Transposition of the Curity https://powcoder.com (TLS)

Add WeChat powcoder

ECEN 4133 Feb 18, 2021

Review: HTTP

```
Assignment Project Exam Help

HTTP/1.1 200 OK

https://powcoder.com

Add WeChaptpow(codercript>
</head>
<img src="//gmail.com/img.png"/>
```

HTTP Threats

GET / HTTP/1.1 Host: gmail.com



Assignment Project Exam Help

https://powcoder.com

Mallory

gmail.com





HTTP Threats

Eve can observe:

- What page you are visiting (e.g. http://gmail.com/email84534)
- Server response (e.g. the content of your empil)
 Cookies (Can now login as you!)
- Submitted forms (passwords, new emails, credit cards, etc) https://powcoder.com

Mallory can:

- Provide you false information (e.A. than we the chartent of whem all r
- Change what data you send (e.g. change the contents of what you post/send!)
- Insert Javascript on your page (e.g. tracking info / steal information from gmail's origin)

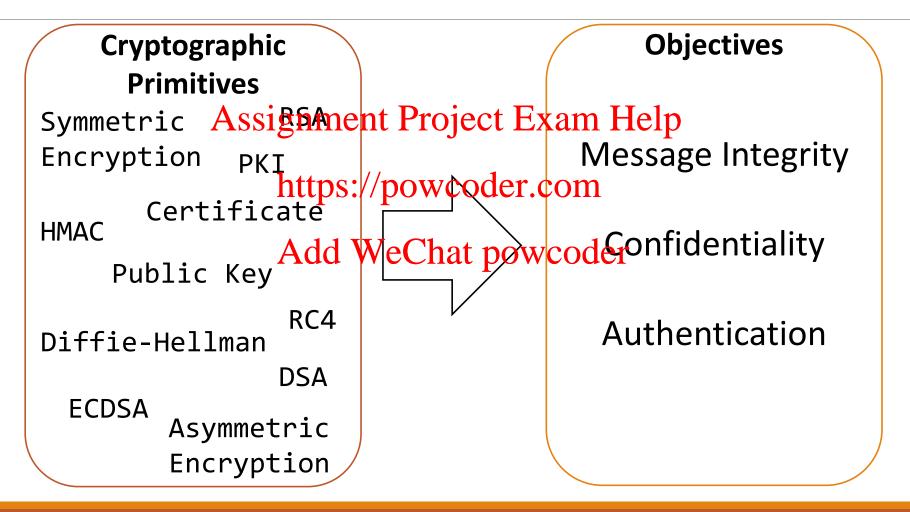
Solution:

- Cryptography! Confidentiality + Integrity
 - ...but how?

How do we translate?

```
Cryptographic
     Primitives
Symmetric Assignment Project Exam Help
Encryption
      https://powcoder.com
    Public Key Add WeChat powcoder
HMAC
               RC4
Diffie-Hellman
              DSA
 ECDSA
       Asymmetric
       Encryption
```

How do we translate?



How do we translate?

```
Cryptographic
     Primitives
Symmetric Assignment Project Texain Plan HTTPS
     Certificate Connection
Encryption
    Public Key Add WeChat powcoder
HMAC
              RC4
Diffie-Hellman
              DSA
 ECDSA
       Asymmetric
       Encryption
```

HTTPS, TLS

Transport Layer Security (TLS)

- Previous versions: Secure Socket Layer (SSL) do not use!
 - SSL 2

Assignment Project Exam Help

- SSL 3.0
- TLS 1.0, 1.1, 1.2 extensions/improvements to SSL 3.0 https://powcoder.com
- TLS 1.3 redesigned TLS (2018)

HTTPS – the S stands for Secure Add WeChat powcoder

HTTP over TLS

Case Study: TLS

Arguably the most important (and widely used) cryptographic protocol on the Internet

Assignment Project Exam Help

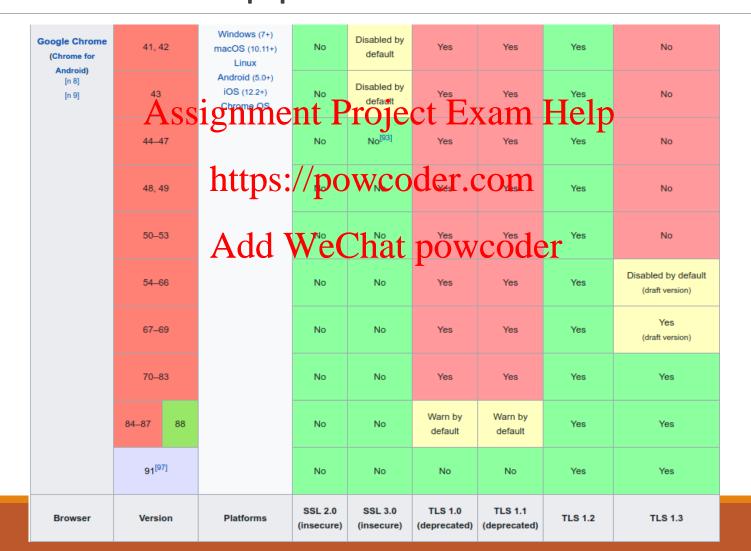
Almost all encrypted protocols (minus SSH) uses TLS for transport encryption https://powcoder.com

HTTPS, POP3, IMAP, SMTP, FTP, Motel We Clabbe p) Open det; SIP (VoIP), ...

