

Input to the Commission on Enhancing National Cybersecurity

Submission date: September 6, 2016

Joint submission made by: **Benjamin Gittins**
Chief Technical Officer
b.gittins@synaptic-labs.com
+356 9944 9390

Ronald Kelson
Chief Executive Officer
r.kelson@synaptic-labs.com
+356 9944 9390

Synaptic Laboratories Ltd.
www.synaptic-labs.com
13 Nadur Heights,
Nadur NDR-1390,
MALTA, Europe

Designers of safe and secure computing and communication architectures. Developers of general-purpose soft IP for FPGA devices, to increase security and performance, and to reduce circuit area.

Topic of this submission:

Significant Progress In The Design Of Backwards Compatible Trustworthy and Dependable computing: Synaptic Labs' Trustworthy resilient universal Secure Infrastructure Platform (TruSIP) platform

RFI topic areas this submission relates to:

- Cybersecurity Research and Development
- Critical Infrastructure Cybersecurity
- Identity and Access Management
- Internet of Things
- International Markets

Input submission contents:

(1) A 1 page executive summary for this comment, in the format requested by the RFI, which “identifies the topic addressed, the challenges, and the proposed solution, recommendation, and/or finding.” Citations in the Executive Summary map back to the references listed at the end of the 30 page document attached to this submission. We have inserted headings that match these points in the executive summary.

(2) A supporting 2 page statement: Brian Snow, “Statement on Synaptic Laboratories Ltd.” (2011) which specifically expresses support for advancing the TruSIP architecture.

(3) A 31 page document: B. Gittins, R. Kelson, “OPEN AND CAPTURE VAST NEW MARKETS BY IMPROVING CYBER SECURITY in practically all systems, including embedded micro, industrial control and public clouds. — Introducing Synaptic Laboratories Limited advanced proposal for a Trustworthy resilient universal Secure Infrastructure Platform (TruSIP) that will support today’s processor instruction sets, operating systems, middleware and business and mission critical software”, 22 May 2012, Synaptic Laboratories Limited. (The URL’s have been updated in 2016)

**Significant Advances in backwards compatible Trustworthy and Dependable computing:
Synaptic Labs' Trustworthy resilient universal Secure Infrastructure Platform (TruSIP)**

1 Page Executive Summary

RFI Topics: Cybersecurity Research and Development, Critical Infrastructure Cybersecurity, Identity and Access Management, Internet of Things, International Markets)

Progress being made: TruSIP offers to revolutionise the Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) markets that were already valued at USD \$20+ billion per annum in 2010. TruSIP will do this by resolving trust and privacy problems identified by ENISA, DARPA and NIST that currently prevent organisations from moving vast amounts of sensitive operations from private systems to public and government clouds. **TruSIP is designed to prevent the public cloud provider and their hardware and software suppliers from maliciously or unintentionally learning or exposing the value of the cloud client's data, even though the data is being processed in the cloud. That is, it protects against malware hidden in the hardware and software employed in the cloud infrastructure. TruSIP can also be used to create community clouds for finance, defence, etc. TruSIP will be suitable for critical infrastructure and industrial control systems as it extends our "Safe and Secure Real-time" (SSRT) computing architecture which is currently being advanced.** Altera / Intel PSG is a collaborator on our SSRT project: <http://tinyurl.com/MCF-SSRT>.

Synaptic Labs' designs for TruSIP, have been independently reviewed by world class computer security and survivability specialists working in Government, industry and academia, including: Brian Snow (for 12 years a Technical Director of the U.S. National Security Agency (NSA R&D, NSA IAD, NSA ADDET), Miles Smid (former acting Chief of the U.S. NIST Computer Security Division), Dr. Santosh Chokhani (has advised the U.S. State Department, U.S. NIST and U.S. NSA on public key infrastructure), Dr. Axel Krings (Professor of Computer Science, University of Idaho; fault-tolerant and survivability expert with more than 100 peer reviewed scientific publications) and Dr. Richard R. Brooks (Associate Professor of Electrical and Computer Engineering, Clemson University; specialist in secure survivable systems and side channel attacks).

TruSIP provides clients and stakeholders with increased privacy and integrity assurances against many external attacks AND insider attacks. It is designed under the explicit assumption that every software and hardware module in the TruSIP deployment has a latent vulnerability and/or embedded malware. TruSIP achieves resilience against potentially devastating insider attacks that could be instigated by the cloud provider, their staff, and even by the cloud's hardware and software suppliers against both the clients and the cloud deployment itself. TruSIP is resistant to internal or external malicious code attacks that are implemented directly in, or exploit unknown vulnerabilities latent in, the software and hardware employed in implementing that cloud infrastructure. TruSIP will offer a range of security controls against external network facing and internal physical side-channel attacks. TruSIP will harden existing client applications running on TruSIP to resist external code-injection attacks that exploit buffer overflows. TruSIP will also offer security controls for clients against their own insider attacks. TruSIP provides the public cloud system provider and administrators greater assurance of safe and reliable cloud operation plus legitimate protection against misplaced assertions, made by clients or stakeholders, that the cloud provider has mishandled or compromised client data. At its heart, TruSIP employs a variety of physical and logical security controls in a system of "**separation of powers**" and "**checks and balances**" to prevent a malicious insider exploiting their privileged position to learn or corrupt the value of client's data. More information on our TruSIP proposal is found in the document included with this submission.

The recommendation: We respectfully propose that the Commission's detailed recommendations to strengthen cybersecurity should include the following points:

1. Perform an in-depth survey to identify, catalogue and evaluate the viability of all candidate next-generation computing solutions that are credibly trustworthy and dependable in multi-jurisdiction, multi-stakeholder Internet-scale environments that can be incrementally deployed to protect existing security software while permitting the transition to higher levels of security assurance and improved capabilities. This should be easy to perform as there are very few high-assurance computing platforms to evaluate.
2. Perform a high-level security aware Failure Mode and Effects Analysis of today's computing architecture that considers the impact of identified security flaws wrt. the stakeholders in multi-jurisdiction, multi-stakeholder Internet-scale environments. Quantify the costs to the global community of those security flaws. Quantify the returns of developing a "fit for purpose" high-assurance computing platform. Fund the top 7 candidate next-generation computing solutions that are credibly trustworthy and dependable, ensuring sufficient diversity between the research agendas / techniques. Ensure equal access and adequate support for (and team building around) innovative small-to-medium sized enterprises.

Sincerely, Benjamin Gittins and Ronald Kelson.

Statement on Synaptic Laboratories Ltd. by Brian Snow
Independent Security Consultant
Former US NSA for 35 years including Technical Director for 12

23 July 2011

Brian Snow has worked as an independent security consultant for Synaptic Laboratories Limited over several years. He has studied the TruSIP design and has approved his following statement for public release:

“In my career at NSA developing secure equipments for government use, whether built by NSA, or built under contract to NSA by commercial firms, or by reviewing commercial products and recommending changes that might make them more suitable for government work, I was frequently depressed by how hard it was to get the design teams to FIRST address the primitives needed to support the security architecture, THEN address the other features and controls needed to interface with non-secure equipments or human users. It really does make a difference!

When security is involved, "He who gets to the interface first, wins" is true, and it REALLY matters.

Synaptic Laboratories Ltd. is one of those rare firms that really tries to address security issues FIRST, as the principal driver of their products. It gives them a "leg up" on getting the overall architecture right. Or if not perfectly right, certainly closer than those who first design around marketable user features, then try to tack on security as an after-thought.

The approach has obvious value in their current TruSIP design effort. It is clear as to what they are about, the content appears sound and it is obvious how each component "fits" in a security sense into the overall architecture. This is work that many other firms shun or slight, but it IS necessary. Their basic approach is directly relevant to Governments and/or any commercial companies that deploy products that must function correctly in high-risk environments (that is, facing targeted malice).

Evaluating products to ascertain they can meet security goals in various environments is never easy; but, in my experience, by addressing security first in design efforts, an evaluation will ALWAYS go more smoothly than an evaluation for a product that tries to meet the same security goals, but does not address security FIRST in its design process.

Synaptic Laboratories has a sound design process; this design approach and TruSIP need to be championed and moved forward to actual products.”

"Brian Snow has done more than anyone I know for national security," Prof. Richard Ford, Director of the Harris Institute for Assured Information, Florida Institute of Technology.

Brian Snow BIO

Mathematician/computer scientist, Brian taught mathematics and helped lay the groundwork for a computer science department at Ohio University in the late 1960's. He joined the National Security Agency (NSA) in 1971 where he became a cryptologic designer and security systems architect.



Brian spent his first 20 years at NSA doing and directing research that developed cryptographic components and secure systems. Many cryptographic systems serving the U.S. government and military use his algorithms; they provide capabilities not previously available and span a range from nuclear command and control to tactical radios for the battlefield. Computer Security, Network Security and strong Assurance were major aspects for these systems. He created and managed NSA's Secure Systems Design division in the 1980s. He has many patents, awards, and honors attesting to his creativity.

His later years at NSA were the model for what it means to be a senior Technical Director at NSA (similar to a Chief Scientist or Senior Technical Fellow in industry); he served in that capacity in three major mission components –

- The Research Directorate (1994-1995),
- The Information Assurance Directorate (1996-2002), and
- The Directorate for Education and Training -- NSA's Corporate University (2003-2006)

He was the first Technical Director appointed at the "Key Component" level at NSA, and the only "techie" at NSA to serve in such a role across three different Directorates. Throughout those years, his Credo was:

*"Managers are responsible for doing things right;
Technical Directors are responsible for finding the right things to do."*

Brian Snow recently had an honor bestowed on him; he is now a "Distinguished Member of the Cryptomathematics Institute (CMI)" at the NSA (2011).

Brian Snow's contact details: briansnow@comcast.net +1-301-854-3255



SYNAPTIC LABORATORIES LTD.

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.
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com
www.ictgozomalta.eu

OPEN AND CAPTURE VAST NEW MARKETS BY IMPROVING CYBER SECURITY *In practically all systems, including embedded micro, industrial control and public clouds*

Introducing Synaptic Laboratories Limited advanced proposal for a Trustworthy resilient universal Secure Infrastructure Platform (TruSIP) that will support *today's* processor instruction sets, operating systems, middleware and business and mission critical software

“The TruSIP design is innovative ... and should be realisable in practice.”

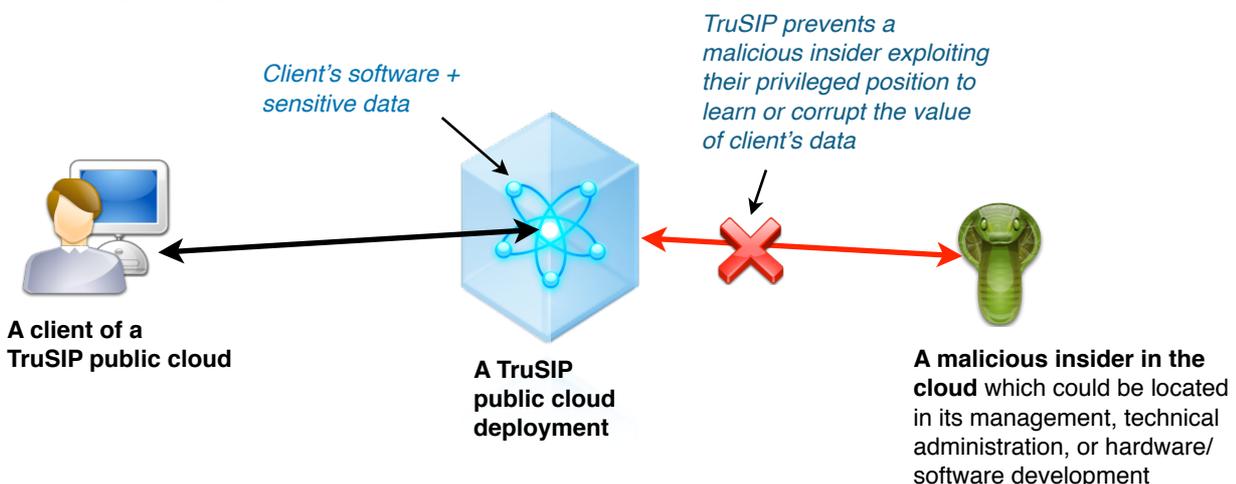
– Independent review team (details in Appendix A3)

“Based on the information provided [Ed: in V0.12 of this document] it looks like a proposal around your TruSIP technology would be in scope as a response to this BAA.”

– [DARPA-BAA-11-55](#), Mission-orientated Resilient Clouds (see A5.1)
(<https://www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-BAA-11-55/listing.html>)

Contents:

- 1 page synopsis
- 3 page introduction
- On page 6 - the Table of Contents for the Appendices
- 21 pages of Appendices containing supporting information and fact sheets
- 3 page bibliography with 93 citations



One page SYNOPSIS of Synaptic Labs' trustworthy computing proposal

Synaptic Labs is a micro research and development company with collaborators spanning a US National Laboratory, US Government security advisers, specialist technology companies and academic experts. Synaptic Labs is seeking a global partner for Government funding applications and for development and global commercialisation of our proposed (backwards compatible) *universal* fault tolerant computing architecture, called the **Trustworthy robust universal Secure Infrastructure Platform (TruSIP)**.

