TDL | Trust in Digital Life

DATA EXPECTATIONS
Data Protection & Open Banking

Open Banking Security Concerns

Cyber Security for Europe

David Goodman, Trust in Digital Life

Friday, 26 October 2018

TDL | Trust in Digital Life

Boosting the Effectiveness of the Security Union

Cyber Security for Europe

H2020-SU-ICT-2018

The objective of this topic is to scale up existing research for the benefit of the cybersecurity of the Digital Single Market, with solutions that can be marketable.

- to propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a **cybersecurity competence network** with a central competence hub.
- to help build and strengthen cybersecurity capacities across the EU as well as provide valuable input for the future set-up of the **Cybersecurity Competence Network** with a **European Cybersecurity Research and Competence Centre**.

What is CyberSec4Europe?

22 countries

44 project partners

40 support letters (global)

26 ESCO members

6 ECSO Working Groups

Existing networks (ECSO, TDL, EOS, CEPIS)

Experience from 100+ cybersecurity projects in 14 key areas

11 technology/application elements

Coverage of 9 vertical sectors

CyberSec4Europe is: Centres of Excellence / Universities / Research Centres /SMEs!

Industrial Sector Demonstration Cases

- Finance
  - Incident reporting
  - Open banking
- Health
  - Medical Data exchange
- Smart Cities
  - Citizen participation/e-Gov
  - Critical infrastructures
  - Education
- Transport
  - Maritime (port critical infrastructure)
  - Supply chain assurance

Industrial Sector Demonstration Cases

- Finance
  - Incident reporting
  - Open banking
- Health
  - Medical Data exchange
- Smart Cities
  - Citizen participation/e-Gov
  - Critical infrastructures
  - Education
- Transport
  - Maritime (port critical infrastructure)
  - Supply chain assurance

Consortium Participants

Project Lead

- Goethe University Frankfurt (DE)

WP Leaders

2. TU Delft (NL)
3. University of Murcia (ES)
4. FORTH (EL)
5. NEC Labs Europe (DE)
6. Trento University (IT)
7. Masaryk University Brno (CZ)
8. Cybernetica (EE)
9. Trust in Digital Life (BE)
10. Conceptivity (CH)

Partners

- ABI Labs (IT)
- AIT (AT)
- Archimede (CH)
- ATOS Spain (ES)
- Banco Bilbao Argentaria (ES)
- University Porto (PT)
- CNR (IT)
- CTI “Diophantus” Patras (EL)
- DAWEX (FR)
- Denmark Technical University (DK)
- Engineering Spa (IT)
- Comune di Genova (IT)
- Banque Populaire (FR)
- IBM Research Rüschlikon (CH)
- International Cyber Investigation Training Academy (BG)
- Intesa Sanpaolo (IT)
- JAMK University of Applied Sciences (FI)
- Karlstad University (SE)
- KU Leuven (BE)
- Norwegian University of Science and Technology (NO)
- Open & Agile Smart Cities (BE)
- Politecnico de Torino (IT)
- Siemens AG (DE)
- SINTEF (NO)
- Time.Lex (BE)
- University College Dublin (LERO) (IE)
- University of Cyprus (CY)
- University of Maribor (SI)
- University of Malaga (ES)
- University of Luxembourg (LU)
- University of Piraeus (EL)
- Université Paul Sabatier Toulouse (UPS-IRIT) (FR)
- VaF (SK)
- VTT (FI)

TDL | Trust in Digital Life

Strategic Aspects

Cyber Security for Europe

Address the various security issues associated with PSD2 to resolve key inhibitors for AISPs, ASPSPs, PISPs and PSUs from moving forward with open banking with confidence.

Boost the EU's ambitions to create a vibrant, open digital market, and create the potential to enable innovation within the traditional financial community as well as Fintech companies, create jobs and opportunities for new citizen-oriented services.

AISP: Account Information Service Provider
ASPSP: Account Servicing Payment Service Provider

PISP: Payment Initiation Service Provider
PSU: The end-user of payment services

TDL | Trust in Digital Life

Use Cases

Cyber Security for Europe

- Social Engineering & Malware Attacks
- Certificate Verification
- GDPR & PSD2
- APIs
- Bank Administration
- Circles of Trust

TDL | Trust in Digital Life

Social Engineering & Malware Attacks

Cyber Security for Europe

New threat scenarios can arise due to the presence of third parties posing between users and ASPSPs, in terms of:

- attacks to data and information stored by and exchanged with a third party
- new social engineering attacks where the fraudsters contact the customer pretending to be the third party

TDL | Trust in Digital Life

Social Engineering & Malware Attacks

Cyber Security for Europe

The use of mobile phones exposes a major vulnerability from not having two separate execution elements in a single device for accessing bank account information

(as specified in PSD2 RTS Article 9 "Independence of the Elements")

Although the devices themselves demonstrate adequate security and are not themselves susceptible to attack, the increase in the volume of social engineering attacks exposes user bank accounts to attacks that can't be easily recognized or intercepted by the banks.

TDL | Trust in Digital Life

Social Engineering & Malware Attacks

Cyber Security for Europe

Banks have become highly successful in intercepting malware attacks by recognizing, through sophisticated tooling, anticipated user behaviours when accessing their accounts.

With PSD2, customer bank accounts will be accessed by third parties (PISPs) making it much harder for the banks' systems to identify between genuine access requests and malware.

