



**SYNAPTIC**  
LABORATORIES LTD.

**Ronald Kelson**  
Chairperson and CEO  
Tel: +356 7956 2164  
Fax: +356 2156 2164  
[ceo@pqs.io](mailto:ceo@pqs.io)

**Benjamin Gittins**  
Chief Technical Officer  
Tel: +356 9944 9390  
Fax: +356 2156 2164  
[cto@pqs.io](mailto:cto@pqs.io)

**Synaptic Laboratories Ltd.**  
PO BOX 5,  
Nadur NDR-1000  
MALTA, Europe  
[www.synaptic-labs.com](http://www.synaptic-labs.com)

Sunday, 15 November 2009

# SYNAPTIC PARTICIPATION IN THE U.S. NATIONAL CYBER SECURITY INITIATIVES – 2009

Synaptic Laboratories Limited has been an active participant in the U.S. National Cyber Security Initiatives. Synaptic submitted three proposals in response to the U.S. Federal Government Calls for “Leap-Ahead” proposals. The 238 public submissions, including Synaptic’s, can be found here<sup>1</sup>.

Consequently the Synaptic CTO was invited to attend the ‘closed’ U.S. National Cyber Security Summit<sup>2</sup>.

Six Synaptic proposals were accepted to the Draft Phase and public feedback can be found here<sup>3</sup>. In section 1 below, we copy an example of one of the six draft proposals taken from their website, and comments from world leading IT experts, such as Dr. Lawrence G. Roberts (one of the founding fathers of the Internet).

All six Synaptic proposals were advanced into the Final Participants Report. The Final Reports can be found here<sup>4</sup>. In section 2 below we copy relevant extracts from that Report and highlight in yellow the proposals originating from Synaptic, and the specific references to Synaptic Laboratories Limited.

---

<sup>1</sup> <http://www.nitrd.gov/leapyear/index.aspx>

<sup>2</sup> <http://www.synaptic-labs.com/news/business/301-news-synaptic-cto-invited-to-usa-cyber-security-summit.html>

<sup>3</sup> <http://www.co-ment.net/text/1451/>

<sup>4</sup> <http://www.nitrd.gov/NCLYSummit.aspx>

View ▾
Actions ▾
Home · Public texts · Login · Register

Comments [View all](#)

List (11) Add

Development manager

Cyber Economics - Multiple Networks Proposal

CEO Anagran, Founder Internet (1969)

ICS Security

CyberSpace Policy Review

Additional Questions

Paper: "Broken Promises of Privacy"

Select and work with an innovator to break down barriers...

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

August 24, 2009

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. 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](mailto: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.

# **National Cyber Leap Year Summit 2009 Participants' Ideas Report**

**Exploring Paths to New Cyber Security  
Paradigms**

September 16, 2009

EXTRACTS

## Introduction

“America's economic prosperity in the 21st century will depend on cybersecurity.”

President Obama, May 29, 2009

The Nation's economic progress and social well-being now depend as heavily on cyberspace assets as on interest rates, roads, and power plants, yet our digital infrastructure and its foundations are still far from providing the guarantees that can justify our reliance on them. The inadequacy of today's cyberspace mechanisms to support the core values underpinning our way of life has become a national problem. To respond to the President's call to secure our nation's cyber infrastructure, the White House Office of Science and Technology Policy (OSTP) and the agencies of the Federal Networking and Information Technology Research and Development (NITRD) Program have developed the Leap-Ahead Initiative. (NITRD agencies include AHRQ, DARPA, DOE, EPA, NARA, NASA, NIH, NIST, NOAA, NSA, NSF, OSD, and the DOD research labs.)

As part of this initiative, the Government in October 2008 launched a National Cyber Leap Year to address the vulnerabilities of the digital infrastructure. That effort has proceeded on the premise that, while some progress on cyber security will be made by finding better solutions for today's problems, some of those problems may prove to be too difficult. The Leap Year has pursued a complementary approach: a search for ways to avoid having to solve the intractable problems. We call this approach changing the game, as in “if you are playing a game you cannot win, change the game!” During the Leap Year, via a Request for Information (RFI) process coordinated by the NITRD Program, the technical community had an opportunity to submit ideas for changing the cyber game, for example, by:

- **Morphing the board:** changing the defensive terrain (permanently or adaptively) to make it harder for the attacker to maneuver and achieve his goals, or
- **Changing the rules:** laying the foundation for cyber civilization by changing norms to favor our society's values, or
- **Raising the stakes:** making the game less advantageous to the attacker by raising risk, lowering value, etc.

The 238 RFI responses that were submitted were synthesized by the NITRD Senior Steering Group for Cyber Security R&D and five new games were identified. These new games have been chosen both because the change shifts our focus to new problems, and because there appear to be technologies and/or business cases on the horizon that would promote a change:

- Basing trust decisions on verified assertions (Digital Provenance)
- Attacks only work once if at all (Moving-target Defense)
- Knowing when we have been had (Hardware-enabled Trust)
- Move from forensics to real-time diagnosis (Nature-inspired Cyber Health)
- Crime does not pay (Cyber Economics)

As the culmination of the National Cyber Leap Year, the NITRD Program, with guidance from OSTP and the Office of the Assistant Secretary for Defense Networks and Information Integration, held a National Cyber Leap Year Summit during August 17-19, 2009, in Arlington, Virginia. Summit participants examined the forces of progress and inertia and recommended the most productive ways to induce the new games to materialize over the next decade. Two reports have been created as the result of the Summit:

1. **National Cyber Leap Year Summit 2009 Co-Chairs Report:** Written by the Summit Co-Chairs, this report presents the vision, the path, and next-step activities in the five game-changing directions as articulated by the Co-Chairs, based on the Summit discussions and Co-Chairs' expertise.
2. **National Cyber Leap Year Summit 2009 Participants' Ideas Report:** This report documents ideas that were introduced by participants and discussed and developed during the Summit. These ideas are presented to the community for inspiration and follow-on activities.