TruSIP satisfies *current EC, UK and USA Government (funded) Calls to unlock new global markets* by resolving a range of hard, high priority, system wide security problems identified by Government and industry, in domains ranging from real time embedded micro, critical infrastructure through to public cloud computing.

Example - public cloud computing: TruSIP offers to *revolutionise* the Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) markets that were already valued at USD \$20+ billion per annum in 2010 *by enabling* public cloud providers to deliver security controls that far exceed those that SME's can achieve with today's *private* cloud technologies. Widespread adoption of cloud computing has the potential to generate over €763 billion of cumulative economic benefits and hundreds of thousands of new jobs over the period 2010 to 2015. In 2010 the Centre for Economics and Business Research (CEBR) cautions that the full shift to cloud computing may not happen if perceptions in relation to security and resilience-related aspects of cloud computing solutions deteriorate. In a 2009 survey by InformationWeek Analytics, 53% of organisations that have NOT adopted the cloud cited confidentiality and security related issues as their primary concern. *TruSIP is designed to address those concerns by preventing the public cloud provider and their hardware and software suppliers from maliciously or unintentionally learning or exposing the value of the cloud client's data. TruSIP can also be used to create community clouds for finance, defence, etc.*

Example - large system of systems: TruSIP is designed to cost effectively address currently unmet, *end-to-end* security, availability and reliability needs in large system-of-system projects (such as smart grids and other critical infrastructures, medical & financial systems, defence, B2B, ...) *by combining the resilience, reliability and availability of safety systems with the access and security controls of ICT systems within one unified ubiquitous computing architecture* e.g. TruSIP enabled clouds will run in high availability and integrity modes to meet fail-safe requirements. Likewise, TruSIP enabled industrial control devices will satisfy ICT confidentiality and access control requirements. TruSIP is designed to protect against insiders, kill switches and code injection attacks that exploit buffer overflows. Clearly, TruSIP has the potential to revolutionise the critical infrastructure protection industry and realise Secure and Resilient Financial Transaction Systems.

TruSIP is universal: Variants of **TruSIP will support today's processor instruction sets, operating systems, middleware and business and mission critical software.** *Software* variants of TruSIP are targeted for use on commercial-off-the-shelf smart cards and hardware security modules. *Hardware* variants of TruSIP are designed to implement trustworthy and dependable sensors, actuators, programmable logic controllers, industrial control systems, embedded micros, network routers, tablets, workstations, Infrastructure as a Service and Platform as a Service clouds (when implemented in FPGA and 3D ASIC).

TruSIP has been designed to achieve efficiency and cost effectiveness: Even with confidentiality, integrity and availability controls in place, **TruSIP in hardware will execute client tasks only a little slower than unsecured computation.** TruSIP in software will match the performance restraints of smartcards.

Validating universality and backwards compatibility: Synaptic Labs is working with leading technology companies to validate and ensure that TruSIP can cost effectively enhance and support their existing technologies and products. TruSIP is expected to enable rapid growth of their respective markets and market share by removing major barriers to market uptake, for example, of public cloud computing.

Independent Security Review: The core TruSIP proposal has been independently reviewed by world class computer security and survivability specialists working in Government, industry and academia (appendix A3).

TruSIP, formal methods, safety and security compliance: Synaptic Labs' has been independently advised that the high-level architecture of the TruSIP proposal is suitable for targeting high IEC 61508 Safety Integrity Levels (SIL). Synaptic Labs' goal is to develop TruSIP using formal methods (such as the B-Method). Synaptic Labs' seeks to simultaneously achieve the highest IEC 61508 Safety Integrity Level (SIL) and Common Criteria (CC) Evaluation Assurance Level (EAL) certifications on implementations of our TruSIP proposal. **END SYNOPSIS.**

3 page INTRODUCTION to Synaptic Labs' trustworthy computing proposal

Synaptic Labs (see appendix A1) is a micro research and development company with collaborators spanning a US National Laboratory, US Government security advisers, specialist technology companies, and academic experts. We are seeking a development and global commercialisation partner for our proposed new (backwards compatible) *universal* fault tolerant computing architecture, called the **Trustworthy robust universal Secure Infrastructure Platform (TruSIP)**. TruSIP is designed to unlock new global markets by resolving a range of hard, high priority, system wide security problems identified by Government and industry in domains ranging from critical infrastructure through to public and government cloud computing (see appendix A6). TruSIP is universal because the one design can ubiquitously meet the needs of fail-safe high-availability embedded micro systems, all the way up to high performance computing servers, including systems-of-systems such as smartgrids (see appendix A7).

Example application - public cloud computing: TruSIP offers to *revolutionise* the Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) markets that were already valued at USD \$20+ billion per annum in 2010 (see appendix A12). TruSIP will do this by resolving trust and privacy problems identified by ENISA, DARPA and NIST that currently prevent organisations from moving vast amounts of sensitive operations from private systems to public and government clouds (appendix A7). In one sentence, TruSIP is designed to prevent the public cloud provider and their hardware and software suppliers from maliciously or unintentionally learning or exposing the value of the cloud client's data, even though the data is being processed in the cloud. TruSIP can also be used to create community clouds for finance, defence, etc.

TruSIP will capture new markets by enabling public cloud providers to deliver security controls that far exceed those that SME's can achieve with today's private cloud technologies, thereby *overcoming barriers* to public cloud take up, *delivering* lower ICT capital and recurrent costs for users, including *lightening* the ever increasing complexity and security burden cost on SME's. Clearly, these TruSIP project goals far exceed those of the currently active EU FP7 - IBM - TClouds (€10.5 m) project (see comparison in appendix A11.1).

Potential Benefits in Public Cloud Market: In 2010 the Centre for Economics and Business Research (CEBR) found that across France, Germany, Italy, Spain and the UK, widespread adoption of cloud computing has the potential to generate over €763 billion of cumulative economic benefits and hundreds of thousands of new jobs over the period 2010 to 2015 [1]. Andrew Moloney, a director of the U.S. based IT firm EMC (ranked 152 in the Fortune 500) which commissioned the study, says:

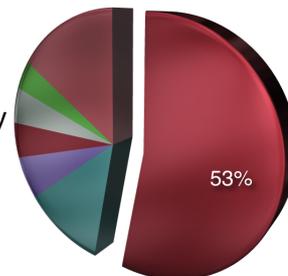
"70 percent of the time in IT departments is spent on keeping the lights on as opposed to innovating and driving new business models." ... "Cloud computing is unlocking that capability." [2]

CEBR predicts that, if public perception remains positive, we could see the current 20% business workload in (public and private clouds) grow to 100% by 2014 on account of the cost savings and increased productivity [3]. For example, CEBR estimates that businesses moving from a standard computing environment to a full public cloud computing environment could see an impressive 39.9% savings in total IT capital expenditure budgets [3].

However, CEBR cautions that the full shift to cloud computing may not happen if **perceptions in relation to security and resilience-related aspects of cloud computing solutions deteriorate** [3]. According to a 2010 report, IDC (a global market intelligence firm) predicts that security controls will be required to protect over 90% of all files and folders in the Digital Universe by 2020 [4]. Failing to protect that data can hurt the bottom line. According to a 2010 study by the Ponemon Institute, the total annualized cost of cyber crime (for a benchmark sample of 45 organizations) ranged from a low of \$1 million to a high of nearly \$52 million [1]. The Institute estimates that the recent 2011 Sony data breaches may cost the company USD ~1.5 billion from a product division with a USD ~500 million annual profit [81].

Governments and businesses are increasingly looking for assurances that the clouds are trustworthy. According to an ENISA report, administrator roles in today's cloud architectures expose cloud customers to extremely high risk [2]. ENISA says these *insider attacks* have a *Medium* probability of occurrence and will have a *Very High* negative impact on stakeholders [2]. As demonstrated by the 2010 **Google privacy breach**, even highly visible insider attacks that deface customers accounts can go on, undetected by a public cloud provider for months [5]. In fact it required several clients to notify Google that insider attacks were being instigated by a Google employee [5]. Discretely executed insider attacks focused solely on the unauthorised duplication of client's data/intellectual property are self evidently *much harder* to detect by the cloud provider or customer.

DARPA pointed [86] to a research report on Cloud Governance, Risk and Compliance [84] by InformationWeek Analytics (July 2009) where 38% of respondents (208 out of 548 surveyed) said that they would **not** use the cloud. Of those 208 who would not use the cloud, **53%** cited security related issues. Security concerns dominate both cloud adopters and non-adopters with **“... 51% of CIOs surveyed ... cited security as their greatest concern surrounding cloud adoption”** as reported in a keynote transcript at the RSA conference March 2010 [85]. See appendix A13 for more information.



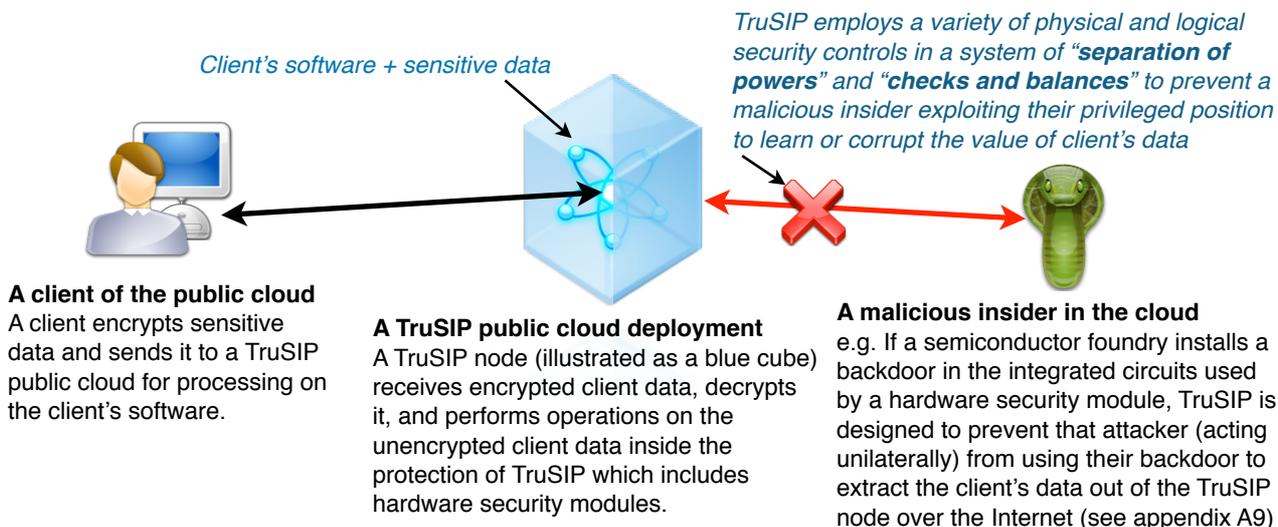
Dr. Howard Shrobe, Program Manager for the pending DARPA-BAA-11-55 I2O Mission Orientated Resilient Clouds project argues **“Clouds are concentrated Vulnerability Amplifiers”** because they are monocultured, have huge concentration of hosts on high speed network without internal checks, have implicit trust among hosts, they have resource sharing and co-residence of unrelated computations, are an obvious target, are vulnerable to activity monitoring and other types of side-channel attack vulnerabilities [86]. **TruSIP is explicitly designed to address the above security problems and more, to enable public clouds that are safer than today’s private clouds** (see appendix 5a).

“It’s not about security, its about Trustworthiness of our digital infrastructure. This means Security and Reliability, Resilience, Privacy and Usability.”

– Dr. Jeanette Wing, Assistant Director for Computer & Information Science and Engineering, U.S. National Science Foundation. Spoken at the NITRD 2010 webcast event [6].

TruSIP is designed from the ground up as a cryptographic project exploiting existing security standards, to **capture and unlock the true potential of the cloud market, by delivering the missing security controls** required to enable individuals and organisations to make the transition from hybrid clouds to public clouds:

- TruSIP provides clients and stakeholders with increased privacy and integrity assurances against many **external attacks AND insider attacks**. It is designed under the explicit assumption that every sw/hw module in the TruSIP deployment has a latent vulnerability and/or embedded malware. TruSIP achieves resilience against potentially devastating insider attacks that could be instigated by the cloud provider, their staff, and even by the cloud’s hardware and software suppliers against both the clients and the cloud deployment itself. TruSIP is resistant to internal or external **malicious code attacks** that are *implemented directly in, or exploit unknown vulnerabilities latent in, the software and hardware employed in implementing that cloud infrastructure* (see also appendix A7). TruSIP will offer a range of security controls against external network facing and internal physical side-channel attacks. TruSIP will harden existing client applications running on TruSIP to resist external **code-injection attacks** that exploit buffer overflows. TruSIP will also offer security controls for clients against their own insider attacks.
- TruSIP provides the public cloud system provider and administrators greater assurance of safe and reliable cloud operation plus legitimate protection against misplaced assertions, made by clients or stakeholders, that the cloud provider has mishandled or compromised client data.



