Trust Management (Blaze, et al.) Paper: March 03 - 2005

General:

Haiyan Cheng: What is the relationship between PolicyMaker and Keynote?

Glenn Fink: Will the KeyNote language enable developers to offer external authorization services similar to what XKMS offers for authentication?

Direct Authorization:

Vedavyas: Where is the need for direct authorization? Does its novelty lie in flexible(programmable) authorization language?

Muhammad Abu-Saqer: If we compare policy maker and keynote system to the existing technologies like for instance PKI , we will see that these technologies more developed and highly deployed. they also satisfy almost most the needs and could accommodate to most of the new raised requirements. So where could the trusted management system located?
According to the paper, why password-based protocols are inadequate in networked computing environments. This technique is still in use in many places even in distributed systems

Glenn Fink: What functionality, if any, do we lose when we authenticate directly, via keys, instead of relying on a name-key binding?

Craig Bergstrom: Conceptually and intuitively, humans break authorization tasks up into, first, authentication and, then, authorization. This seems to be the motivation for many authorization systems doing the same. This being said, what is the advantage of removing the authentication from this process, as is described in the paper on Keynote?
Don't most systems strive to reduce a user's cognitive workload by having computer systems work with our cognitive models rather than counter to them?

Muhammed Abu-Saqer: I see in most cases that it is natural the authorization process to come after and may be dependent on the authentication process. Systems as banking system must authenticate she user before it authorize him/her to do any transactions. The question is why bother by trying to separate the authentication and authorization process.

Policy Assertions:

Haiyan Cheng: What is a monotonic assertion? How to understand that?

Muhammed Abu-Saqer: In the introduction section “Virtually every user of the Internet is at least aware of languages such as Java,...”. I think this is relatively not true. Another
thing, in order for a user to check his bank account why does he need to know or even to be aware of any programming languages. Why are the authors insisting the need for the system to be programmable? In my point of view this thing will complicated the systems, which is apposite to the objectives of the trust management system.

**Darrell Hyatt:** PolicyMaker: What's the point of claiming to allow developers to use “any” language, then turning around and saying that, due to scalability, support issues, and whatever else, really only a few will be supported?

**Muhammad Abu-Saquer:** In page 7, “the recipient of the request must have interpreter for the language in which the assertion is written” could this thing put limit the use of policy maker system and degrade the performance of the system.

**Corban:** What is the advantage of trust management systems over SPKI using ACL’s?

**Security:**

**Haiyan Cheng:** What are the disadvantages of Trust Management system, what are the potential vulnerabilities?

**Glenn Fink:** In PolicyMaker, how are the assertion-checking programs obtained? Could a malicious one be substituted for a good one?

**Darrell Hyatt:** KeyNote vs. SPKI: while having the authorization mechanism be programmable make it more malleable, could this also make it less secure?

**Leeland Smith:** Is there any need or system in place to 'trust' the access condition code? Could someone write malicious code on the assumption that anyone wanting to access their resource would have the execute that code? AWK is a pretty flexible language.

**Key Management:**

**Leeland Smith:** If credentials are bound to public keys, then would all users of a trust management system be required to share the same PKI authentication namespace? Does that affect the distributed goal of the TM system? How the public keys are acquired seems to be left as an exercise to the reader.

**Revocation:**

**Glenn Fink:** Can a "certificate of non-revocation" be revoked?

**Glenn Fink:** Doesn't cryptographic signature verification (used by both PolicyMaker and KeyNote) drag us back into the world of indirect authorization where the whole trust chain must be searched?
Ranjit Randhawa: With respect to revocation, is it possible to add a timestamp/lifetime to a trust management relationship similar to what we have seen in this class earlier?

Proof-of-Compliance:
Glenn Fink: In PolicyMaker, what causes the run-order of assertions to vary the results?

Muhammad Abu-Saqer: Could “general-purpose compliance checker” meets all the needs. in practice, is it a practical solution?

Active Networks:
Ranjit Randhawa: I would be interested in knowing more about security and mobile code. How exactly is the (trust) information for a piece of code delivered to the interested parties? It would have to be a separate entity unlike a digital signature, wouldn't this incur additional overhead?
Bharat Ramesh: In the scenario of a mobile security code a malicious user can cause a denial-of-service attack by sending bad mobile code to host which might spend all its CPU cycles on verifying the validity of request. This still doesn’t mitigate the problem of denial-of-service attack on the service provider.
Darrell Hyatt: Is this the idea behind some of IBM's “On Demand” pitches?

Deployment:
Leeland Smith: If a system using this TM scheme is to be used in a distributed environment, with each entity specifying their own access conditions, so using it on the internet seems natural, but it seems it would be difficult to deploy this approach in a large organization such as a company.

Muhammad Abu-Saqer: In page 5, “Each entity that receives requests must have a policy that serves as the ultimate source of authority in the local environment”. This thing will add overhead on the burden of the network administrators. How this thing could comply with the objective of the trusted management system, which put less responsibilities on the network administrators.

Darrell Hyatt: Has REFEREE been adopted anywhere?

SPKI Certificate Theory Paper:
Glenn Fink: SPKI defines no direct mapping of authorization to name, requiring two certificates from two different authorities (identity and authorization) to complete the mapping. Then they claim that if either authority is compromised, an attacker could gain illegitimate authorizations (p. 13). Thus they suggest that "both issuers need to be trusted with the authorization decision." Isn't this even worse than Ellison's criticism of PKI that
points out that CAs are not real authorities?

**Muhammad Abu-Saquer**: Could The SPKI vague specification that makes it flexible compromise the security protections

**Names**

**Glenn Fink**: How are fully qualified SDSI names essentially (not syntactically) different from fully qualified Distinguished Names?

**Glenn Fink**: Does using a hash of the public key as a name space allow the user to assume multiple different "local names" while still remaining the same entity from the SPKI perspective?

**Glenn Fink**: If keys are changed routinely, and key hashes are used as part of the distinguished name, then names will change as often as the keys do. Is this worth the security it purports to bring?

**Glenn Fink**: Since a hash is a one-way function, doesn't using it as part of the name make finding the right public key by name in a large directory nearly impossible? Even if you do find the correct text name, every potential public key must be hashed to find out which one produces the correct hash, right?

**Glenn Fink**: Regarding Group Names: Does each member of the group have a unique key that shares the same common name? How does this work in practice?

**Revalidation & Revocation**:

**Glenn Fink**: With one-time revalidation, aren't we moving back before certificates where a central authority had to validate each claim?

**Ranjit Randhawa**: What happens when certificates expire during active use and what can the user do in this situation?

**Delegation**:

**Muhammed Abu-Saquer**: Could the certificate issuer by different than the keyholder