, 2017]

ShadowHammer

- A trojanized ASUS live updater file (setup.Exe), was signed with legitimate certificates i.e. “ASUSTeK computer inc.”.
- The attackers most likely obtained a copy of the certificates or abused a system on the ASUS network that had the certificates installed.
- The goal was to target an unknown pool of users, who were identified by their network adapters’ MAC addresses.
- Two binary injection scenarios.
  - The attackers replaced the winmain function in the binary with their own.
  - Patched the code inside the c runtime (crt) library function.



[Operation ShadowHammer: a high-profile supply chain attack, Kaspersky, 2019]

What to do ?

S4Lab

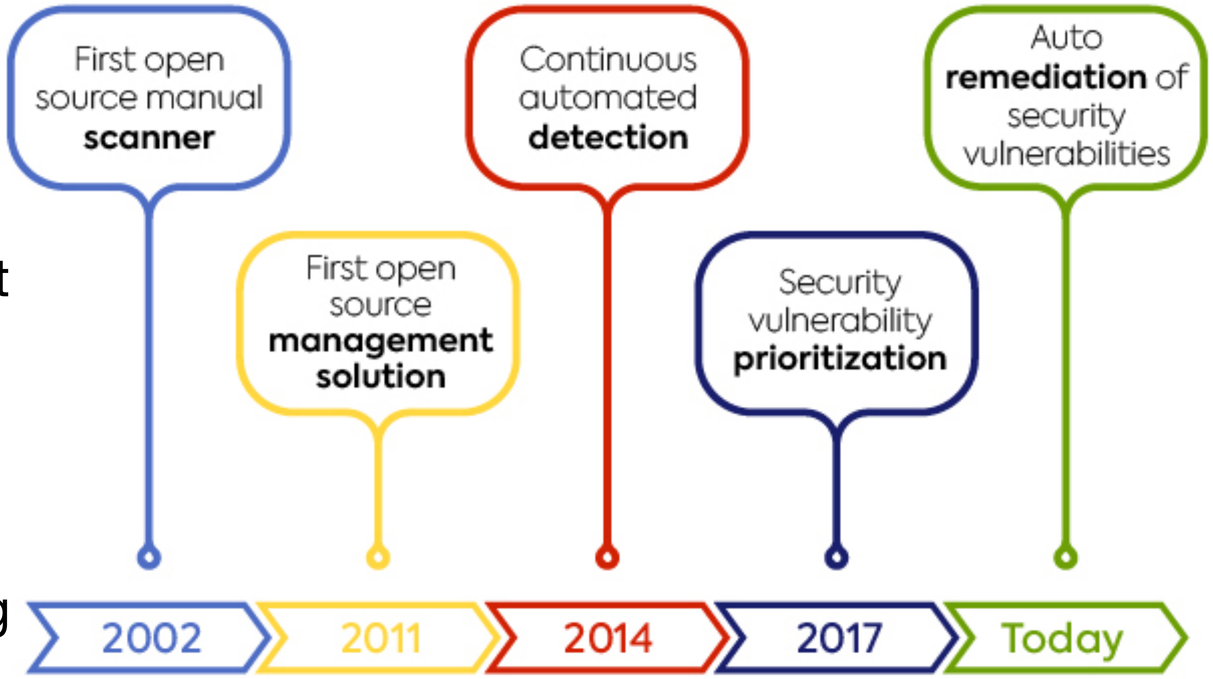
- Defining regulatory compliance requirements
  - Companies should consider defining reasonable levels of security and associated controls.
  - Requiring sub-contractors, vendors, and critical supply chain partners to meet or exceed those standards as terms and conditions of established business agreements.
  - PCI-DSS for data security
  - ITAR for military
  - ….
- Establishing boundaries and limiting access/control/monitor those boundaries.

[Supply Chain Cybersecurity: Experts on How to Mitigate Third Party Risk, Nate Lord, Digital Guardian, 2020]

Software Composition Analysis

S4Lab

- Up to 80% of typical applications are now third-party code, should be able to analyze these components.
- Software Composition Analysis (SCA) is an emerging subfield of application security concerned with precisely this problem.
- SCA tools inspect package managers, manifest files, source code, binary files, container images, and more
- Evaluate security, license compliance, and code quality.
- Auxiliary services such as interfaces for viewing software inventories, enforcing organization-wide policies, and integration with CI/CD setups may also be present.



[Image:https://www.whitesourcesoftware.com/]

[Software Composition Analysis, Synopsys, 2021]

[The dynamics of software composition analysis, Foo, D., et al., arXiv:1909.00973, 2019]

How SCA works?

S4Lab

- Clone detection.
- Static/dynamic/hybrid dependency analysis.
- Binary rewriting.
- ….

QA