Browser TLS Support

	Version	Platforms	SSL protocols		TLS protocols			
Browser			SSL 2.0 (insecure)	SSL 3.0 (insecure)	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3 (proposed)
Google Chrome (Chrome for Android) [n 8] [n 9]	1-9	nment	Disabled by default	Enabled by default	Yes	No	No	No
	ASS18		P1(DEJ a Ged Condition	EX	am .	Help	No
	21 }	nttps://	pďw	Enabled by	er.c	om	No	No
	22–25	Windows (7+) OS X (10.9+) Linux Android (4.1+) iOS (9.0+) Chrome OS	No	Enabled by default	Yes	Yes ^[50]	No[50][51][52][53]	No
	26–29		eCh No	default	OW	code	er No	No
	30–32		No	Enabled by default	Yes	Yes	Yes ^{[51][52][53]}	No
	33–37		No	Enabled by default	Yes	Yes	Yes	No
	38, 39		No	Enabled by default	Yes	Yes	Yes	No
	40		No	Disabled by default [55][59]	Yes	Yes	Yes	No
	41, 42		No	Disabled by default	Yes	Yes	Yes	No
	43		No	Disabled by default	Yes	Yes	Yes	No

Browser TLS support



Where does TLS live?

Application (HTTP)

Assignment Project Exam Help

Transport (TCP)
https://powcoder.com

Network WeChat powcoder

Data-Link (1gigE)

Physical (copper)

Atsignment Projects Expan Kep'

https://powcoder.com

Add WeChat powcoder

Client Hello: Here's what I support and a random

Assignment Project Exam Help

https://powcoder.com

Add WeChat powcoder

Client Hello: Here's what I support and a random

Server Hello: Chosen Cipher (and a random)

Certificate: Here is my "X509 Certificate" (public key)

Certificate: Here is my "X509 Certificate" (public key)

[Key exchange message (g^x mod p), and signature]

https://powcoder.com

Add WeChat powcoder

Client Hello: Here's what I support and a random Server Hello: Chosen Cipher (and a random) Certificate: Here is my "X509 Certificate"

[Key exchange message (g^x mod p), and signature] https://powcoder.com Client Key Exchange: [encryated (sever) detg/y mod p)] Change Cipher Spec and Finished

Client Hello: Here's what I support and a random Server Hello: Chosen Cipher (and a random) Certificate: Here is my "X509 Certificate" [Key exchange message (g^x mod p), and signature] https://powcoder.com Client Key Exchange: [encrypted(sever)detg^y mod p)] Change Cipher Spec and Finished Change Cipher Spec and Finished

Client Hello: Here's what I support and a random Server Hello: Chosen Cipher (and a random) Certificate: Here is my "X509 Certificate" [Key exchange message (g^x mod p), and signature] https://powcoder.com Client Key Exchange: [encrypted(sever)detg^y mod p)] Change Cipher Spec and Finished Change Cipher Spec and Finished **Encrypted Communication Channel (Symmetric)**

Cipher Suites

DHEST RSA PAES 256 HEST HA

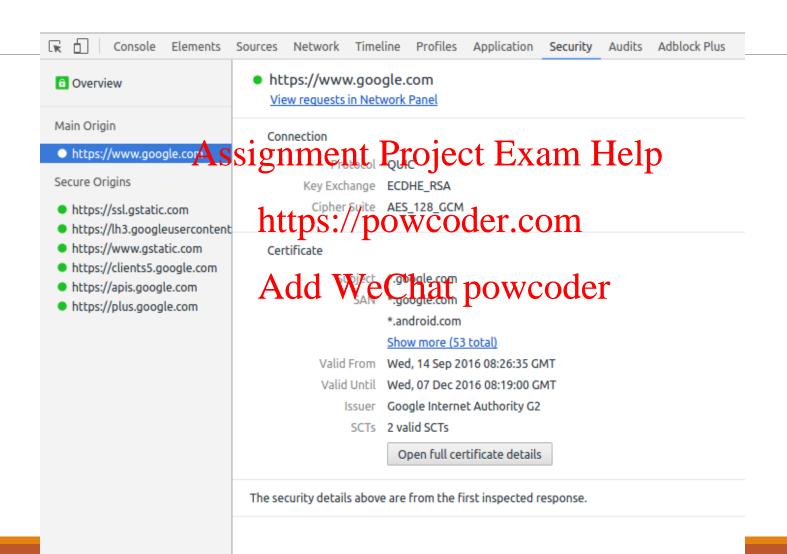
https://powcoder.com

Ephemeral Key Exchange

Identity Authentication

Add WeChat powcoder Data Transfer Cipher

Message Digest



Goals



Confidentiality

Assignment Project Exam Help



https://powcoder.com Message Integrity Add WeChat powcoder



Authentication

X509 Certificates

Subject: C=US/O=Google Inc/CN=www.google.com

Issuer: C=US/O=Google Inc/CN=Google Internet Authority

Serial Number 01:b1:04:17:be:27048:b4:8e:1e:8b:a0:781691ac:83 **Expiration Period:** Jul 12 2010 - Jul 19 2012

Public Key Algorithm: rşaEncryption

Public Key: 43:1d:53.2e.19.ef:d2:90.54:0a:f5.9a:f0:fa.14:58:ad:a0:81:b0:3d

7c:be:b1:82:19:b9:7c3:8:04:e9:1e5d:b5:80:af:d4:a0:81:b0:b0:68:5b:a4:a4

:ff:b5:8a:3a:a2:29:e2Actrd3:8004 e911atcpto:vc6:8:04e19:39:23:46

Signature Algorithm: sha1WithRSAEncryption

Signature: 39:10:83:2e:09:ef:ac:50:04:0a:fb:9a:f0:fa:14:58:ad:a0:81:b0:3d 7c:be:b1:82:19:b9:7c3:8:04:e9:1e5d:b5:80:af:d4:a0:81:b0:b0:68:5b:a4:a4 :ff:b5:8a:3a:a2:29:e2:6c:7c3:8:04:e9:1e5d:b5:7c3:8:04:e9:1e:5d:b5

