A reasonable project. Some sloppy English

38/50

Project Summary

Yang Liu, Francis Meng

Background

Several weeks ago, we read a blog posted on a Chinese website. The author is a hacker and the blog post has a very detailed description of how he hacked into his neighbor's router. This blog post brought our concern of the router security. So we decided to research and explore the role of Cryptography in the router security.

Preliminary Research

After some general research, we found several most commonly used router encryption. The brief introduction of the security protocol are shown below.

router encryption schemes or algorithms

protocols

Don't use an abbreviation without describing it before the first use.

WEP

WEP stands for Wired Equivalent Privacy, which is an encryption algorithm that is introduced for IEEE wireless network in 1999. WEP intends to provide the same level of security for the wireless network as the security of traditional wired network. Even though, the intention is to provide a high security for the wireless network. It has been proved that there are numerous flaws. WEP is relatively a weak encryption algorithm comparing to the other encryptions.

networks

Too informal

vague

Clumsy. how about relative to the other encryption algorithms discussed in this paper

WPA and WPA2

WPA is a short form for Wi-Fi Protected Access. It is a security protocol and a certification program developed by the Wi-Fi Alliance to secure computer wireless network. Since WEP has several major flaws in the encryption algorithm, WPA is designed to avoid the encryption flaw in WEP and provide more secure encryption. We will explain more about the functionality in the encryption details section.

flaws

Project Focus and Subject

WEP Implement

Is there any barrier to this that causes you to express some doubt about being able to do so?

or perhaps you mean basis

Missing word or words

Since WEP is the basic of the current router encryption. We want to start our work from WEP protocol. WEP uses a stream cipher that is symmetric key cipher. Even though symmetric cipher is covered in class, there are still some encryption protocols that we have never encountered before. So our first step is to research and understand the protocols that is involved with in the WEP encryption, such as ICV algorithm and RC4 algorithm. After we have a decent understanding of WEP. We will implement WEP encryption/decryption.

a

ciphers are

WEP Attack

WEP has some security flaws, which can be utilized to construct attacks on it. A good way to understand these flaws is to implement attack algorithms. Then we can

defends against

further research ~~on~~ how WEP defend itself on these attacks and how other encryption protocols are designed to fix them. So the second focus of our project is to implement some attack algorithms to hack our implementation.

WEP Flaw Analysis

described may be a better word here logical?

As ~~what~~ we have illustrated above, the intention of WPA and WPA2 is to fix the logic flaws in WEP. We can probably gain a deeper understanding of WEP and WPA by studying finding out these improved mechanisms. So the third aspect we are going to focus on is to analyze how WPA approach to eliminate the flaws in WEP.

Enforce Security(optional)

This part of research depends on whether we have enough time. We got our idea from the blog post about the brute force attack of WPA encryption. We will try to come up with an effective way to enforce the security of WPA encryption. Hopefully, our solution will make it harder to brute force attack WPA.

Encryption Details (WEP)

I'm not sure what you mean by that

WEP encryption protocol aims at three security goals, namely access control, data integrity, and confidentiality. These goals ensure that your wireless infrastructure is not used; your data packets are not modified in transit and the contents of your wireless traffic is not learned relatively. A shared secret key is established between sender and receiver, encrypting packets before transmission. An Integrity check is also introduced to ensure packets are not modified in transit.

To send a message M:

1. Compute a checksum of M.
2. Pick an initialization vector and generate a keystream.
3. XOR M and the checksum with the keystream to get ciphertext. Write a complete sentence
4. Transmit the vector and ciphertext over a radio link.

When M is received:

1. Use the vector and the shared key to generate the keystream.
2. XOR with the keystream? received message to get M' and checksum.
3. If this checksum is identical ~~as~~ to the former one, accept M' as M.

Project Plan

May 10, 11

Research on encryption/decryption related algorithm. ~~And~~ start implementation.

May 14

Finish the WEP implementation and start implementing attack algorithm

May 17

Finish attack algorithm and flaw analysis.

May 19

replication of a

Finish replicate WPA brute force attack on a router. And analyze the possible way ways to enforce the encryption algorithm.

Reference

1. Security of the WEP algorithm. (n.d.). (In). Retrieved May 9, 2014, from http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

2. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (n.d.). . Retrieved May 9, 2014, from http://standards.ieee.org/getieee802/download/802.11-2012.pdf

3. The State of Wi-Fi® Security Wi-Fi CERTIFIED™ WPA2TM Delivers Advanced Security to Homes, Enterprises and Mobile Devices. (2012, January). . Retrieved May 9, 2014, from http://www.wi-fi.org/system/files/20120229_State_of_Wi-Fi_Security_09May2012_updated_cert.pdf

4. JUWAINI, M., ALSAQOUR, R., ABDELHAQ, M., & ALSUKOUR, O. (2012, June 12). A REVIEW ON WEP WIRELESS SECURITY PROTOCOL . . Retrieved May 9, 2014, from http://www.jatit.org/volumes/Vol40No1/6Vol40No1.pdf

5. Singh, J., & Singh Kang, E. S. (n.d.). Security Enhancement in WEP by Implementing Elliptic Curve Cryptography Technique. . Retrieved May 9, 2014, from http://www.ijsce.org/attachments/File/v2i5/E1039102512.pdf

6. Gupta, Sourav Sen. Analysis and Implementation of RC4 Stream Cipher. Diss. INDIAN STATISTICAL INSTITUTE Kolkata, 2013, from https://www.iacr.org/phds/134_SouravSenGupta_AnalysisndImplementationRC4Str.pdf

Authors?