

Game Change Group-1:

Digital Provenance → basing trust decisions on verified assertions

Program Co-Chairs:

- *Mr. Eric Fleischman, Technical Fellow, Boeing*
- *Mr. Hugo Teufel III, Director, Advisory Services, PricewaterhouseCoopers*
- *Mr. Mike Stiglianese, Techpar Group*

Definition:	2
Towards a Partial Vision:.....	2
What are the current problems that suggest a need for digital provenance?.....	3
What does the game change to resolve those problems look like?.....	3
What domains should digital provenance operate within?	4
If digital provenance operates within many different domains, should the digital provenance systems within different domains be related?	4
Does digital provenance require identity (e.g., does trust require verifiable identity)? ...	4
Does identity require transparency?	4
Are transparency and privacy necessarily in conflict with each other?	5
Why now? Environment	5
Dynamic Identity Verification and Authentication™ (DIVA™)	5
Why (technically) are digital provenance solutions feasible at this time?.....	5
Why (environmentally) is this feasible at this time?	6
Why have we not done this before?.....	6
Traditional problems of distributed key systems needed to be solved	6
What would mitigate our concerns?	7
Performance Analysis	7
Security Analysis	7
What are reasonable paths to this change?	8
What would accelerate the change?	8
What would derail the change?.....	8
Contacts:	9
Overall Objective:.....	9

Digital Provenance → basing trust decisions on verified assertions

Definition:

For the purpose of the working group, Digital Provenance is defined as the set of policies, technologies and incentives which, in combination, provide an appropriate level of attribution to users of, and/or resources accessible via the Internet, allowing for trust decisions to be based on verified identity assertions.

Towards a Partial Vision:

Digital provenance enables the creation of trustworthy identity systems that can be leveraged by authentication and authorization systems. This foundation enables networked entities to strongly authenticate the originator of packets. For example, packets are associated with a cryptographic ID of the sender such that it is computationally infeasible to impersonate another host's identity. A host (or application or person) can prove that it is talking to another host (or application or person) that it knows by name and discard or de-prioritize packets from less trusted entities. Network administrators can prove that packets on any given network segment are authorized to be present and block access to unauthorized hosts. The architecture should permit hosts to delegate authority to other entities to act on their behalf. This would, for instance, allow a host that wants to hide its current location to use network proxies to forward its traffic. Denial of service attacks could also be deflected to network proxies.

DIVA could be used to solve this problem through the use of meta-servers. This is accomplished with the current access server passing on responsibility to another meta-server that is already authenticated and authorized within the system. This allows for rerouting of valid traffic away from a denial of service attack and conversely to redirect the denial of service attacks to a monitoring or tracking system. This would allow the study of the attack for identification purposes in real time.

The approach ideally should resolve 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.

Because DIVA is independent of the IP address, the IP Identity problem is a non-issue as the end user is directly authenticated regardless of the number of branches and modifications that are handled through the network. It is simply an endpoint-to-endpoint authentication system that is virtually impossible to access illegally without detection.

What are the current problems that suggest a need for digital provenance?

- National security threat to critical infrastructures
- Cyber warfare
- Pandemic Cyber crime

What does the game change to resolve those problems look like?

The game changer is the simple addition to network login protocols that would require a call to DIVA™. The server requests DIVA™ authentication at login and throughout a session. The server contains the only copy of the distributed key and compares single use tokens (of arbitrary length) bit-by-bit in order to authenticate the user. This protocol provides secure network access, dynamic authentication, inherent intrusion detection, repudiation/non-repudiation, authorization, and automatic revocation. DIVA™ used in a DRM capacity is very effective. Digital Rights management is easily established in a tiered architecture based on unique distributed keys, rules and schemas. DOORS, Digital Object Online Resource Sharing, is an example.

- Dynamic Identity Verification and Authentication™ [DIVA™] is a simple and small utility that creates random, deterministic key streams greater than 10^{60} bytes in length and greater than 250,000 bits in strength (scalable).
- These key streams are used not to encrypt data but to uniquely log all traffic on a network, to provide continuous authentication throughout a session (not just at login), inherent intrusion detection and automatic revocation to criminal behavior.
- A 20k software module can be downloaded over the web onto any electronic device (i.e. phone), USB drive, smart cards, etc.
- Only memory and connectivity are required
- Must be able to write dynamic offsets
- Electronic distribution of utility
- No physical manufacturing

The server would have a copy of the DIVA™ utility.