Certificate Chains

Trust everything signed by this "root" certificate

I authorize and trust this certificate; here is my signature

I authorize and trust this certificate; here is my signature

Browser Root CA store

bigtpature/3010:830209:eforp0:04:0a:fb:9a:38:c9:d1

SABJECT: N=05/.L/at = 000 gle October Authority

Issuer: C=US/.../OU=Equifax Secure Certificate Authority

Public Key:

Signature: be:b1:82:19:b9:7c:5d:28:04:e9:1e:5d:39:cd

Subject: C=US/.../O=Google Inc/CN=*.google.com

Issuer: C=US/.../CN=Google Internet Authority

Public Key:

Signature: bf:dd:e8:46:b5:a8:5d:28:04:38:4f:ea:5d:49:ca

Goals



Confidentiality (Symmetric Crypto)

Assignment Project Exam Help



https://powcoder.com Message Integrity (HMACs) Add WeChat powcoder



Authentication (Public Key Crypto)

Certificate Authority Ecosystem

Each browser trusts a set of CAs

CAs can sign certificates for new CAs

CAs can sign certificates fassignment Project Exam Help

If a single CA is compromised, there entre system is compromised

Add WeChat powcoder
We ultimately place our complete trust of the Internet in the weakest CA

Immediate Concerns

Nobody has any idea who these CAs are...

1,500+ known browser trustesignment Project Exam Help

https://powcoder.com

History of CAs being hacked (e.g. Diginotar)

Add WeChat powcoder

Oooops, Korea gave every elementary school, library, and agency a CA certificate (1,324)

Luckily invalid due to a higher-up constraint

Getting a Certificate

Certificates are free and easy to get!

https://letsencrypt.org/

https://powcoder.com
Identity validated via e-mail in whois, or proving control over a certain webpage on the domain

• What can go wrong?

Add WeChat powcoder

Setting up TLS manually is hard. People are terrible at it!

DigiNotar

DigiNotar was a Dutch Certificate Authority

On June 10, 2011, *.google.com cert was issued to an attacker and subsequently used to orchestrate MITM attacks in Iran https://powcoder.com

Nobody noticed the attack until Act do We that how to de in the wild... and posted to pastebin

DigiNotar Contd.

DigiNotar later admitted that dozens of fraudulent certificates were created

Assignment Project Exam Help Google, Microsoft, Apple and Mozilla all revoked the root Diginotar certificate

