National Cyber Leap Year Summit 2009:
Exploring Paths to New Cyber Security Paradigms
Draft Report

August 24, 2009

Additional Ideas

The following unedited ideas were contributed by participants at the National Cyber Leap Year Summit as additional ideas for consideration and comment. The Summit is managed by QinetiQ North America at the request of the NITRD Program, Office of the Assistant Secretary of Defense Networks and Information Integration, and the White House Office of Science and Technology Policy.

Please **provide your comments**, if any, **by September 3, 2009** for utilization by the Summit's program co-chairs at http://www.co-ment.net/text/1451/. To add a comment, select the "Add" tab in the left navigation menu, select (highlight) the portion of the document you are commenting on, and provide your comment. If commenting on an entire section, you may select the section heading to anchor your comment.

If you have any further questions or comments, please visit the National Cyber Leap Year Web site at the following address: http://www.nitrd.gov/NCLYSummit.aspx, or send email to leapyear@nitrd.gov.

A new virtualisable network architecture

Authors (Alphabetical Order): Benjamin GITTINS (Synaptic Laboratories Limited), Larry D WAGONER (NSA)

- **Idea/Description**: What does this change look like?

A new virtualisable network architecture (VNA) that rides on the current Internet that offers advanced identity management including but not limited to: authentication, non-repudiation, attribution and network introspection. Access to the VNA may be limited to hardened thin client running on a hardened hyper-visor complemented by a hardware token.

To enter an accountable virtual network domain, a multiple-attested federated id will be employed. The ID would be issued by a nation-state or other recognised entity (equivalent to and maybe leveraging passports ID's). For example this issuance of the electronic id could possibly be managed by the US Postal Service and/or US State Department in the United States.

There could exist multiple sub-domains for different sectors such as one for the medical establishment, defense industry, financial industry, e-commerce, etc. Each sub-domain could

potentially have unique policies appropriate for that environment. For example a sub-domain could create a strictly accountable universe for all transactions.

This would largely eliminate Spam, Phishing, Identity Fraud/Spoofing, significantly raise the risks of hacking attacks by having authentication and attribution.

For particular applications, sub-domains could exist on a purpose built communications substrate based on a semi-regular lattice/mesh based communications infrastructure to create to increase availability, performance and security.

The new network architecture should be built using modern security and safety techniques so that it is fit for purpose in critical industrial systems, financial, medical, nuclear, mining, Government, e-commerce.

- **Inertia**: Why have we not done this before?
    - Some of the techniques were not available / we didn't recognise the need for security and safety to extent needed / we didn't rely on technology at the same level we do now
- **Progress**:
    - Significant research in the underlying enabling technologies,
    - Recognised need and appreciation of the need for this particularly in the defence, financial and commercial sectors, there is an acceptance if it was appropriately managed, there is a need for post quantum evolution of security systems, opportunity as e-medical is emerging.

- What would mitigate our doubts?
    - Transparency of system design, It is now technologically feasible

- **Action Plan**:
    - Identify a first team of stake holders interested in participating
    - Explore cross-cutting identity, policy and functionality requirements
    - Develop action plan and secure funding
    - Develop a prototype for a particular sub-domain such as for an emerging sector (e.g, medical establishment) or an critical sector (e.g, the energy sector)

- Who can help (in no order)
    - NITRD, DoE, USPS, US State Department, HHS, IBM, Naval Research Laboratory, the organisations represented by the authors.

A global electronic identity management system

Author: Benjamin GITTINS (Synaptic Laboratories Limited)

- **Idea/Description**: What does this change look like?

A new robust (post quantum secure) global electronic identity management system that more accurately reflects the way human's reason about trust relationships. The proposed GEID system would implement a multiple-attested federated id, that combines the best features of centrally managed certificate authorities, with the ability to have more than one entity attest to an identity. It should also be possible to electronically aggregate multiple issued id tokens to attest a single entity.

The hardware token managing an identity could be issued by a nation-state or other recognised entity. For example this issuance of the electronic ID could possibly be managed by the US Postal Service and/or US State Department in the United States.