TruSIP efficiency and cost effectiveness: Synaptic Labs has completed significant design work on the TruSIP proposal (see appendix A10), including identifying techniques to increase efficiency, control cost and ensure universality of application (see appendix A8). By way of a single data point comparison, the U.S. Defense Advanced Research Projects Agency's (DARPA) PROCEED project [7] seeks to improve secure computation in un-trusted servers/clouds by a factor of 10+ million times, to achieve a result that will *still* be 100,000x times *more* computationally expensive than conventional unencrypted processing [8]. TruSIP's alternate approach to achieving security in the cloud requires only ~2.5x to ~3.5x more computational effort (for fail-safe and non-stop solutions respectively) when implemented in hardware (see appendix A8.1).

TruSIP in hardware will execute tasks only marginally slower than an unsecured computation (see appendix A8.2). TruSIP in software will match the performance restraints of smartcards.

TruSIP goes well beyond improving the trustworthiness of public and private clouds

TruSIP is universal: TruSIP is designed to cost effectively address currently unmet, *end-to-end* security, availability and reliability needs in large system-of-system projects (such as smart grids and other critical infrastructures, medical & financial systems, defence, B2B, ...) by combining the resilience, reliability and availability of *safety systems* with the access and security controls of *ICT systems* within one unified ubiquitous computing architecture (see A7). **To achieve ubiquitous end-to-end scope:** Software variants of TruSIP are targeted for use on commercial-off-the-shelf (COTS) smart cards and hardware security modules. Hardware variants of TruSIP are targeted to create trustworthy and dependable sensors, actuators, programmable logic controllers, industrial control systems, embedded micros, network routers, tablets, workstations, servers, and clouds (in FPGA and ASIC). See appendix A14 for a list of markets targeted by the software and hardware variants.

Validating universality and backwards compatibility: Synaptic Labs is working with leading technology companies (see appendix A4) to validate and ensure that TruSIP can cost-efficiently enhance and support their technologies, as well as grow their respective markets. Hardware variants of **TruSIP will support today's processor instruction sets, operating systems, middleware and business and mission critical software** (see appendix A7.3).

Independent Security Review: The core TruSIP proposal has been independently reviewed by world class computer security and survivability specialists working in Government, industry and academia (appendix A3).

TruSIP is the real deal: Responding to market pressures, some organisations make bold claims that their *software* products running on COTS blade servers can protect enterprises from privileged cloud provider administrators. If software alone was sufficient, why do organisations invest in hardware security modules to protect keys? Unfortunately these **customer applied** countermeasures cannot stop cloud administrators from gaining access to the unprotected memory of the client's virtual machine, from where they can then trivially acquire the client's secret keys, and all the customer applied security controls unravel... In contrast, TruSIP is designed to comprehensively address this and related types of attacks.

A winning proposal: Synaptic Labs' TruSIP proposal is winning interest in both industry and Government. In Malta we have support for our project (see appendix A2, www.ictgozomalta.eu) at both the Ministerial and Government Agency level, from business chambers and academia and have now received seed funding from the Malta Government. We are bringing together an international team of collaborators to support the development of TruSIP in software, field programmable gate arrays and 3-D integrated circuits over the next few years (development speed will be dependant on the level of resourcing and collaborative participation).

An invitation to join the revolution: [Synaptic Laboratories Limited seeks a global commercial partner whose existing product portfolio and cloud/industrial control marketing objectives can be significantly enhanced by TruSIP.](#) They could also join or lead our consortium in funding bids discussed in appendix A5. Synaptic Labs would like to open up technical discussions to enable you to learn more about our proposal, validate our claims, explore how we can best support your technology stack and customer base, and to identify potential synergies in joint collaboration in Malta and internationally, with a view towards global marketing.

Funding opportunities: Governments are currently offering funding for cyber security including secure cloud computing implementation projects. Please see A5 for details on EU and US opportunities. The TruSIP independent review team (Appendix A3) are willing to support such bids.

This completes the three page introduction text. Supporting information, bibliography and Fact Sheets appear in the appendices attached - see the Table of Contents for the appendices on page 6.



SYNAPTIC
LABORATORIES LTD.

“There’s no such thing as ‘secure’ anymore” ... “We have to build our systems on the assumption that adversaries will get in.” ... “We have to, again, assume that all the components of our system are not safe, and make sure we’re adjusting accordingly.”

- Debora Plunkett, Director IAD, U.S. National Security Agency (Dec 2010) [10]

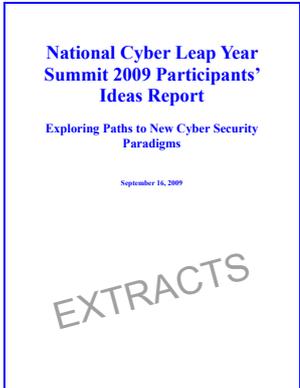
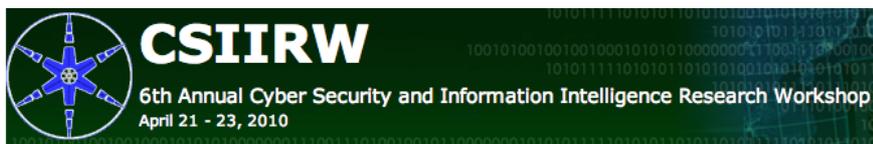
Table of Content in Appendices

A1. About Synaptic Laboratories	7
A2. About ICT Gozo Malta and Synaptic Labs’ Projects	8
A3. World class experts in security and survivability have reviewed TruSIP	10
A4. Companies assisting with technical questions at key points throughout the TruSIP design process	11
A5. Funding opportunities in next generation cybersecurity	11
A5.1 Example funding opportunity: DARPA BAA 11-55 call	11
A5.2 Example funding opportunity: UK Government GBP 650 million cyber security initiative	12
A6. Synaptic Labs’ continues to align our R&D proposals to the community’s calls	13
A7. What is TruSIP	14
A7.1 A very high-level description of the TruSIP architecture	14
A7.2 Techniques used in TruSIP	14
A7.3 TruSIP will support and enhance today’s mainstream technologies	15
A7.4 TruSIP hardens existing CPU architectures	15
A8 TruSIP’s performance	16
A8.1 Comparing the performance and efficiency of TruSIP against the nearest competitor in the security space	16
A8.2 Comparing the performance and efficiency of TruSIP with systems that employ double and triple modular redundancy	17
A8.3 Comparing the performance of TruSIP and conventional hardware security modules	18
A8.4 Comparing the power efficiency of TruSIP and commodity processors	18
A8.5 TruSIP performance and efficiency when using advanced ASIC techniques	19
A9. Kill switch resistance	19
A10. The current development status of TruSIP	20
A11. Comparing TruSIP with other proposals funded by Governments	21
A11.1 Comparing TruSIP with the EU FP7 / IBM TClouds Project (2010 -2013)	21
A11.2 Comparing TruSIP with the DARPA BAA 10-70, Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) (2010-active)	22
A11.3 Comparing TruSIP with the DARPA AFRL-IF-RS-TR-2006-237 (2006)	23
A11.4 Comparing TruSIP with the Malicious-and Accidental-Fault Tolerance for Internet Applications (MAFTIA) project (2003)	23
A11.5 Comparing TruSIP with the DARPA Scalable Intrusion Tolerant ARchitecture (SITAR) - 2003	24
A12. Cloud market size in 2011 and projected for 2020	24
A13. Primary reasons for not using cloud services	25
A14. Market spaces that can be targeted by different variants of TruSIP	26

A1. About Synaptic Laboratories

Synaptic Laboratories [26] is a private micro Research and Development company managed by Australian citizens with Directors in Gozo, Malta (Europe) and Australia. We are operating internationally on a 'virtual' basis with more than ten years of completed research and design. Our core business is cutting edge cross domain research and design for trustworthy and dependable computing (including cloud), information security (identity management, cryptography), and next generation wide area network designs. Our proposals offer a holistic response to a wide range of the hard open problems identified in recent calls by Agencies such as DHS, NIST and NITRD (see appendix A6). Our proposals seek to protect the legitimate interests of all stakeholders in multi-jurisdiction, co-operative and collaborative, Internet-scale environments.

Synaptic Labs is/has been active in various EU and US Federal Cyber Security initiatives. For brevity, we will focus on our US activities. Our CTO was one of the few foreign participants invited to the U.S. Federal Networking and Information Technology Research and Development (NITRD) [12] National Cyber Leap Year Summit (NCLY), where six of our proposals were accepted for publication [26].



Synaptic Labs presented twice [13], [14] at the April 2010 [Oak Ridge National Laboratory](http://ornl.gov/) (ORNL <http://ornl.gov/>) [15] 6th Annual Cybersecurity and Information Intelligence Research Workshop [16] on topics relating to global-scale identity and cryptographic key management. Synaptic Labs' collaborator [Sonalysts](http://www.ictgozomalta.eu/vision-and-projects/international-cyber-security-context/112-popup-sonalysts.html) (www.ictgozomalta.eu/vision-and-projects/international-cyber-security-context/112-popup-sonalysts.html) published reference to our solutions at the [NATO Cyber Security Symposium](#) [17] event and co-presented with us at the ORNL event in the context of new security for smart-grids.

Synaptic Labs also presented twice [18], [19] at the May 2010 [IEEE Key Management Summit](http://2010.keymanagementsummit.org) [20] (<http://2010.keymanagementsummit.org>) on identity management and cryptographic key management subjects and was promoted as a sponsor of the event.

As part of the USA Federal Cyber Security Initiatives, in 2009 NIST launched a new Project in cryptographic key management. The Project has several functions. It is currently creating a new standard (suitable for international use) on "Designing Cryptographic Key Management Systems". NIST is also creating a new Profile (of that standard) that specifically prescribes the future USA Federal requirements on new cryptographic key management products. Synaptic Labs provided 157 pages of feedback in response to NIST's call (out a total of ~200 pages received by NIST) that related to both the framework and the Government profile. Over 95% of all feedback chosen by NIST for focused discussion (see a screen shot above) at their 2 day industry workshop was found only in, or had overlap with, Synaptic Labs' feedback, and key points were endorsed for inclusion in the next revision of the draft document.

Synaptic Labs has also provided extensive comments to the U.S. National Telecommunications and Information Administration on their Privacy calls. Please visit our company website www.synaptic-labs.com for more detailed information on the above mentioned activities in the US and our many activities Europe.

A2. About ICT Gozo Malta and Synaptic Labs' Projects

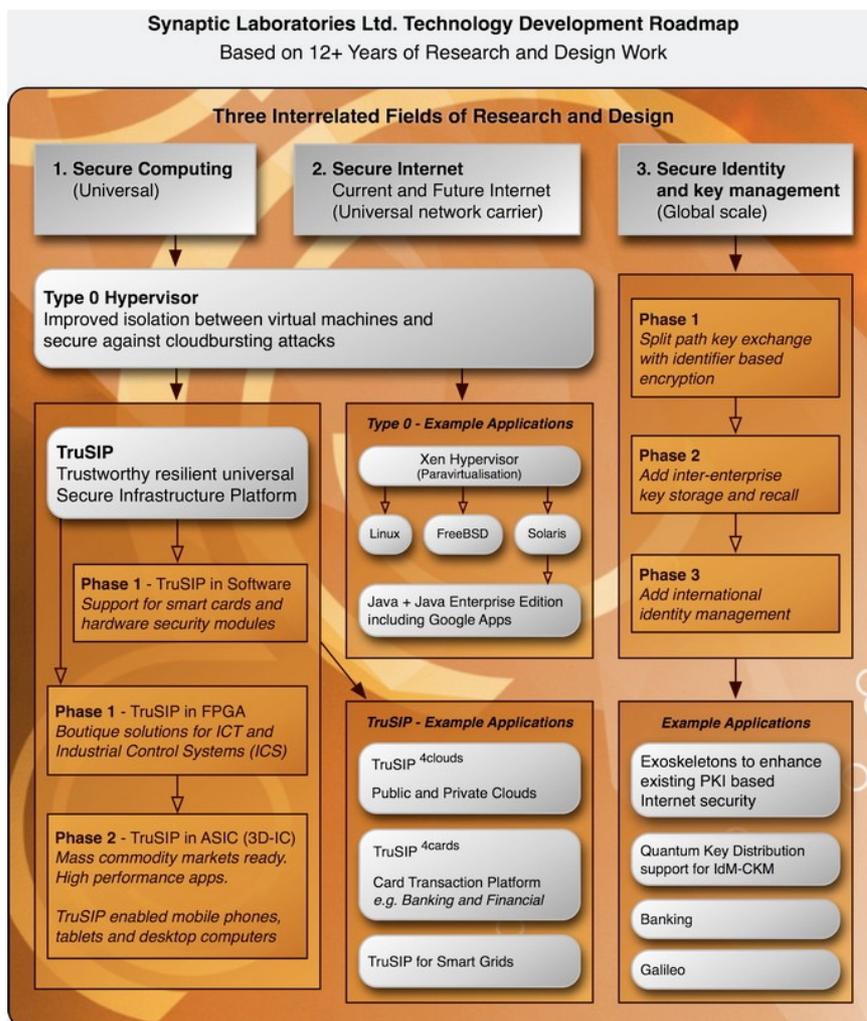
The [ICT Gozo Malta project](https://www.ictgozomalta.eu/) [21] was co-founded by [Synaptic Laboratories](#) [36] and the [Gozo Business Chamber](http://www.gozobusinesschamber.org/) [22] and officially launched in December 2010. Working in close collaboration with key Government and other stakeholders and selected leading International companies, ICT Gozo Malta's objective is to support the realization of the Synaptic Laboratories Limited global vision based on their 10+ years of research. In Malta, the ICT Gozo Malta Project has extensive support at both the Ministerial and Agency level, with organisations such as the [Malta Information Technology Agency](http://www.mita.gov.mt/) [23] and [Malta Enterprise](http://www.maltaenterprise.com/) [24], publishing [21] their support for the ICT Gozo Malta Project. In 2011 the project has received seed funding from the Malta Government. The Project has also received industry support from the [Malta Chamber of Commerce, Enterprise and Industry](http://www.maltachamber.org.mt/) [25].

