Take-Home Exam # 1.

Submitted by: Prosunjit Biswas (@01232785)

1.

Strong points of the paper:

(1). Assuming a Client-Server model as the test bed , this paper discusses ways to enhance security on 'session' on both client & server side. The enhancement in the client side, starts with session establishment through two step verification (2sv) and continues with session maintenance against session hijacking, cookie theft through binding client cookies with client initiated session. On the other hand, for the server side, it (the paper) enhances the session security by using Smartcard-Like USB token (by client) which provides enhanced immunity to authentication database theft.

(2). Secondly, in the 2sv, the use of mobile phone as 'something user has', is very appropriate due to the fact that, today mobile phone has appeared as the most ubiquitous device and almost everyone who uses Internet also use a mobile phone.

Weak points of the paper:

(1). In 2sv, the use of mobile phone as 'Something user has' has pushed the adversaries one step forward toward knowing 'Something user knows' due to the fact that an adversary can forward a call from a victim phone to a target phone he controls by using solely mobile operator's online interface without possessing the phone. For example, enabling and disabling call forwarding with Verizon wireless does not even need a mobile phone.[1]

(2). This paper does not address or recognize the issues of 'Man-in-the-middle' or 'Man-in-the-browser' attack with respect to the 2sv which it cannot efficiently handle.

Reference:

[1] http://support.verizonwireless.com/how_to_use/caller_forwarding.html

Acknowledgement: I have not taken any help on this examination from anybody and have not given any help to anybody.

3.

The vision reflected in the design of the Identity Ecosystem is appropriate because

(i). The design of the Identity Ecosystem & its components can be utilized to emulate how identification & verification of an Identity occurs in the real world. For Example, in the real world when an individual applies to a Passport Agency (acting as Relying Party) for of a new passport, it (Passport Agency) may need to verify the documents being provided by contacting state vital office, Social Security Office (acting as Identity providers) and performs background checking by Police Department (act as Attribute Provider). So, the elements of the design (Relying party, Attribute provider, Identity provider etc) can be utilized to capture real world scenarios.

(ii). The design, recognizes some facts that are equally important in real world. Such as: (a). necessity of multiple Trust Framework or Trust Domain, (b). Necessity of varying attribute provider or Identity provider based on Trust Framework in use, (c). Necessity of a Governing authority (Accreditation authority) to control Trust framework, (d). Necessity of Identity Ecosystem Framework which is analogous to universal norms, policy and standards that everyone has to follow in the real world.

Whether the vision is feasible depends on the existing tools and techniques for securely implementing the components (ex. Identity Provider, Attribute Provider, Identity Ecosystem Framework etc) of the model. On the other hand, Trust establishment and Trust maintenance among the component of the Trust Framework would be challenging. **Nonetheless, I think, the vision of Identity Ecosystem is feasible.**

Acknowledgement: I have not taken any help on this examination from anybody and have not given any help to anybody.

4. ***Summary of the Paper***

(1). The authors presents a theory of trust in the network of humans and computers that consists of elements of Computational Trust and Behavioral Trust. For Computational Trust (which does not include indeterministic human behavior), they have specified how different level of trust can be achieved through different level of isolation of sender and receiver. They have also explain how Trustworthiness plays stronger role than Correctness in the context of Computational Trust.

(2). While depicting a model for Behavioral Trust for network that includes human elements, they have identified different factors namely Risk Aversion, Betrayal Aversion and Trustworthiness beliefs. They have also implied how these factors can be utilized along with the factors of Computational Trust model to build a better trust environment for the forthcoming cyber world.

Significance of the paper for the future of Cyber Security:

(1). Along with bringing more computational devices, future Cyberspace would engage more and more human elements into the picture which means besides a mechanism for trusting computers, we need to derive model for trusting humans . Behavioral Trust model is an important direction toward mitigating the risks and challenges with human elements.

(2). Behavioral trust model provides mechanism for usable security. It realizes the fact that the weakest point in the network of Humans and Computers are the human elements. This new model can potentially be utilized for discovering human behavioral pattern associated with fraud and anomalous activities.

Acknowledgement: I have not taken any help on this examination from anybody and have not given any help to anybody.

2.

The fraud scam can be seen as an organized traditional crime because:

(1). The fraud did not exploit weaknesses or vulnerabilities of available networks, protocols or computing system rather it may have used computers / networks (eg. creating online account, submitting fraud request etc) as a way (among many alternates) to commit the fraud activities.

(2). The ultimate target of the fraud was harvesting money which may have representation in cyberspace but eventually has values only in the physical world.

The fraud scam can be seen as cybercrime because:

(1). Online banking, credit card business, online transaction are the consequence of the Cyberworld. Eventually, any exploitation in the infrastructure of the Cyberwold, should be treated as a cybercrime.

Addressing the fraud with Cyber Security Techniques:

(1). Whether the fraud is a traditional crime or cybercrime, it could be addressed with cyber security techniques. For example, when a request for a new credit account is received, it (the request, requester etc) could be co-related with all other credit accounts with all available credit providers to test the **validity or feasibility of the request**.

(2). The complaints fraudulently used one after another merchant processor. This **fraud pattern** between merchant processor could be identified with sophisticated **fraud detection techniques**.

(3). The defendants, with the help of fraud cards and accounts, conducted sham transactions which could have been detected with the **provenance data** of the transactions and associated proceeds.

Acknowledgement: I have not taken any help on this examination from anybody and have not given any help to anybody.