PSD2 and Cyber Security Practices in the EU

COMP-116 Final Project Supporting Material

Juliet Yue

Acronyms

PSD2	The Second Payment Directive
ASP (AISP)	Account (Information) Service Provider
PSP (PISP)	Payment (Information) Service Provider
TPP	Third Party Platforms
EC	European Commission
RTS	Regulatory Technical Standards — regulation issued by EC
SCA	Strong Costumer Authentication
DDoS	Denial of services attack

What is PSD2

- Target the payment service market (the burgeoning fin-tech market)
    - Increased transparency among financial institutions and provide opportunities to TPP
- The Second Payment Services Directive
    - Enlarge the scope of the Directive
    - Establish regulations on customer authentication
    - Require account service

To the community

- Background: An era when we are trying to find proper ways to regulate payment markets
- Action: EU chooses demands open-banking for all organizations operating in the EU
- Result:
  - Encourage technology innovation
  - Increase security/compliance risks

Technology and PSD2

- Important document: Regulatory Technical Standards by European Commission (http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf)

- Major takeaways:

    - ASP and PSP each has its own responsibility to ensure information security during the process

    - Some thoughts: HTTPS, Complex encryption methods, strong authentication methods

The Berlin Group

- An initiative to standardize technical services among financial institutions in pan-European countries

- Include most major players in the payment market in pan-European countries

- Guideline recommended to comply with PSD2 (https://docs.wixstatic.com/ugd/c2914be05c90dbfe4447149e36d48e1dd08339.pdf)

Discussion on the Guideline

Transport Protocol

- The Berlin Group: HTTPS (as of 11/20/2018)
  - HTTP + TLS 1.2
- TLS 1.3 is faster, more secure, and provide a more streamlined process
- Recommendation: HTTP + TLS 1.3

Discussion on the Guideline

Authentication Protocol

- The Berlin Group: OAuth2/redirect, embedded, decoupled (as of 11/20/2018)

- Phishing risk: OAuth2/redirect vs Decoupled

- Recommendation: decoupled + embedded

Discussion on the Guideline

API

Risk:

- DDoS Attack
- Mis-management of Mobile API routes
- Open Source Libraries (Heartbleed OAuth2: CVE-2014-0160)

Mitigation:

- Separate Mobile/Web API host
- Apply multiple layers of authentication (PSP + ASP)
- User input striping
- Be aware of the risk of open source libraries
- Develop new technology to defend against security risks

Conclusion

- Pros: Encourage technology innovation in the EU, bring security in as a serious compliance matter to organizations
- Cons: Increase risks of security breech
- Look forward to see the impact of this regulation in a few years
- For detailed report about this presentation and references, place refer to my paper written on the same topic

References

- Summary of PSD2: https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption
- TLS1.3:https://www.ssl.com/blogs/need-know-tls-1-3
- Technology Guideline by the Berlin Group: https://docs.wixstatic.com/ugd/c2914be05c90dbfe4447149e36d48e1dd08339.pdf
- Authentication Methods: https://www.thepaypers.com/interviews/api-authentication-during-psd2-towards-an-inclusive-approach/773432-38
- Cloud API Risk: https://blog.cloudsecurityalliance.org/2013/04/13/cloud-apis-the-next-battleground-for-denial-of-service-attacks/