The server would have to add only three database fields to their client data:

- a unique identifier field
- a distributed key field that would contain the unique key structure
- a current offset field

It is critical to note that if the implementation is done by the server requesting DIVA™ verification then there are NO changes that need to be done to the firmware of any kind of device that can access a secure network. The device simply needs memory/storage to download a copy of the DIVA™ utility (approximately 20K.) The hacker, criminal or thief gains nothing by circumventing this routine on the device because the server is requiring the information. If a correct DIVA™ token is not provided, there can be no network access.

What domains should digital provenance operate within?

DIVA™ is a protocol that is interoperable at all network levels giving it the broadest flexibility and interoperability.

To date we have successfully and easily implemented Dynamic Identity Verification and Authentication™ at all levels.

- Network Layer – the tunnel
- Transport Layer – tunnel
- Application Layer – Media Streaming
- Specific Applications – keyMail, Secure File Interchange
- Within data at rest? Hard Disk Drive Encryptor; PFS, email encryptor
- FPGA

Whitenoise/DIVA™ in Virtex™-II and Virtex-E devices. This inexpensive hardware deployment offers a secure, low latency encryption layer and Identity Management capacity for telecommunication and wireless devices. It is easily channelized to scale speed/channels to any transmission speed requirement.

- Very low cost and very high speed
 - 1.6 Gb/s Encryption and Transmission Speed
- Channelized
- 2 bytes/clock cycle (scalable by channelizing)
 - More Powerful Chips = Higher Speed/More throughput
 - Current Xilinx Chip \$5-\$10 (Volume) = 1.6 Gb/s
 - Next Model Up \$80 = 16 Gb/s
 - ASIC Implementation in 3rd Party Electronics

If digital provenance operates within many different domains, should the digital provenance systems within different domains be related?

Ideally yes, because it allows for the highest level of security and authenticity.

With Dynamic Identity Verification and Authentication™, it is possible for different domains to use the same key but different offsets to manage multiple domains simultaneously from the same authentication system.

Does digital provenance require identity (e.g., does trust require verifiable identity)?

Yes, however, degrees of identity can be scaled to accommodate degrees of privacy.

It is possible to allow a user to have an anonymous identity that is verifiable in the future should the context demand it. A current weak example is the use of cookies. Cookies allow for a verifiable anonymous access from an individual user.

Does identity require transparency?

No. It is possible to have an individual that requires an identity to access a system to get an anonymous identity that can be reused by the individual to access the system anonymously but still have the accountability of monitoring actions based on the anonymous account.

Should the need arise, there could be mechanisms that would allow for identifying the individual at a later time if they access the system after more stringent identification mechanisms were added to that account.

Are transparency and privacy necessarily in conflict with each other?

No. While they appear to be in conflict there are mechanisms that allow privacy while allowing sufficient identification.

Why now? Environment

While anonymity might have been one of the selling points of the early Internet, those who want to use it to make money or run an organization are beginning to clamor for the basic security guarantees fundamental to e-commerce. These are authenticity or provenance— where did the object come from, integrity or pedigree—is it what it says it is, and nonrepudiation or attribution—who can be held accountable.

Cryptography seems to be the core enabler. Distributed keys can be used for both identity management and for encryption. They can also be used as random number generators to dynamically create and distribute additional distributed keys or to create session keys (specific topologies).

- Dynamic Authentication - unique key and IdM
- Authorization – rules, DRM
- Automatic Revocation – network access denial
- Repudiation non-repudiation (Common Criteria 3rd Party)
- Intrusion detection
- Distributed keys creating new distributed or session keys

Dynamic Identity Verification and Authentication™ (DIVA™)

These enormous, random, deterministic key streams and dynamic offsets embed characteristics of a one-time-pad. The key or key segment (token) is only used once; the key streams are perfectly random.

Even if a thief were able to get a copy of the user's DIVA™ key, there are only two possible DIVA™ outcomes.