Taming this new frontier will require the contributions of many. The Summit, as the National Cyber Leap Year itself, should be seen as a tool for the community to use to build the shared way forward. The Summit reports clarify destinations with specific instantiations of the game changes and make the path visible through practical action plans. For those who wish to begin immediately on next-step activities, the Summit community should be a great source of traveling companions.

The Summit's outcomes are provided as input to the Administration's cyber security R&D agenda and as strategies for public-private actions to secure the Nation's digital future.

More information about the National Cyber Leap Year and how to get involved can be obtained at: <http://www.nitrd.gov>.

The Summit was 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. Ideas and recommendations expressed in this report are solely those of the Summit participants.

## Summit Framework

The Summit utilized the Six Thinking Hats (see Edward de Bono's *Six Thinking Hats*) process and the Summit goals and deliverables to structure the working sessions. The Summit's goal was to clarify the vision by describing specific instantiations of the game changes, and to make the vision tangible by building practical action plans. To create maximum momentum, the participants were challenged to identify activities they can begin immediately. These are a smaller subset of the action plans. By considering forces of both progress and inertia, participants attempted to determine the most likely way forward.

The structure to capture each idea and associated questions below illustrate this thought process:

**Idea:** What does this change look like?

**Description:** Further explanation of the idea.

**Inertia:** Why have we not done this before? What would derail the change?

**Progress:** Why technically is this feasible now? Why environmentally is this feasible now? What would mitigate our doubts?

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

**Jump-start Plan:** Pieces of the action plan that can be started now.

## 6 Additional Ideas

The following ideas were contributed by participants at the end of the National Cyber Leap Year Summit as additional ideas for consideration and next-step activities.

### 6.1 Idea - Virtualisable Network Architecture

#### 6.1.1 Description

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 recognized 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.

#### 6.1.2 Inertia

Some of the techniques were not available / we didn't recognize the need for security and safety to extent needed / we didn't rely on technology at the same level we do now

#### 6.1.3 Progress

- Significant research in the underlying enabling technologies
- Recognized need and appreciation of the need for this particularly in the defense, 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

#### 6.1.4 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

## 6.2 Idea - Global Electronic Identity Management System

### 6.2.1 Description

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 recognized 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 organizations or other individuals such as friends and family members. The information used to reason about an identity assertion should be managed in a distributed decentralized 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 authorization by identity being queried.

The system should support "composite" identities, such as Corporations and Organizations, allowing operations to be attested to by an organization that is separate 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 multiple entities, 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.

### 6.2.2 Inertia

Some of the techniques were not available / identity systems have traditionally been centrally managed.

### 6.2.3 Progress

- Significant research in the underlying enabling technologies,
- Recognized need and appreciation of the need for this particularly in the defense, 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 organizations
- That assertion information should be distributed and decentralized, where information is selectively released by individual authorization, i.e. No single database store. Each attestation 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.

### 6.2.4 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 organizations 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, PricewaterhouseCoopers, **Synaptic Laboratories Limited**, EU EID-STORK, and others to be identified

## **6.3 Idea - Global Post-Quantum Secure Cryptography Based on Identity**

### **6.3.1 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 organization 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.

### **6.3.2 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](http://citeseer.ist.psu.edu/765675.html), <http://citeseer.ist.psu.edu/765675.html>].
- 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](http://www.win.tue.nl/hashclash/rogue-ca/)", <http://www.win.tue.nl/hashclash/rogue-ca/>.
- 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).

### 6.3.3 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 centers.
- **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](http://synaptic-labs.com/resources/security-bibliography/53-asymmetric-key-exchanges-classical/78-bib-celebrating-the-30th-anniversary-of-pkc.html) by Whitfield Diffie, <http://synaptic-labs.com/resources/security-bibliography/53-asymmetric-key-exchanges-classical/78-bib-celebrating-the-30th-anniversary-of-pkc.html>).
- **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 infrastructures 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 its trust relationships, where as this proposal supports the real-time authenticated key exchange operation between those identities.

### 6.3.4 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 organizations 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

## 6.4 Idea - Evaluating the Effectiveness of Data Depersonalization Techniques and It's Impact on the Community

### 6.4.1 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 depersonalized 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.

### 6.4.2 Inertia

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

### 6.4.3 Progress

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

### 6.4.4 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.

### 6.4.5 Jumpstart Activities

Collect a large representative sample of commercial exchanged depersonalized 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-personalize 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.

## **6.5 Idea - Measuring the Impacts of Unauthorized Information Disclosure**

### **6.5.1 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 organization to establish the value of information loss to stakeholders, 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 organizations on how to manage their IT infrastructure and risks.

### **6.5.2 Inertia**

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

### **6.5.3 Progress**

Technologies exist which can be used to collect this information.

### **6.5.4 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.

### **6.5.5 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 organizations to perform surveys and collect the data.

## **6.6 Idea - Semiconductor Intellectual Property Protection**

### **6.6.1 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 unauthorized 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 finalized 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 behavior into each manufactured chip from a remote location or a tamper proof module.

### **6.6.2 Inertia**

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

### **6.6.3 Progress**

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

### **6.6.4 Action Plan**

Identify one or more semiconductor organizations. 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).

### **6.6.5 Jumpstart Activities**

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