PROTECTION OF PERSONAL DATA IN SECURITY ALERT SHARING PLATFORMS

Friday 1st September, 2017
Introduction

Collaborative Security

- Emerging trend in cyber security,
- popular among CSIRT/CERT teams,
- hot topic of current security research.

Cyber Security Alert Sharing Platforms

- Technical means of automated information exchange,
- provide timely information about current security events,
- examples – MISP, STIX, SABU, etc.
Motivation

Privacy Issues

- Cyber security data are sensitive and security alerts contain personal information (IP addresses are also personal data!).
- Cyber crime knows no borders, but it is complicated to transfer sensitive data to other country.
- Privacy issues may interfere with cyber security practice.

Novel Legal Frameworks

- Legal compliance of sharing platforms is not assured by design.
- Focus on European law and legal framework, namely GDPR (General Data Protection Regulation).
Sharing Platforms

Purpose of Information Sharing

- Increased capability of intrusion detection systems (IDS),
- early warning and preemptive security measures,
- global situational awareness and cyber threat intelligence.

What is Being Shared

- Almost everything may be a IoC (Indicator of Compromise),
- raw data – PCAP files, malware binaries, …
- security alerts – formatted reports of security events,
- potentially private pieces of information – IP addresses, e-mail addresses, URLs, domain names, …
Legal Framework

Evolution of Data Protection in the EU

- “Data privacy laws are spreading globally, and their number and geographical diversity accelerating since 2000.” [Graham2003]
- EU law focuses on protection of individual’s fundamental right to privacy in general.
- 1998 Data protection directive (no. 95/46/EC) did not anticipate rapid development of information technology.

GDPR

- General Data Protection Regulation (2016/679),
- not a directive, thus directly applicable to all EU member states,
- main intent – to give individuals more control over their personal data.
Legal Framework

Personal Data and It’s Use

- GDPR defines personal data very broadly as “any information about identified or identifiable person”.
- Online identifiers can be provided by devices, applications, tools and protocols, such as IP addresses, cookie identifiers or others.
- Alert sharing platforms process personal data – when and for what purpose can we use them?
- GDPR provides six legal grounds for personal data processing:
  - consent of the data subject,
  - performance of contract with data subject,
  - legal obligation of the controller,
  - protection of vital interest of the data subject,
  - public interest,
  - legitimate interest of the controller.
Legal Framework

Legal obligation

- NIS directive (No. (EU) 2016/1148) is partially applicable,
- operators of essential services are required to notify authorities of any significant security incident.

Legitimate Interest

- The most fitting legal ground, but also the most complicated.
- Common misunderstanding by security professionals – security operations does not give instant right to process personal data.
- Legitimate interest must be balanced against the rights of the data subject – proportionality test.
Legal Framework

Proportionality Test

- There must be a legitimate aim for a measure.
- The measure must be suitable to achieve the aim (potentially with a requirement of evidence to show it will have that effect).
- The measure must be necessary to achieve the aim, that there cannot be any less onerous way of doing it.
- The measure must be reasonable, considering the competing interests of different groups at hand.
Legal Framework

Proportionality Test

- Statements of Article 29 working party and the GDPR: *cyber security is a field, in which it is likely that the personal data will be processed due to legitimate interest.*

- NIS directive: “*[Providers] … should be encouraged to pursue their own information cooperation mechanisms to ensure the security of network and information systems.*

- Additional notes:
  - sharing the data benefits all users of affected systems,
  - in case of IoCs, very little data is actually shared,
  - it is complicated to connect the data to the data subject.
Legal Framework

Other Issues to Consider

- Different position of involved entities – different legal obligations for operators, senders, and receivers.
- Data analysis may fall within the definition of profiling, e.g., using IP address reputation database to blacklist network traffic violates Art. 22 of the GDPR.
- Transfer of private data outside the EU is forbidden unless adequate level of data protection is provided.
How to assure legal compliance

Privacy by Design and Default

- Art. 25 of the GDPR:
  - “The controller shall [...] implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing.”
  - “The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.”
How to assure legal compliance

Technical Measures

- Security of storage and data transfer.
- Discard the data after they are used.
- The law does not provide any complete list of possible measures, but refers useful tools and state of the art.
How to assure legal compliance

Organisational Measures

- Data minimisation – share and receive only relevant data,
- Limitation of storage period,
- Data protection and impact assessment – risk analysis is directly recommended by GDPR,
- Regular checks of safeguards.

Legal Measures

- Platform – common rules of usage, service-level agreement.
- Individual nodes – internal directive, non-disclosure agreement.
Conclusion

Data protection in alert sharing platforms

- Information exchange interferes with privacy,
- legal issues are not taken into account while designing cyber security alert sharing platforms.

Legal compliance of alert sharing platforms

- Compliance with the EU law and GDPR,
- technical, organisational, and legal measures proposed,
- open question – how to share the data with non-EU partners?
THANK YOU FOR YOUR ATTENTION!

@csirtmu

Martin Husák
husakm@ics.muni.cz