Kunal Mukherjee

Cryptography

Dr. Robert Morse

4/26/18

Comments

1) Cryptographic Hash Functions- Jacob Ball

The paper is well written and gives a good over-view of Hash functions, but it was not an in-depth paper. The paper was well informative about how SHA-1 Hash algorithm works and what requirements must be fulfilled by a hash function. One of the major component of the paper that I thought was missing was how does a user verify that a hash is from a trusted source and that the specific hash is not for just some random malicious document. I did some further research on my own and found that the developers usually provide the official list of hashes on their website and the user has to run the hash function to conform the authenticity of the original file. I was curious about the mechanism about MD5 hashing and why it is arguable more secure? I have not much exposure to hashing, so the concept of creating a hash table was a bit unclear. For example, why did git create a hash for every repository as compared to just sequential numbering. The paper was a good introduction, but many critical sections seemed missing.

2) Steganography - Shawn Leedy

The paper was moderately written with no mentioning of the mathematical process or cryptographically secure procedure to create an encrypted picture or text. The paper does explain extensively where Steganography is used. Much of the information was repetitive and general knowledge information. For my senior project, I was researching into Steganography maybe that's why I felt most of the information was known. The title of the paper was misleading, the paper gives an overview of Steganography and then delves deep into the uses of Steganography. Therefore, I believe that the title of the paper should be uses of Steganography. I was looking forward to a little bit of the mathematical models or methodologies used in Steganography and attacks on how to break or decode the encrypted messages. There were certain claims made throughout the paper that were not backed up by any sources, e.g "mysterious stations where an automated voice reads out a list of numbers", I would be much more interested to see which source mentions it as it sounds like a movie plot. Even for certain examples I wanted to learn how it was done or some technical details behind the mentioned claims, e.g. "Criminal communication, ... can all be spread widely through the use of steganography".

3) One-Time Pads - Turki AlHarbi

Well written and a comprehensive paper with mathematical proof that explains when using a OTP why knowing the encrypted message does not do us any service in respect to knowing the content of the message or any the future encrypted messages. I think my paper is a good precursor to this paper. This topic was extremely interesting as the concept of randomness, which was my topic comes into play while generating the key. The possible vulnerability in the system, that Turki mentioned that if the keys are reused that the system becomes unsecure, is basically what I explained in Yarrow's algorithm that if the output of the reseeding mechanism is known then the generated random number could be guessed too, and intuitively if this random number is used to generate the key, then this key would be insecure too. The disadvantage of OTP was its inefficiency that the key length has to be the same length as the message. It was interesting to read about the proposed mechanism by Turki about how it could be overcome by sending many keys using the initial transmission of the OTP. But, for this methodology to work the sender has to know before hand and know how many messages would be sent, so the number would be used to create that many keys for transmission and the message length have to be stayed constant. If they have to meet physically then, the identity of the sender and the receiver would be known, and it will cause other issues, for example, what if someone else meet with the sender physically harm him and take the information away anyhow. At the end of the paper, I wanted to know a more about was this procedure implemented before and how successful was it comparing the security and properties of OTP.

4) Lattice-based Cryptography - Duy Nhan Cao

This is my first exposure to lattice-based cryptography. I had certain questions regarding the application which were mentioned by him. I did not understand what did the statement, “picks e1 and e2 with m relatively small entries”, so I went to his source and did a bit of self-research. For example, are e1 and e2 vectors with entries that are smaller than m, or e1 and e2 have the same entries m, but they are small compared to the modulus q. Except for that, the mathematical concept was well written and easily understandable. The lattice-based cryptography seems extremely in-efficient as, the computation would need to be performed multiple of times, to transfer bits that makes a file or even a message as one computation only produces 0 or 1. When I researched further, I found that his application is called Ring learning with errors key exchange. I read the paper, Ding, Jintai; Xie, Xiang; Lin, Xiaodong (2012). A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem. They explained the application in terms of polynomial and I was able to follow it better as I have had more mathematical education regarding polynomials compared to vector and matrices. The private vector x, needs to be updated constantly, or else it could leak information. There is a software implementation can be found in a GitHub repository at https://github.com/vscrypto/ringlwe. I compiled and ran the programs and it had all the examples, of how does the public key, private key, mu, mv look in reality and also, the software implementation of Lattice based cryptography. Another interesting aspect was to generate the random number, the makefile has two compilation lines, one if OpenSSL was available and one if it was not. This ties back to my paper as to how weak PRNG can make the key generation unsecure and ultimately lead to a weak cryptosystem.

5) How Trustworthy are Package Signatures? – Keenen Cates

This topic was very interesting, and I always wanted to know how the package managers like apt-get, yum knew from which source to get the files from and how did they verify who created the program. The statement, “Session keys are a randomly generated number for each entity and is bound to the object as it is only used once.”, is connected to my paper. All my sources said that random numbers are extensively used in field of cryptography and information security, I was kind of sceptic about it. But, as I continue reading my peers paper, I can see that random number play an intricate role in the maintaining the strength of the algorithm and to preserve the property of computational complexity. Because in OpenPGP the session keys are encrypted with the receiver's public key, it does add to the notion that the session key need not be truly random. But, if the public key is generated using ELGAMAL, where a random number is used then the discussion comes back to the fact that the strength of the key exchange depends on the random number generated that makes the private key of the receiver. The paper does a great job in explaining how OpenPGP provides confidentiality and how digital signatures works. Now, I know at least how apt-get knows from where to download the source file and authenticate its source. The most mind-boggling fact was that even after all the mathematical computations, there was no absolute answer but rather there was a "leap of faith" that the user needs to be a diligence manager of keys. Hopefully, in the future something absolute comes up that the files would not be permissible to be uploaded to the database if the creator is not found to be diligent manager of keys, in that way the users are not taking any leap-of -faith.