More than one party can attest to the identity managed by that token, including Governments, large organisations or other individuals such as friends and family members. The information used to reason about an identity assertion should be managed in a distributed decentralised federated system. The system should ensure interactivity, data minimization, privacy, least privilege, confidentiality, integrity, authenticity and have the ability to be audited by all stake holders. Any enrolled user should be able to request appropriate levels of information to authenticate an identity, however each such request must be audited and in some cases require authorisation by identity being queried.

The system should support "composite" identities, such as Corporations and Organisations, allowing operations to be attested to by an organisation that is seperate from the individuals. For example "Authorised by 3 out of 5 directors of company X". See work by NRL.

The system should be designed to protect against collusions of 'assertion' failure, and provide increased transparency into how an identity has been asserted. The system should include soft and hard reasoning ("I believe this is my child", "I have established this is my child using DNA tests").

Furthermore the system can be adapted so that when a high value transaction takes place, the identity of the actors and the transaction must be attested to by mulitple entites, where the entities are held legally accountable for attesting to that identity/transaction. The accountability is limited only to matters of identity, and knowledge of the transaction, but not the transaction itself.

- **Inertia**:
    - Why have we not done this before?
        - Some of the techniques were not available / identity systems have traditionally be centrally managed.
- **Progress**:
    - Significant research in the underlying enabling technologies,
    - Recognised need and appreciation of the need for this particularly in the defence, financial and commercial sectors, due to international collaboration.
    - Requirements of several different nations have been effectively captured by international implementations of first/second generation public key certificate

authority architectures (See Transglobal Secure Collaboration Program) and European studies (see EU EID-STORK)

- What would mitigate our doubts?
  - It is now technologically feasible,
  - Transparency of system design,
  - Allow identity to audit who has access what information about them at what time and to provide varying level of access control to different oganisations.
  - That assertion information should be distributed and decentralised, where information is selectively released by individual authorisation. i.e., No single database store. Each attestion authority is responsible for managing accuracy of their data.
  - Can leverage existing certificate authority efforts, and allows them to be integrated into new environment.
  - Must be capable of supporting different national/regional policies. Must support interoperable communications between different countries.

- **Action Plan**:
  - Identify a first team of stake holders interested in participating
  - Explore cross-cutting identity, policy and functionality requirements
  - Develop action plan and secure funding
  - Develop a prototype for a particular sub-domain such as for an emerging sector (e.g, medical establishment) or an critical sector (e.g, the energy sector)

- Related to other work group projects:
  - Moving Target Defense : Resilient Cryptographic Systems. The current proposal outlines techniques for relying on multiple non-intersecting security domains to attest to an identity.
  - Digital Provenance : Reputation Engine. The current proposal can be seen as a type of reputation engine.
  - Digital Provenance : Data Provenance Security. The current proposal will share many requirements o the Data Provenance Security group.
  - Digital Provenance : Data Provenance Definition and Management. A global electronic identity management system is required to support the DPD&M proposal.
  - Digital Provenance : Government Role. The current proposal supports one or more Governments participating together with commercial organisations in the administration of a identities in a global system. Each Government can maintain their own identity assertions on an ID while taking advantage of assertions made by one or more over Governments/institutions. This proposal addresses the concern of single point of assertion failure, and mitigates fears of a single ID document.
  - Additional ideas : Virtualisable Network Architecture
  - Additional Ideas : Global post quantum secure cryptography based on Identity. The current proposal can be hosted within the Global PQS CBI proposal.

- Who can help (in no order)
    - NITRD, CyberSpace Sciences and Information Intelligence Research - ORNL - DoE, US State Department, HHS, (Hugo Teufel III of) PricewaterhouseCoopers, Synaptic Laboratories Limited, EU EID-STORK, and others to be identified

Global post quantum secure cryptography based on Identity

Author: Benjamin Gittins (Synaptic Laboratories Limited)

- **Description**

Global cryptographic services (authenticated key exchange, digital signatures, etc) based on identity that is robust and secure against both classical and quantum computer attacks. The system exploits a federated architecture, where at least one organisation from each of the federations participates in identifying users, assisting with key exchange operations and other related functions. This proposal describes an infrastructure suitable to IMPLEMENT the core functionality required on desktops and supporting public infrastructure.