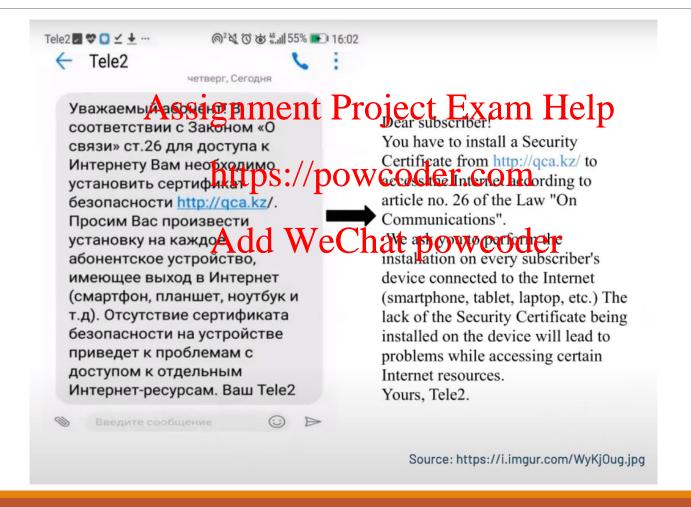
https://powcoder.com

Dutch Government took over Diginotar

Add WeChat powcoder

Diginotar went bankrupt and died

Kazakhstan TLS MITM



Kazakhstan TLS MITM

Injected Certificate of rcku.kz located in AS9198 Trusted Certificate of rcku.kz located in AS9198 Certificate chain Certificate chain 0 s:/businessCategory=Private 0 s:/businessCategory=Private Organization/jurisdictionC=KZ/serialNumber=050440008395/C=KZ/L=Nur-Su OrganizationOrganizati 1tan/0=T00 \xD0\x98\xD0\xBD\xD1\x84\x08\BS\xD1\x81\pD1\B\c1 -\xD0\x41\xD0\xB8\xD1\x81\xD1\x82\x12\x85\xD0\xBC/0U=1T DEPARTMENT/CN=rcku.kz DEPARTMENT/CN=rcku.kz i:/C=KZ/CN=Security Certificate i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=Thawte EV RSA CA ----BEGIN CERTIFICATE----2018 MIIEWDCCA0CgAwIBAgIQDQTtk969f4etNJ6W1ZPyOjANBQkqhkiG9W0BAQSFADAS MQswCQYDVQQGEwJLWjEdMBsGA1UEAxMUU2VjiXUIdkkqQ2VcGGImaWVhGGHhick MTkwNDI0MTgwMDAwWhcNMjEwNDE2MDYwMDAwWjeBv2EqMBs6A10EDwWUJHJPHmF0 (I) (72: (8-0) JAWIBA) (Q) (19:9) f4etNJ6VhYBD6DANBgkqhkiG9w0BAQsFADBf MgswCqrDvQQErJVo2EvMBmGArUEChMMRG1naUNlcnQgSW5jMRkwFwYDVQQLExB3 ZSBPcmdhbml6YXRpb24xEzARBgsrBgEEAYI3PAIBAxMCS1oxFTATBgNVBAUTDDA1 d3cuZGlnaWNlcnQuY29tMR4wHAYDVQQDExVUaGF3dGUgRVYgUlNBIENBIDIwMTgw MDQ0MDAwODM5NTELMAkGA1UEBhMCS1oxEzARBgNVBAcTCk51ci1TdWx0YW4xJjAk HhcNMTkwNDI1MDAwMDAwWhcNMjEwNDE2MTIwMDAwWjCBvzEdMBsGA1UEDwwUUHJp BgNVBAoMHVRPTvDomNC90YTOvtGA0Lwt0KHOuNGB0YLOtdC8MRYwFAYDVOOLEw1J dmF0ZSBPcmdhbm16YXRpb24xEzARBqsrBqEEAYI3PAIBAxMCS1oxFTATBqNVBAUT VČBERVBBUlRNRÚSUMRAWDGYDVQQDEWdyY2t1Lmt6MIIBIDANBgLqhkiG9W0BAGEE AAOCAQOAMIIBCAKCAQEAOdx3G+V6xOrv1kzJy DDA1MDQ0MDAwODM5NTELMAkGA1JEBhMCS1oxEzARBgNVBAcTCk51ci1TdWx0YW4x TAKRONYAN MENRATODOM 90 TON GWOLWEOKHQUNGBOYLQEDGKRYWFAYDVQQL LW1JYCDERY BMMNI USUR MOO YQODEWDYY211Lmt6MIIBIjANBgkqhkiG9w0B sJQUW8Wr0VilkH3WipXFg2QGqyFfVsVFVOL@/AZ_/\tbt2rz\$Y71Mex/PDSSsM72 +tMxvM2gljheC5+yUYc+DIzgil0aYsGL3umcxBqJsZovAy5578txsLD1r9RhfCh0 AQEF-AOCAQ8AMIIBCqKCAQEApQNLX4xjCEo2vHwZ1Xs1DkEw/nHo81iqZxqiuYGa +U190V4O3K167vLU5oMuVZ9JeXtfZR1vVqADWuqvrPPtkjwVi1ck+vteuvLLFKku Q139R2CUsArb0zUh46QGe4YiLq4MqxPsWNeCkBYvYq8XqGOuzekQp2niMRxwAxs5 11Ago4FGkKJT9WD9p1wZkXU3g1/6FU+QJCwtI9TuKMAB2JbvHiCwcgcQCdRqQplY BGhA55XV9Kta9eW2MNhjMQ7j9OkbFPJy4Rkv/W/tXsieDeoh7+eIH+iIzR2cpMEJ ER24nkRImJiKn/2wJHs0P9NMbu8JjoK5QcHa+10uMQIBA60B4zCB4DAdBgNVHQ4E PTq6LKcI8Z0N53FMf+oAdHNShEMjdNzIPye66KtdOtn4rqHCdeVN2v24/KvWKHuh FqQU1owRPo/dE3y0HX25d0V6wKs8BpswZwYDVR0jBGAwXoAUXk2Qqn+G61r0qxX0 q6Nmv4W0XHMOUdHQeNtH412R8C+E+E1t1JkNynVuL7sPpDfD9d0sXt26T4YDwZHB UI6rOulyTamhMKQuMCwxCzAJBqNVBAYTAktaMR0wGwYDVQQDExRRYXpuZXQqVHJ1 NftDSbpUooWslPJFuZriY9w35cu8b+/049HuLyVZERrSGQIDAQABo4IDIDCCAxww c3QgTmV0d29ya4IUXk2Qgn+G61r0gxX0UI6r0ulyTakwCQYDVR0TBAIwADALBgNV HwYDVR0jBBgwFoAU5wH8DBYYyn2yjOyHJ6NvYYE7hDkwHQYDVR00BBYEFDfcto19 HO8EBAMCBaAwHOYDVR01BBYwFAYIKwYBBOUHAwEGCCsGAQUFBwMCMB8GA1UdEQQY T6Ysh/mfBY2Bnd520axzMB8GA1UdE0QYMBaCB3Jia3Uua3qCC3d3dy5yY2t1Lmt6 MBaCB3Jja3Uua3qCC3d3dy5yY2t1Lmt6MA0GCSqGSIb3DQEBCwUAA4IBAQBuDLg+ MA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw fIGuQP5uIWOVsmS41pAqpM9C9dj1I6QmohHq/RuqpXu55TSk7EH6mrM8Nxb38ScN PAYDVR0fBDUwMzAxoC+qLYYraHR0cDovL2NkcC50aGF3dGUuY29tL1RoYXd0ZUVW RQat1SUS1MJ08BYhcS8kiwuqy9umtEAs1SPjo81AzMLZTQZVnkn1ANt1uLqhRyU4 U1NBQ0EyMDE4LmNybDBLBqNVHSAERDBCMDcGCWCGSAGG/WwCATAqMCqGCCsGAQUF vXSqVNX1r6XE8+juM8//pJWx9VzLUxVqNeU4q60QBjKCIBGkLF/hfRKjI1366F8K BwIBFhxodHRwczovL3d3dy5kaWdpY2VydC5jb20vQ1BTMAcGBWeBDAEBMHEGCCsG 4aGnGmw2YtbA1wvxn/m0xANeB0GwCeM26UouHVbmv0r1KbkocK1bd7H27XcwhWwU AOUFBWEBBGUWYzAkBggrBgEFBOcwAYYYaHR0cDovL3N0YXR1cv50aGF3dGUuY29t unK82vO5pPIZ6aVdzm333iLi5khPrsubH2sVvL7E75TBRbL8+Z00L0ZwaChxudaM MDsGCCsGAQUFBzAChi9odHRwOi8vY2FjZXJ0cy50aGF3dGUuY29tL1RoYXd0ZUVW UlnBQ0EyMDE4LmNydDAJBgNVHRMEAjAAMIIBfwYKKwYBBAHWeQIEAgSCAW8EggFr JiXu7BCUvrK1SN1J ----END CERTIFICATE----AWkAdqCkuQmQtBhYFIe7E6LMZ3AKPDWYBPkb37jjd800yA3cEAAAAWpSkBsKAAAE 1 s:/C=KZ/CN=Security Certificate AwBHMEUCIDGdtx9PFzK9QL+GNUDKrXEvJhZ0iW6YU1YGt/zBqLy6AiEA2Zkh590x CdPkUTsVri9XCdBNXKpSmPkQQ0pn6eQ4JD8AdwBWFAaaL9fC7NP14b1Esj7HRna5 i:/C=KZ/CN=Qaznet Trust Network ----BEGIN CERTIFICATE---vJkRXMDvlJhV1onQ3QAAAWpSkBYkAAAEAwBIMEYCIQCQGcB78vSGuB7/0iPGrWlk