1. If the legitimate user logs onto a network first, the offset changes, and the hacker has to start all over again.
2. If it were possible to make a perfect copy of a key, and the hacker could break the other additional authentication layers (i.e. device identifier, user name and password, etc.) and the hacker was to log onto a network first, then the legitimate user would no longer be able to log onto the network because they would no longer have the correct current offset. The breach is recognized and the key revoked. Because the authentication is continuous, shortening the time between periodic authentication calls makes any undetectable breach completely infeasible.

Why (technically) are digital provenance solutions feasible at this time?

- It exists, has been tested and is implemented
- It requires no physical manufacturing, just distribution of a software module and implementation of a call for DIVA™ at a server
- It requires virtually no change by any network players and providers beyond a call to DIVA™ and three additional data base fields for login: a unique identifier, a key structure field, and a current offset field for the database that controls login. It works with any kind of network including SCADA and in conjunction with Public Key Systems.

Why (environmentally) is this feasible at this time?

- Realization of how fragile our critical infrastructures are
- Vague public acknowledgement of the problems
- Cost
 - lack of disruption in the implementation of a game changer
 - as the economy gets worse the level of crime gets worse
 - inverse relationship – as security gets worse the amount of funds gets worse
 - we are at a societal point of change

Why have we not done this before?

- This technology did not exist before
- This technology has unique characteristics that allow for new security protocols

Traditional problems of distributed key systems needed to be solved

Key management of these systems explodes into an exponential headache.

Historically the number of keys to manage is the square of the number of secure endpoints on a network. DIVA™ Identity Management has a one-to-one relationship between the number of keys and endpoints on a secure network.

Key storage – long keys are a better source of identification and security but storing large keys is a nightmare.

Identity Management keys generate unique key streams on the order of 10^{60} bytes in length. However, only the internal key structure and the offset are required to recreate any key segment. This is a small amount of data. For example, 158 bytes of this information will generate a random key stream over 1 hundred billion bytes long. You can learn about multiplicity: View a brief description of an [Identity Management Key Algorithm](#) (Presentation).

Key distribution is a major problem for distributed key systems.

This is not true any longer – Dynamic Distributed Key Infrastructure topologies allow distributed keys to in turn securely generate and distribute more encrypted keys. It allows the easy creation of secure tiered networks.

With all the traditional problems solved, DIVA™ Identity Management provides a secure digital network architecture that is far easier and less expensive to use than asymmetric key systems and there is NO reliance on Trusted Third Parties (outside of the government/law enforcement) for your security.

Distributed symmetric systems have always been the prevalent architecture and are the approach that has the least impact on user behavior and is the architecture that consumers worldwide are familiar with. This is evidenced by all the important documents that individuals carry daily: drivers' licenses, credit cards, employee ID cards and passports are all examples of distributed keys which people rely on daily.

The flexibility of the DIVA™ Identity Management architecture allows the systems to be used with existing public key systems to add continuous authentication, 100% accurate inherent intrusion detection, and automatic denial of network access to criminals. Add the DIVA™ to your security protocols without replacing existing systems and without the need for additional hardware. All you require is an Internet connection.

What would mitigate our concerns?

Performance Analysis

The performance analysis was conducted against the NIST test suite. Whitenoise was tested to an order of magnitude greater stringency than the usual NIST tests. There were not even any statistical failures against the randomness test suites. This has never occurred before. Keys could not be compromised by super computer arrays.

Performance Analysis

“From these results, it appears that Whitenoise encryption process is very fast compared to available cryptosystems, and that it can be used equally to encrypt various kinds of data formats, and hence can be used for various kinds of applications. The outcome of this evaluation is that Whitenoise is an efficient and cost-effective algorithm for securing direct communications from point-to-point over different media and processes including wireless, microwave, radio waves, remote controls, cables, wires, disks, etc. It is also ideal to be utilized to create a secure network layer for the Internet.”

*University of Victoria, Department of Electrical and Computer Engineering Technical Report No ECE03-3
February 2003 Authors: Dr Issa Traore, Michael Yanguo Liu*

WN is “useful to encrypt never-ending streams of communications traffic.”

Dr. Issa Traore, Michael Yanguo Liu, University of Victoria, February 2003

Security Analysis

A security analysis was conducted by David Wagner of the University of California, Berkeley on an early version of Whitenoise. Mr. Wagner has testified as an expert to the US Supreme Court.

“Exhaustive key search is not a threat.