- **Inertia**
    - Technologies exist, but have trust scalability limitations which prevent the creation of a global authentication/encryption network:
        - Voltage Security offer a commercial public key identity based encryption (IBE) product which is ideal for enterprises and small groups of enterprises. However this system has a central point of trust in the server which would prevent acceptance of single global IBE infrastructure being deployed.
        - KERBEROS is an example of a symmetric federated Key Distribution Centre based technology that supports key negotiation by identity. Unfortunately there are security limitations in this context. See the paper [FORMAL ANALYSIS OF KERBEROS 5].
    - Current proposals are not considered to be post quantum secure:
        - Voltage's IBE system does not claim to be post quantum secure.
        - KERBEROS running as a federated system relies on known "at risk" classically secure public key algorithms to achieve scalability. Furthermore, user's access the system using passwords which may not be sufficiently secure.
    - Previously no method for internationally managing name spaces in a way that protects against cyber-warfare by one large agent over another. See the problems that exist with today's public key infrastructure "MD5 considered harmful today - Creating a rogue CA certificate".
    - The use of online servers has prevented up-take in some contexts, but is generally not a problem for Internet communications (which already relies on 24/7 online servers such as the Internet Domain Name Server infrastructure).

- **Progress**
  - Wireless ad-hoc mesh network architectures have advanced the study of multi-path key exchanges over distinct paths using symmetric techniques.
  - Modern Smart cards can be used as trusted couriers for key material between an enrolled user and one or more online key translation centres.
  - Synaptic Laboratories has introduced technologies to express scalable symmetric key authenticated encryption systems where no single trusted third party [or collusion of (n-1) out of n participating third parties] can discover the final key exchanged between two users. This addresses the core trust problem that spurred the design of public key technology (See Quote by Whitfield Diffie).
  - Synaptic has proposed techniques for rapidly integrating the global authenticated encryption scheme into existing products based on SSL/TLS, SSH, IPsec, SSL VPN, and e-mail by "post-processing" the output of unmodified products. This allows all current infrastructure to use current public key standards and maintain FIPS 140-2 compliance and be incrementally upgraded to achieve post quantum security against known attacks.

- **Integration**
  - This proposal can act as a platform for hosting the global electronic identity management proposal, and can support the global key exchange operations based on ID required for the Virtualisable Network Architecture.
  - The Global electronic identity management proposal provides a platform for "describing and reasoning" about an identity and it's trust relationships, where as this proposal supports the real-time authenticated key exchange operation between those identities.

- **Jumpstart Activities**
  - Identify and bring together interested stake holders
  - Explore existing technologies (digital signatures, manage security functions, integrated risk management systems, current public key certificate authority requirements) and draft a high-level requirements document.
  - Perform further independent evaluation of next generation proposed technologies (Independent cryptanalysis on Synaptic's proposal has already been performed by Prof Jacques PATARIN).

- **Further Action Plan**
  - Identify and bring together identity stakeholders into a conference to refine requirements
  - Independent evaluation of next generation proposed technologies
  - Begin development of key exchange technologies and infrastructure

- Related to other work group projects:
  - Moving Target Defense : Resilient Cryptographic Systems - Secret Key Compromise. The current proposal outlines techniques for relying on multiple non-intersecting security domains, where a cryptosystem remains secure against a collusion/compromise of (n-1) out of (n) security domains.

    - Digital Provenance : Global identity-based cryptography. The current proposal outlines a more concrete proposal or achieving Global identity-based cryptography.
    - Digital Provenance : Government Role. The current proposal supports one or more Governments participating together with commercial organisations in the administration of a global identity management system. This proposal addresses many the concern of single point of failures.
    - Additional ideas : Virtualisable Network Architecture
    - Additional Ideas : A global electronic identity management system

- Who can help (in no particular order)
    - NITRD, ORNL - DoE, US State Department, MITRE, Secure Systems - IBM, Boeing, Naval Research Laboratory, ICSA labs, PricewaterhouseCoopers, Terra Wi, Synaptic Laboratories Limited

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

Author: Benjamin GITTINS (Synaptic Laboratories Limited)

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

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

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

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

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

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

Measuring the wider impacts of unauthorised information disclosure

Author: Benjamin GITTINS (Synaptic Laboratories Limited)

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

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

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

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

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

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

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

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

Semiconductor Intellectual Property Protection

Author: Benjamin GITTINS (Synaptic Laboratories Limited)

- **Description -**

Synaptic Laboratories has proposed a method of designing semiconductor devices with improved trust characteristics that protect the Intellectual Property rights and profits of the fabless semiconductor design house.

