Feasibility of attacks against weak SSL/TLS ciphers

Kim van Erkelens

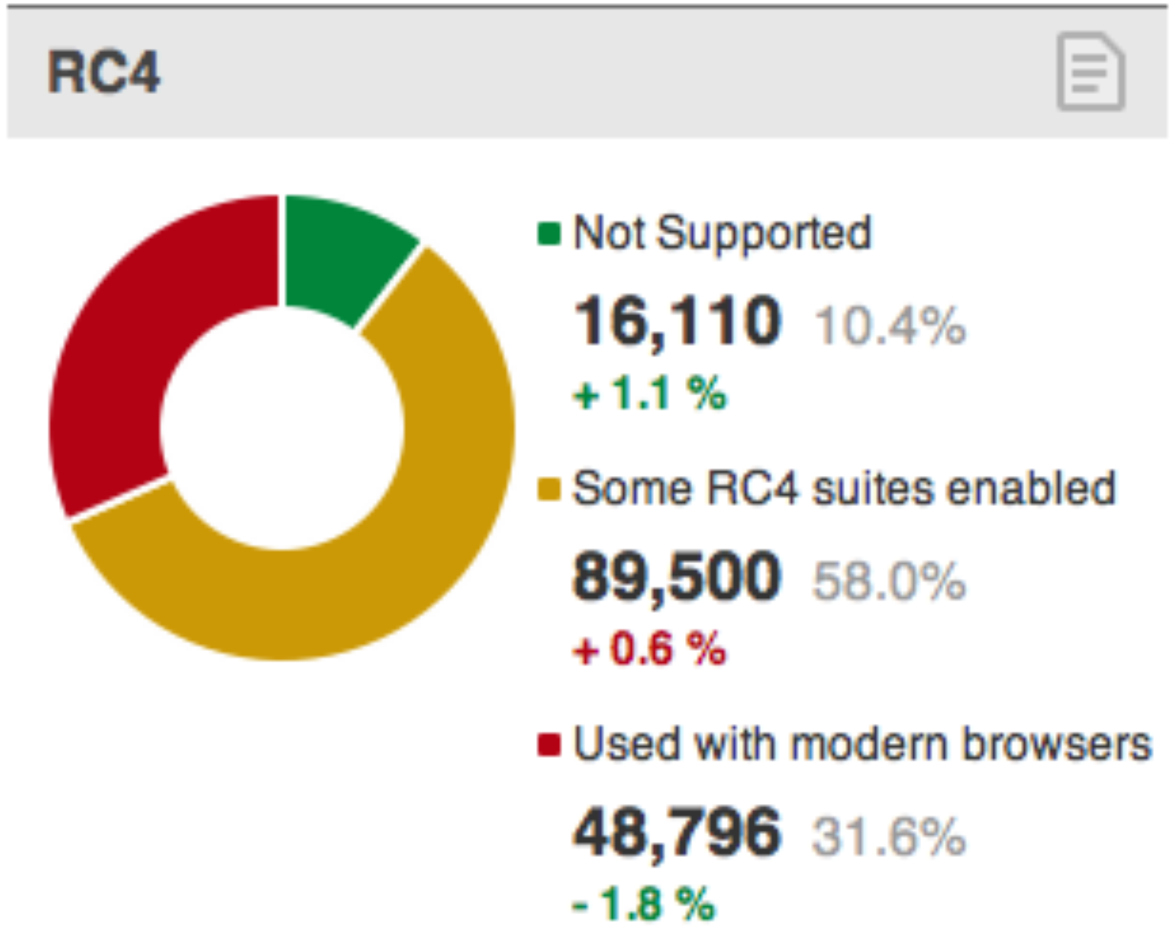
Supervisors: Jeroen van der Ham & Marc Smeets

Master System and Network Engineering
University of Amsterdam

2 July 2014

Motivation

- Ciphers like DES and RC4 are considered weak
- Weak ciphers still widely used
- No practical feasibility of attacks described



SSL Pulse

Previous Research

- Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security
- Yearly Report on Algorithms and Keysizes
- SSL/TLS: What's Under the Hood