Kazakhstan TLS MITM

Domains impacted:

allo.google.com, android.com, cdninstagram.com, dns.google.com, docs.google.com, encrypted.google.com, facessignum.com, project. Laxa groups google.com, hangouts.google.com, instagram.com, mail.google.com, mail.ru, messages.android.com, messenger.com, news.google.cdnttpkr//piowcgrdele.com/plus.google.com, rukoeb.com, sites.google.com, sosalkino.tv, tamtam.chat, translate.google.com, twitter.com, video.google.com, vk.com, vk.ma, ukuseraudio net, vkuservideo net, www.facebook.com, www.google.com, www.instagram.com, www.messenger.com, www.youtube.com, youtube.com

Browser response:

Remove KZ root cert even if user explicitly added it!

Attack Vectors

Attack the weakest Certificate Authority

Attack browser implementation gnment Project Exam Help

https://powcoder.com
Magically notice a bug in a key generation library that leads you to discovering all the private keys on the Internet

Add WeChat powcoder

Attack the cryptographic primitives

Math is hard, let's go shopping!

TLS Attacks

User concerns

- Deploying site leaks private key
- Client users ignore HTTPSArsgrignment Project Exam Help

Attack (weakest) CA

• DigiNotar, Comodo, WoSign/Starttons://powcoder.com

Attack Browser

Attack Browser Add WeChat powcoder

• SSL Strip, Null Prefix, Padding Oracle, BEAST, CRIME, goto fail, POODLE, FREAK, LogJam, DROWN, ...

Attack Server

Heartbleed



Q

Search

About 274,000 results (0.24 seconds)

Everything

-----BEGIN RSA PRIVATE KEY - Pastebin.com - #1 paste tool since ...

pastebin.com/TbaeU93m

Images 19 Apr 2010 – ... the difference. Copied. -----BEGIN RSA PRIVATE KEY-----.

MIICXwIBAAKBpenis1ePqHkVN9IKaGBESjV6zBrIsZc+XQYTtSlVa9R/4SAXoYpl ...

Maps

Videos

----BEAssignment Project Exama Helpince ...

pastebin.com/sC7bGw30 News 18 Apr 2010 different

18 Apr 2010 - ... difference. Copjed. ----BEGIN RSA PRIVATE KEY----.

MIIEogIBAAKCA #FATIBATIZKMPO WWW O O GETWO 179 AHLqm3+0+gpPbk ...

Shopping

More

site:pastebin.com "-----BEGIN RSA PRIVATE KEY-----" - Posterous cdevers.posterous of the contract of the contr

All results

MIICXwlBAAKBpenis1ePqHkVN9IKaGBESjV6zBrlsZc+ XQYTtSlVa9R/4SAXoYpl .

Related searches

More search tools

<u>help/en/howto/sftp - Cyberduck</u> trac.cyberduck.ch/wiki/help/en/howto/sftp

Private keys containing a DSA or RSA private key in PEM format are supported (look for -----BEGIN DSA PRIVATE KEY----- or -----BEGIN RSA PRIVATE KEY----- ...

SSH access with a private RSA key [Archive] - VanDyke Software For...

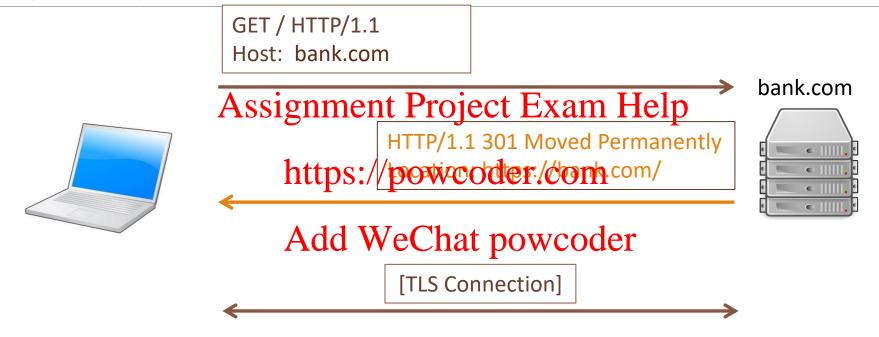
forums.vandyke.com/archive/index.php/t-2185.html 2 Sep 2011 – ----BEGIN RSA PRIVATE KEY-----

MIIEogIBAAKCAQBujdbtxyIX4KaQPeTf5F/

aOSBwSpZN4MjTixU2Yq8JkipjMYpYwpNj1TODzRJf ...