Synaptic Labs' projects are focussed on technology proposals and solutions that have already started to win international recognition and that match international high priorities (such as EU and USA), in cutting edge ICT fields such as [Secure Internet](http://www.ictgozomalta.eu/vision-and-projects/project-future-internet-janelda.html) (www.ictgozomalta.eu/vision-and-projects/project-future-internet-janelda.html), [Secure ID and key management](http://www.ictgozomalta.eu/vision-and-projects/project-global-scale-idm-and-ckm.html) (www.ictgozomalta.eu/vision-and-projects/project-global-scale-idm-and-ckm.html) and [Secure Computing](http://www.ictgozomalta.eu/vision-and-projects/project-trusip-for-clouds.html) (www.ictgozomalta.eu/vision-and-projects/project-trusip-for-clouds.html). Projects will involve several of the 6 proposals from Synaptic Labs that were presented at and published [26] in the proceedings of the United States Government [Cyber Security Summit](http://www.nitrd.gov/nitrdgroups/index.php?title=National_Cyber_Leap_Year_Summit_2009) (NITRD NCLY), August 2009. (https://www.nitrd.gov/nitrdgroups/index.php?title=National_Cyber_Leap_Year_Summit_2009)

Synaptic Labs' is focused on new solutions that solve hard problems and that offer the essential features called for by Government Agencies and leading industry organisations such as the Cloud Security Alliance.

In particular, Synaptic Labs' solutions are explicitly designed to enable competitors to obtain stronger security for themselves by collaborating with their opponents.

These designs offer global deployment (and marketing) potential, not just because of their technical design, but also because they address the human trust problems that currently prevent true global cyber security.



<https://www.ictgozomalta.eu/vision-and-projects/introduction-and-overview-map.html>
(The above image described our development roadmap on the 11th July, 2011)

The ICT Gozo Malta Steering Committee:

Position	Organisation	Person	Job Title
Chair	The Gozo Business Chamber (GBC) www.gozobusinesschamber.org/	Joe Grech	President
Vice-Chair	Synaptic Laboratories Limited www.synaptic-labs.com	Ron Kelson	CEO
Government Members	Malta Information Technology Agency (MITA) www.mita.gov.mt/	Claudio Grech	Chairman
		Peter Xuereb	Director
	Malta Communications Authority (MCA) www.mca.org.mt/	Philip Micallef	Chairman
		Steve Agius	CIO
	Malta Enterprise (ME) www.maltaenterprise.com/	Alan Camilleri	Exec Chairman
		Dennis Vella	Head of Internationalisation Unit and Enterprise Europe Network
	Malta Council for Science and Technology (MCST) www.mcst.gov.mt/	Nicholas Sammut	CEO
		Eric Flask	Director
	Malta College of Arts, Science & Technology (MCAST) www.mcast.edu.mt	Maurice Grech	Principal
		Prof. Mario Pace	ICT Director
Ministry of Gozo www.gozo.gov.mt	Manuel Tabone	Director (nominated by the Minister for Gozo)	
Industry Members	Malta Chamber of Commerce, Enterprise and Industry www.maltachamber.org.mt/	Ray Muscat	Director General
	The Gozo Business Chamber (GBC) www.gozobusinesschamber.org/	David Pace	ICTGM Project Manager

A3. World class experts in security and survivability have reviewed TruSIP

The core technical description of TruSIP proposal has been independently studied (under NDA) by:

- **Mr. Brian Snow** (Bio [27], LinkedIn <https://www.linkedin.com/in/brian-snow-46b0131>)
An independent security and ethics consultant; formerly a cryptologic designer, security systems architect and then for 12 years a Technical Director of the U.S. National Security Agency (NSA R&D, NSA IAD, NSA ADET).
- **Mr. Miles Smid** (Resume [28], LinkedIn www.linkedin.com/in/milessmid [29])
President of Orion Security Solutions which is owned by ENTRUST (www.entrustdatacard.com/profile/) [30]; former acting Chief of the U.S. NIST Computer Security Division; twice received the highest civilian honor from the USA Department of Commerce, one being for leadership developing the Advanced Encryption Standard (AES) which is now used worldwide; selected as a NIST distinguished scientist. Currently in the NIST Cryptographic Key Management (CKM) framework project [31] team.
- **Dr. Santosh Chokhani**
President of CygnaCom Solutions which is wholly owned by ENTRUST (www.entrustdatacard.com/profile/) [30]; has advised the U.S. State Department, U.S. NIST and U.S. NSA on public key infrastructure and is a member of the NIST CKM framework project [31] team.
- **Dr. Axel Krings** (www2.cs.uidaho.edu/~krings/ [34])
Professor of Computer Science, University of Idaho; fault-tolerant and survivability expert with more than 100 peer reviewed scientific publications.
- **Dr. Richard R. Brooks** (www.clemson.edu/ces/departments/ece/faculty_staff/faculty/rbrooks.html [35])
Associate Professor of Electrical and Computer Engineering, Clemson University, South Carolina; specialist in secure survivable systems and side channel attacks.

All of the above information security and survivability experts independently agree:

1. That the TruSIP design is innovative and appears to offers a unique capability.
2. None are aware of any specific publicly available work comparable to the TruSIP architecture.
3. That the design should be realisable in practice.

Concerning covert channels attacks, the reviewers are confident that TruSIP's security addresses covert storage channel attacks by a privileged insider in the cloud. Several are now specifically reviewing TruSIP's security against covert timing channel attacks by privileged insiders in the cloud.

In addition to the expert opinions of the TruSIP reviewers, it is also Synaptic Labs' opinion that the TruSIP design is unique. This opinion is based on our own survey of 150+ publications in trustworthy and dependable computing, plus another 60+ publications (selected for relevance out of 240+ publications [36]) on covert channel attacks¹.

While it is not the official policy of the US Government's [Department of Energy](http://www.energy.gov/) (DOE) www.energy.gov/ to endorse products, TruSIP has also been studied by:

- **Dr. Frederick Sheldon** (www.csm.ornl.gov/~sheldon/) [33]
Sr. Research Staff Member at U.S. [Oak Ridge National Laboratory](http://www.ornl.gov/) (ornl.gov) [15]; a specialist in Secure and Dependable Systems.

Consequently ORNL has agreed to join with other TruSIP reviewers, their respective organisations and with Synaptic Labs in support of US Government contract bids to advance the TruSIP design.

The text in this appendix (A3) has been approved for publication by the individuals named.

¹ Of those 240+ publications on covert channels [36], we contributed the references to some ~40 of those papers as a result of our internal survey process.

A4. Companies assisting with technical questions at key points throughout the TruSIP design process

Synaptic Labs is currently expanding the number of companies providing technical advice on key points throughout the TruSIP design process to help ensure existing globally deployed products and other new cutting edge technologies are supported:

- Oracle Java SE Embedded, UK
- ARM, UK
- Entrust, USA (through it's wholly owned subsidiaries)
- Tezzaron Semiconductor, USA [37]
- Aeroflex Gaisler, USA [38]
- Others

A5. Funding opportunities in next generation cybersecurity

As described in appendix A6 the TruSIP design proposal is aligned with many important calls made by Governments and Industry relating to cybersecurity in computing systems. This strategic alignment ideally positions TruSIP in funding calls. For example, TruSIP specifically addresses Technical Target Areas in the current USA DARPA BAA 11-55, I2O Mission-oriented Resilient Clouds [9] (closes July 25, 2011). The UK Government has recently allocated GBP 650 million for cyber security initiatives. The Malta Government offers funding opportunities, as does EC FP7. We provide a little more information on two example Calls for new solutions with funding opportunities below.

A5.1 Example funding opportunity: DARPA BAA 11-55 call

The USA DARPA BAA 11-55, I2O Mission-oriented Resilient Clouds [9] opened on June 8 and closes on July 25, 2011. DARPA is soliciting innovative research proposals in the area of security and resilience of large-scale networked computing systems including both Cloud Computing infrastructures and large-scale distributed systems. Quoting DARPA [9]:

“DARPA believes that we must not only address host vulnerabilities but must also pursue clean-slate approaches to the design of networked computations and cloud-computing infrastructures.

The Mission-oriented Resilient Clouds (MRC) program is intended to be a companion program to the existing Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) effort. CRASH takes a clean-slate approach to limiting the vulnerabilities within each host. Mission-oriented Resilient Clouds is concerned with the amplifying effect of the network, seeking to turn this around and use the network as a vulnerability damper and a source of resiliency. The focus of the Mission-oriented Resilient Clouds program is to support mission-oriented computation running on an ensemble of interconnected hosts acting in concert. The goal is to provide resilient support to the mission through adaptation.”

DARPA anticipates making multiple awards in each technical area, with typical awards ranging between \$500K and \$1.5M per effort per year [9]. TruSIP addresses goal and objectives found in 3 Technical Areas of Interest in this call:

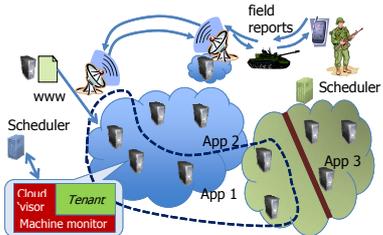
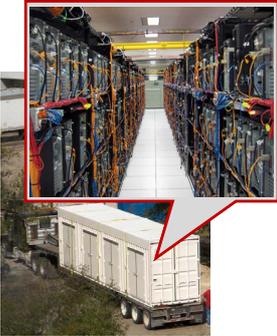
- Scalable and tunable innate distributed defenses
- Optimizing missions and resources
- Manageable and taskable diversity

TruSIP is designed to address key issues in the points raised in the “Required Capabilities for DoD Clouds”:

DARPA Required Capabilities for DoD Clouds
(ISAT War Clouds Study)

Current commercial clouds don't do these at the level required for DoD mission software

- Security: Confidentiality & Integrity of data and computation
- Accountability: Auditing, logging, forensics
- Heterogeneity: Hardware, OS, Job mix
- Agility: Prioritization of tasks in changing environment. Resource management steerable by applications
- Performance/Availability: Guarantees on latency, bandwidth, capacity.



3/14/2011 Approved for Public Release, Distribution Unlimited 6

A5.2 Example funding opportunity: UK Government GBP 650 million cyber security initiative

In October 2010, the UK government pledged to invest over £500m to boost critical national infrastructure and improve cybersecurity as part of its five-year defence plan, the Strategic Defence and Security Review (SDSR) [56]. This figure was later set at £650m [87], [88]. The £650m will go towards the National Cyber Security Programme (NCSP), a series of projects designed to enhance unity of action against cyber threats across government, the private sector, individuals and international entities [87].

Ian McGhie, deputy director of the Office of Cyber Security and Information Assurance (Ocsia), said that GCHQ will plug some of the money into the 'Five Eyes' forum [87], which consists of the UK, US, Canada, Australia and New Zealand.

The UK Centre for Defence Enterprise, the UK Ministry of Defence's gateway for science and technology for industry, academia and innovators, has made a call for research proposals for Trustworthy Digital systems [89]. The call opens 13 July 2011 and closes Tuesday 13th September 2011 [89].

This CDE call is for research proposals for innovative software developments in digital systems and information communication technology that [89]:

4. Define future architectures and interfaces that enable a comprehensive approach through open, dynamic, trustworthy sharing of information and services across systems, organisations and nations.
5. **Enable assurance of mission critical, safety critical and secure Digital capabilities to high levels.**

Synaptic Labs anticipates TruSIP will be directly relevant to point 2 above, and the following identified issue [89]:

Response to “... the spectrum of technological threats and opportunities in a timely manner ... in support of ... the longer-term requirements of future capability.”

Additional information about the call will be made available by the CDE call after July 13.