Research Questions

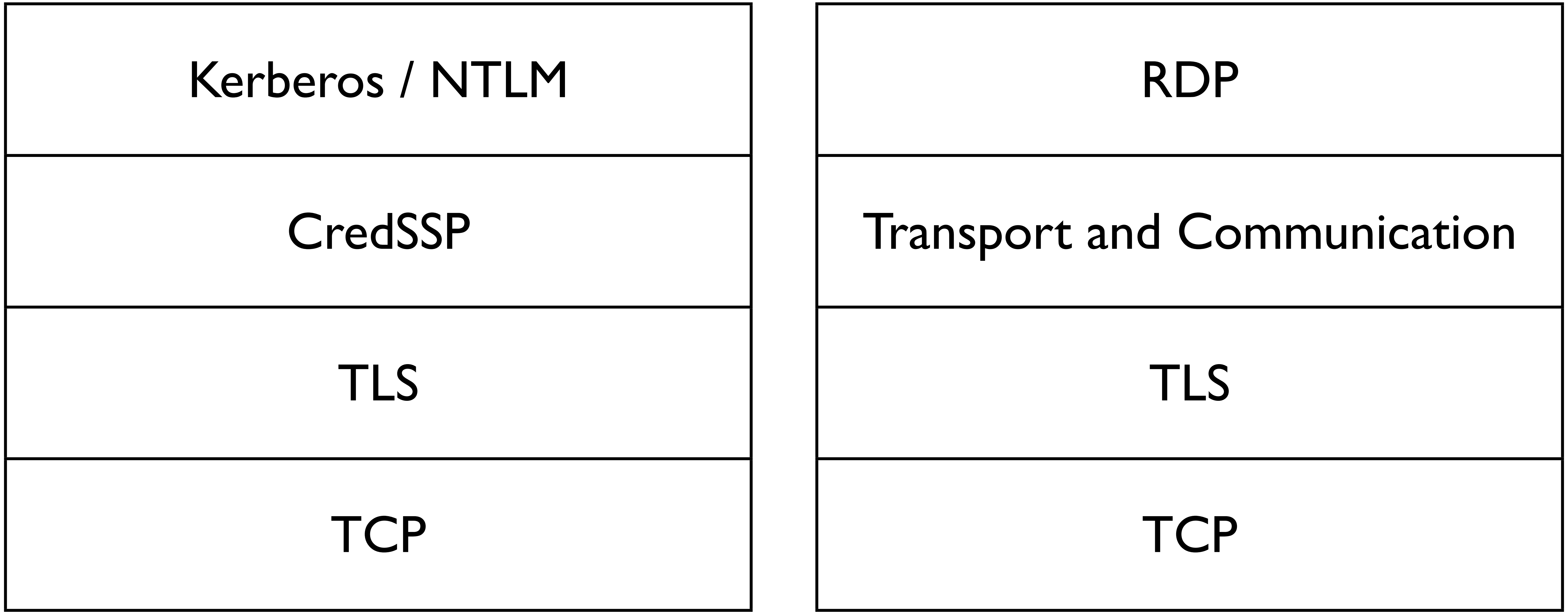
What is the feasibility of cracking weak ciphers based on resources required?

1. Which SSL/TLS ciphers are considered weak?
2. How can intercepted traffic be decoded and which tools can be used?
3. What are the requirements?
4. How can the attack be classified based on time, money, and resources?

TLS and RDP

- TLS = Transport Layer Security
    - Applications: HTTPS, SMTP, RDP etc.
- RDP = Remote Desktop Protocol
    - Standard and Enhanced Security (uses TLS)
    - Open specification