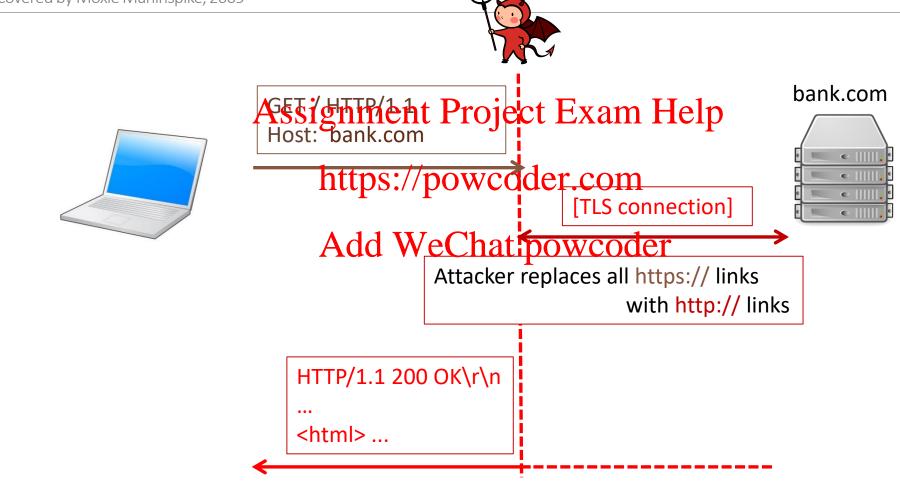
SSL Strip

Discovered by Moxie Marlinspike, 2009



SSL Strip

Discovered by Moxie Marlinspike, 2009



Null Termination Attack

Discovered by Moxie Marlinspike, 2009

ASN.1 utilizes Pascal-style strings

Web browsers utilize use C-style strings
Assignment Project Exam Help

```
https://powcoder.com
gmail.com.evil.com
Add WeChat powcoder
```

gmail.com\0.evil.com

```
strcmp("gmail.com\0.evil.com", "gmail.com") == 0
```

Discovered by Thai Duong and Juliano Rizzo, 2011

"Browser Exploit Against SSL/TLS"

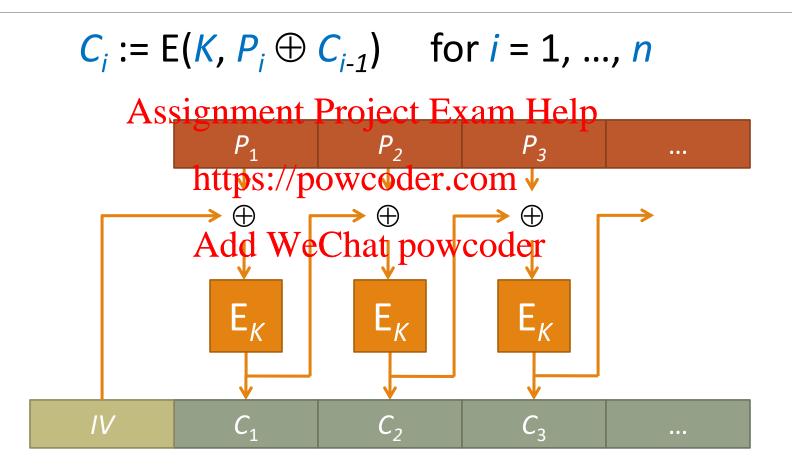
Chosen Plaintext attack against CBC-mode Assignment Project Exam Help

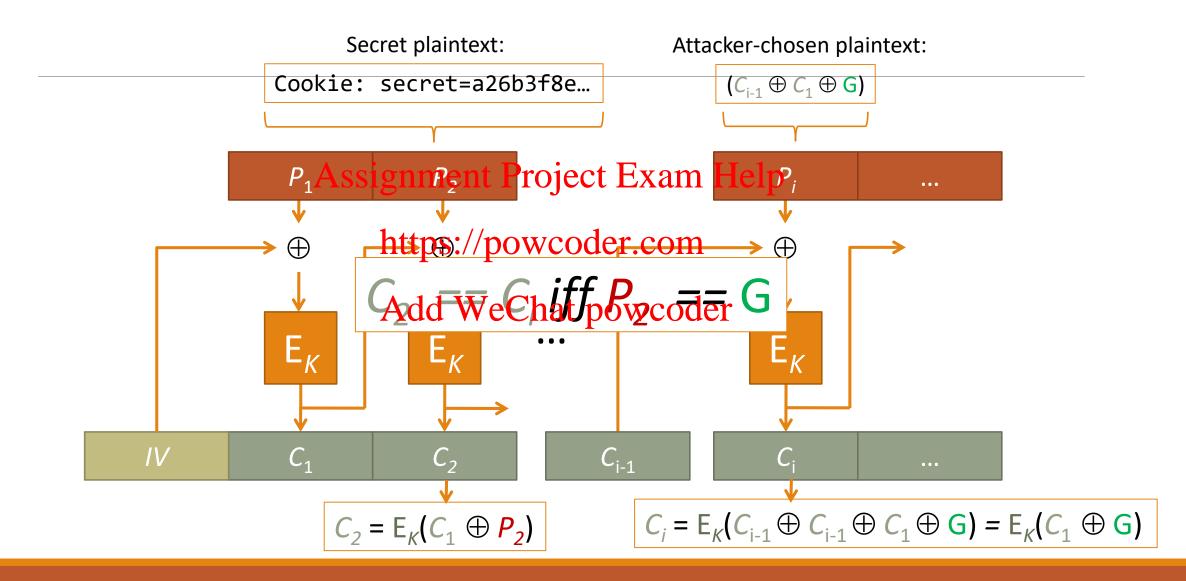
Attacker can:

https://powcoder.com

- Observe Alice's Ciphertext
- Make Alice to send secret plainted PWe Chat powcoder
 - E.g. HTTP Cookie
- Make Alice to send arbitrary plaintext over same TLS session

CBC: Cipher-Block Chaining Mode





Problem: Attacker has to guess G entirely

Solution: force part of P2 Assignment Pipe ject Exam Help

Cookie: secret=a26b3f8e_com

P₂ Add WeChat powcoder P₃

AAAAA\r\nCookie: secret=a 26b3f8e...

Only have to guess 1-byte now!

256 guesses and we're sure to get it

Once we guess a, we can redo the attack, with less padding:

```
Assignment Project Exam Help
```

AAAA\r\n**ottpki/powsederetera**2 6b3f8e...

