Ronald Kelson
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

Benjamin Gittins
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

Synaptic Laboratories Ltd.
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Thursday, 28 January 2010

PART 5 OF SYNAPTIC LABORATORIES LIMITED INPUT TO THINK-TRUST's CONSULTATION ON THEIR DRAFT "D3.1B RECOMMENDATIONS REPORT" TO THE EUROPEAN COMMISSION

The need to evaluate the effectiveness of data depersonalization techniques and it's impact on the community; and

Measuring the wider impacts of unauthorised information disclosure, the loss of data integrity and lack of system availability/responsiveness so as to guide resource management and improve EU marketplace international competitiveness.

1. The need to evaluate the effectiveness of data depersonalization techniques and it's impact on the community

Pseudo-anonymity and true anonymity are core themes that run through the text of T-T D3.1b.

Of critical importance is establishing a comprehensive framework for measuring data depersonalization (also called data anonymisation in section 4.4 of T-T D3.1b), in all its forms, and then reviewing the effectiveness of existing and proposed techniques.

Without an objective benchmark, how can the EU community be sure that privacy enhancing technologies are effective?

For this reason, it is important to survey data depersonalization techniques currently used by the civilian industry and establish to what extent they are effective.

We need to assess the positive and negative impacts of the resale of this depersonalized data in the community.

Most critically we need to study the way consumers of depersonalized data use the information and specifically evaluate if they are able to re-personalise the data in meaningful ways that undermine the objectives of de-personalization. If the depersonalization techniques are not adequate to protect identity (before or after sale), we need to identify what techniques and what parameters are appropriate for commercial data depersonalization and what limitations must be placed on those who consume/use depersonalized data.

Synaptic argues that after adequate open international peer review, there is a need to enforce effective techniques and parameters across the entire life cycle of depersonalized data as Government policies. Furthermore, this review process should be continuous and accumulative so that new and improved data mining techniques, and adaptive behaviors of the data-consumers, can be monitored and compensated for.

Synaptic advanced these issues at the US National Cybersecurity Summit and consequently they were advanced to be included in the Summit's deliverable, the Summit Participants Idea Report. That Report has been used as input the US Administrations cybersecurity planning. See Appendix A1 for a short action plan as written up in the US Summit Participants Idea Report on these issues.

2. Measuring the wider impacts of unauthorised information disclosure, the loss of data integrity and lack of system availability/responsiveness

We quote the following requirement stated in section 4.10 of T-T D3.1b:

> *"There should be constant engineering vigilance about economic viability. Is it more cost-effective to prevent a data breach or just address the consequent damage when one occurs?"*

This raises the question: what is the impact of data breach to the individual?

The US have defined an extensive "Information Assurance Risk Management Framework" to assess IA risks arising from information systems, prioritize those risks, implement security controls to mitigate the risks and meet their information assurance priorities, assess the operational performance and effectiveness of those controls, and maintain the appropriate level of trust that enables the sharing of national security information with other enterprises. *For more information on the comprehensive American risk frameworks, see CNSS Policy No. 22, FIPS 199, FIPS 200, FIPS SP 800-53, CNSSI-1253 and FIPS SP 800-60 as starting points.*

This comprehensive framework attempts to ensure that the security controls applied to a particular information system are commensurate with the potential adverse impact on organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

There are three potential impact levels: low, moderate, and high.

A fair amount of human judgement is required to correctly classify the potential impact levels to each risk.

For example, in US national security systems, the definition of low potential impact is: if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States. (Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.) The potential impact is defined as High if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States.

These frameworks are excellent and should be applauded, promoted and adapted so they are most suitable for wider adoption outside of US Federal Systems. This appears to Synaptic to be an area where EU and US can collaborate with mutual benefits.

This said, and without detracting from the value of the existing work, we argue that insufficient data exists to enable an organisation to accurately establish the value of information loss to stake-holders, including customers and clients. Without such information it is not possible to make an informed decision about the necessary level of security mechanisms required. Without this information, decisions are made on personal and subjective opinions which may not accurately reflect the perspective of the full stake-holder community. This is an area that can be improved with potentially great rewards for the global community.

Large scale field studies are required to establish the value of information loss with respect to different classes of data including financial, medical, intellectual property, relationship information and geolocation of time for different groups including Enterprises, SME, and individuals.

These studies must be considered in a global context. Simple services provided in one country (Such as web email services hosted by Google) may be used for sensitive purposes (such as communications between human rights activists) and have serious ramifications if security mechanisms fail.

