iMinds

AN iMINDS ICON RESEARCH PROJECT | PROJECT RESULTS

ICT

TRU-BLISS

Helping financial institutions cope with the digital era's security threats

The financial sector – just like many others – is in the midst of a digital transformation. On the one hand, this brings a great deal of opportunities as it allows for the creation of innovative services such as mobile phone banking. Yet, the move to digital also brings a number of challenges that might jeopardize the sector's trusted relationship with its customers. Cyberattacks, which are becoming increasingly complex and powerful, are one concrete example.

Since there is a lot at stake, TRU-BLISS investigated how banks can better cope with security threats in the digital era – both operationally, technically and legally.

"As banks bring their digital innovations to market, they are forced to make a continuous trade-off between introducing user-friendly products and applying strict security measures," says Patrick Wynant (Febelfin). "We wanted to investigate which security measures are being used by financial institutions already, evaluate their effectiveness, and support banks to work together to face upcoming cybersecurity threats."

THE OUTCOMES

1. Prototyping an interbank risk warning system that allows banks to better cope with fraud

Fraud incidents are becoming increasingly complex, and are no longer isolated to a single bank's activities. What is needed, is an interbank collaboration model that enables the timely and secure exchange of information – with guaranteed confidentiality.

"We basically looked at two approaches," says Nathan Van de Velde (iMinds - KU Leuven). "On the one hand, we laid the legal foundation for a platform that includes the exchange of personal data to share info on fraud incidents; for this approach, we're currently ascertaining whether there is political backing for the proposed platform. The other path we explored makes use of an existing platform that does not leverage personal data; here, we restricted ourselves to conducting a platform audit."

2. A requirements document that helps banks prepare for upcoming legislative changes in the digital domain

As a second legal research track, a requirements document has been developed that helps financial institutions assess the impact of – and prepare for – upcoming legislative changes in the digital domain. Examples of such legislative changes include the General Data Protection Regulation (GDPR) framework (which intends to strengthen and unify data protection for individuals within the European Union), the updated Directive on Payment Services (which provides the legal foundation for the creation of an EU-wide single market for payments) and the updated Anti-Money Laundering (AML) directive.

3. The analysis and development of security metrics for safer web-based communications

Since the Internet is one of the main vehicles to get access to financial institutions' digital services, TRU-BLISS analyzed and developed a number of security metrics for safer web-based communications, including:

- A document that recaps today's security best-practices (as well as their soft spots).
- A website vulnerability tool that automatically and continuously tests financial institutions' websites against a number of security parameters; the results are visualized in a dashboard that reflects potential weaknesses; as such, the tool allows banks to benchmark their web security posture against the European and global average and to follow up on improvements.
- A holistic internal defense approach against 'Advanced Persistent Threats'; the TRU-BLISS approach includes a state-of-the-art analysis of the APT problem, a reference architecture for near real-time analysis of internal network data (using rule, blacklist and anomaly-driven detection), and an operational prototype of this architecture.

NEXT STEPS

One important next step will be the implementation of the interbank risk warning system that leverages personal data, following the buy-in from the Belgian privacy commission.

A second question is how the TRU-BLISS web tools can be kept up-to-date (to include the latest threats and technologies), and how it could be made available to all financial institutions (and potentially even to other businesses in totally different sectors).

"TRU-BLISS has been a real first: it was actually the first time that Belgium's largest banks collaborated with academic researchers in a formal research project. And this is more disruptive than it may sound; after all, collaborating on security is not a trivial thing to do – as it involves sharing highly sensitive data. Yet, TRU-BLISS has shown that we are able to flexibly cope with the stakeholders' various requirements. I think this project has laid the foundation for further collaboration between academia and the financial sector," concludes Nathan Van de Velde.

FACTS

NAME	**TRU-BLISS**
OBJECTIVE	Helping financial institutions cope with the digital era's security threats
TYPE	ICON project
DURATION	01/04/2014 – 31/03/2016
PROJECT LEAD	Patrick Wynant, Febelfin
RESEARCH LEAD	Peggy Valcke & Nathan Van de Velde, iMinds - CiTiP - KU Leuven
BUDGET	3,755,000 euro
PROJECT PARTNERS	Belfius, Belgian Internet Service Center (BISC), BNP Paribas Fortis, DNS Belgium, Febelfin, Federal Computer Crime Unit (FCCU), KBC, ING
IMINDS RESEARCH GROUPS	COSIC - KU Leuven Distrinet - KU Leuven CiTiP - KU Leuven

WHAT IS AN

ICON PROJECT?

iMinds is the digital research center and business incubator for Flanders, Belgium. Its ICON research projects are agile and demand-driven, combining academia and industry partners. ICON projects typically have a duration of two years, yet quickly adapt to the rapidly-evolving digital landscape. ICON partners intend to use the project results in their products or services.

TRU-BLISS project partners:

Belfius · BNP PARIBAS FORTIS · dnsbelgium · FCCU · febelfin · Federale Overheidsdienst FINANCIEN · ING · KBC