RDP Stack



Kerberos / NTLM

CredSSP

TLS

TCP

User authentication

RDP

Transport and Communication

TLS

TCP

RDP data

Decoding Traffic

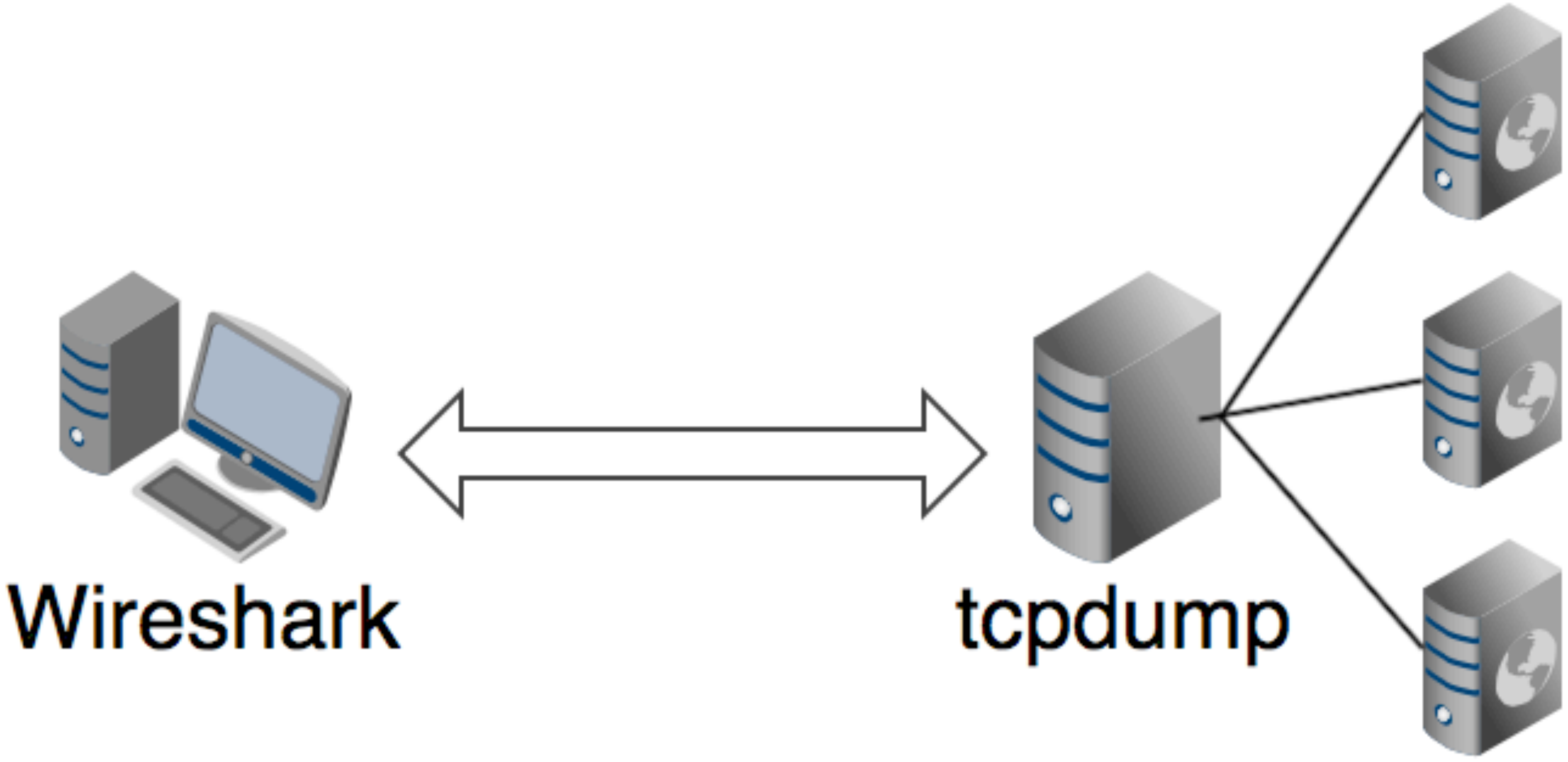
1. Obtaining session or private key
   - Exhaustive key search
   - Crypto-analytical attacks
   - RSA factorisation

