Trustworthy Systems that Leverage Distrust Amongst Sovereigns

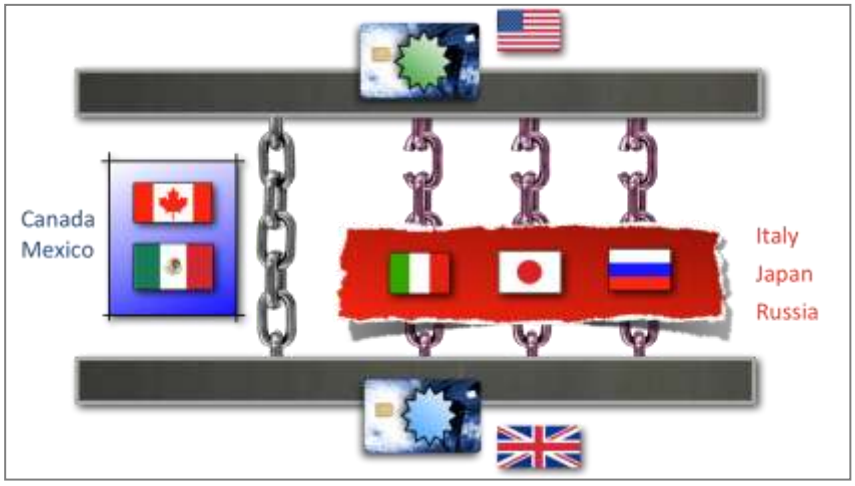
Ronald Kelson
Chairperson & CEO, Synaptic Laboratories Limited, Malta
Vice Chair, ICT Gozo Malta

Benjamin Gittins
Chief Technical Officer, Synaptic Laboratories Limited, Malta
Chief Technical Officer, ICT Gozo Malta

Abstract

Modern societies are almost totally dependent upon cyber systems that are not safe or secure. To paraphrase [7] the Director of the U.S. National Security Agency (NSA): there is no such thing as secure anymore... we must assume the attacker is or can get inside our systems (2010). Successful cyber-physical attacks can strike instantly, destroying critical infrastructure, including nuclear power facilities (e.g. Stuxnet virus) [8]. Many cyber attacks defy accurate attribution [4]. They can gain access to top secret intelligence, industrial control systems, components required to support and/or build nuclear bombs, and so on [20]. Due to the scale of potential (financial and physical) damage from such cyber attacks, any of these activities could fuel an escalation to nuclear war – particularly if physical destruction coincides with a conventional conflict situation [22]. See [23] for global cyber status survey.

As demonstrated by the recent strategy driven nonviolent struggles around the world, grievance groups are increasingly successful at over-throwing powerful institutions that do not uphold the legitimate interests of that grievance group, even in the face of severe sanctions, violent repression, and even death (Dr. Gene Sharp [1]).



We believe it is possible to design credible regional, international, and global-scale Information and Communication Technology (ICT) systems that drastically reduce reliance on deterrence strategies and power struggle to build trust between the mutually suspicious participants. These are pragmatic systems that do not rely on the altruism of any party, and that simultaneously leverage distrust between active participants to create trustworthy systems.

This paper discusses threshold based computer systems that can securely distribute power across sovereign service providing entities, in which each entity: a) provides services ($) to the community, b) can guarantee their own security, and c) gains increased security when they collaborate with other entities that are either strangers, competitors, and in particular hostile adversaries [14]. The political tension that discourages collusion between the service

provider entities (nations) can be exploited to provide higher assurances of security to all clients/stakeholders:

This new ICT architecture adapts political techniques that were originally designed to reduce fear between humans of unequal power.

1. Are there alternatives to (violent) sanctions?

In our view it is possible to design and deploy global-scale systems (that perform formally-defined and agreed services for all stakeholders) that:

a) drastically reduce reliance on deterrence strategies (the threat of sanctions/terror) or on power struggle (the threat of severing the institutions various sources of power) to build trust between the mutually suspicious participants; and

b) do not rely on the altruism of any of the parties, but rather simultaneously leverage any pair-wise association of: integrity, (unilateral or mutual) distrust, and even outright hostility between participants, to create trustworthy systems.

Over-riding self-interest within various institutions and organisations has resulted in the global deployment of, and dependency on, fundamentally insecure computing and communication systems. However, the same myopic self-interests can be intelligently leveraged to begin to make these systems safer in a manner whereby each participating nation state can trust in its own security controls, but gains stronger security through collaboration with other nation states, where each state's security becomes like an independent, redundant strand in a woven steel rope. In this model, any one strand is strong enough. The model can scale up to create international, multi-jurisdiction, global-scale ICT systems. A similar model can also be adapted all the way down to singular computer chips.

