National Cyber Leap Year Summit 2009:
Exploring Paths to New Cyber Security Paradigms
Draft Report of Participants' Ideas

August 24, 2009

New Game: Basing trust decisions on verified assertions.

This document explores Digital Provenance as a path to this new game.

The following ideas were captured in unedited form at the National Cyber Leap Year Summit. The ideas are a summary of the discussion of the participants in the Digital Provenance session. They do not necessarily represent the opinions of the co-editors or the organizations they represent. 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/1447/. 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.

What is the new game?

In today's game we have to expend considerable energy to discover whether to trust digital objects for any intended purpose. We are in the situation of a shopper who walks into the meat department of his grocery store and finds a case full of wrapped but unlabeled meat. While he might be able to determine if it is safe to eat through laborious chemical and microbiological analysis, some things he will never know: is it kosher; did the animals range free; what were they fed? Fortunately, USDA regulations ensure that each consumer does not have to invest in sophisticated laboratory equipment to analyze his beef, but in the digital world, this is often the very situation he finds himself in. Today, with no guarantees as to the source and integrity of digital content we have to check everything to be sure it is not harmful; with reliable digital provenance we can concentrate our resources instead on how we wish to handle the varieties of authorized content we receive.

1 Stable Network Identity

1.1 Description

Remove the semantic overloading of IP addresses by disambiguating network topology location function from the host identity function.

1.2 Inertia

- Global IP software changes
- Institutional resistance
- Complex roll out strategy
- Non-Reversibility (reverse lookups very difficult)
- No community-wide incentive

1.3 Progress

- Proven technology with limited deployment
- Host Identity Protocol (HIP): a multi-year working group within the Internet Engineering Task Force (IETF) which
  - Enables mobility and multi-homing
  - Supports convergence of mobile and multi-homed devices
  - Has been used to secure previously non-securable devices (machine controllers, [e.g., Supervisory Control and Data Acquisition (SCADA])
- Has an open-domain code base

1.4 Action Plan

- Migration of standard into communication stack products
- International Regulatory Awareness Programs
- Pick one of the jumpstart activities to advance with funding

1.5 Jump-Start Plan

- Create use cases of how to use HIP to secure:
  - SCADA
  - Utility grid
  - Hive and composite communications
  - Healthcare remote telemetry
  - Location-based services
  - Increasing trustworthy micro-payments
- Finish standardizing HIP within the IETF / Have the approach verified by a government national lab in this domain

2 DP Security

2.1 Description

Managing and securing DP information. Authorizing and controlling access of principals to DP. (Data minimization, privacy, least privilege, confidentiality, integrity, and authenticity.) This is predicated on “DP definition and management” (see above).

2.2 Inertia

- Scalability
- Tendency of organizations to default to high levels of information (doesn’t sufficiently manage risk)
- International laws and policies differ
- No existing technology

2.3 Progress

- Availability of new policy- and attribute-based cryptographic techniques
- Recognized need for DP in a variety of circumstances

2.4 Action Plan

- Standardize technology in standards bodies like IRTF and W3C
- Strategic use cases in areas like the intelligence and healthcare communities

2.5 Jump-Start Plan

Design for secure provenance of immutable objects (e.g., issued patents)

- Extend to “append only” objects (e.g., log files, audit trails)
- Create a general model of secure provenance

3 Data Provenance Definition and Management

3.1 Description

Attaching context to data to track chain of custody, transformation (modification), and provenance of messages and attachments (for software, data at rest, or packets). Establish standard labeling system for quality (analogous to food labels).

3.2 Inertia

- Scalability
- No standards
- Complexity of the ontological model
- Privacy concerns

3.3 Progress

- Industry experience designing markup languages
- Existing means of cryptographically binding data and it's provenance
- Advancements in meta-data cataloging and search capabilities
- Existence of pervasive time and location services (e.g., GPS)

3.4 Action Plan

- Work with browser developers to incorporate into the browser and present to users (e.g., Chrome)
- Work with OS vendors to incorporate as file system meta-data and with GUI/explorer hooks for presentation to users
- Revise/extend existing government standards and software (government meta-data working group standards) to meet Data Provenance requirements
- Build upon, coordinate, and integrate with trusted systems work (including hardware trust group from this summit)
- Develop HW acceleration for attaching DP context data at network (or lower) layers
- Develop policy/legal framework for resolving DP disagreements or conflicts (e.g.,

3.5 Jump-Start Plan

Create a standards group (e.g., Defense Research and Development Canada (DRDC) efforts)

4 Reputation Engine

4.1 Description

Credibility quantification of principals and entities (by tracking popularity, responses, scoring, and other kinds of trust data) to establish reliability. Leverages cognitive sciences (perceptions) that build in mechanisms for both crisp logic and fuzzy logic systems. Enables claims-based (name, reputation, etc.) ID.

