

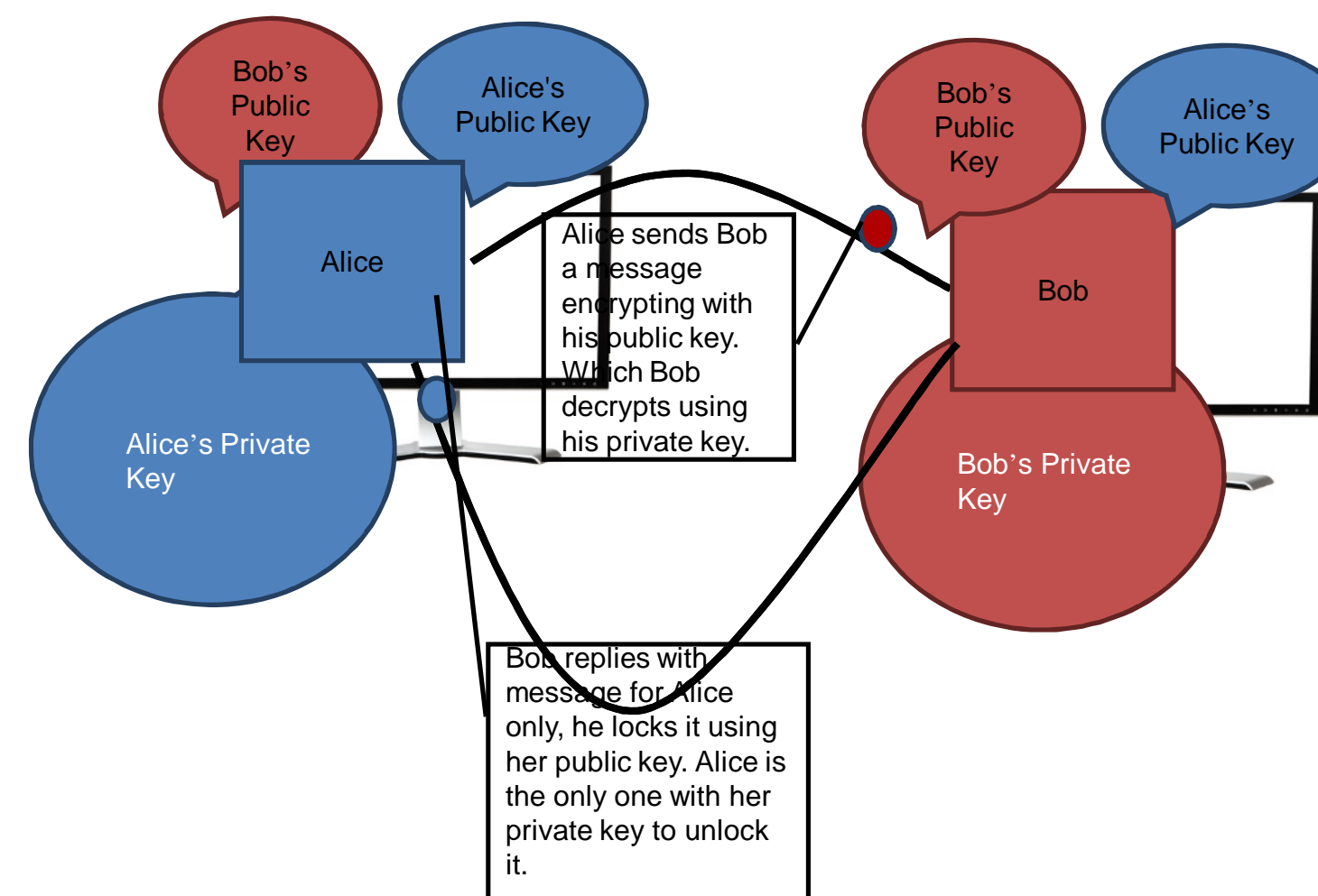
## Insecure SSL Remote Desktop Protocol Traffic