2. Tell me again, what has ICT got to do with nuclear deterrence?

Today ICT is as essential as water and electricity. We are all reliant on the same hardware, software, protocols and systems. Unfortunately, today's ICT infrastructure is not trustworthy and cannot be depended upon. To quote [5]: *"[Security] Threats to cyberspace pose one of the most serious economic and* ***national security challenges*** *of the 21st Century for the United States and our allies."*

To quote Melissa Hathaway (who led [5]): "In director *[ed. of U.S. National Intelligence] Blair's testimony to the Senate in February, he stated: 'The national security of the U.S., [and] our economic prosperity [is] threatened.'* ***And I would say that it is compromised.****"* (2010) [6] To quote Debora Plunkett, Director of the Information Assurance Directorate (IAD), U.S. NSA: "There is no such thing as **Secure** anymore." (2010) [7], [8].

To quote Isaac Ben-Israel, Director of the Defense R&D Directorate in the Israel Ministry of Defense (1998-), *"If you want to hit a country severely you hit its power and water supplies.* ***Cyber technology can do this without shooting a single bullet.****" (2012)* [9].

Unlike nuclear weapons, generally speaking cyber-attacks against critical infrastructure can originate from any location, and successfully strike within the Observation-Orientation-Decision-Action loop [7] of human defenders.

Latent vulnerabilities and malware, sometimes deliberately built in at point of manufacture, could be exploited at any time. Fundamental vulnerabilities in the conceptual design of these systems are well known inside expert circles.

To quote Brian Snow, former Technical Director of the U.S. NSA IAD for 12 years: *"The creators of the Internet knew that MALICE was a serious issue." ... "However, [they]*

pushed security aside due to the perceived difficulties, or cost, and that is the start of our problems today. To put it bluntly, the Internet was not built to address the known risks. By design, the Internet naïvely relies on the honesty of every network user, and places far too little emphasis on healthy mutual suspicion! The cost and risks were not eliminated -- rather they were both shifted away from the designers and the manufacturers, and transferred to the Global user base. You and me pick up the check!" (2012) [17]

To quote a security expert from CISCO on the Civilian Identity Management Infrastructure: *"In practice is it snake oil? It is somewhat indistinguishable [ed. from placebo] in practice because of the problems."* (2010) [14]

To quote a Director at the U.S. Center for Strategic & International Studies (CSIS) [8]:

"The electrical grid. A popular target in the military." ... "If I was a hacker, and I hacked into the control system, kinda like stuxnet, of one of these big huge room-sized generators, what could I do to it?

The answer is: you can make it jump up and down, emit smoke, and shake itself to pieces."

To quote a Former U.S. NSA Director's Fellow [21]:

- An attack could bring down the electricity grid for 6 months;
- This would lead to no communications, no banking, and food production ceasing.
- It would require months to bring the country back online.

See [23] for a high level survey of expert opinions wrt. the known problems undermining today's ICT ecosystem.

3. Cyber attacks on critical infrastructure as a catalyst leading to nuclear war

According to the World Economic Forum's Global Risks 2012 Report [19]: Critical systems failure was identified as *"a key concern for world leaders from government, business and civil society" and that this will "most likely be caused by cyber attacks".* Today, cyber attacks rank 4th out of 50 global risks.

Today, potentially more than 140 countries have a cyber weapon development programme. Many nation states, acting out of fear, will imitate DARPA's global cyber-offensive "Plan X" [10], [11].

It is exceeding difficult to assign attribution to cyber attacks [4]. A cyber attack may *appear* to originate from a specific computer. However that computer may have been compromised with malware, malware that is under third party control and forwarding the attack without the legitimate owner's knowledge or consent. Attacks can be relayed through many computers and countries.

We only have to imagine a modern "Cuban missile crisis" like situation in which an anonymous third party starts destroying critical infrastructure in either the USSR or the U.S. The situation will aggressively escalate if at first viewing it appears that the attack originates from the other country. However, it is quite possible that this other country's computers are *also* compromised, and simply form a link in a chain where the ultimate attacker is beyond identification or reach during the critical go/no go decision window of any retaliation or preemptive strike by either of those two countries.