“Whitenoise uses keys with at least 1600 bits of randomness. ... Even if we hypothesized the existence of some magic computer that could test a trillion trillion key trials per second (very unlikely!), and even if we could place a trillion trillion such computers somewhere throughout the universe (even more unlikely!), and even if we were willing to wait a trillion trillion years (not a chance!), then the probability that we would discover the correct key would be negligible (about $1/2^{1340}$, which is unimaginably small).

“In this report, I tried every attack I could think of. All of them failed. This provides evidence for the hypothesis that Whitenoise is cryptographically secure.”

Professor David Wagner, Berkeley, October 2003

Security Evaluation of Whitenoise™ - David Wagner (PDF)

Simply try to break the security. Enlist CIA, NSA, Homeland Security, Defence, intelligence black hats or NIST to try to break into a network deploying DIVA™.

The algorithm has been published since 2004. There was an insured \$100,000 contest over six months and no one was able to break it.

What are reasonable paths to this change?

Whitenoise Laboratories can set up a test server in Vancouver that anyone can try to breach.

We can provide you a server with Secure File Interchange for testing and evaluation.

Secure File Interchange is an application that encrypts documents for safe exchange over the Internet. This has two advantages for testing:

1. It deploys DIVA™ so you can evaluate and try to circumvent or defeat this authentication protocol. DIVA™ is using keys to log traffic.
2. Whitenoise in this particular context is also used to encrypt documents.

When keys are used simply to log traffic, the only available technique to try to break them is brute force attacks because in this context there is no key exchange (after initial distribution) and there is NO cipher text.

The University of Victoria ECE department was unable to find any security weaknesses in Whitenoise keys with a super computer array. Try to break a Whitenoise key with any supercomputers or technology at your disposal, including the RoadRunner at Los Alamos which can do a petaflop which is a thousand trillion calculations per second.

What would accelerate the change?

- Investment in a joint research project, possibly at a provincial or national level
- Objective and science based testing
- Start immediately
- Determination, courage and commitment

What would derail the change?

Politics and uneven competition

- Impartiality? US Cybersecurity Exec Leaving For Job With RSA: Report ChannelWeb
- Evaluating science from the basis of self-interest, corporate interest or political interest instead of public interest or scientific method
- Health

Contacts:

See the complete presentation correlating the Leap Year goals, and the Cybersecurity goals of the White House, and how they correlate point-by-point with Dynamic Identity Verification and Authentication™ [DIVA™] and Dynamic Distributed Key Infrastructures at www.wnlab.com.

Overall Objective:

To develop “game changing” strategies and ideas which have the potential to significantly alter the Digital Provenance landscape. The following questions should be considered:

This section provides links to Host Identity Protocol (HIP; see RFC 5201), receptacles such as X.500 directories, DNS entries, or certificates, **which don’t work or are insufficient.**

Host Identity Protocol (HIP): <http://www.ietf.org/dyn/wg/charter/hip-charter.html>

Public Key Infrastructure (X.509): <http://www.ietf.org/dyn/wg/charter/pkix-charter.html>

Operational Security Capabilities for IP Network Infrastructures: <http://www.ietf.org/dyn/wg/charter/opsec-charter.html>

KeyNote Trust-Management System: <http://www.ietf.org/rfc/rfc2704.txt>

- Host Identity Protocol (HIP): <http://www.ietf.org/dyn/wg/charter/hip-charter.html>
- Public Key Infrastructure (X.509): <http://www.ietf.org/dyn/wg/charter/pkix-charter.html>
- Operational Security Capabilities for IP Network Infrastructures: <http://www.ietf.org/dyn/wg/charter/opsec-charter.html>
- KeyNote Trust-Management System: <http://www.ietf.org/rfc/rfc2704.txt>
- Center for Democracy and Technology, Privacy and the White House Cyberspace Policy Review: http://www.cdt.org/security/20090619_cybersec_actions.pdf.
- Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.
- Intelligence and National Security Alliance, Critical Issues for Cyber Assurance Policy Reform: http://www.insaonline.org/assets/files/INSA_CyberAssurance_Assessment.pdf.
- Internet Security Alliance, The Cyber Security Social Contract Policy Recommendations for the Obama Administration and 111th Congress: <http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20The%20Cyber%20Security%20Social%20Contract.pdf>.
- White House, Cyberspace Policy Review: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.