Cyber security

Current challenges

Ludovic Mé, septembre 2019

3 properties ...

- **Confidentiality** (including personal data)
- **Integrity**
- **Availability**

3 properties ...

- Confidentiality
- Integrity
- Availability

... to be enforced by

- **Prevention**
  - > Formal methods
  - > Cryptography
  - > Authentication
  - > Access control
  - > etc.

3 properties ...

- Confidentiality
- Integrity
- Availability

... to be enforced by

- Prevention
- **Detection**
  - > Intrusion detection
  - > Anomalie detection
  - > Alert correlation

3 properties ...

- Confidentiality
- Integrity
- Availability

... to be enforced by

- Prevention
- Detection
- **Reaction**
  - Blocking attacks
  - Recovering the system
  - Counter-attacking ?

3 properties ...

- Confidentiality
- Integrity
- Availability

... to be enforced by

- Prevention
- Detection
- Reaction

Physical, logical, organizational

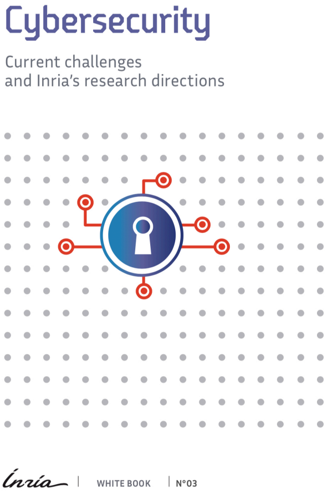
3 properties ...

- **Confidentiality**
- **Integrity**
- **Availability**

... to be enforced by

- **Prevention**
- **Detection**
- **Reaction**

~~Physical~~, **logical**, ~~organizational~~



- Published Jan. 2019
- Kremer, Mé, Rémy, Roca
- Around 20 contributors
- Overview of the field
- **Challenges**
- Inria's contributions

Access to Inria's white book

html

https ://files.inria.fr/dircom/extranet/livre_blanc_cybersecuritelivre_blanc_cybersecurite.html

pdf

https ://files.inria.fr/dircom/extranet/LB_cybersecurity_WEB.pdf

epub

https ://files.inria.fr/dircom/extranet/livre_blanc_cybersecurite/livre_blanc_cybersecurite.epub

HTML PDF ePub

Cyber security ? Many challenges !

Threats Analysis

Prevention

Detection and reaction

Privacy

Special cases of some application domains

Threats Analysis

1. A more systematic study of vulnerabilities (by the academic world)
2. Hardware-targeted software attacks (à la Spectre or Meldown)

Prevention

Detection and reaction

Privacy

Special cases of some application domains

Cyber security ? Many challenges !

Threats Analysis

Prevention

3. Scrutiny of cryptography
4. Computing on encrypted data
5. Quantum and postquantum Cryptography
6. Formal methods and cryptography
7. Formals methods for network and system security

Detection and reaction

Privacy

Special cases of some application domains

Threats Analysis

Prevention

Detection and reaction

8. Effectively detecting intrusion/anomaly (machine learning ?)
9. Accurately diagnosing causes of security violations (the 4 W)
10. Automatically deploying counter-measures

Privacy

Special cases of some application domains

Threats Analysis

Prevention

Detection and reaction

Privacy

11. Specific properties (e.g., unlinkability), concepts (e.g., differential privacy) and difficulties (e.g., anonymization) : understanding privacy and deriving practical tools – especially in the context of the EU General Data Protection Regulation (GDPR)
12. Machine Learning and Privacy

Special cases of some application domains

Threats Analysis

Prevention

Detection and reaction

Privacy

Special cases of some application domains

13. IoT : towards a secure and privacy preserving smart connected world
14. Cyber-physical / industrial systems
15. AI systems

You want some more challenges ?

Humanities

16. Usability of security and privacy tools
17. Social and economical aspects of security and privacy
18. Education

The cybersecurity threat is real and serious

- Attacks always more and more sophisticated
- We (probably) only see the tip of the iceberg
- The “Knowing your enemy” principle applies

The cybersecurity threat is real and serious

Challenge

- A deeper involvement of the academic world
- A scientific approach (experimental science)

A new trend of attacks...