These studies can be extended to assess the financial and emotional impact of down-time or availability of access to services[1]. For example how does a call center establish the financial impact on the wider community for a given average wait time of *x* minutes before reaching a human on the other end of the line? Is it appropriate to achieve 100% loading on call centers staff to maximize profits for share holders at the expense of people on the end of the line? **Can EU norms be set to ensure a level playing field inside EU and in a way that optimizes the overall efficiency and international competitiveness of the European marketplace?**

A greater understanding of the value of different types of information, as held by the different portions of the community, can inform those responsible for managing that information on behalf of others so that appropriate risk management strategies can be put in place. (See section A.7 of the Appendix in this document for more information on our proposal submitted to the US NITRD).

Synaptic advanced these issues at the US National Cybersecurity Summit and consequently they were advanced to be included in the Summit's deliverable, the Summit Participants Idea Report. That Report has been used as input the US Administrations cybersecurity planning. See Appendix A2 for a short action plan as written up in the US Summit Participants Idea Report on these issues.

[1] Modern risk assessment techniques such as those proposed in the paper by Aissa, Anis Ben, Abercrombie, R.K., Y., Sheldon, F.T. and Mili, Ali called "*Quantifying Security Threats and Their Impact: Theory and Practice*" published in Innovations in Systems and Software Engineering, Springer London, ISSN 1614-5046 (Print), ISSN 1614-5054 (Online) that takes into account all stake holders might be adapted to the task.

3. Synaptic's recommendations to Think-Trust

We argue that D3.1B should strongly point to the need for the studying the effectiveness of existing data depersonalization techniques, to identity ways in which depersonalization may be being re-personalized by corporations, and to propose a framework for a) appropriate methods for data depersonalization by providers, b) guidelines and limitations on how depersonalized data can be used by its consumers to prevent re-personalization, c) continual monitoring and improvement.

We argue that D3.1B should strongly point to the need for the studying the wider impacts of unauthorised information disclosure, the loss of data integrity and lack of system availability/responsiveness as a deliverable that will feed into the assessment of appropriate risk management technologies and resource management for information processing systems.

See the two appendixes for further recommendations.

END

APPENDIX

A1. Evaluating the effectiveness of data depersonalization techniques and it's impact on the community

Author: Benjamin GITTINS (Synaptic Laboratories Limited)

Found in the "National Cyber Leap Year Summit 2009: Exploring Paths to New Cyber Security Paradigms Draft Report" (http://www.co-ment.net/text/1451/) and published in official the "National Cyber Leap Year Summit 2009 Participants Idea's report" (http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Participants_Ideas_Report.pdf)

Description - Establish if data depersonalization techniques used by the civilian industry are effective and assess the impacts of re-sale of depersonalized data in the community. Study the way consumers of depersonalised data use the information. If the depersonalization techniques are not adequate to protect identity (before or after sale), identify what techniques and parameters are appropriate for commercial data depersonalization. After adequate peer review, enforce these techniques and parameters as Government policies.

Inertia - Commercial interests for selling data / Poor community-wide awareness of the risks associated with sale of personal data collected by organisations.

Progress - Several papers have identified that it is possible to identify the persons present in some depersonalized data released by large organisations.

Jumpstart Activities - Collect a large representative sample of commercial exchanged depersonalised data (find data sold by a large online commercial store, and a mobile phone provider selling location data), bring together experts in the field to evaluate how easy it is to re-personalise the data, bring together legal team to evaluate the implications of data that is not effectively disassociated from the user. Compile any changes required to law.

Action Plan - Identify the security and legal experts / acquire large representative data sets of the type of information sold / start a conference and advance it with funding.

Who can help - NITRD, US State Department, Electronic Freedom Foundation, Jeff Jonas of IBM, weak signal analysis, other published researchers in this field.

A2. Measuring the wider impacts of unauthorised information disclosure

Author: Benjamin GITTINS (Synaptic Laboratories Limited)

Found in the "National Cyber Leap Year Summit 2009: Exploring Paths to New Cyber Security Paradigms Draft Report" (http://www.co-ment.net/text/1451/) and published in official the "National Cyber Leap Year Summit 2009 Participants Idea's report" (http://www.qinetiq-na.com/Collateral/Documents/English-US/InTheNews_docs/National_Cyber_Leap_Year_Summit_2009_Participants_Ideas_Report.pdf)

Description - Methodologies for Evaluating appropriate security controls based on the confidentiality, integrity and availability of IT systems now exist. However insufficient information exists to allow an organisation to establish the value of information loss to stake-holders, including customers and clients. Without such information it is not possible to make an informed decision about the necessary level of security mechanisms required.