Combinatorial locks can be implemented in a hardware circuit by inserting or replacing hard-wired logic with programmable logic. The logic for the look up table is locked away in a private database such as a smart card until it is used to unlock the device. An attacker must select the correct value to unlock the programmable logic that ensures correct and reliable operation of the device. This value can be remotely programmed using symmetric cryptographic techniques. To improve the utility of combinatorial locks we propose splitting the circuit design across at least two teams (Yellow and Orange) such that each team is responsible for managing independent locks in their respective modules. The remaining unlocked source code can be exposed to all teams enabling more efficient development practices over other existing more restrictive approaches. This process allows global placement and routing of performance sensitive code without risk of chip over manufacture due to unauthorised disclosure. Simulation of the chip design is efficiently achieved using an enhanced distributed chip simulator of two or more machines. The yellow and orange teams are responsible for ensuring their portions of locked code are simulated at full speed by machines they trust will not expose their locked logic. After a circuit is finalised traditional risk management techniques are recommended to prevent modification of the circuits before and/or during manufacture of the wafer masks, there by providing assurance against a wide range of attacks. Each team is responsible for securely loading their portion of the locked circuit behaviour into each manufactured chip from a remote location or a tamper proof module.

- **Intertia -** There are currently no split team development, synthesis, place-and route or simulation tools that can be used to compartmentalise portions of code.

- **Progress -**
  - New techniques to ensure verilog/VHDL software protection through to manufacture have been recently proposed.

- **Jumpstart Activities** -
  - Identify a large semiconductor organisation, such as Intel, that is sensitive to IP theft, and get them to perform an initial evaluation of the techniques.

- **Action Plan -** Identify one or more semiconductor organisations. Perform an independent evaluation of the techniques. If validated, work with a company like Synplicity to modify EDA tools, and develop a complete process for working with fabrication facilities. Work

with companies such as Certicom who offer chip programming facilities for supporting per-chip enabling.

- Who can help:
    - NITRD, DoE, Intel, Certicom, Synplicity, Universities of Michigan and Rice (EPIC).

Dynamic Distributed Key Infrastructures (DDKI) – a topology

- **Idea**:

Dynamic Distributed Key Infrastructures (DDKI) – a topology & Dynamic Identity Verification and Authentication (DIVA) – a process & Whitenoise – a cryptographic algorithm

Authors: Andre Brisson & Stephen Boren

- **Description**:

For 35-40 years we have relied on Public Key Infrastructures (PKI). They have always been vulnerable to man-in-the-middle attacks. They do not scale well. They are very expensive. It is a given that they will not be post quantum computing secure (PQCS). DDKI provides a complete, new generation identity-based, cryptosystem that incorporates: Complete federated and distributed key and identity management configuration, for example:

Horizontal implementation example

- Complete identity can be aggregated at a central location like an non-government organization trusted third party that brings together the stakeholders from public-private partnerships i.e. government, law enforcement, industry, watch groups such as an international or national body comprised of privacy and security experts from all articulated stakeholders.

- Complete identity can be parsed and federated horizontally between different stakeholders within government to create checks and balances that reflect democratic societies. No one entity/department would have the complete identity of an individual/entity/device and act on a complete identity without transparency to other sectors of the government i.e.:

- Department of Census: responsible for issuing identity

- Department of Homeland Security: responsible to integrate sharing of identity with all levels of law enforcement, military, and intelligence

- Privacy Commissioner: responsible for creating the transparency to all private stakeholders including citizens, commercial entities etc. to reflect the values inherent in democratic societies (this is the "sunlight is sanitizing" element). They would be mandated to enable the sharing of responsibility for cyber-security. They would enable and oversee effective information sharing/incidence response.