2. Decryption using private key or session key

Experimental Setup

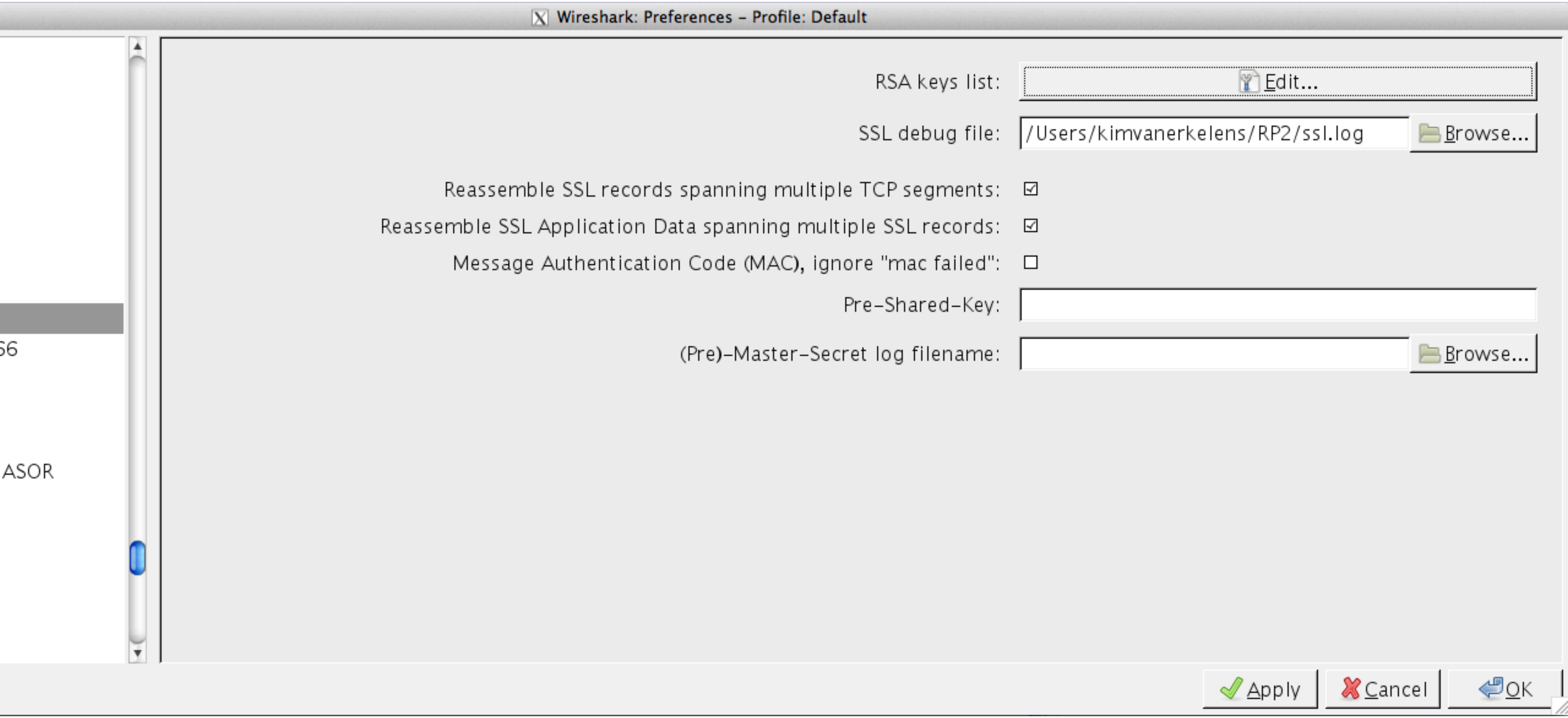
- Virtual servers:
  - Ubuntu with Apache and mod_ssl
  - Windows Server 2003, 2008 & 2012
- Known private and session keys are used
- HTTPS
- RDP Enhanced Security
- RDP Standard (different encryption levels)

Tools



- **openssl**: enforce cipher suite
- **tcpdump**: traffic capture
- **Wireshark**: decryption and analysis
- **Mimikatz**: export Windows Server private key

Methodology



Wireshark: Preferences – Profile: Default

RSA keys list: Edit...

SSL debug file: /Users/kimvanerkelens/RP2/ssl.log Browse...

Reassemble SSL records spanning multiple TCP segments: ☑

Reassemble SSL Application Data spanning multiple SSL records: ☑

Message Authentication Code (MAC), ignore "mac failed": ☐

Pre-Shared-Key:

(Pre)-Master-Secret log filename: Browse...