We need an effective global-scale inclusive common cyber defence that does not rely on the threat or use of violent sanctions. Key objectives are to design ICT systems:

1. from the onset take into account the human trust factor to manage known risks;
2. that maintain integrity when latent faults or undetected malware are exploited; and
3. that employ parallelism and redundancy where each instance is independent (sovereign) and sufficiently secure; in which some non-trivial number of different instances must be broken to break the system.

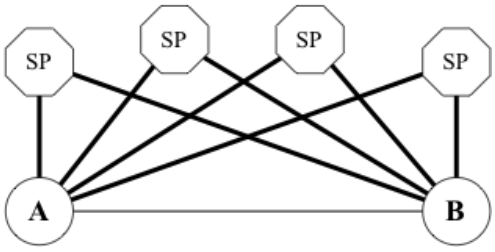
Synaptic Labs has successfully pursued advanced research and design based on these approaches.

4. Decentralising power

Systems, involving humans or computers fail in countless ways. We cannot rely on any "entity" to behave consistently in our best interest. Dictatorships are a prime example of "single point of trust failure". We must build trustworthy systems from potentially untrustworthy entities. One technique is to employ separation of powers [2]. In principle, if one branch of state malfunctions, the other two (or more) can limit the damage and rebalance the system – this being the key goal.

5. Decentralising trust in computer systems

In 1976, Hellman, Diffie and Lamport proposed a simple computer system [12] that decentralised power. In this case, instead of relying on 1 service provider (SP), the burden of responsibility was distributed over 4 (or more) service providers. Unlike in "human systems", in computing it is trivially easy for many computers to perform **exactly** the same operation.



This computer system was designed to provide "identity management" and "secure communication" services. User A could ask to send a message to User B. User B would receive that message and receive 4 assertions regarding the identity of the sender. Without going into the technical details of *how*, for the purpose of *privacy* only 1 service provider had to behave honestly with regard to users A and B. For the purpose of *availability* you could deploy the system to remain operational in the face of 1, 2 or even 3 *simultaneously exploited* arbitrary faults (collusion or third party attack).

6. Leveraging distrust to increase trustworthiness

The goal is to create a decentralised system of nodes that avoids imploding on itself (resulting in a centralised system) or exploding (disintegrating). When power is decentralised across entities, we want to ensure each entity wishes to participate in the system but not collude, and ensure that the system is tolerant to arbitrary operational faults.

All systems that decentralise power are a type of *threshold* system. After some threshold is met or exceeded, it is assumed the correct decision has been made (e.g. taking the consensus opinion regarding a question decided by vote).

The system's integrity is compromised if some number of entities greater than or equal to that threshold, are coerced into colluding together as a single entity in a malicious way.

A problem with popular democratic systems is that individual stakeholders typically cannot ensure their security acting unilaterally. This can expose minority groups to prejudices of the majority group. This occurs when democratic principles are misapplied as a tool to decide "*what is in the best interest of the majority*" as opposed to deciding *"what is in the best interest of all stakeholders*."

What is fascinating in Hellman, Diffie and Lamport's 1976 proposal, is that security (privacy) can be maintained by the presence of just ONE honest service provider, even when all other ($N - 1$) participating service providers are colluding. Modern invasion of privacy is a silent/covert failure: we do not know when it is happening, and so we must seek the greatest assurances that it is not happening. In contrast, a divergent decision by one or two parties is a visible/overt failure. This visibility of failure on each client transaction notifies the stakeholder(s) in question and permits them to make a choice to substitute a new service provider for the "faulty" service provider (this can be automated). We make 2 observations regarding tension between service providers:

1. Every entity participating as a service provider can ensure it's own privacy;
2. If a service provider X is a large organisation, the participation of the ($N - 1$) other service providers offers security against insider attacks performed by X's staff provisioning that service.

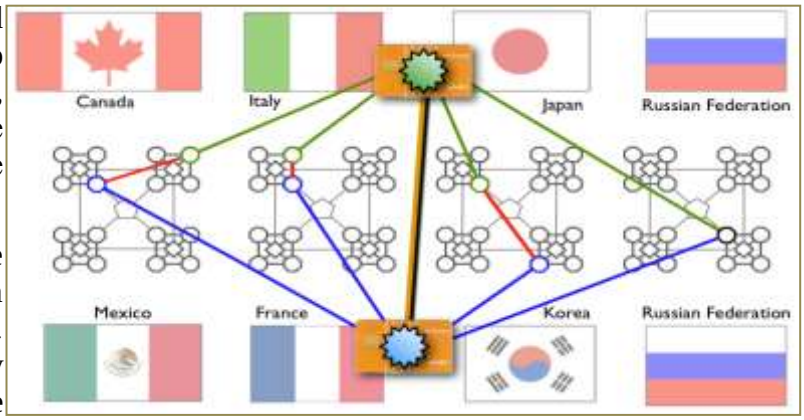
Additional properties can be achieved:

1. A service provider X gains increased assurances that other service providers will not collude against X by ensuring competitors and opponents of those service providers are actively participating in X's client transactions.
2. In global-scale systems, most stakeholders (clients) using the system are NOT service providers. Those stakeholders gain increased assurances the system will protect their legitimate interests if the service providers are strangers to each other, fierce opponents, or preferably adversaries.
3. If each service provider is also a client of the system, they have the ultimate reason not to collude. This increases security assurances for all stakeholders of the system.
4. An unassociated attacker must breach the security of at least 4 independently secure service providers before they can breach the security of the end users' transaction (or attack the clients computer directly).
5. Synaptic Labs' TruSIP computer is designed to to provide similar types of security fault tolerance to the client's and service provider's computers [23]. (Protect all stakeholders.)

7. A scalable decentralised ICT System: A simplified one-page description

In this section we offer a simplified description of part of our peer-reviewed [13] global scale identity management service cited in [18] at NATO. Find a highly accessible video presentation of this technology online at the 2010 IEEE Key Management Summit [14]. Also see [15], [16]. *This system has greater flexibility, security, and capabilities, than briefly described here.*

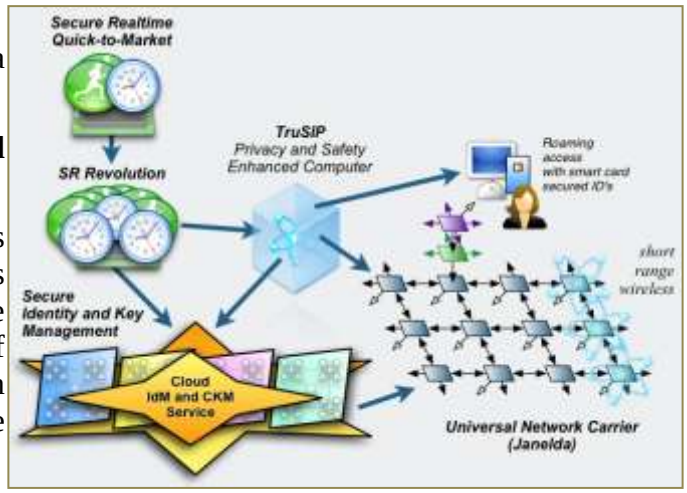
Just like in the Hellman, Diffie and Lamport 1976 proposal, we also **distribute trust** over *N* different entities, in this case we replace "service providers" with confederations of service providers:



Hundreds of different service providers, from different countries, can be members within each "confederation". Advantageously, client transactions only need to employ *at most* 2 service providers from each confederation to enable secure services between them. If one service provider is compromised, or goes rogue, only a small subset of the stakeholders are potentially effected.

In this hypothetical configuration, the system **maintains privacy** for the end users so long as none of the service providers in one confederation colludes with one service provider from each of the other confederations. In short, collusion is difficult due to existing political tensions.

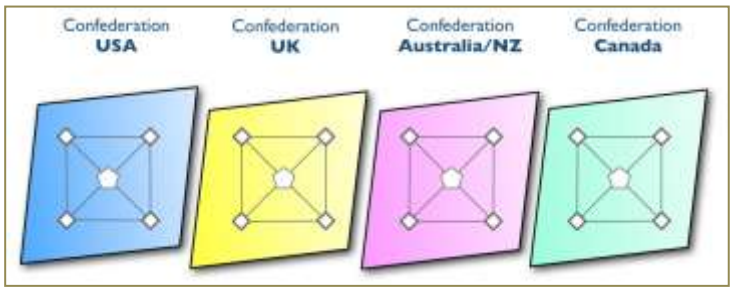
This simplified system is strengthened in a variety of additional ways not described here.



8. Foundations of a trustworthy and dependable ICT ecosystem

In the same way that some Governments employ a wide variety of political techniques (originally [2]) with the goal of protecting the legitimate interests of its citizens, the creation of a trustworthy and dependable ICT ecosystem requires a variety of different techniques to be adapted to the particulars of each component.