A6. Synaptic Labs' continues to align our R&D proposals to the community's calls

In Europe and the U.S.A governments and agencies have openly published several high priority objectives, identifying open hard challenges that they feel need to be addressed, to improve the trustworthiness and dependability of our interconnected and interdependent computing systems. These publications are employed to constantly guide and refine Synaptic Labs' designs and proposals. Publications include:

- **U.S Office of the White House**
 - *U.S. 60 day Cyberspace Policy Review* (2009) [39]
- **U.S. Federal Networking and Information Technology Research and Development (NITRD)** [12]
 - *Federal Plan for Advanced Networking Research and Development* (2008) [40]
 - *National Cyber Leap Year Summit (NCLY) Proceedings* (2009) [26], [41], [42]
 - *Cybersecurity R&D Themes Webcast* (2010) [6]
- **U.S. Department of Homeland Security** [43]
 - *A Roadmap for Cybersecurity Research* (2009) [44]
- **U.S. National Institute of Standards and Technology** [45]
 - *Cryptographic key management workshop summary*. Interagency Report 7609 (June 2009) [31]
 - *Guide to Industrial Control Systems (ICS) Security*. Special Publication (Draft) 800-82 (2008) [46]
 - *Guidelines for Smart Grid Cyber Security*. Interagency Report 7628 (Sep. 2010) [47]
- **EU FP6 SecurIST Advisory Board** [48]
 - *Recommendations for a Security and Dependability Research Framework: from Security and Dependability by Central Command and Control to Security and Dependability by Empowerment* [49]
 - *ICT Security and Dependability Research beyond 2010 - Final strategy* (2007) [50]
- **European Network and Information Security Agency** [51]
 - *Cloud Computing - Benefits, Risks and Recommendations for Information Security* (2009) [52]
 - *Security & Resilience in Governmental Clouds* (2011) [53]

Singling out a few points that the TruSIP design addresses, the above papers are calling the community to:

- **SecurIST:** Design user-centric systems that empower all stakeholders of a system [49] [50].
- **DHS:** Build scalable trustworthy ICT and industrial control systems [44].
- **DHS, NITRD:** Combat insider threats (including at the architectural level) [44], [41], [42].
- **NITRD:** Create digital immune systems that employ decentralised, layered security [42].
- **DHS:** Combat malware and botnets [44].
- **DHS:** Design privacy aware security [44].
- **NSA:** Ensure survivability and availability of critical security services [31].
- **NIST:** Address the known looming threat of code-breaking Quantum Computers [31].
- **NIST+ENISA:** Address the known problems that lower the trustworthiness of public clouds [52], [54].

Recently, the Department of Homeland Security (DHS) Science and Technology (S&T) Homeland Security Advanced Research Projects Agency (HSARPA) Cyber Security Division's (CSD) announced a Broad Agency Announcement (BAA) for Fiscal Year 2011 to improve the security in both Federal networks and the larger Internet with a budget of USD \$40 million [55]. The TruSIP design addresses over 70 goals and objectives listed in that DHS BAA 11-02 call, including the following small sample [55]:

- Protect against insiders compromising integrity, availability, and total system survivability.
- Employ redundancy with assurance to make sure that single points of failure are not present.
- Employ technologies that safely tolerate malware (safe transactions in unsafe systems).
- Implement intrinsically auditable systems that are, by design, instrumented for detection.
- React and recover, including changing the system during operation to break adversarial planning.
- Promote an environment where individuals have "ownership" of their personal data, are aware of its provenance, and control its authenticated and authorized distribution, use, destruction with improved understanding of the economic value of such data. (Echoes EU calls for user-centric empowerment [50].)

“We must find more effective ways to tackle risks to our national security ... to identify risks early and treat the causes, rather than having to deal with the consequences.”

– U.K. 2010 Strategic Defence and Security Review [56]

A7. What is TruSIP

A7.1 A very high-level description of the TruSIP architecture

TruSIP is a new fault-tolerant computing architecture designed to maintain uniform Confidentiality, Integrity and Availability under intrusion and insider attacks, under the explicit assumption that every module in the TruSIP deployment has a latent vulnerability and/or embedded malware. TruSIP is designed from the ground up as a cryptographic project exploiting existing standards and employs a combination of logical and physical security controls.

TruSIP has been explicitly designed to address problems raised by the U.S Department of Homeland Security [44], the U.S. Federal Networking and Information Technology Research and Development [41], [42], U.S. National Institutes of Standards and Technologies [46] and the European Network Information Security Agency [52] (ENISA) with regard to secure computing and insider attacks.

<< REDACTED, further information available under NDA upon request >>

A7.2 Techniques used in TruSIP

Similar to other computing solutions that offer fail-safe and non-stop, TruSIP employs redundant computation of client tasks to provide the necessary integrity and availability assurances against benign faults. Unlike most traditional fail-safe and non-stop solutions, TruSIP is also designed to resist malicious faults in any software or hardware module of a TruSIP deployment. See appendix A8.2 for more information.

To achieve enhanced isolation security properties while maintaining excellent resource efficiency, the hardware variant of the TruSIP proposal hardens (one or more) commercial-off-the-shelf processor cores using a range of innovative techniques. See appendix A7.4 for more information.

<< REDACTED, further information available under NDA upon request >>

(intentionally left blank for formatting purposes)

“The business case for cloud computing is obvious – it’s computing on tap, available instantly, commitment-free and on-demand. But the number one issue holding many people back is security – how can I know if it’s safe to trust the cloud provider with my data and in some cases my entire business infrastructure?”

– Giles Hogben, an ENISA expert and editor of the ENISA cloud risks report (2009) [57].

A7.3 TruSIP will support and enhance today’s mainstream technologies

Synaptic Labs has begun reaching out and working with leading technology companies to validate and ensure that TruSIP can cost-efficiently enhance and support their technology portfolio, as well as grow their respective markets.

The TruSIP architecture is being designed to offer security hardened virtual machines optimised for two types of message passing architecture:

2. Security enhanced **hypervisor** for running Xen paravirtualization compliant operating systems with full memory management unit (MMU) and multi-core support.
3. Security enhanced **microkernel** with support for fine-grain security controls on every isolated address space. TruSIP will offer optional multi-core support in each isolated address space.

The first type of TruSIP message passing architecture is optimised for delivering Infrastructure as a Service (IaaS) where as the second type of message passing is optimised for delivering Platform as a Service (PaaS).

Variants of TruSIP will support:

- Today’s processor instruction sets:
 - Near term: SPARC v8, ARM low-end, MIPS
 - Mid term: x86, Itanium, SPARC v9, ARM high-end
- Today’s operating systems:
 - Near term: Xen paravirtualization compliant OS such as Linux, Solaris, FreeBSD, ...
 - Mid term: HP-UX, Windows, OS/X, QNX, SafeRTOS, OIS PCsexpress.
- Today’s middleware
 - Java, Java Enterprise Edition
 - CORBA
- Today’s business and mission critical software running on the above mentioned platforms.

A7.4 TruSIP hardens existing CPU architectures

Isolation between applications and virtual machines is a universally important security feature. The need for stricter isolation between virtual machines in public clouds was identified by ENSIA’s report on cloud computing [52] as an important security requirement currently unmet by today’s cloud solutions.

In today’s private and public clouds, virtual machines share the CPU and memory subsystems in a way that enables unwanted crosstalk and interference between virtual machine instances [58]. This occurs because the low-level computer and CPU architectures have been designed to maximise throughput at the cost of lowered security assurances.

To achieve significantly stronger isolation security properties while maintaining excellent resource efficiency, the hardware variant of the TruSIP proposal hardens (one or more) commercial-off-the-shelf processor cores using a range of innovative techniques. **Further information available under NDA upon request.**

A8 TruSIP's performance

A8.1 Comparing the performance and efficiency of TruSIP against the nearest competitor in the security space

A distinguishing feature of Synaptic Labs' TruSIP proposal is that it enables clients to securely send client software and data into a device managed by a 3rd party in such a way that none of the technical or managerial administrators of that device, or the privileged persons involved in the design, implementation or maintenance of any of the components used by that device, can unilaterally learn the value of the client's data.

The closest competing proposals to achieve this property are based on the relatively new fully homomorphic encryption schemes. Fully homomorphic encryption, if it could be efficiently realised, is considered ideal for ensuring client confidentiality in public cloud computing systems [2].

In 2009, Craig Gentry showed [61] the first [62] fully homomorphic encryption scheme [60]. This scheme is impractical for many applications because the ciphertext size and computation time increase sharply as one increases the security level. For example, performing a Google search process with encrypted keywords would multiply the necessary computing time by around 1 trillion, Gentry estimates [63]. Unlike TruSIP, current fully homomorphic encryption (FHE) schemes **cannot** be used to provide a hardened hypervisor for running existing operating systems because they do not efficiently support a general purpose CPU based architecture. **TruSIP's ability to efficiently protect existing operating systems and software will make TruSIP far more attractive than FHE schemes for the vast majority of organisations and applications.**

The U.S. Defense Advanced Research Projects Agency (DARPA) has taken a serious interest in Gentry's fully homomorphic encryption scheme as part of its Broad Agency Announcement PROCEED project [7]. The U.S. Intelligence Advanced Research Projects Activity (IARPA) has also issued an independent Broad Agency Announcement to find practical fully homomorphic encryption solutions [64]. DARPA has earmarked USD 20 million over 5 years into a project with a primary focus to improve the performance of FHE [8] to only **100,000x** computationally more expensive than unencrypted computing [7]. We note that according to DARPA, "[ed: Currently] *Computation on encrypted data preserves the confidentiality of the data being computed on, but does not inherently protect the integrity of the computation, nor provide strong protection of the program, among other potentially desirable security goals.*" [7]

By way of comparison TruSIP, when implemented in hardware, is only approximately 2.5x to 3.5x computationally more expensive than unencrypted computing for fail safe and non-stop applications respectively. Another advantage of TruSIP over current Fully Homomorphic Encryption schemes is that TruSIP provides strong confidentiality protection for the client's program by default.

With regard to winning international acceptance, all Fully Homomorphic Encryption proposals result in the creation of a new public key encryption algorithm. Based on historical precedence with schemes such as elliptic curve cryptography, due to their complexity, all new public key encryption schemes necessarily require many years (and sometimes more than a decade) of international cryptanalysis by the open community to win sufficient trust for it to be broadly used in the community. In sharp contrast, TruSIP draws extensively on existing and accepted standards based information security techniques. By relying on internationally trusted components, and by using a formal methods development process, TruSIP will dramatically simplify the external cryptanalysis process required to win acceptance, meaning that TruSIP can be more readily adopted by the community/market.

In short, TruSIP is designed to be a commercially relevant solution that can be adopted both rapidly, and at low cost, by the marketplace to address today's real-world concerns.

Side Note: TruSIP can be deployed in a manner that uses techniques widely considered resilient against anticipated quantum computing attacks. This problem is gaining increased attention as quantum computers grow in size such as the 2010 sale of a 128 Qubit system by DWave Systems to Lockheed Martin.

A8.2 Comparing the performance and efficiency of TruSIP with systems that employ double and triple modular redundancy

All higher safety, higher availability computing systems employ redundancy. For example, enterprise storage systems frequently use Redundant Array of Indexed Drives (RAID) technologies. Enterprise computers often use hot swappable $N+1$ power supply configurations. Today, some high-end Intel server chipsets also offer double modular redundant memory to protect against SDRAM module failures.

In industrial control systems it is not uncommon to find *double modular redundant* configurations used to ensure **safety under benign faults**. In these systems, the output of the two identical modules are checked for consensus to ensure a fault in any one module is detected. These systems typically call both redundant modules at the same time, which means that the *time* to run double modular systems is roughly the same speed as just calling one module. Not surprisingly, these systems require at least $2x$ the computation of systems that do not employ redundancy.

In aerospace systems, it is not uncommon to find *triple modular redundant* configurations used to ensure **availability under benign faults**. In these systems, the majority of 2 out of 3 *identical* modules outputs is taken as the correct value. This ensures that the aircraft remains operational during an arbitrary fault in any of the redundant components. These systems require (at least $2x$ computation under fault-free operation and normally) $3x$ the computation of systems that do not employ redundancy.

Double modular and triple modular configurations have been used in commercial high-availability solutions, such as Hewlett Packards' Integrity non-stop servers. In this case, modular redundancy is used to achieve availability against benign component failures in a redundant processor. Again, because the redundant execution of tasks occurs in parallel, these systems run only a little slower than if just one processor was used.

There are many other different ways in which redundancy can be employed [65], [66], [67], [68], [69].

Based on Synaptic Labs' survey of over 150+ publications in the trustworthy and dependable computing space, and the expert opinion of our collaborators who are industry veterans in this space, we can say with confidence that **the TruSIP architecture, which also includes a new and innovative adaption of a range of well-understood redundancy techniques, results in important new capabilities.**

On account of this redundant computation, TruSIP requires at least $2x$ and $3x$ computational overhead over unencrypted computing systems that do not use redundancy to deliver safety or availability assurances respectively. We conservatively describe our overhead as $\sim 2.5x$ and $\sim 3.5x$ to take into account the circuitry required for cryptographic operations and support logic. However, similar to some other systems that employ double or triple modular redundancy, the TruSIP architecture is only a little slower at executing a client task than when executing that task on a single processor.

To place TruSIP's small speed penalty for a single thread into a commercial context, the business model of 'Infrastructure as a Service' providers involves multiplexing/sharing the resources of a high-end server chip to several clients. IaaS providers such as Amazon Web Services lease virtual machine instances that run up to 3 times slower than one CPU core used in the multi-core server. Clearly, a slight reduction in single-thread top-speed in TruSIP to accommodate the value-add properties of high-confidentiality and high-availability in TruSIP will not act as a significant barrier in the IaaS market. TruSIP, like other IaaS offerings, is designed to support multi-core configurations to deliver increased computing power and responsiveness to every virtual machine instance.

Further information available under NDA upon request.