Classification

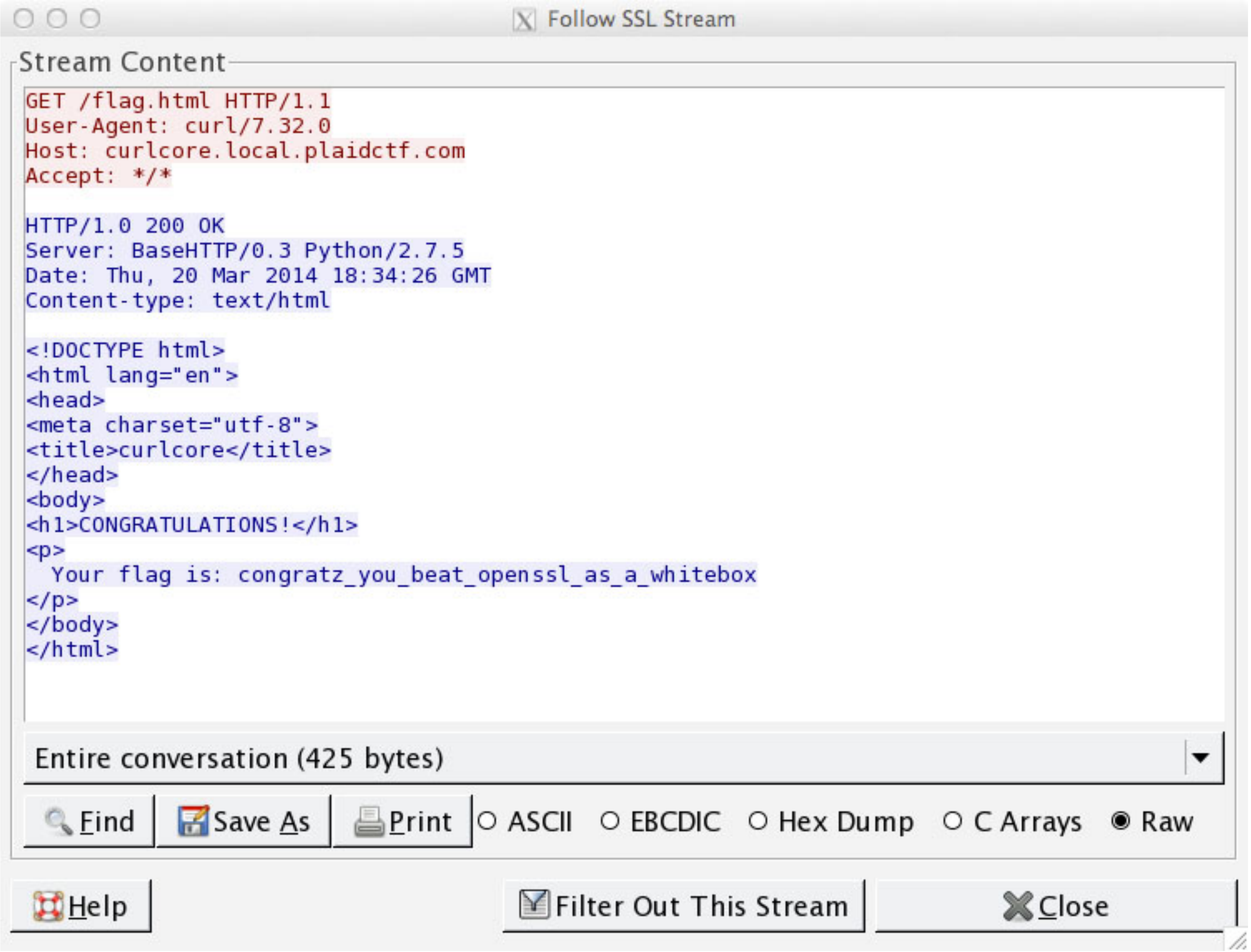
- Budgets ranging from $400 - $300M
  - **56-bit**: **$750** in **30 days** (2008)
- Attack can be realised in ***d/w* days** by a device costing ***cw* dollars**
  - i.e. larger budget results in shorter recovery time
- Application of Moore's law:

  cost of attack drops by a factor 2 every 18 months

Weak Cryptography

- Cipher suites with **key sizes smaller than 128 bits**
  - 3DES ($<$ 128 bits of security), EXPORT cipher suites
- Ciphers with **cryptographic weaknesses**
  - RC4 (statistical biases in the key table)
- RSA keys with short moduli

Findings



```
GET /flag.html HTTP/1.1
User-Agent: curl/7.32.0
Host: curlcore.local.plaidctf.com
Accept: */*

HTTP/1.0 200 OK
Server: BaseHTTP/0.3 Python/2.7.5
Date: Thu, 20 Mar 2014 18:34:26 GMT
Content-type: text/html

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>curlcore</title>
</head>
<body>
<h1>CONGRATULATIONS!</h1>
<p>
  Your flag is: congratz_you_beat_openssl_as_a_whitebox
</p>
</body>
</html>
```

Entire conversation (425 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

source: fail0verflow

```
userName: 410064006d0069006e006900730074007200610074006f00... (Administrator)
password: 700061007300730077006f00720064000000 (password)
```

clientInfoPDU

Requirements

- Traffic can't be decrypted with private key for:
  - Diffie-Hellman (DHE) key exchanges
  - Ephemeral suites
- Whole session is captured
- Correct format RSA key file
- Correct format session key (master secret)

Practical Feasibility

Feasible

- Exhaustive key search: 40 or 56-bit session key
- RSA factorisation: $<$ 512-bit modulus

Less feasible

- Crypto-analytical attack on RC4: (13 * 2^20 sessions needed)

Conclusions

- Attacks are feasible for short key lengths
- Crypto-analytical attacks are less feasible
- HTTPS and RDP (standard & enhanced) decryption possible
  - RDP requires more effort for extracting information

Future Work

- Decompression of RDP traffic and extraction of information
- Decryption without Session ID
- Other applications with TLS

Questions?