- Software attacks targeting hardware "vulnerabilities"
  - A physical property of matter
  - Optimization mechanisms implemented in modern OS's and processors, such as caches, branch prediction, or speculative execution
  - Especially dangerous : makes hardware attacks possible at a distance
- Examples
- A common root cause : abstraction !
- Mitigation

A new trend of attacks...

- Software attacks targeting hardware “vulnerabilities”
- Examples
  - **Rowhammer** : exploits electrical interaction between neighbor cells $\rightarrow$ flips memory bits while reading and writing another cell
  - **Spectre** : exploits branch prediction and speculative execution $\rightarrow$ exfiltrates information through a covert channel based on cache access
- A common root cause : abstraction !
- Mitigation

A new trend of attacks...

- Software attacks targeting hardware “vulnerabilities”
- Examples
- A common root cause : abstraction !
  - When proposing a security mechanism at a given level of abstraction, tendance to consider that the lower layers are correct and safe
  - Attackers have had a tendency these last years to target less and less abstract layers : applications, OSes, kernels, firmware, and hardware
- Mitigation

A new trend of attacks...

- Software attacks targeting hardware “vulnerabilities”
- Examples
- A common root cause : abstraction !
- Mitigation
  - Prevention is costly
    - limiting the reduction of the component’s surface
    - refresh the cells (read / re-write) periodically
  - Detection is Difficult : no trace at the operating system or application levels

A new trend of attacks...

Challenge

- Clear typology, better understanding about deployment, hard and soft countermeasures
- Requires expertise at the hardware, firmware, and operating system levels

The foundation of confidence we have in crypto primitives

- The more we analyze crypto primitives, the more we can trust them
- A never-ending work, searching for possible weaknesses
  - > Threats may evolve over time with the progress of algorithms, mathematics, or computers
  - > The attacker's capabilities evolve as well
    - – Expl : physical access to an implementation in the IoT context

The foundation of confidence we have in crypto primitives

Challenge

Always searching for new attacks against :

- Crypto algorithms : by classical or quantum means
- Implementations : generally by physical attacks (physical measures correlated to the secret key manipulated)

Cloud environment : classical encryption is not enough...

- When encrypted, the confidentiality of the data is guaranteed, but no processing can be performed on the data
- Homomorphic operations
- Functional encryption

Cloud environment : classical encryption is not enough...

- When encrypted, the confidentiality of the data is guaranteed, but no processing can be performed on the data
- **Homomorphic operations**
  - From the encryption of two messages : produce the encryption of the sum or of the product, without any secret information
  - "Fully" homomorphic encryption is still expensive (computation + communication)
  - Result still encrypted : can only be shared with those who could already decrypt the inputs
- Functional encryption

Cloud environment : classical encryption is not enough...

- When encrypted, the confidentiality of the data is guaranteed, but no processing can be performed on the data
- Homomorphic operations
- **Functional encryption**
  - > Functional decryption keys : compute the result of a given function on the plaintext
  - > Allows for example some aggregation on data (statistical analysis) without revealing the data

Cloud environment : classical encryption is not enough...

Challenge

- Current propositions impractical (poor performance) $\rightarrow$ new homomorphic and functional primitives needed

A new age of cryptography

- Quantum computers would break classical **asymmetric** cryptosystems $\rightarrow$ need to find new alternative primitives
- Replacements must be ready soon as far as long-term confidentiality (e.g., more than 50 years) is concerned
- New primitives already proposed, based on new mathematically complex problems
  - code-based : hardness of decoding an arbitrary linear code
  - lattice-based : hardness of finding short vectors in an euclidian lattice
  - multivariate-based : hardness of polynomial system solving

A new age of cryptography

Challenge

Perform an in-depth security analysis of these new code, lattice or multivariate-based primitives

- Long process (several years)
- Likely to see a major crypto system broken in the 20 next years

Remark

Using quantum communication, it is possible to construct an unconditionally secure key distribution protocol