A8.3 Comparing the performance of TruSIP and conventional hardware security modules

The TruSIP proposal is designed to employ hardware security modules [70]. Hardware security modules typically employ physical security controls to provide tamper evidence, resistance, and sometimes defensive response against physical attacks. Hardware security modules come in many sizes and form factors. Smart cards are an example of one of the most common forms of hardware security module.

Typically high-performance hardware security modules use commercial off the shelf processors found in general purpose computing designs. For this reason, hardware security modules offer performance comparable to general purpose computing designs using the same general purpose processor.

The hardware security modules in TruSIP securely receive client data in authenticated encrypted form, decrypt that data inside the hardware security module, perform an arbitrary number of operations on the decrypted data, and send the final result back to the client in authenticated encrypted form.

Even though TruSIP uses hardware security modules **TruSIP does not rely on them behaving honestly towards the client.** For example, TruSIP is designed to protect the client from exfiltration attacks by hardware security module vendors. That is, where the HSM tries to leak the client's sensitive data. Today, a 'trusted' network attached hardware security module could be easily designed to exfiltrate sensitive key materials to the attacker using an undetectable [71] covert timing channel [72]. For example, the hardware security module can modulate the pace and timing of network traffic packets sent over the Internet in a way that encodes key material or client secrets. The attacker will be able to decode the message encoded in the timing of the packets, with the attack going undetected by everybody else. If the hardware security module vendor is based in a foreign country, that vendor may have no choice but to install such hidden backdoors against their international clients.

TruSIP is explicitly designed to address this real-world threat by employing various innovative security controls and protocols in the TruSIP architecture that are designed to either expose or prevent (private or public) network based covert channel attacks.

In fact, TruSIP is designed to deliver countermeasures against attacks involving a subversive collusion between the hardware security module vendor and the public cloud provider!

The ability for proposed TruSIP deployments to protect against these and other types of insider attacks uniquely positions TruSIP to address trustworthiness and dependability problems that hinder the level of adoption of public clouds.

In fact, TruSIP offers the potential to bolster the security of public clouds beyond what is possible today in private clouds. This is why we argue that TruSIP may not just revolutionise the public cloud computing market, but capture a large market share of the private cloud market as well.

Further information available under NDA upon request.

A8.4 Comparing the power efficiency of TruSIP and commodity processors

As indicated in appendix A7.4 TruSIP hardens existing CPU architectures to provide the necessary (currently missing) security controls to address insider attacks and enable secure public cloud computing and harden the security TruSIP in all other applications.

As indicated in appendix A8.2 TruSIP also innovative employs double or triple modular redundancy as required to achieve fail-safe or high-availability modes of operation.

This raises the question of power efficiency and total cost of ownership. For example, is TruSIP going to have a 2.5x to 3.5x larger power bill than today's COTS server processors?

Today's commercial processors range significantly in their power efficiency to execute any given program. There are several reasons for this, but first we will cite a publication comparing two competing processors advertising "low-power" properties. According to a paper [73] published by the University of Texas at Dallas

titled: “ARM Cortex-A8 vs. Intel Atom: Architectural and Benchmark Comparisons”, there is a 6x power consumption difference per Dhrystone Million Instructions per Second (DMIPS) between ARM Cortex-A8 processor and the low power Intel Atom processor.

Simply speaking, the ARM Cortex A-8 processor can perform 6 operations for every 1 operation performed by the Intel Atom, even though the ARM processor is manufactured on an older (more power hungry) semiconductor technology. Intel have designed their processor in a way that consumes 6x more power in exchange for the ability to execute single thread tasks faster than the ARM processor.

Speaking simply, CPU cores frequently stall while waiting for the value of some memory location to arrive from outside the CPU chip. Whereas the ARM processor is more inclined to wait patiently for the value to arrive, the Intel processor is more likely to run ahead and try and “guess” the value before it arrives. If the guess is right, Intel’s chip can use the calculations based on that guess, otherwise the Intel processor has to throw away all that work. In any event, this means the Intel chip will either be as fast as, or faster than, the ARM processor at every step. But Intel achieve this at the cost of a larger, more complex, more expensive circuit to implement the acceleration techniques, and that circuit consumes more power than a simpler circuit.

It is widely accepted that the reason why Intel and other chip manufactures employ aggressive techniques to improve single thread performance is that there is a high value segment in the processor market (computer gamers, graphics designers) that will pay top dollar to achieve the absolutely highest performance for a single thread. That market is not typically concerned with security or maximum power efficiency. It is also widely recognised that ARM processors offer slower performance but lower power consumption. ARM processors are dominant in mobile phone markets where maximising battery life is important.

In the context of achieving a computing platform that balances security and performance objectives, based on the above figures, **TruSIP could use a modified ARM Cortex-A8 processor in a double or triple modular redundant configuration and still be more power efficient per instruction** than Intel’s Atom chip!

In public cloud contexts, where we must consider the total cost of ownership, including initial purchase cost and ongoing power consumption, TruSIP will be engineered to exploit the best price/performance/power sweet-spot at the time of development. We believe a TruSIP implementation that balances these properties will appeal to the broadest market place on account of it’s increased security properties.

To achieve lower power consumption across all applications, including mobile, we employ 3-D IC techniques to win a number of advantages including improve total system power efficiency as described in appendix A8.5.

A8.5 TruSIP performance and efficiency when using advanced ASIC techniques

Further information available under NDA upon request.

“We have to, again, assume that all the components of our system are not safe, and make sure we're adjusting accordingly”

– Debora Plunkett, Director of the Information Assurance Directorate
at the US National Security Agency, December 2010

A9. Kill switch resistance

TruSIP is designed to manage both benign and maliciously introduced faults. In particular, certain configurations of TruSIP are designed to continue operating in the presence of an activated kill switch in any software or hardware module. More specifically, TruSIP is designed to survive every instance of that compromised module in a TruSIP deployment having it's kill switch activated simultaneously!

TruSIP targets the highest safety and security levels in a unified, backwards compatible, computing platform

We will now quote two sources that outline the market drivers that have led Synaptic Labs to design TruSIP in a way that could provide end-to-end protection against kill switches.

According to a NIST publication [47]:

“maintaining the resiliency and continuous availability of the power grid itself as a critical national infrastructure is an important mandate”

furthermore:

“... the unique nature of the electrical grid is that it supplies key elements toward the well-being of these other critical infrastructure elements. And additionally, there are reverse dependencies emerging on Smart Grid being dependent on the continuous well-being of the telecommunications and digital computing infrastructure, as well as on the continuing flow of the raw materials to generate the power. These interdependencies are sometimes highly visible and obvious, but many remain hidden below the surface of the detailed review for each. There is little current understanding of the cascading effect outages and service interruptions might have, especially those of a malicious and judiciously placed nature with intent to cause maximum disruption and mass chaos.”

According to P. Strassmann [74], a 1993 recipient of the Defense Medal for Distinguished Public Service - the U.S. Defense Department's highest civilian recognition [79]:

“One of the major cyber threats to organizations that require high levels of security is the chance that commodity microprocessors, currently manufactured in places without adequate security oversight and inspection, may be installed into its servers. Such microprocessors would come with “back-door” openings already installed.

A longstanding fear has been that cyber attacks against the U.S. might result in disruptions to power, banking, and communications systems at a critical moment. Efforts by the Defense Advanced Research Projects Agency (DARPA) to improve verification capabilities highlight the limitations of current computer engineering skills in, for example, diagnosing cyber intrusions. Initial studies on the Trusted Integrated Circuit program, seeking to create a secure supply chain, were requested in 2007. As of late 2010, DARPA was still seeking new research proposals for determining whether a given chip was reliable, and whether it had been maliciously modified, as part of the Integrity and Reliability of Integrated Circuits (IRIS) program.

A more recent worry is vulnerabilities “hardwired” into the physical infrastructure of the Internet. In the last several years, the FBI has warned that counterfeit computer parts and systems may be widespread. A growing concern is that a few countries that now manufacture most of the commodity microcircuits, can exploit their position to affect American and allied infrastructures.

The 2005 Defense Science Board Task Force on High Performance Microchip Supply identified the growing security problem of microchips being manufactured (and more and more often designed) outside the United States.”

TruSIP has been designed to address the above concerns while opening up and capturing vast new markets that are not adequately addressed by the competition. See also appendix A14.

A10. The current development status of TruSIP

As of June 2011, TruSIP is at the design and specifications stage. We have completed the process of describing how the topology of our architecture, and certain software and hardware techniques, will be used to achieve the overall security goals of the platform. We have explored a range of techniques to control the

implementation and running costs of TruSIP. TruSIP is now actively undergoing its second stage of independent analysis.

TruSIP is working with potential funding bodies and collaborators to identify the first application space for TruSIP e.g. do we target kill switch resistance in the first design, do we aim for embedded micro or servers first, and so on. With a selected target market, development path and funding approach in mind, we will then be moving into a more formal specifications and development process. Where possible our goal is to ensure the analysis and development done in any part or stage of the design can be readily reused. We are in the process of actively engaging with Governments and Industry in E.U. and U.S. to identify their high-priority targets to guide the selection of our first target design to implement.

A11. Comparing TruSIP with other proposals funded by Governments

A11.1 Comparing TruSIP with the EU FP7 / IBM TClouds Project (2010 -2013)

TClouds [65] is an EU FP7 funded cloud project that includes researchers from IBM Research, Philips Electronics Nederland, and Technische Universität Darmstadt. Phase 1 (2010 -2013) has a project cost of €10,536,129.00 and was funded €7,500,000.00 through the EU FP7.

The stated mission of TClouds [65] is to:

1. develop an advanced cloud infrastructure that can deliver computing and storage that achieves a new level of security, privacy, and resilience yet is cost-efficient, simple, and scalable; and
2. change the *perceptions* of cloud computing by demonstrating the prototype infrastructure in socially significant application areas: energy and healthcare.

One of the technical objectives is to create a *“A Trustworthy Infrastructure Cloud enables individual providers to offer more resilient and privacy-aware infrastructure clouds.”* We note they do not go as far as to say that their objective is for individual providers to be able to offer privacy preserving cloud services. Their next technical objective is to achieve *“Privacy and Resilience for Commodity Clouds”* by enabling *“end users to put a security layer on top of existing commodity infrastructure clouds to enforce their security objectives.”* This security layer, or *“framework will provide multiple back-ups of the TClouds data and applications in case of a hardware failure or intrusion”*.

In the table found below on the next page we compare some of the publicly available literature on the EU FP7 TClouds project with some of the properties of Synaptic Labs' TruSIP proposal when implemented in hardware (FPGA or ASIC):

	EU FP7 TClouds (€10.5 m)	TruSIP (FPGA, ASIC)
Strategy	Create new middleware that sits on top of existing cloud systems	Address the core security problems at the hardware level up (a software only proposal is available for smart cards)
Compatibility	Entirely new software must be written to run on the middleware	Many existing applications and operating systems can be recompiled and run on our platform without change
Privacy against cloud provider	No controls to prevent the cloud provider from learning the value of data sent to it	Prevents the cloud provider learning the value of any client data
Manage risks	Split program over private (trusted) clouds and less trusted clouds, use Byzantine agreement programming approaches	Use a system of separation of powers and checks-and-balances implemented inside each TruSIP device
Performance	Byzantine fault resistant programs are slow, particularly over the Internet	A little slower than the general purpose processors used inside TruSIP
End-to-end	No mention of securing smart sensors, embedded micros, work stations, ...	Targeted to embedded micro, workstation, and clouds in real-time, industrial control and ICT contexts for ubiquitous 'end to end' security in systems of systems

A11.2 Comparing TruSIP with the DARPA BAA 10-70, Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) (2010-active)

The currently active Defense Advanced Research Projects Agency (DARPA) CRASH project solicited proposals in 2010 [75] for innovative research into the design of new computer systems that:

1. Are highly resistant to cyber-attack;
2. Can adapt after a successful attack in order to continue rendering useful services;
3. Learn from previous attacks how to guard against and cope with future attacks; and
4. Can repair themselves after attacks have succeeded.

Based on the DARPA presentations made to industry, the CRASH project [75] appears to be based around the TIARA [78] tag processor. The TIARA tag processor assumes that the hardware can be trusted to behave honestly with regard to the client / stakeholders. The TIARA processor does not appear to address kill switches embedded in the processor, nor does it appear to address the exfiltration of data through value, covert storage, or covert timing channel attacks.

In contrast Synaptic Lab's TruSIP is designed to address insider attacks and kill switches, and therefore appears to exceed the scope of the DARPA CRASH project in this respect. In principle the TruSIP project will support mainstream commercial processor architectures in use today, and therefore we expect that we could enhance the TIARA/CRASH CPU deliverables to enhance its security for use in private/public cloud computing environments. Also see appendix A5.1

A11.3 Comparing TruSIP with the DARPA AFRL-IF-RS-TR-2006-237 (2006)

This DARPA project's goals were to increase intrusion tolerance via scalability redundancy [66]:

“The project worked toward dramatically increasing the scalability of fault- and intrusion-tolerant services, particularly in the efficiency of tolerating significant numbers of failures and compromises. This project has built upon foundational work laid in two previous, independent and concurrent DARPA projects: Information Processing Technology Office (IPTO) PASIS project for implementing survivable data storage, and Advance Technology Office (ATO) Fleet project for implementing an intrusion-tolerant object-oriented system, integrating the lessons and advances of these individual projects as a basis for further innovation.”