4.2 Inertia

- Scalability
- No cohesion
- No standard
- Identities lack anchors and are easily manufactured
- Reputations may be spoofed and misused

4.3 Progress

- Technology exists today
- Acceptance by consumers and stakeholders

- Proven value to consumers and suppliers
- Value in its ability to propagate, amplify, and degrade

4.4 Action Plan

- Build one or two real applications (proof of concept)
- Start down RFC path (proposal, review, standards, etc.)
- Build a community
- Build common exchange/interop format (e.g. genealogy as good example of similar model and format)
- Build a reputation common data model - include entities, attributes, and relationships
- Minimize spoofability

4.5 Jump-Start Plan

- Pick three or four commercially used reputation engines for analysis (e.g., eBay, site advisor, credit rating services)
- Find commonality and build rules.
- Pick use cases for test/verification (e.g., phishing and anti-phishing)

5 Trustworthy Systems

5.1 Description

Expanding trustworthy systems foundation to create trustworthiness (integrity) in how software treats DP Inertia

5.2 Progress

- Increased need recognition
- The SCAP, FDCC, and Software Assurance efforts have attracted new adopters and inspired new areas of investigation and investment Action Plan

5.3 Action Plan

To be determined; depends on the outcome in the short term

5.4 Jump-Start Plan

DoJ pilot use of Digital Evidence attestation meta-data about chain of control providence

- Repositories of reusable code - DHS S&T Open Source project as a starting point
- ESAPI (OWASP) for JAVA - libraries of hard to do right security relevant functions
- Define "food label" attributes for trustworthiness of software and hardware.

6 Government Role

6.1 Description

Government to serve as authoritative certification authority of digital identity.

6.2 Inertia

- Potential single point of failure
- Governments are not the originators of identity in US
- Privacy and civil liberties fears

6.3 Progress

- Consumer receptivity due to concerns about identity theft, phishing, etc.
- Need for health care information exchange
- Shifting economies, scale, and scope of cyber-attacks

6.4 Action Plan

- Address liability for reliant parties
- Full range of use cases
- Policy framework (US domestic, global/international)
- Forums to address issues
- Collaboration with private sector around CIP (e.g., SCADA and industrial control systems)
- Consumer outreach
- R&D on implementation approaches

6.5 Jump-Start Plan

- Identify early adopter use cases in financial services, energy/industrial control systems, health care information exchanges (regional cooperatives, PHR/EHR), ICT/internet
- Plan/establish pilots

7 Trusted Path

7.1 Description

A secure interface between user and trustworthy system entities that will permit provenance of actions at any layer of the protocol hierarchy

7.2 Inertia

- Expensive
- Not supported in current architecture
- User interface

7.3 Progress

- SAK feasible – just need device driver to do this
- May be hardware mechanisms to support now. Host ID embedded in hardware with cryptographic protection
- The great need for interoperability is a driving force for remote TP

7.4 Action Plan

- Expand to other domains (financial)
- Use TP to mitigate spam and phishing by tying IP disambiguation via attribution
- Create anonymous access to high integrity information via public libraries

7.5 Jump-Start Plan

- Small field demos to show TP
- Investigate TP in situ/on platform for multi-care processors. Core to core, KUM to core

8 Global Identity-Based Cryptography

8.1 Description

Global encryption based on identity that is robust

8.2 Inertia

- No proven technology
- Reliability
- Management
- No revocation
- Not post-quantum secure
- No global system available
- Privacy issues
- No compromise recovery
- Online servers

8.3 Progress

Technologies now exist to express scalable symmetric key authenticated encryption systems where no single trusted third party knows the final key.

8.4 Action Plan

- Development teams to integrate proposals into open source applications
- Identify and bring together identity stakeholders into a conference to refine requirements
- Independent evaluation of next generation proposed technologies

8.5 Jump-Start Plan

- Draft a high-level requirements document
- Create use cases
- Survey candidate technologies
- Independent evaluation of next generation proposed technologies

APPENDIX A: Acronyms

CIP	Critical Infrastructure Protection
DOJ	Department of Justice
DP	Digital Provenance
DRDC	Defense Research Development of Canada
EDI	Electronic Data Interchange
EHR	Electric Health Run
ESAPI	Enterprise Security Application Programming Interface
FAR	Federal Acquisition Regulation
FDCC	Federal Desktop Core Configuration
GUI	Graphical User Interface
HW	Hardware
ICT	Information & Communication Technologies
ID	Identity
IEC	International Electro-technical Commission
IETF	Internet Engineering Task Force

IP	Internet Protocol
IRTF	Internet Research Task Force
ISO	International Organization of Standardization
ITD	International Telecommunication Union
MANET	Mobile Ad Hoc Networking
NAC	Network Access Control
OS	Operating System
OWASP	Open Web Application Security Project
PHR	Personal Health Records
R&D	Research and Development
RFC	Request for Consent
S&T	Science and Technology
SAK	Secure Attention Key
SCADA	Supervisory Control and Data Acquisition
SCAP	Secure Content Automation Protocol
SOA	Service Oriented Architecture
SW	Software
TP	Trusted Path
TPM	Trusted Platform Module
W3C	World Wide Web Consortium