Large scale field studies are required to establish the value of information loss with respect to different classes of data including financial, medical, intellectual property, relationship information and geolocation of time for different groups including Enterprises, SME, and individuals. Such studies could be extended to assess the financial and emotional impact of down-time or availability of access to services.

A greater understanding of the value of information managed by others, and its management, by the stake holders can better inform organisations on how to manage their IT infrastructure and risks.

Inertia - Commercial interests for selling data / Commercial interests to maintain 'just-enough' security to protect against legal liability. There is little incentive for organisations to identify the true cost of security breaches against individuals.

Progress - Technologies exist which can be used to collect this information.

Jumpstart Activities - Identify the financial, social sciences, security and legal experts. Develop a set of questions to measure metrics on. Engage many universities and some organisations to perform surveys and collect the data. Process the data publish reports and set metrics for depersonalisation standards.

Action Plan - Identify interested financial, social sciences, security and legal experts. Develop action plan and secure funding. Perform studies in hospitals and other medical practices.

Who can help - NITRD, CyberSpace Sciences and Information Intelligence Research - ORNL - DoE, RTI International, Universities, EU Think Trust.

About Think Trust

Think-Trust (T-T) (www.think-trust.eu/) is an F5 Coordination Action under Framework Program 7 (FP7) Challenge 1, Objective ICT-2007.1.4 – Secure, Dependable and Trusted Infrastructures. T-T has been allocated the task of helping to coordinate the response to the needs of a trustworthy ICT future in Europe, through working groups, surveys and consultations resulting in Reports with recommendations and priorities about what needs to be done. Its target audience is the European Commission and policy-makers responsible for future direction, strategies, and priorities for European ICT. T-T deliverables complement the RISEPTIS (Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society [2]) work by providing feedback on priorities based upon input from their various activities and input from the perspective of participants in the European ICT Framework Programme. T-T has completed and published a Report entitled "Recommendations Report" D3.1a [3] and has provided to Synaptic Laboratories Limited a draft of D3.1b for our input prior to its publication. This document forms Part 1 of Synaptic Laboratories Limited input to D3.1b.

About Synaptic Laboratories Limited

Synaptic Laboratories Limited is developing the next generation of secure communications products and protocols to protect global communication networks. Synaptic is guided by a vision of "Long term, high-assurance global data security for all stake-holders".

Synaptic drives data security through the development of innovative security technologies founded on well studied cryptographic techniques. Synaptic can be found on the Web at http://synaptic-labs.com

The Synaptic CTO has been the guest speaker on post quantum security **without the use of quantum cryptography** for three consecutive years at the World Smartcard and Electronic Identification Congress CARTES held each year in Paris, FRANCE.

Synaptic responded with three submissions to the public calls for new 'leap ahead' cybersecurity proposals issued by the US Government's Networking and Information Technology Research and Development Program (NITRD).

Consequently Synaptic Laboratories CTO was formally invited to attend their 'closed' by invitation only' National Cyber Leap Year Summit. The Summit brought together government, industry and academia including the USA's leading innovators to identify requirements and proposals for next generation cyber security solutions. Several Synaptic proposals were taken forward at the Summit.   At this Summit Synaptic also actively promoted SecureIST and ThinkTrust deliverables, and consequently Think-Trust is referenced by name along with Synaptic authored proposals in the Summit Participants Idea Report. This Report has been fed as input into the US Administration's cybersecurity planning. More on the Synaptic participation in the US Cybersecurity Initiatives can be found here[4].

Through its participation in US cybersecurity initiatives Synaptic Laboratories Ltd. acts as a bridge to promote European ICT research and planning projects, such as Think-Trust, to an extensive and influential audience in the USA. At the same time we seek to promote the US cybersecurity initiatives and their outcomes in Europe at every opportunity, for example in our presentations at the CARTES World Congress. Our objective is to encourage and accelerate international collaboration in cybersecuriy initiatives with a focus upon globally scalable identity management and cryptographic key management that offers long term assurance (without requiring the use of quantum cryptography) even into the quantum future.

[2] http://www.think-trust.eu/riseptis.html

[3] http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html

[4] http://media.synaptic-labs.com/downloads/pub/publications/NCLY/20091115-NCLY-Summit2009-Participants_Ideas_Report-Extracts.pdf