- Department of Justice: legally (public liability rests here) responsible for "following the letter of the law" by ensuring there is no abuse or manipulation of legislation regarding identity and privacy

- Department of Education: responsible for building the capacity for a digital nation

- Department of Foreign Affairs: responsible to bring likeminded nations together on a host of issues

- National Institute of Standards and Technology: responsible for enabling the building of the architect of the future. Building the architect of the future is a technological reality with the goal that the technology works securely, is accessible to any stakeholder, and that it integrates identity management. It reflects the values of democratic societies.

The architect of the future must be elastic enough that it inherently can adjust to historical context in terms of the appropriate balancing of privacy and security. For example, during times of war security may require greater latitude (by legislation) and during times of peace there are degrees of greater privacy. This is the inherent democratic challenge of balancing privacy and security in technology.

Note: for stakeholders frightened of "growing government" this structure can be condensed into one department for efficiencies with the same kind of mandate as Department of Homeland Security whose task is to integrate all elements of law enforcement and military.

Vertical implementation example
Complete identity can be parsed, federated and distributed vertically between government/law enforcement/military and industry and citizenry. For example:

- Government is the repository for the abstract of universal identity – i.e. they issue master identity keys to authorized and trusted private commercial entities like telecommunications providers and private national security entities like the military etc.

- In public sectors, telecommunication providers can issue identity management keys to citizens and entities (devices/non human nodes) reflecting the degree of anonymity required by different activities. Note – this places a burden of responsibility upon this layer which creates incentives to act securely. For example, if they want to provide complete anonymity for their clients, then private commercial entities assume the same complete responsibility and liability as the users of their services to comply with the law. When the law is breached both the criminal and the facilitator of criminal activity assume the same (or proportional) liability. There are degrees of legislated opt out of liability

paths by adjusting the degree of liability the criminal and provider have dependent on the amount of specific user information they share with law enforcement and government entities. This provides a disincentive to allow cyber crimes like hate speech, electronic fraud, etc. This provides an incentive for private commercial entities to monetize varying degrees of privacy.

- This is a flexible reality that can effectively be dialed in between stakeholders through legislation: it is not "all or nothing at all" liability. It can balance 'the profit motive' versus 'the responsibility' conundrum.

- Depending upon what the public commercial sector decides to provide, citizens and entities can each choose what level of identity they wish to utilize to use critical telecommunication infrastructures. Complete anonymity of "users" places equal liability upon the private commercial sector. Pseudo anonymity shares the responsibility between network infrastructure users and network infrastructure providers. Use of reasonable legislated Identity places the entire burden of liability upon the government. All stakeholders can 'opt in' or 'opt out' of varying levels of identity and privacy. This allows all stakeholders (government/public and corporate/citizen/private to have both public and private identities, as well as multiple kinds of Identities.

Note: at the ends of the liability/responsibility spectrum we have one of two realities:

1. The private commercial sector shares equal responsibility with the criminal private citizenry sector.

2. The government sector shares equal responsibility/liability with the private criminal sector and the private commercial sector has no responsibility/liability at all.

In between, degrees of liability/responsibility are directly proportional to the degree of anonymity that the commercial private sector can monetize.

- **Inertia**: Why have we not done this before?

    - Lack of interoperability

    - The technology did not exist before. It exists and is available today.

    - Competing political, philosophical and economic interests

    - Complexities and costs of implementation such as scalability, access control, key manageability, reversibility (forensics), checks and balances, elasticity of systems, overall overhead and complexity of systems, and 'privacy fears' while remaining secure.

    - Ease of use and understanding

- Lack of will power, vision, direction, incentives

- **Progress**: Why is this feasible now?