- Based on physical properties of matter (superposition and intrication)
- Expl : using photons to transmit information (keys)
- Challenge for physicists : transmission over long distances ($>$ 1000 or 10.000km)

Security of cryptographic protocols is extremely difficult to ensure

- Pencil and paper proofs regularly contain errors
- Formal methods appears increasingly as the only way to achieve the expected security level
- Computer-aided security proofs from the specification down to the implementation

Security of cryptographic protocols is extremely difficult to ensure

Challenge

- Proofs still require carefully crafted code and a very high level of expertise $\rightarrow$ make them applicable to more general code and usable by a wider audience
- Verifying certain properties, such as anonymity
- Considering stronger adversary models
  - > Adversary that may control part of the computer through malware

Formal methods : a key for the security-by-design approach

- Network and system security often relies on more classical engineering approaches
- Some proof needed
  - Proving that a system whose model is provided is immune to a particular class of attacks whose model is also provided

Formal methods : a key for the security-by-design approach

Challenge

- From protocol to software formal verification (scalability of FM ?)
- Evaluate FM contribution to the security of **real** systems
- Apply FM to reactive security
- Analyse cost vs. benefits of using FM
- FM and regulation in security and privacy

Useful but still relatively inefficient detectors

- Mainly network-based intrusion detection systems (IDS)
- Many false alarms (false positives) for both anomalie detection and misuse detection

Useful but still relatively inefficient detectors

Challenge...

- Tackling the “problem” of enciphered network traffic
- New approaches for producing alerts
- Test and certification of detection

Useful but still relatively inefficient detectors

Challenge...

- **Tackling the "problem" of enciphered network traffic**
  - Analyzing enciphered network traffic
  - Application, OS, firmware-based intrusion detection
- New approaches for producing alerts
- Test and certification of detection

Useful but still relatively inefficient detectors

Challenge...

- Tackling the "problem" of enciphered network traffic
- **New approaches for producing alerts**
  - Misuse detection : multi-events matching
  - Anomaly detection :
    - A better learning process : machine learning, of course. Data ? Explainability ?
    - Alternative approaches without learning : specification or policy-based
  - Privacy respectful detection
- Test and certification of detection

Useful but still relatively inefficient detectors

Challenge...

- Tackling the "problem" of enciphered network traffic
- New approaches for producing alerts
- **Test and certification of detection**
  - Benchmark and platforms
  - Formal methods for proving :
    - that a given class of attacks can (or cannot) be detected
    - more generally, that an intrusion detection system could detect all violations of a given security policy
    - the absence of false alarms for a supervision system ?

Useful but still poor correlation engines

- Mainly alert normalization and fusion
- Poor capacity in reconstructing global attack scenarii
- Poor capacity in explaining attackers objectives
- Correlation remains mainly a human-based analysis

Useful but still poor correlation engines

Challenge...

- Taking the environment into account
- Possible contribution of AI
- Apply FM to reactive security
- Visualization of security events

Useful but still poor correlation engines

Challenge...

- **Taking the environment into account** : local and global
- Possible contribution of AI
- Apply FM to reactive security
- Visualization of security events

Useful but still poor correlation engines

Challenge...

- Taking the environment into account
- **Possible contribution of AI**
  - Generation of correlation rules
  - Reasoning on the flow of alerts
  - Implicit correlation (clustering)
- Apply FM to reactive security
- Visualization of security events

Useful but still poor correlation engines

Challenge...

- Taking the environment into account
- Possible contribution of AI
- **Apply FM to reactive security** : proof that an alert correlation engine will properly fusion information relative to the same attack but spread over several alerts or security events
- Visualization of security events

Useful but still poor correlation engines

Challenge...

- Taking the environment into account
- Possible contribution of AI
- Apply FM to reactive security
- **Visualization of security events**
  - Automation of the representation according to the nature of the data
  - Interaction with the operator

Today's limits to automatic reaction to attacks

- Very simple automatic reactions : closing firewall ports, killing processes
- No real evaluation of the impact of the counter-measure
- No real global reasoning about the security policy

Today's limits to automatic reaction to attacks

Challenge...