Nick Novotny, Tom Scheel, Ryan Weber, Jasraj Sandhu, Isaac Mpofu

### Abstract:

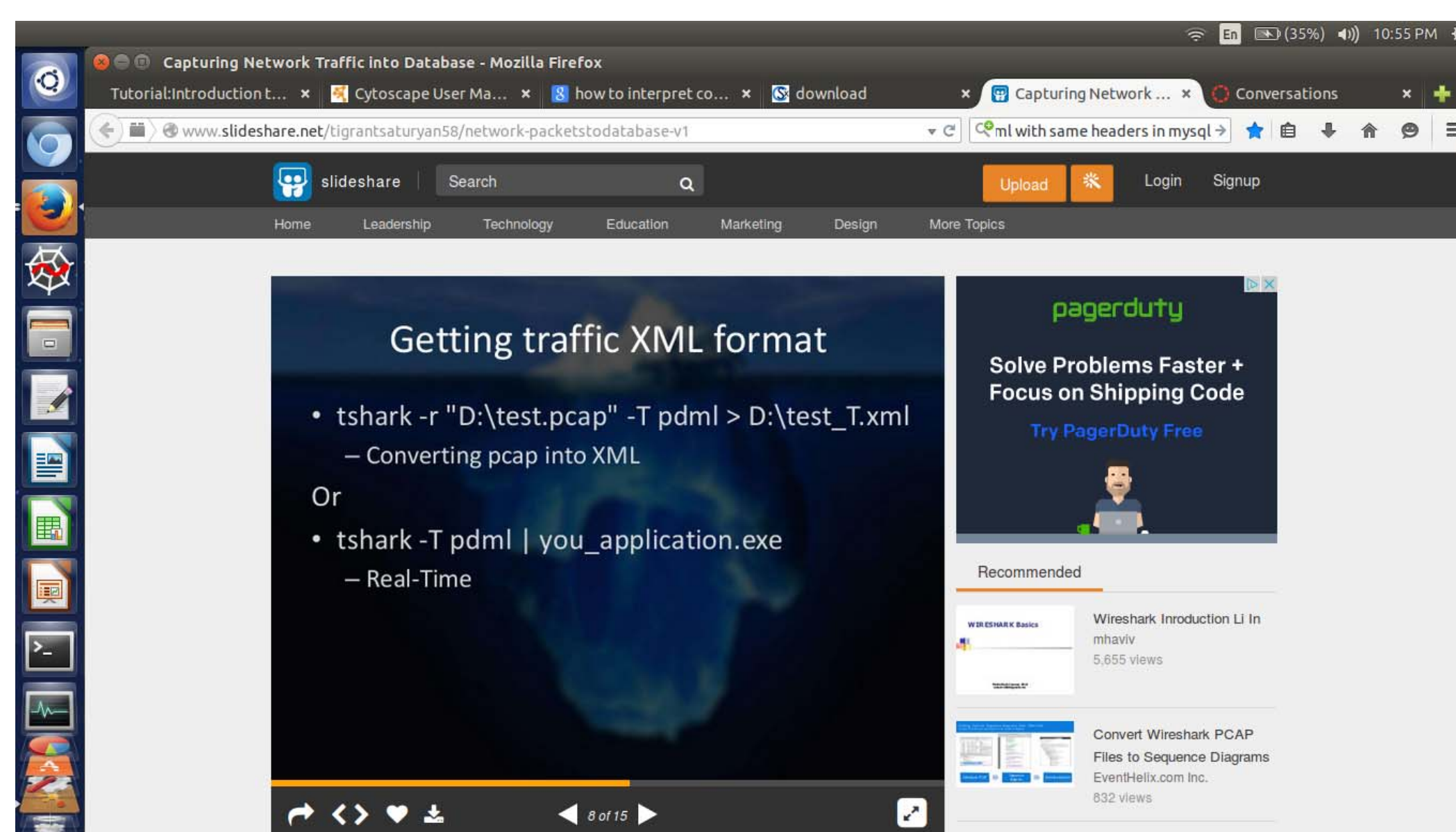
The goal of this project was to show how vulnerable SSL-secured Remote Desktop Protocol communication using RSA is. This project will develop a method to capture authentication packets of an RDP session and decrypt the SSL key used. A secondary goal is to develop a method to replay the authentication packets with the RDP server after the snooped session has ended. The motivation of this project is to demonstrate the insecurity of RSA-encrypted SSL encryption in Remote Desktop Protocol connections used by many network operating systems. This project will build a Linux installation which can capture Remote Desktop Protocol packets and develop a method to decrypt the confidential communication between the client and the server. Database Security Techniques used in this project will include: access security in authentication to the operating system and encryption of data at rest because Linux hashes passwords in the users database of the operating system. This project will be exploiting access control to the RDP server. The secondary goal of this project will be to authorize an untrusted user to access confidential data assets. The expected result of this project is to successfully capture and monitor the packets associated with authentication to an RDP server and secondarily to be able to successfully masquerade as the previously authenticated user. Evaluations will include the ability to successfully capture 10 RDP sessions, decrypt them, and store the packet information into an SQL database.