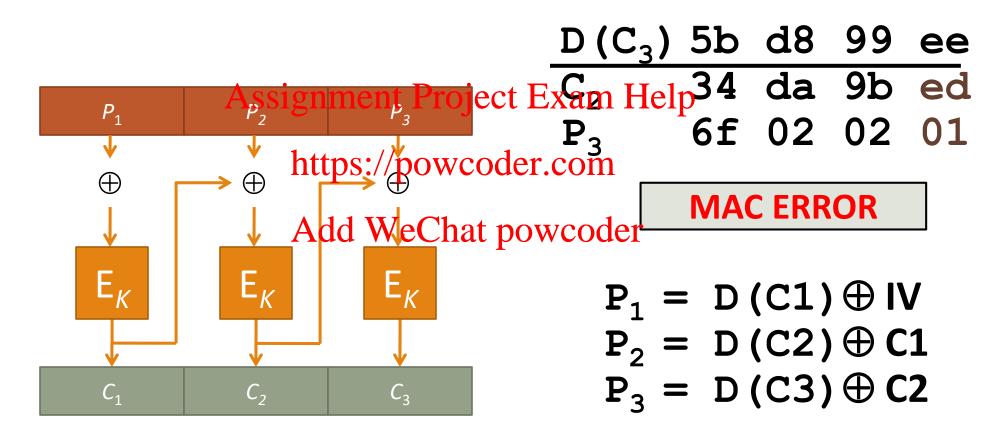
Add WeChat powcoder AAA\r\nCookie: secret=a26 b3f8e...

AA\r\nCookie: secret=a26b 3f8e...

A\r\nCookie: secret=a26b3 f8e...

Padding oracle attack

Discovered by Serge Vaudenay, 2003



Discovered by Thai Duong and Juliano Rizzo, 2012

Compression Ratio Info-leak Made Easy

Client compresses HTTP header

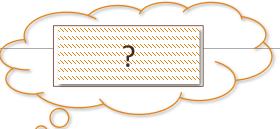
· Contains attacker controlled Saignment Project Exam Help

https://powcoder.com

Attacker can:

- Make Alice send HTTPS requests with some data secret
- Observe encrypted data (length)

Discovered by Thai Duong and Juliano Rizzo, 2012



Assignment Project Exam Help

https://powcoder.com

GET / HTTP/1.1

Addb We Chat powcoder
Cookie: a2bf6c89... 320 bytes

320 bytes

bank.com





Discovered by Thai Duong and Juliano Rizzo, 2012



bank.com



Discovered by Thai Duong and Juliano Rizzo, 2012



Discovered by Thai Duong and Juliano Rizzo, 2012



bank.com



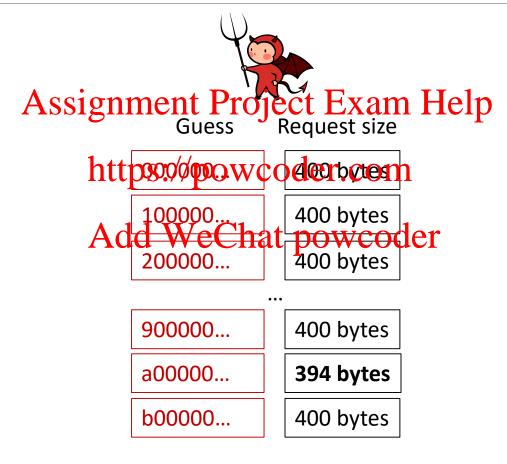
Discovered by Thai Duong and Juliano Rizzo, 2012



bank.com



Discovered by Thai Duong and Juliano Rizzo, 2012



bank.com

• |||||:

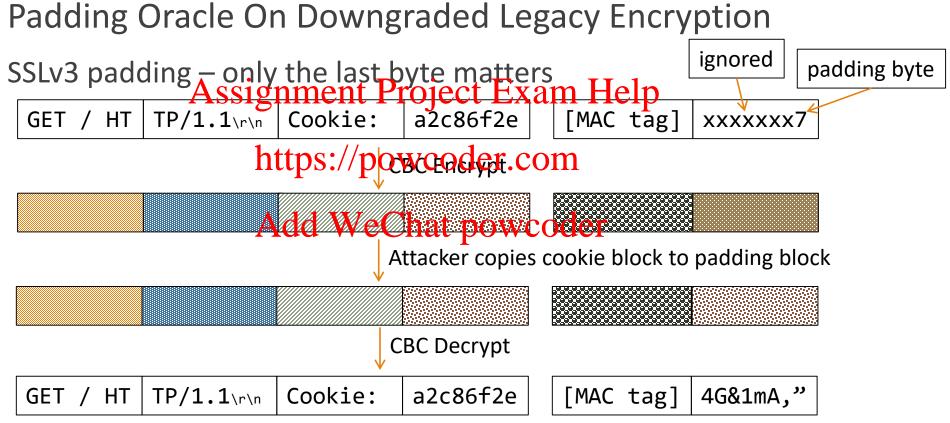
@ |||||

goto fail;

```
hashOut.data = hashes + SSL MD5 DIGEST LEN;
                                             2014 Apple TLS library – SSLVerifySignedServerKeyExchange()
hashOut.length = SSL SHA1 DIGEST LEN;
if ((err = SSLFreeBuffer(&hashCtx)) != 0)
                             Assignment Project Exam Help
   goto fail;
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
   goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, https://powcoder.com
   goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, Aere Rawe Chat powcoder
   goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
   goto fail;
   goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
   goto fail;
err = sslRawVerify(...);
fail:
   // Cleanup buffers, etc. Return err
   return err;
```

