Idea 2
Dynamic Distributed Key Infrastructures (DKI) – a topology 2
Dynamic Identity Verification and Identification (DIVA) – a process 2
Whitenoise – a cryptographic algorithm 2
Complete federated and distributed key and identity management configuration 2
Horizontal implementation example 2
Vertical implementation example 4
Inertia 5
Progress: Why is this feasible now? 6
Jumpstart activity 9
Action Plan 10

Idea

Dynamic Distributed Key Infrastructures (DDKI) – a topology

&

Dynamic Identity Verification and Authentication (DIVA) – a process

&

Whitenoise – a cryptographic algorithm

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:

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.

Note that a properly designed architecture would not have a single point of attack or failure; these can be removed through redundant servers and distributed databases.

Note that DDKI can be deployed in any horizontal or vertical fashion or any combination therein.

Inertia

- Lack of interoperability
- 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-enabled trust.

    This swings the cost/benefit dynamic towards the greater interests of society by making illegal behavior prohibitively expensive and approaching technological 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. This simply needs to be recognized and managed.]

- 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 such as the 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: when this Identity Management cryptosystem uses encryption that files, data and streams are encrypted bit for bit and the file size or bandwidth does not increase.

--

Note on BOTS – As we move over to an 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.

Jumpstart activity

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. CSE has studied the Whitenoise algorithm internally in Ottawa.

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. Involve government and large private industry/telecoms.]

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. Electronic provision of endpoints with the DIVA utility (20kB – 150kB) on any network enabled entity/endpoint/device is simple and can be no cost.

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.

Action Plan

- 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 i.e. Intelligence/military/law enforcement, health care, financial and insurance, and utilities (SCADA – System Control and Data Acquisition) and critical infrastructures. Identify and measure the globalization and interoperability characteristics across all communities of interest and stakeholders.