6) HTTPS Overview – Clayton Brutus

I really enjoyed reading the paper and learning about how to run a security test on the website and gain different information parameters regarding its data communication security. It is a handy tool to have, because as a researcher I might need to visit different untrusted website and I might be susceptible to man in the middle attacks. But, if I could learn or understand what kind of security parameters are in place I would be able to better classify those sources as reputed or non-reputed. This paper gave a good overview of how HTTPS works but as compared to the title of the paper, I felt the paper was very focused key exchange algorithms, which Clayton did mention. Certain information's seemed missing e.g. the software implementation in code behind ephemeral elliptic curve Diffie-Hellman, as in class we learnt how about how this works and the mathematical concepts behind it but in reality how this is implemented in software would have been great. Learning about certificate generations makes a certain phenomenon in browser much more explainable which I was unsure about, where chrome would say while visiting certain website hosted by second or third world countries that the connection is unsecure that the website certificate has been expired. Now, I know exactly what has happened and how to update the certificate or validate the source.

7) Multiuser Cryptography – Ryan Pastelak

One of the best paper I have read so far. In class, we mainly focused in single user cryptography, so having read this paper, I got some exposure to cryptography regarding multiuser user across the network. This paper also, makes use of the knowledge of Chinese remainder theorem, Diffe-Hellman key exchange and Elgamal. The paper explained Shamir's threshold scheme, Bloom filter, Merkel Hash tree and different authentication scheme really in-depth and I feel I understood the mechanism behind it well as the explanations were well written as well as explained. My topic of random number is relevant to this topic as Bloom filter also uses random number to map the hashes. So, the collision domain can be made huge if weak random number are generated. Something, that I found would have been a great addition to the paper would be the software implementation of any of the authentication system or mentioning any source that implements it. My senior project must use one of these authentication scheme as my location-based cryptography make use of usbs that will be the three nodes that will act as anchors and one receiver node. Having exposed to the software implementation, I would be able to refer back to this source while working for my senior project.

8) Tor Network – Simon Owens

This paper exemplifies that Simon have work experience in cryptographic field. The fact that he had not only told about the implementation but rather he had implemented it himself and gave examples from his real life dealing with Tor Nodes. This is an excellent paper, I don't have any negative feedback. But, some additional requirements for this paper would be nice to see details of the handshakes being made between the nodes or how the encryption decryption process is being done and the mathematical treaties behind it. I hypothesis it will be some sort of public key exchange, Diffe-Hellman key exchange. This paper is a well comprehensive paper regarding the Tor browser. After, reading the paper I got a well understanding as to the need for this browser and the use of the browser. Most importantly, I learnt how the TOR network in addition to the TOR browser keep the users anonymous to other and give then uncensored access to the internet. The diagrams were very informative as well, as it facilitated the explaining the deep web, dark web and the internet. This paper touches many important topic in regards to secure connection key management and internet surveillance. Simon's overview makes a good complement with Clayton's, HTTPS, and Ryan's, Multiuser Cryptography papers.

9) An Introduction to Zero-Knowledge Proofs – Asher Trockman

One of the most advanced and well written paper of our group that dealt with extensively with the theoretical aspect of NP-Completeness. This paper had certain mathematical and theoretical computer science concepts that I had no exposure to. So, had to learn about the concepts regarding Jacobi symbol, non-deterministic Turing machine and Hamiltonian cycle. Because of Dr. Morse's lecture on NP completeness, Asher's section of NP Problems and zero-knowledge proof was comprehendible without much personal research. I gain a through understanding of the NP problems and theoretical aspects of algorithms. If I had taken formal languages theory already this paper would have made more sense but, nevertheless after I researched the unknown terms I was able to comprehend the overview why all NP problems have zero-knowledge proofs and zero knowledge of graph 3 colorability. Asher did an excellent job in explaining the main concepts in layman's terms, so that anyone with a little background of probability and graph theory could understand the definitions of zero knowledge proof as well as how NP problems satisfy them and zero knowledge of graph 3 colorability. For example, after my self-research, I was able to understand the characteristics of the zero-knowledge proof was maintained for graph 3-colorability and under what conditions would the verifier reject the proof. I do not have any questions or suggestions regarding this paper. I imagine this is what my graduate school would be like, I would read a paper then do my own self research to understand the paper full and finally use that knowledge in my own research. The definition of Zero-knowledge proof mentions Manuel Blum, interestingly he has also worked on a cryptographical secure pseudo-random number generator that I came across while doing research for my paper. The CSPRNG algorithm is called Blum Blum Shub algorithm. The seed in this generator is an integer that is co-prime to the modulus m. The two primes, p and q, should both be congruent to 3 (mod 4) as this guarantees that each quadratic residue has one square root which is also a quadratic residue.