To progress authenticating third parties, it could be possible to use AI/ML for some online operations, making it unnecessary in those cases to strongly authenticate users.

TDL | Trust in Digital Life

Certificate Verification

Cyber Security for Europe

Even after the AISP (and the third party) registers with a national certificate authority, the ASPSP is not able to verify the certificate electronically, as currently the registration is not accessible.

- An EU-wide mandatory and standardised exchange between CAs on business model assessments under PSD2 is of specific importance for innovative services and models which was not considered when PSD2 was finalised.
- When the PSU wishes to revoke the authority given to the PISP, they are faced with an extension of the problem

GDPR & PSD2

Under PSD2, third parties will be able to access customer account information directly, provided they have the customer's explicit consent, and enable the customer to exercise their right to data portability under GDPR.

- GDPR also stipulates the responsibility of the data controller – in this case the bank or ASPSP – to safeguard their customers' data with the threat of considerable fines if there is a failure to do so.
- In this confluence of the objectives of both regulations, it's not clear which party is responsible for obtaining the customer's consent and, significantly, which organization – the PISP or the ASPSP – is culpable if the customer suffers any loss due to a data breach or cyber attack.

TDL | Trust in Digital Life

GDPR & PSD2

Cyber Security for Europe

In making a payment to a third party, unless the third party is trusted by the PSU, the PISP opens up a potential vulnerability in terms of financial loss but more importantly a lack of certainty in case of a data breach or data misuse.

- PSD2 articles 66 and 67 forbid banks sharing 'sensitive payment data' with third parties, but there is no clear definition of what it is.
- Without clarification banks will err on the side of safety, particularly from the perspective of GDPR compliance.

TDL | Trust in Digital Life

Cyber Security for Europe

APIs

New threat scenarios can arise due to the presence of third parties posing between users and ASPSPs, in terms of attacks to the availability of APIs and other interfaces services

For PISPs and ASPSPs not utilising the same ‘open banking API’, some form of mediation may be used that could introduce an unforeseen security risk.

Some **FinTechs** may want to continue to use screen-scraping as well as web-scraping including APIs, attempting to simulate a bank’s interfaces.

Some **banks** may continue to offer it since they are not API-ready and/or because the their API solution isn’t sufficient and they have to offer "direct access”, a deep type of access that avoids verification.

APIs

In these cases PSD2/RTS/GDPR demand that the third party be reliably identified and only access data that is allowed.

How can that be ensured in a screen-scraping environment?

If a third party impersonates a user logging on to online banking, identification *(i.e., it really is that rogue third party)* and restriction of access *(i.e., not looking at all the other data seen on the browser screen)* are very difficult and a real security/GDPR challenge.

Bank Administration

A different set of security challenges is presented in the scenarios described above when the user is a corporate administrator.

- Although most PSD2 focus is on consumers, some of the often neglected areas of the regulation but with high potential are the new opportunities for corporates.
- The special requirements of corporates *(e.g. multiple roles of authorising users, multiple signatories, authentication depending upon limits, etc)* present an additional layer of complexity and security risks in the context of PSD2.

TDL | Trust in Digital Life

Bank Administration

Cyber Security for Europe

Another issue is how to secure a bank's information systems.

- Specifically, how to verify that the security policies of TPPs that interact with the bank are compatible with those of the bank.
- More generally, how can a bank trust how TPPs' security mechanisms work, an issue which is not just relevant to PSD2?

The issue is not just with users but between partners, requiring that security mechanisms should be flexible.

- Today's bank perimeter is moving, with TPPs coming and going.
- Security comes to the weakest link requiring an evaluation and maturity assessment of each partner.

TDL | Trust in Digital Life

Circles of Trust

Cyber Security for Europe

PSD2 should not be seen as a constraint but an opportunity, presenting options to develop new types of services, such as building an eco-system of partnerships.

However, there is an issue with how to securely authenticate each partner and to create a ‘circle of trust’.

TDL | Trust in Digital Life

Impact on the European Market

Cyber Security for Europe

PSD2 enables innovative services, new market players, greater transparency and consumer choice, for promoting a digital single market in Europe and at the same time guaranteeing a high level of security.

One of the best innovations comes from having third party providers in the payment chain being able to access bank accounts and make payments on behalf of customers, thus enabling the concept of open banking.

To securely communicate, third parties and ASPSPs can rely on dedicated interfaces (APIs), that should be properly configured to reduce the risk of frauds and attacks.

TDL | Trust in Digital Life

Impact on the European Market

Cyber Security for Europe

The Regulatory Technical Standards (RTS) under PSD2 come into force on 14 September 2019 and require PSPs to adopt measures guaranteeing adequate levels of security to access and authorize remote payments, and to properly operate with third parties.

TDL | Trust in Digital Life

Impact on the European Market

Cyber Security for Europe

- Although both GDPR and PSD2 share the same objectives – to put customers in control of their own data and to keep that data safe – because they were designed independently of each other, there are apparent deployment incongruities that could lead to security holes and vulnerabilities.
- All in all, there are unresolved issues which are inhibiting the full realization of the objectives of PSD2, which has a key role to play in the drive towards the digital single market in Europe.

TDL | Trust in Digital Life

Cyber Security for Europe

Thank you!

david@trustindigitallife.eu

DATA EXPECTATIONS
Data Protection & Open Banking