POODLE

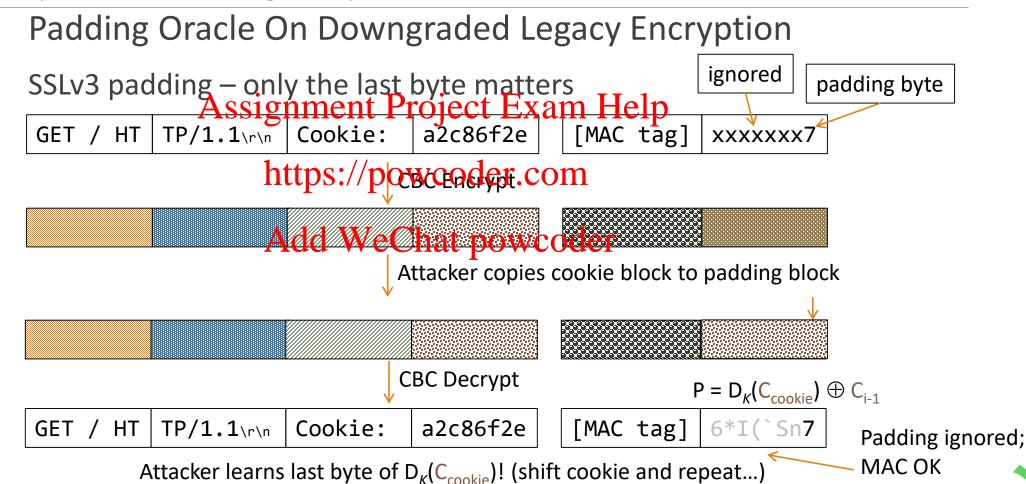
Discvoered by Bodo Möller, Thai Duong and Krzysztof Kotowicz, 2014



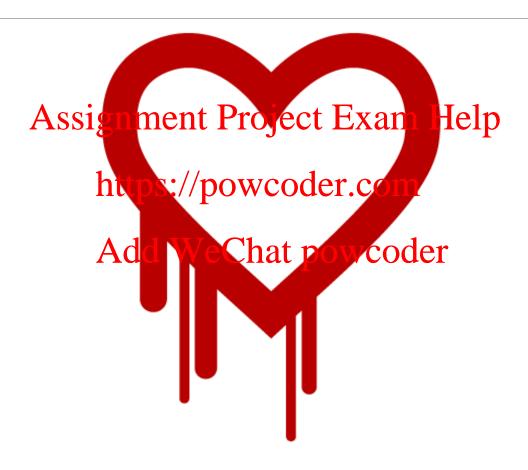


POODLE

Discvoered by Bodo Möller, Thai Duong and Krzysztof Kotowicz, 2014

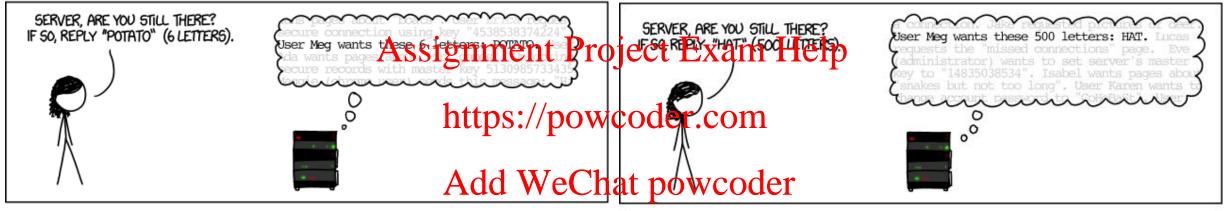


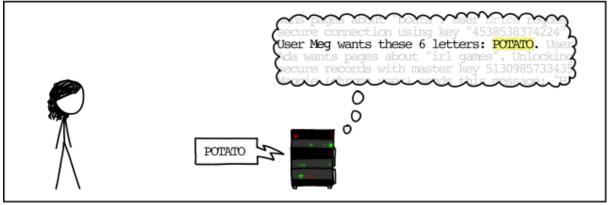
Heartbleed

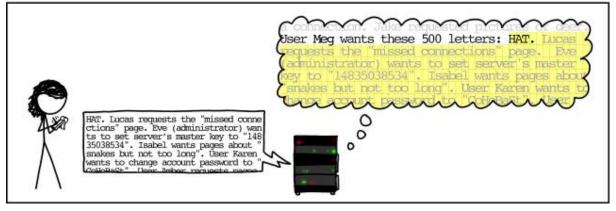


Heartbleed

HOW THE HEARTBLEED BUG WORKS:







MD5 Considered Harmful Today

Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger

In 2008 (at CCC), a group of researchers showed that they could create a rogue CA certificate

using an MD5 collision

A S	serial number signment Pro validity period	ject Exam He	lp rogue CA cert	
	https://poworeal cert domain AddatweCha	codense omix (difference) at powcoder	rogue CA RSA key	− CA bit!
			rogue CA X.509 extensions	
	real cert RSA key	collision bits (computed)	Netscape Comment Extension (contents ignored by	
	X.509 extensions	identical bytes (copied from real cert)	browsers)	
	signature		signature	

MD5 Considered Harmful Today

Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger

This kind of md5 collisions takes a bit more processing than **fastcoll** from the crypto project...

• So researchers used a Assignmenta Projecta Exam He

Took 4 attempts (CA signatures)

https://powcoder.com

Add WeChat powcoder



"Mining Your Ps and Qs"

Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman

In 2012, a team of researchers performed a global analysis of SSL/TLS and SSH keys

- 5.6% of TLS and 9.6% of SSH hosts shared cryptographic keys in a vulnerable manner
- Calculated the private keyAfgsignment the private keyAfgsignment to private keyAfgs
 - What if two RSA servers generate the same p but different q? $N_1 = pq_1$ and $N_2 = pq_2$ [Find p given N_1 and N_2 ?]
- Uncovered vulnerabilities in Linux et Bandon Dumber depertured / dev/urandom)