Among other things, the U.S. DARPA / U.S. Air Force Research Laboratory (AFRL) project developed protocols for highly resilient distributed object-based systems that offer linearizable method invocations, including nested invocations in which one object is invoked by another, where some replicas of each may be corrupt.

The DARPA / AFRL project makes no claim of maintaining confidentiality of data under intrusion.

In contrast, Synaptic Laboratories' TruSIP platform will support a distributed object-based system (Platform as a Service) that supports confidentiality of sensitive data managed by the objects, even when under intrusion.

A11.4 Comparing TruSIP with the Malicious-and Accidental-Fault Tolerance for Internet Applications (MAFTIA) project (2003)

MAFTIA was a European IST Research Project IST-1999-11583 [67] that ran from 1 January 2000 to 28 February 2003. MAFTIA [67] describes fault tolerant schemes that employ trusted hardware security modules in each compute element. MAFTIA deliverables make no claim of maintaining confidentiality of sensitive data under intrusion.

In contrast Synaptic Labs' TruSIP:

1. Does NOT rely on the absolute trustworthiness of hardware security modules or trusted platform modules. Instead it employs a system of checks and balances to protect against malware in any software or hardware component.
2. Maintains confidentiality if the chip, hypervisor, operating system, or hardware security modules processing sensitive client data have latent faults or embedded malware that is exploited to exfiltrate data through value faults, covert storage channels or covert timing channels.

(intentionally left blank for formatting purposes)

A11.5 Comparing TruSIP with the DARPA Scalable Intrusion Tolerant ARchitecture (SITAR) - 2003

The DARPA SITAR project [68] was designed to provide high-availability, intrusion resistant delivery of web pages using unmodified commercial of the shelf web servers and hardware. SITAR employed N-variant software diversity with N-redundancy to detect and survive network borne vulnerability exploits against an array of N-variant COTS web servers.

In the paper [69] studying the security properties of SITAR it is claimed that “*Systems based on the SITAR architecture can recover from security attacks that may otherwise result in loss of availability, integrity or confidentiality automatically through redundancy and diversity.*”

However there is insufficient information to determine which security attacks are addressed within SITAR. For example that paper [69] specifically :

1. Does not qualify the level or extent of the confidentiality properties in SITAR.
2. Does not consider covert storage / timing channel attacks.
3. Does not consider physical / network side-channel attacks.
4. Does not consider insider attacks by the administrators / software vendors / hardware vendors.

In contrast, Synaptic Labs’ TruSIP addresses all the above points. The goals and objectives of TruSIP far exceed those of SITAR.

A12. Cloud market size in 2011 and projected for 2020

According to a report on sizing the cloud [80] by Forrester Research (2011):

Market	2011	2020
Public cloud	USD 25.5B	USD 159.3B
Virtual private cloud	USD 7.5B	USD 66.4B
Private cloud	USD 7.8B	USD 15.9B

(intentionally left blank for formatting purposes)

A13. Primary reasons for not using cloud services

DARPA pointed [86] to a research report on Cloud Governance, Risk and Compliance [84] by InformationWeek Analytics (July 2009) where 38% of respondents (208 out of 548 surveyed) said that they would **not** use the cloud.

Of those 208 who would not use the cloud, **53%** cited security related issues as the primary reason for not adopting the cloud. The high-level break down of issues identified in that survey is as follows:

Security concerns dominate both cloud adopters and non-adopters with

“... 51% of CIOs surveyed ... cited security as their greatest concern surrounding cloud adoption.”

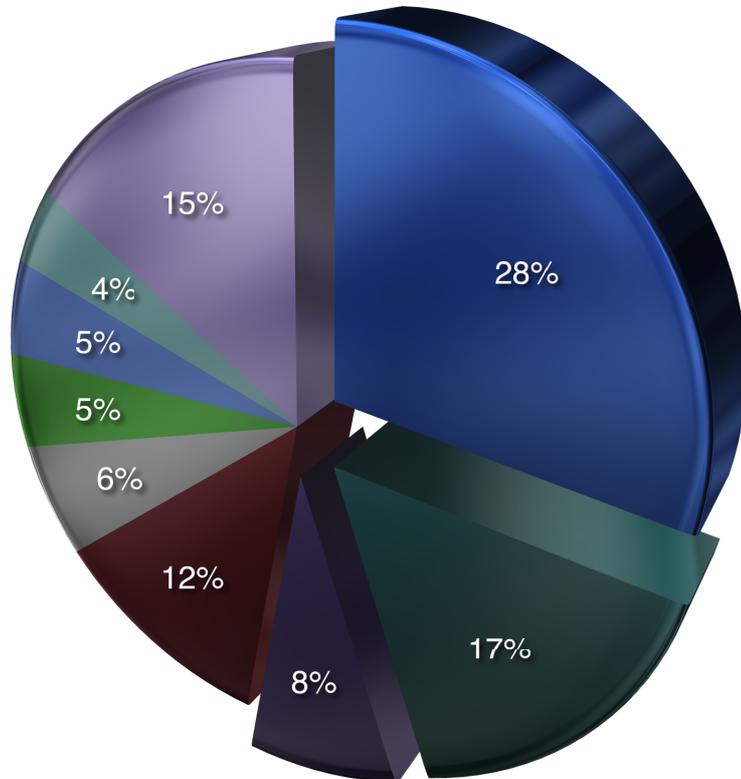
as reported in a keynote transcript at the RSA conference March 2010 [85].

Recent Cloud Reports from ENISA [2], NIST [90, 91, 92] and the Cloud Security Alliance [93] perform indepth survey's listing the unresolved security issues. TruSIP specifically resolves many of these issues.

A14. Market spaces that can be targeted by different variants of TruSIP

TruSIP can be implemented incrementally with varying levels of up-front non-recurring expenses, enabling an incremental approach into the market. Both the software and hardware variants have security controls against insider and outsider attacks. The hardware version of the TruSIP proposal offers a range of superior capabilities including enhanced auditing capabilities, stronger isolation between tasks, support for Xen paravirtualization operating systems and significantly improved overall-performance. In principle the FPGA and ASIC versions of the system should have the same functionality, but of course the ASIC version will

- Fear of unauthorised access to or leak of our proprietary information
- Fear of unauthorised access to or leak of our customer's information
- Security defects in the technology itself
- Features and general maturity of the technology
- Unpredictable costs
- Business viability of provider; risk company will fail
- Vendor Lock in
- Application System Performance
- Other



have far higher throughput and responsiveness than the FPGA solution. All software and hardware versions can support either fail-safe or non-stop modes of operation. In principle software variants could implement availability under the activation of a **kill switch** in any module, however we prefer to offer that feature for FPGA/ASIC variants.

Sw/Hw	Device	Applications and Markets
Software	Smart cards	Examples: Two factor authentication (Personal identity management and cryptographic key management token); Technical safeguards for protecting very small amounts of privacy or commercially sensitive information and low transaction rates (pin numbers, passwords, email account details, visa card details, performing online e-commerce transactions, other financial information).
Software	Network attached HSM	Examples: Technical safeguards for protecting small to medium amounts of privacy or commercially sensitive information (pin numbers, passwords, email account details, visa card details, performing online e-commerce transactions, other financial information). Suitable for running some Java business applications on a scalable Platform as a Service system. Markets include business, financial, medical.
Hardware Phase 1	FPGA + optionally structured ASIC	Examples: Suitable for embedded micro, industrial control devices, industrial control workstation, public and private TruSIP cloud computing. Markets include business, financial, medical, industrial, personal, cloud, ...
Hardware Phase 2	3-D IC (ASIC) <i>1 variant with low memory</i> <i>1 variant with high memory</i>	Widest market penetration with lowest per unit cost, supporting high-volume commodity use in embedded micro, smart sensors/actuators, industrial control systems, safety systems, mobile phones, tablets, business workstations, full-scale private and public clouds. Markets include business, financial, medical, industrial, applications in the home, private and public cloud, ultra-reliable high-end smart cards for critical infrastructure applications, ...

END of Appendices

REFERENCES

- [1] Arcsight, and Ponemon Institute. First annual cost of cyber crime study with Ponemon institute. Survey, ArcSight HP, July 2011.
- [2] Catteddu, D., and Hogben, G. "Cloud Computing - Benefits, Risks and Recommendations for Information Security". Report, European Network and Information Security Agency, Nov. 2009.
<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>
- [3] CEBR. The Cloud Dividend: Part One, The economic benefits of cloud computing to business and the wider EMEA economy - France, Germany, Italy, Spain and the UK. Report for EMC, Centre for economics and business research Ltd, December 2010.
- [4] EMC, and IDC. Digital universe decade - are you ready? Tech. rep., May 2010.
- [5] Krazit, T. Google fired engineer for privacy breach. News article, news.cnet.com, Sep. 2010.
http://news.cnet.com/8301-30684_3-20016451-265.html
- [6] NITRD. NITRD 2010 Cybersecurity R&D Themes Webcast. In Federal Cybersecurity Game-change R&D website (May 2010), NITRD.
- [7] DARPA. PROgraming Computation on EncryptpEd Data (PROCEED). Broad Agency Announcement DARPA-BAA-10-81, Defense Advanced Research Projects Agency (DARPA), 3701 North Fairfax Drive, Arlington, VA, July 2010.
- [8] Greenberg, A. DARPA Will Spend \$20 Million To Search For Crypto's Holy Grail. Tech. rep., Forbes, Apr. 2011.
<http://blogs.forbes.com/andygreenberg/2011/04/06/darpa-will-spend-20-million-to-search-for-cryptos-holy-grail/>
- [9] DARPA. I2O Mission-oriented Resilient Clouds (MRC). Broad Agency Announcement DARPA-BAA-11-55, Defense Advanced Research Projects Agency (DARPA), 3701 North Fairfax Drive, Arlington, VA, Jun 2011.
- [10] Wolf, J. U.S. code-cracking agency works as if compromised. Newspaper article, Reuters, Dec. 2010.
<http://www.reuters.com/article/idUSTRE6BF6BZ20101217>.
- [11] Synaptic Laboratories Limited, <http://www.synaptic-labs.com>
- [12] Networking and Information Technology Research and Development (NITRD), <http://www.nitrd.gov/>
- [13] McCusker, O., Gittins, B., Glanfield, J., Brunza, S., and Brooks, S. The Need to Consider Both Object Identity and Behavior in Establishing the Trustworthiness of Network Devices within a Smart Grid. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (New York, NY, USA, 2010), CSIIRW '10, ACM, pp. 53:1–53:4. Authors copy of 4 Page paper (PDF):
<http://media.synaptic-labs.com/downloads/pub/publications/csiirw/20100423-CSIIRW6-TrustworthinessIdentityBehavior-Paper.pdf>
Authors copy of the Slideshow (PDF):
<http://media.synaptic-labs.com/downloads/pub/slideshows/csiirw/20100423-CSIIRW6-TrustworthinessIdentityBehavior-Slideshow.pdf>
- [14] Gittins, B. Overview of SLL's proposal in response to NIST's call for new global IdM/CKM designs without public keys. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (New York, NY, USA, 2010), CSIIRW '10, ACM, pp. 60:1–60:4. Authors copy of the 4 Page paper PDF:
http://media.synaptic-labs.com/downloads/pub/publications/csiirw/20100422-CSIIRW6-SLL_Global_IdM_CKM_Proposal.pdf
- [15] Oak Ridge National Laboratory, <http://ornl.gov/>
- [16] ORNL, 6th Annual Cybersecurity and Information Intelligence Research Workshop,
<http://dl.acm.org/citation.cfm?id=1852666>
- [17] NATO Information Assurance and Cyber Defence Symposium in Turkey. Website, Apr. 2010.
- [18] Gittins, B., and Kelson, R. A survey and low-level comparison of network based symmetric key distribution architectures. Video. In IEEE Key Management Summit 2010 website (Lake Tahoe, Nevada on May 4-5, 2010., May 2010), IEEE. <https://www.youtube.com/watch?v=1EhNPCTIB0o>
- [19] Gittins, B., and Kelson, R. Overview of SLL's proposal in response to NIST's call for new global IdM/CKM designs without PKC. Video. In IEEE Key Management Summit 2010 website (Lake Tahoe, Nevada on May 4-5, 2010., May 2010), IEEE. <https://www.youtube.com/watch?v=8Z3Prkc2eng>
- [20] IEEE Key Management Summit 2010. Website. Available at <http://2010.keymanagementsummit.org/>.
- [21] ICT Gozo Malta Project, <https://www.ictgozomalta.eu/>
- [22] Gozo Business Chamber, <http://www.gozobusinesschamber.org/>
- [23] Malta Information Technology Agency, <https://www.mita.gov.mt/>
- [24] Malta Enterprise, <http://www.maltaenterprise.com/>
- [25] ICT Gozo Malta, Page on the Malta Chamber of Commerce, Enterprise and Industry
www.maltachamber.com