DDKI and DIVA technically provides:

- Federated, distributed Identity Management
- Intrusion detection making the architecture real-time for legitimate forensic use and optimal system integrity
- Continuous Authentication providing a moving target defense
- Automatic revocation ensuring an attack can only happen once
- Repudiation/non-repudiation which is integral to 'need to know', 'chain of command', forensics, liability, and responsibility. This can be inherent within the design due to how DIVA manages authentication.
- Digital Rights Management which is integral to 'need to know', 'chain of command', forensics, liability, and responsibility. This can be accomplished by Digital Object Online Resource Sharing [DOORS].
- Authorization which is integral to 'need to know', 'chain of command', forensics, liability, and responsibility
- Complete and secure federated key and identity distribution capacity that allow systems to scale infinitely, allow 'on the fly configuration' to reflect changing political and social context

DDKI and DIVA and Whitenoise also:

- exploits revolutionary identity based cryptography that embeds characteristics of a one-time pad (moving target defense)

- exploits revolutionary identity based cryptography that is bit independent (immune to current and known cryptanalytic attacks and vulnerability) and which makes it indifferent to current technological limiters such as data/memory/key leakage which is the basis of current cryptanalytic attacks like "Side Channel" attacks in Hardware. It also makes it immune to "mathematical shortcut attacks" as well as 'brute force' attacks. It plugs the security hole in Hardware-enable trust. This swings the cost/benefit dynamic towards the greater interests of society by making illegal behavior prohibitively expensive and approaching technologically infeasibility. This plugs the Cyber Economic hole and ensures in the vast majority of user cases that 'crime doesn't pay.'

- exploits revolutionary identity based cryptography that is post quantum computing secure because the security strength of the architecture is exponential and inherently scalable 'on the fly' by the simple addition of subkeys to existing Identity Management and encryption (both cryptographic) keys to readily scale strength by exponential orders of magnitude.

- exploits revolutionary identity based cryptography that will always stay ahead of the exponential computing processing threat curve because in software the speed of the

cryptographic algorithm is limited by the existing computational power at any time because the speed of the cryptography is limited by the processing capacity of any hardware at any given time. This is because this cryptography is the first secure cryptographic technology that predominantly exploits the fastest available computer mathematical function, the X/Or process. This plugs the security hole inherent in current Hardware-enabled trust.

- exploits revolutionary identity based cryptography that allows 'virtual manufacturing and provisioning' and lower costs by orders of magnitude, and increases accessibility (very democratic) because of the reality that software based critical infrastructure security is more secure and flexible because it is dynamic and not static. [Note: capitalistic profit motive systems have a natural tendency to drift towards a state of industry choosing the most expensive option with the least amount of service in order to solely enlarge profit margins at the expense of greater social responsibility i.e. systemic failures creeping into such systems as financial, insurance, and health care/provision]

- exploits revolutionary identity based cryptography that allows analyzing of 'communities of interest', and then modeling of simulated systems utilizing key-stream as input to fractal models for evaluating health and nature inspired networks at either macro or micro levels.

- exploits revolutionary identity based cryptography to ensure digital provenance across all technical layers of the Internet and critical communication infrastructures, enables interoperability across all platforms/operating-systems/domains, and all technological layers application-layer, network-layer, data-layer, physical-layer etc. It also enables interoperability between abstracted communities of interest: technological, social, political, philosophical etc.

- exploits revolutionary identity based cryptography to ensure digital provenance by resolving the IP overload issue (the 'IP Identity Problem') caused by the semantic overloading of IP addresses containing both an IP address locator (network topology location) function from a node identity function. This enables networked entities to know the identity of its networking peers and to use that identity as a basis for authentication and authorization. This is resolved because DIVA is independent of the IP address and provides direct authentication regardless of the number of branches and modifications that are handled through the network. It is simply an end-to-end authentication system that is virtually impossible to access illegally without detection.
- exploits revolutionary identity based cryptography to resolve the packet ordering issue. UDP headers have only routing information and no packet ordering information. TCP/IP is supposed to manage packets in their proper order. DIVA can be used as an alternative mechanism to not only authenticate but to order the incoming packets without adding bandwidth.

- exploits revolutionary identity based cryptography to secure digital provenance of data at rest and data in the 'cloud.'

- exploits revolutionary identity based cryptography which is the single common denominator and enabler that is required to achieve all articulated goals of the Leap Year 2009 Summit including allowing global encryption based on identity that is robust and enduring, attaching context to data, expanding trustworthy systems, facilitating unspoofable trusted paths/channels and securing data provenance on a 'need to know' basis.