### How RSA Encryption Works

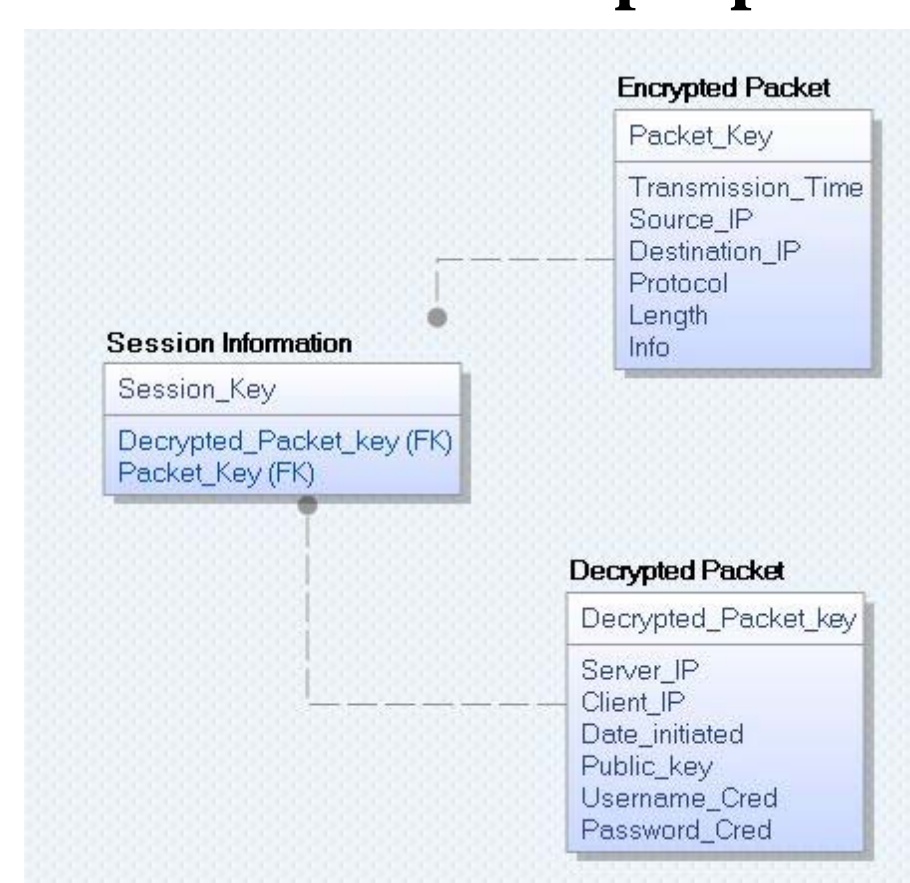


### Convert Captured Traffic in XML Format to Extract Information and Insert it to MySQL Database

Live iso of a Preconfigured Linux Operating System



### Insert Authentication Packets to MySQL Database for demonstration purposes



tshark and wireshark with a start capture script



the world's foremost network protocol analyzer  
Wireshark • Go deep.

### Conclusions and Future Work:

Brute forcing the RSA private key is unrealistic without a general formula for deriving all of the possible keys in a specified key space.

Future work will add Google Rapid Response Server to allow for remote installation of software like mimikatz which allows extraction of the private key from RAM.