Synaptic Labs has been working ~12 years studying the open hard safety and security problems in today's ICT ecosystem, and designing commercially viable solutions in fields ranging from safe and secure realtime computing (used for critical infrastructure applications) through to a next-generation network to improve the security and performance of today's Internet system.



Our technologies are explicitly product and vendor neutral. In many cases our solutions can be adopted by today's market leading ICT companies to harden the next generation of *their* existing product families.

Synaptic Labs' goal is to protect as much of today's existing ICT software and hardware as possible at the least cost. Visit http://ictgozomalta.eu and [23] to learn more.

9. Closing statement

Todays's ICT ecosystem was not built to be trustworthy or dependable [6]. Cyber-physical attacks against critical infrastructure can lead to situations that escalate to nuclear war. As countries become increasingly cognisant of their almost total dependence on today's ICT ecosystem [5], countries will seek to protect their sovereignty and "secure their interests". Fear has already driven many countries to develop cyber-offensive [10], [11] capabilities as a deterrence strategy. It is difficult to attribute the true origin of cyber attacks, making accountability difficult, sanctions complicated, and opportunities for abuse high.

What is required is an inclusive global-scale ICT ecosystem that encourages mutually suspicious entities to collaborate in a way that results in a system that seeks to protect the legitimate interests of all stakeholders, irrespective of their relative power relationship, without reliance on violent sanctions. We have shown how to adapt the spirit of some political techniques in the architecture of a global-scale Identity Management ecosystem. It is the authors experience, that almost any ICT system can be hardened to be much more trustworthy and dependable.

Any entity supporting the design, development and deployment of these approaches will increase regional, national and global stability by improving the trustworthiness of our common ICT foundations, and by building a more stable base from which to reduce our perceived dependency on, and desire to own, nuclear weapons.

References

1. G. Sharp. *There Are Realistic Alternatives.* The Albert Einstein Institution, December 2003. Free LibriVox Audiobook.
2. B. d. M. de Secondat, Charles. The Spirit of the Laws.
3. F. Osinga. Science, Strategy and War, The Strategic Theory of John Boyd. Universiteit Leiden, Jan. 2005.
4. UK Strategic Defence and Security Review. 2010.
5. Cyberspace policy review, United States, May. 2009.
6. M. Hathaway. Plenary speaker. CSIIRW-6 ORNL, 2010.
7. J. Wolf. U.S. code-cracking agency works as if compromised. Newspaper article, Reuters, Dec. 2010.
8. AtlanticLIVE. The atlantic and government executive cyber security forum. Video, The Atlantic, 2010.
9. Grauman. Cyber-security: The vexed question of global rules. Security & Defence Agenda, Brussels, Jan. 2012.
10. Fed Biz Opps.Gov, DARPA-SN-12-51, 2012.
11. Ellen Nakashima, With Plan X, Pentagon seeks to spread U.S. military might to cyberspace, The Washington Post, 2012.
12. W. Diffie and M. E. Hellman. Multiuser cryptographic techniques. In AFIPS '76, June 1976. ACM.
13. B. Gittins. Overview of SLL's proposal in response to NIST's call for new global IdM/CKM designs without public keys. In Proceedings of the CSIIRW-6, ORNL, 2010. ACM.
14. B. Gittins and R. Kelson. 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. http://storageconference.org/2010/Presentations/KMS/Videos-HD.html#16

15. B. Gittins. Outline of a proposal responding to E.U. and U.S. calls for trustworthy global-scale IdM and CKM designs. Report 2011/029, Cryptology ePrint Archive, 2011.
16. B. Gittins and R. Kelson. Feedback to NIST DRAFT Special Publication 800-130. Comment, August 2010.
17. B. Snow, Our Security Status is Grim (and the way ahead will be hard), Video. Nov. 2011.
18. O. McCusker, et al. Combining Trust and Behavioral Analysis to Detect Security Threats in Open Environments. In NATO IACDS 2010, RTO-MP-IST-091, April 2010.
19. Global Risks 2012, Insight Report. World Economic Forum, seventh edition, 2012.
20. J. Brenner. America the Vulnerable - Inside the new threat matrix of digital espionage, crime and warfare. Penguin Press HC, The, Sep. 2011.
21. O. S. Saydjari. Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action. Testimony before the House Committee on Homeland Security Subcommittee, Apr. 2007.
22. Beyond War - A New Way of Thinking, Handbook, 1985. Editors: Dr Martin Hellman, et al.
23. Synaptic Labs 2012 Annual Cyber Status video & slideshow series: http://tinyurl.com/SynapticLabs2012CyberStatus