- It is completely non-disruptive and allows seamless transition to Leap Ahead network cyber-security.

- It is ready today. It addresses all the inertia problems.

-- **Note** on BOTS – As we move over to a identity based network system BOTS will be able to be controlled and managed in a more effective way. In situations where they are not warranted they can be precluded.

- **Action Plan**: What are reasonable paths to this change? What would accelerate this change?

    - Commit to these initiatives with funding, education, resources (both public and private) and the full endorsement of the National Cyber Leap Year initiative.

    - Strategic use cases in environments of stakeholders – intelligence/military/law enforcement, health care, financial and insurance, and utilities (SCADA – System Control and Data Acquisition) and critical infrastructures i.e. identifying and measuring the globalization and interoperability characteristics across all communities of interest and stakeholders.

- **Jumpstart Plan**: (Pieces of the action plan that can be started now)

joint testing and certification

- Immediately bring in technology for joint testing and certification involving the National Institute of Science and Technology (United States of America) and Communications Security Establishment (Canada) and any willing International Standards Boards and International Regulatory entities for complete transparency throughout the process.

joint development and deployment

- Engage in a joint development and deployment of DDKI, DIVA and Whitenoise into the Intelligent Grid at the British Columbia Institute of Technology and a project site in the United States of America simultaneously. [Apply scientific methodology by using a blind verification of reliability and validity of the technology and topology.]

trial and measurement of the implementation

- Encourage trial and measurement of the implementation in a large commercial telecommunications carrier – one in the United States and one in Canada – with the simple deployment of DIVA in a secure network access protocol. This requires simply the addition of three data base fields in the login database of the carrier: a unique identifier field, a unique key structure field, and a dynamic offset field at the carrier server. Electronically provision the endpoint with the DIVA utility (20kB – 150 kB) on any network enabled entity/endpoint/device.

  Note: this eliminates any needed integration with any firmware (all proprietary). The physical endpoint simply needs connectivity, memory/storage, and write back capacity for the dynamic, continuously-changing offset. This eliminates the possibility of impeding project progress because of lack of agreement between conflicting communities of interest or commercial private entities. Democratically, they are free to opt in or opt out without affecting the goal attainment framework.

  Note: this eliminates any risk to removal or bypassing of the protocol because there can be no network access without the continuous authentication verification. If the endpoint cannot provide the required authentication token there can be no network access.

implement a DIVA/Whitenoise enabled FPGA

- Immediately implement a DIVA/Whitenoise enabled FPGA and test for vulnerabilities against Side Channel attacks.

Removing barriers to entry for crypto products into Federal Use

Author: Unknown

- **Idea**: Streamline and expedite the approval process for Federal use of new security technologies
- **Description**: Many commercial security technologies are unavailable for Federal use even though they are well accepted and widely deployed in the private sector. These technlogies often allow dramatic cost savings and efficiency gains over older technologies, but Federal agencies are unable to use them because the technologies have not received the necessary certifications and approvals. In some cases, the existence of rigorous, formal proofs of security should eliminate the need for the long certification and review process and allow Federal agencies to receive the same benefits that the private sector is now realizing. A decade or more is too long for Federal agencies to wait to realize the benefits of new security technologies. Let's find a way to get new technologies used more rapidly.
- **Inertia**: This has not been done yet beause the Federal agencies involved in approving new security technologies have relied on the "wait and see if it's secure" model so far. This approach usually determines which technologies are sound and which ones are not,

but takes many years and leaves Federal agencies unable to use the innovative security technologies that are being invented today.

- **Progress**: Provable security has made the "wait and see" model unnecessary in many cases. If there is a peer-reviewed formal proof of the security of a technology, that should be enough to get approval for Federal use. If the proof is correct then the technology is secure. Why wait ten years or more if that's the case?
- **Action Plan**: NIST should determine a way to quickly approve provably-secure technologies for Federal use and should review existing regulations and identify ways to allow provably secure technologies within them. This should involve, as a minimum, granting a blanket IATO to new encryption technologies with peer-reviewed proofs of security, and adding provably-secure public-key encryption technologies to the list of techniques that are allowed by FIPS 140-2. In the long run, standards and policies shoud be changed to allow the rapid adoption of new technologies that are provably secure.
- **Jumpstart Plan**: Within 90 days, NIST should define and implement a way to approve provably secure tecnologies for Federal use. Within 180 days, a pilot of one of these technologies should be started at a Federal agency.