- [26] Gittins, B. Synaptic Labs participation in the U.S. National Cyber Security Initiatives - 2009. White paper, Synaptic Laboratories Limited, Jun. 2009.
http://media.synaptic-labs.com/downloads/pub/publications/NITRD/20091115-NCLY-Summit2009-Participants_Ideas_Report-Extracts.pdf
- [27] ISAPIA, Brian Snow Biography, http://ispia.ucalgary.ca/people/biographies/brian_snow
- [28] Miles Smid, Full Resume, 24 June 2011,
<http://media.synaptic-labs.com/downloads/pub/milessmid/20110624-Miles-Smid-Full-Resume.pdf>
- [29] Miles Smid, LinkedIn Page, <http://www.linkedin.com/in/milessmid>
- [30] Entrust, About Entrust Datacard, <https://www.entrustdatacard.com/profile/>
- [31] Barker, E., Branstad, D., Chokhani, S., and Smid, M. Cryptographic key management workshop summary (final). Interagency Report 7609, NIST, June 2009. <http://csrc.nist.gov/publications/nistir/ir7609/nistir-7609.pdf>.
- [32] Dr. Santosh Chokhani (His biography page is no longer online).
- [33] Frederick T. Sheldon, ORNL webpage, <http://www.csm.ornl.gov/~sheldon/>
- [34] Dr. Axel W. Krings, University of Idaho webpage, <http://www2.cs.uidaho.edu/~krings/>
- [35] Associate Professor Richard R. Brooks
http://www.clemson.edu/ces/departments/ece/faculty_staff/faculty/rbrooks.html
- [36] Centre for Advanced Internet Architectures. Covert Channels Bibliography. Website page., Swinburne University of Technology, 2011. <http://caia.swin.edu.au/cv/szander/cc/cc-index.html>
- [37] Tezzaron Semiconductor, <http://www.tezzaron.com/>
- [38] Aeroflex Gaisler, <http://www.gaisler.com/>
- [39] USOWH. Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure (may 26, 2009). United States, Office of the White House.
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- [40] NITRD. Federal Plan for Advanced Networking Research and Development. Report by the interagency task force on advanced networking, US Networking and Information Technology Research and Development Program, (Arlington, VA, USA), Sep. 2008. Available at <http://www.nitrd.gov/PUBS/ITFAN-FINAL.pdf>
- [41] QinetiQ. National Cyber Leap Year Summit 2009 – Participants’ Ideas Report. On behalf of the US NITRD.
http://media.synaptic-labs.com/downloads/pub/publications/NCLY/NITRD-NCLY-National_Cyber_Leap_Year_Summit_2009_Participants_Ideas_Report.pdf
- [42] QinetiQ. National Cyber Leap Year Summit 2009 – Co-Chairs’ Report. On behalf of the US NITRD Program.
media.synaptic-labs.com/downloads/pub/publications/NCLY/NITRD-NCLY-National_Cyber_Leap_Year_Summit_2009_Co-Chairs_Report.pdf
- [43] U.S. Department of Homeland Security, <http://www.dhs.gov/>
- [44] Department of Homeland Security. A Roadmap for Cybersecurity Research. Roadmap, DHS Science and Technology Directorate, Nov. 2009.
<https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf>
- [45] U.S. National Institute of Standards and Technology, <http://csrc.nist.gov/>
- [46] Stouffer, K., Falco, J., and Scarfone, K. Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). Special Publication (Final) 800-82, National Institute of Standards and Technology, Sep. 2008. <http://dx.doi.org/10.6028/NIST.SP.800-82>
- [47] The Smart Grid Interoperability Panel Cyber Security Working Group. Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. Interagency Report 7628, National Institute of Standards and Technology, Sep. 2010.
- [48] FP6 SecurIST, <https://web.archive.org/web/20130128014444/http://securitytaskforce.eu/> (Archived copy of the website)
- [49] SecurIST Advisory Board. Recommendations for a Security and Dependability Research Framework: from Security and Dependability by Central Command and Control to Security and Dependability by Empowerment. Deliverable 3.0, SecurIST EU-FP6-004547, Jan. 2007.
https://web.archive.org/web/201211222083842/http://www.securitytaskforce.eu/dmdocuments/securist_ab_recommendations_issue_v3_0.pdf
- [50] Dooly, Z., Clarke, J., Fitzgerald, W., Donnelly, W., Riguidel, M., and Howker, K. ICT Security and Dependability Research beyond 2010 - Final strategy. Deliverable 3.3, SecurIST EU-FP6-004547, Jan. 2007.
https://web.archive.org/web/20130203034818/http://securitytaskforce.eu/dmdocuments/d3_3_final_strategy_report_v1_0.pdf
- [51] European Network and Information Security Agency (ENISA), <http://www.enisa.europa.eu/>

- [52] Catteddu, D., and Hogben, G. Cloud Computing - Benefits, Risks and Recommendations for Information Security. Report, European Network and Information Security Agency, Nov. 2009.
<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>
- [53] Catteddu, D. Security & Resilience in Governmental Clouds – Making an informed decision. Report, European Network and Information Security Agency, Jan. 2011.
- [54] Jansen, W., and Grance, T. Guidelines on Security and Privacy in Public Cloud Computing. (Draft) Special Publication 800-130, National Institute of Standards and Technology, January 2011.
- [55] DHS. 2011 DHS S&T Cybersecurity Research and Development BAA. Broad Agency Announcement 11-02, DHS Science and Technology Directorate, Jan 2011. https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/BAA_11-02/listing.html
- [56] A Strong Britain in an Age of Uncertainty: The National Security Strategy. Cabinet Office, UK, 70 Whitehall, London SW1A 2AS, 2010.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf
- [57] Curtis, S. Government's new ICT strategy could save £3.2bn. News article, eWeek Europe, Dec. 2009.
<http://www.eweekurope.co.uk/news/news-security/governments-new-ict-strategy-could-save-32bn-2623>
- [58] Salaün, M. Practical overview of a Xen covert channel. J. Comput. Virol. 6 (November 2010), 317–328.
<http://digikod.net/public/XenCC/xencc-eicar2009.pdf>
- [59] Kortchinsky, K. CLOUDBURST. A VMWare Guest to Host Escape Story. In BlackHat USA (June 2009).
- [60] Wikipedia, Fully Homomorphic Encryption, http://en.wikipedia.org/wiki/Homomorphic_encryption
- [61] Gentry, C. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009.
<http://crypto.stanford.edu/craig/>
- [62] Micciancio, D. Technical Perspective: A First Glimpse of Cryptography's Holy Grail. In Communications of the ACM (Mar. 2010). <http://cacm.acm.org/magazines/2010/3/76275-technical-perspective-a-first-glimpse-of-cryptographys-holy-grail/abstract>
- [63] Greenberg, A. IBM's Blindfolded Calculator. In Forbes Magazine (July 2009).
<http://www.forbes.com/forbes/2009/0713/breakthroughs-privacy-super-secret-encryption.html>
- [64] IARPA. Security And Privacy Assurance Research (SPAR) Program. Broad Agency Announcement IARPA-BAA-11-01, Intelligence Advanced Research Projects Activity, Washington, DC, Dec. 2011.
<https://www.fbo.gov/notices/c55e38dbde30cb668f687897d8f01e69>
- [65] EU FP7 TClouds Project, Website: <https://web.archive.org/web/20150331224019/http://www.tclouds-project.eu/> (Archived Copy of the Website), IBM
- [66] DARPA AFRL-IF-RS-TR-2006-237, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA611350>
- [67] Ver'issimoo, P., Ferreira, N., and Correia, N. M. The middleware architecture of MAFTIA: A blueprint. In ISW-2000: Proc. of the IEEE Third Information Survivability Workshop (Boston, Massachusetts, USA, Oct. 2000), SEI and IEEE CS.
- [68] Wang, F., Gong, F., Sargor, R., Goseva-popstojanova, K., Trivedi, K., and Jou, F. "SITAR: A Scalable Intrusion-Tolerant Architecture for Distributed Services". In DARPA Information Survivability Conference and Exposition (April 2003), vol. 2, pp. 153 - 155.
- [69] Wang, D., Madan, B. B., and Trivedi, K. S. Security analysis of sitar intrusion tolerance system. In SSRS '03: Proceedings of the 2003 ACM workshop on Survivable and self-regenerative systems (New York, NY, USA, Oct. 2003), ACM, pp. 23–32.
- [70] NIST. Security requirements for security modules. Federal Information Processing Standard 140-2, National Institute of Standards and Technology, May 2001. Available at <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.
- [71] Kothari, K. MIMIC: An active covert channel that evades regularity-based detection. Thesis, degree master of science computer science, The University of Texas at Arlington, May 2010.
- [72] Virgil D. Gligor, J. K. M. A guide to understanding covert channel analysis of trusted systems. Technical guideline NCSC-TG-030, Library No. S-240,572, National Computer Security Center, Fort George G Meade, Maryland, Nov. 1993.
- [73] Hegde, P., and Roberts-Hoffman, K. ARM Cortex-A9 vs. Intel Atom: Architectural and Benchmark Comparisons. Tech. rep., University of Texas at Dallas, Sep. 2009.
- [74] Paul A. Strassmann, Biography, <http://www.strassmann.com/bio/>
- [75] DARPA BAA 10-70 CRASH, <https://www.fbo.gov/spg/ODA/DARPA/CMO/DARPA-BAA-10-70/listing.html>
- [76] Ma, Z. New approaches to reliability and survivability with survival mode analysis, dynamic hybrid fault models and evolutionary game theory. Dissertation, degree of doctor of philosophy, University of Idaho, May 2008.

- [77] Ma, Z., Krings, A. W., and Sheldon, F. T. An outline of the three-layer survivability analysis architecture for strategic information warfare research. In CSIIIRW '09: Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research (New York, NY, USA, Apr. 2009), ACM, pp. 1–7.
- [78] Shrobe, H., Knight, T., and de Hon, A. Tiara: Trust management, intrusion-tolerance, accountability, and reconstitution architecture. Tech. Rep. MIT-CSAIL-TR-2007-028, Computer Science and Artificial Intelligence Laboratory, May 2007.
- [79] Strassmann, P. Securing Microprocessors for Software-as-a-Service. Blog entry, Strassmann's Blog, May 2011. <http://pstrassmann.blogspot.com/2011/05/securing-microprocessors-for-software.html>
- [80] Ried, S., Kisker, H., Matzke, P., Bartels, A., and Lisserman, M. Sizing The Cloud - Understanding And Quantifying The Future Of Cloud Computing. Tech. rep., Forrester Research, Apr 2011. <https://www.forrester.com/report/Sizing+The+Cloud/-/E-RES58161>
- [81] Layne, N., and Hals, T. Sony faces global legal action over data theft. Tech. rep., Reuters, Apr. 2911. <http://www.reuters.com/article/2011/04/28/us-sony-idUSTRE73R0Q320110428>
- [82] SafeNet, www.safenet-inc.com
- [83] Cloud Switch, <http://web.archive.org/web/20121015175355/http://www.cloudswitch.com/> (Archived copy of the website)
- [84] Shipley, G. Research: Cloud Governance, Risk and Compliance. Tech. rep., InformationWeek Analytics, July 2009. <http://analytics.informationweek.com/abstract/83/1075/IT-Business-Strategy/research-cloud-governance-risk-and-compliance.html>
- [85] Coviello, A. Keynote transcript. Transcript, RSA Conference 2010, March 2010. <http://www.emc.com/collateral/legal/coviello-rsac-us-2010-keynote.pdf>
- [86] DARPA. I2O Mission-oriented Resilient Clouds (MRC) Proposers Day Webcast. Defense Advanced Research Projects Agency (DARPA), 3701 North Fairfax Drive, Arlington, VA, May 2011. <http://events.dvimaging.net/008/00172/2011DARPAod/?contid=2011DARPAod>
- [87] Espiner, T. UK cybersecurity spending plans revealed. Newspaper article, ZDNet, Apr. 2011. <http://www.zdnet.co.uk/news/security-management/2011/04/20/uk-cybersecurity-spending-plans-revealed-40092586/>
- [88] Espiner, T. Whitehall official outlines cybersecurity funding plan. Newspaper article, ZDNet, Nov. 2010. <http://www.zdnet.co.uk/news/security/2010/11/17/whitehall-official-outlines-cybersecurity-funding-plan-40090898/>
- [89] Centre for Defence Enterprise. Trustworthy Digital Systems. Call for research proposals, UK Ministry of Defence, July 2011. http://webarchive.nationalarchives.gov.uk/20140410091116/http://www.science.mod.uk/events/event_detail.aspx?eventid=125
- [90] NIST Cloud Computing Program, <http://www.nist.gov/itl/cloud/>
- [91] Jansen, W., and Grance, T. Guidelines on Security and Privacy in Public Cloud Computing. (Draft) Special Publication 800-130, National Institute of Standards and Technology, January 2011.
- [92] Badger, L., Grance, T., Patt-Corner, R., and Voas, J. DRAFT Cloud Computing Synopsis and Recommendations. (Draft) Special Publication 800-146, National Institute of Standards and Technology, May 2011.
- [93] Cloud Security Alliance. Top Threats to Cloud Computing V1.0. Tech. rep., Cloud Security Alliance, Mar. 2010. <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>

Several Icons used in this document are from the GNU LGPL Crystal Clear icon set by Everaldo Coelho.