- Technical questions
- Ethical and legal questions

Today's limits to automatic reaction to attacks

Challenge...

- **Technical questions**
  - > React as quickly as the attack : stop the attack, its progression, its diffusion
  - > Get a quick diagnosis : modification of the security policy and/or its implementation
    - – Automatic generation of implementation from policy specification
  - > Proof of the relevance of the correction
  - > Formal methods ? (Symbolic) AI ?
- Ethical and legal questions

Today's limits to automatic reaction to attacks

Challenge...

- Technical questions
- **Ethical and legal questions**
  - > Counter-attack ?
  - > Instantaneous and proportional (legitimate) self-defense ?

From regulation to effective implementation

- Currently :
  - lack of transparency : many services and devices behave as black boxes
  - lack of user control : how to express consent or opposition when there is neither information, nor user interface
- The GDPR promotes privacy concepts and goals, but little or no guidance about the effective implementation

From regulation to effective implementation

Challenge

- Privacy risk analysis
- Evaluate attack against privacy : visible and invisible leaks
- Individualized management and control over one's personal data
- Expression of consent or opposition (in the absence of information or user interface)
- "Optimized" balance between utility and privacy
- Formal frameworks that enable to bring guarantees about the correctness of a certain design

An attacker who has access to the trained network could gain information about the training data

- Extracting training data or simply deciding whether a given input was part of the training data
- Back box or white box (e.g. : access to the neural network internals ?)

An attacker who has access to the trained network could gain information about the training data

Challenge

- Transform the data prior to storage, so as to discard any private information that is useless for the task
  - Robust anonymization, that effectively resists de-anonymization attacks
- Train in a distributed online fashion, in order to avoid storing all data in a single place which increases the risk of a security breach

Attacks in the IoT context

- Still relatively easy (no security-by-design)
- Especially invasive
- Potential major impact
  - > Multiplication factor made possible by the large number of devices available
  - > Impact in the physical world (e.g., connected cars)

Attacks in the IoT context

Challenge

- Need for secure-by-design frameworks, protocols, and operating systems
- Design of lightweight cryptographic primitives adapted to limited resources
- Ability to securely update embedded devices' software
- Detection and mitigation of intrusions or misbehaving devices

Cybersecurity of Industrial Systems is an emerging topic

- Industrial systems rely more and more on software mechanisms that can be attacked
- Cyberattacks against industrial systems show that the problem is open
- Difficult context
  - Potential disasters...
  - No security-by-design
  - Specifications often not publicly available
  - Industrial protocols not handled by classical tools (firewalls, IDSes)
  - End devices built with slow processors unable to use standard cryptography

Cybersecurity of Industrial Systems is an emerging topic

Challenge

- Adapting traditional security mechanisms to the specificities of this new context
- Communication protocols used in this context cannot be modified overnight $\rightarrow$ transition during which legacy communications should be embedded in secure protocols
- Real-time control of the system is usually required $\rightarrow$ security must thus also be applicable in real time
- Often impossible to modify industrial devices : preventive security mechanisms cannot be used and reactive security is thus extremely important $\rightarrow$ study how effective attack detection mechanisms could be deployed in this context

Machine learning techniques suffer from two main threats in relation to cybersecurity

- Privacy : extracting information about training data from a trained network
- Adversarial machine learning : adding carefully designed noise (barely visible to human eye) to an image, leading to misclassification

Machine learning techniques suffer from two main threats in relation to cybersecurity

Challenge

- Privacy : see above
- Adversarial machine learning : understand, and then control

To conclude...

Autonomous security and cyber resilience

- Autonomous security : system is able to detect attacks against itself, react and reconfigure
- Cyber-resilience : system remains operational even under attack

Autonomous security and cyber resilience

A general and global challenge

- From “security-by-design” to “cyber-resilience by design”
- Reactive security or malware detection are here of utmost importance
- Preventive security is also relevant : applying formal methods to critical parts of systems

Thanks !

Questions ?