REAL-TIME INTERNET “MRI” (ORTHOGONAL VIEW)

Author: Peter Canestaro (Northrop Grumman)

- **Idea**:

Organizations such as the Cooperative Association for Internet Data Analysis (CAIDA) take great pains to measure aspects of the internet, such as internet topology, traffic flow and Autonomous System (AS) interactions. The data retrieved and analyzed by CAIDA and similar organizations are invaluable in attempting to understand the nature and complexities of the internet. However, the collection tools at our disposal are constrained by the internet itself. There is currently no “orthogonal view” of activity on the internet. Unlike tools within the medical profession where an outside observer can take an x-ray or MRI to see a global view of the situation, our view of the internet is very constrained. We are using the internet to observe itself, from an “inside the tube” view. It is as if we are attempting to map the human nervous system from the perspective of the synapse.

If a real-time orthogonal view of the internet were observable by all, then many benefits to global cyber health are enabled, in terms of diagnosis, prediction and defense.

- **Description**:

An orthogonal view of the internet is possible with a simple innovation. Placing information flow sensors at each AS could capture distilled information (such as number of packets per protocol sent to its neighboring AS’s). This information would be continually collected and sent outside of normal channels (perhaps via satellite communications) to a common collection point for consolidation and dissemination. A number of new possibilities are enabled:

- Real-time traffic pattern and "weather" data would be viewable by all;
- Turbulence, anomalies and emerging problems could be observed and perhaps rectified;
- If the collection mechanisms were real-time configurable, they could be commanded (by some national authority) to "drill-down" to provide more specific information concerning a particular attack pattern, tracking that particular threat.
- An "over the horizon" threat detection could utilize this ability to see activity numerous "hops" away, before malicious activity arrived;
- It would be virtually impossible for a coordinated attack to spoof information from all collection mechanisms to hide his activity. Network outages between and among AS elements would not affect the data collected and disseminated; it would be fault tolerant.

- **Inertia**:

This has been done before, on small scales. "Back channels" of communication are a common means of segregating communication for different purposes. Diagnostics or configuration control messages can be segregated from normal network activity in a test/development network. However, this technique has not been attempted an anything as massive as the internet, or significant portions of the internet, because:

- No one takes ownership for the internet (or significant portions of it)
- There is an initial investment to be made that cannot be done by any single commercial or government entity.

There are a few forces that would be natural impediments to implementing the idea:

- Funding: There would be an up-front cost associated with building the infrastructure to collect, integrate and disseminate this data. Additional hardware resources (including perhaps satellite resources) would be needed.
- Corporate Acceptance: Additional cost and effort to install and maintain the collection equipment would be a deterrent, unless there was demonstrable offsetting benefit.
- Consumer Suspicion: The idea that government may be involved with viewing internet traffic may not be accepted with enthusiasm by a suspicious public, unless done in a transparent manner.

- **Progress**:

Technologically, this is already feasible. All needed components exist and could be aggregated for this purpose. Environmentally, the political and economic will may be at a tipping point to where bold, demonstrable action may be welcome, if that action seems to aide internet security

- **Action Plan**: What are reasonable paths to this change? What would accelerate this change?

- Create a of a community of interest to devise specifications and implementation plan
- Specific funding requirements will arise from the implementation plan

- Enact legislation to subsidize the cost of the collection equipment, to improve chances of widespread (national) adoption.
- Momentum: As the number of adopters grows, the benefits of the system increase non-linearly. If a small core group of adopters shows early success, the number of later adopters will accelerate.
- Patriotism: A campaign to contribute to the national cause to help secure the infrastructure within the US could encourage ISPs to participate. Similar campaigns could exist in other countries

- **Jumpstart Plan**: (Pieces of the action plan that can be started now)

- Create a of a community of interest to devise specifications and implementation plan
- Announce X-Prize for best specifications and implementation plan