Cryptography in the real world

PCMI 2022 Undergraduate Summer School

Lecture 12

Christelle Vincent

University of Vermont

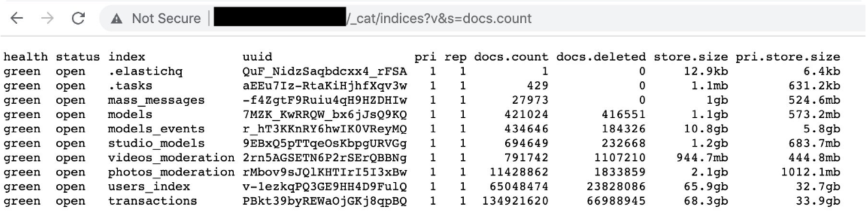
August 5, 2022

Why have this lecture?

Designing secure systems is **hard**!

The Stripchat incident

On Nov 5, 2021, Diachenko found a database available in plaintext.



Not Secure | [redacted]/_cat/indices?v&s=docs.count

```
health status index             uuid                   pri rep docs.count docs.deleted store.size pri.store.size
green  open   .elastichq        QuF_NidzSaqbdcxx4_rFSA   1   1          1            0     12.9kb          6.4kb
green  open   .tasks            aEEu7Iz-RtaKiHjhfXqv3w   1   1        429            0      1.1mb        631.2kb
green  open   mass_messages     -f4ZgtF9Ruiu4qH9HZDHIw   1   1      27973            0        1gb        524.6mb
green  open   models            7MZK_KwRRQW_bx6jJsQ9KQ   1   1     421024       416551      1.1gb        573.2mb
green  open   models_events     r_hT3KKnRY6hwIK0VReyMQ   1   1     434646       184326     10.8gb          5.8gb
green  open   studio_models     9EBxQ5pTTqeOsKbpgURVGg   1   1     694649       232668      1.2gb        683.7mb
green  open   videos_moderation 2rn5AGSETN6P2rSErQBBNg   1   1     791742      1107210    944.7mb        444.8mb
green  open   photos_moderation rMbov9sJQlKHTIrI5I3xBw   1   1   11428862      1833859      2.1gb       1012.1mb
green  open   users_index       v-1ezkqPQ3GE9HH4D9FulQ   1   1   65048474     23828086     65.9gb         32.7gb
green  open   transactions      PBkt39byREWaOjGKj8qpBQ   1   1  134921620     66988945     68.3gb         33.9gb
```

Data included email addresses, usernames, and IP addresses, and the database was indexed by search engines.

The NordicTrack treadmills

NordicTrack treadmills force users to use their proprietary software and watch their videos.

Until Oct 2021, users could access the underlying Android OS on their treadmill by tapping the screen 10 times, waiting 7 seconds, then tapping the screen 10 more times.

Sending an email from the FBI

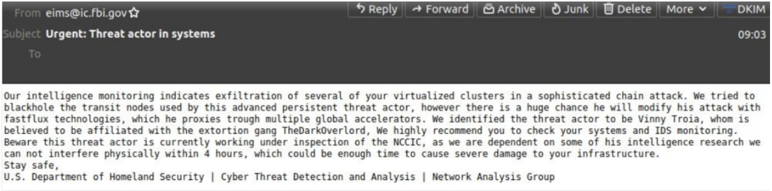
LEEP is a public website with resources for law enforcement. Anyone can make an account.

An email is sent from `eims@ic.fbi.gov` with a one-time passcode to confirm the address.

Sending an email from the FBI

The email was generated **client-side** then sent via a POST request, which included the email subject and content.

Pompompurin figured out how to modify them, and sent thousands of emails from the FBI on Nov 12, 2021.



From eims@ic.fbi.gov

Subject Urgent: Threat actor in systems

09:03

To

Our intelligence monitoring indicates exfiltration of several of your virtualized clusters in a sophisticated chain attack. We tried to blackhole the transit nodes used by this advanced persistent threat actor, however there is a huge chance he will modify his attack with fastflux technologies, which he proxies trough multiple global accelerators. We identified the threat actor to be Vinny Troia, whom is believed to be affiliated with the extortion gang TheDarkOverlord, We highly recommend you to check your systems and IDS monitoring. Beware this threat actor is currently working under inspection of the NCCIC, as we are dependent on some of his intelligence research we can not interfere physically within 4 hours, which could be enough time to cause severe damage to your infrastructure.
Stay safe,
U.S. Department of Homeland Security | Cyber Threat Detection and Analysis | Network Analysis Group

Short detour: digital signatures

Encryption/decryption ensures secrecy but not authenticity.

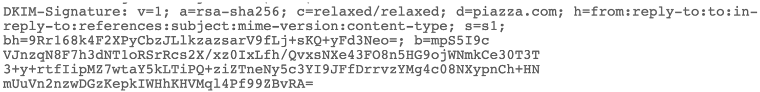
For that we have digital signatures, which are ways a person can prove knowledge of its secret key without disclosing it.

Sending an email from Google

Email is as old as ARPANET, and worked on the honor system.

This allowed spammers to impersonate anyone they wanted.

Enter DKIM, which tacked a digital signature on email.



```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=piazza.com; h=from:reply-to:to:in-
reply-to:references:subject:mime-version:content-type; s=s1;
bh=9Rr168k4F2XPyCbzJLlkzazsarV9fLj+sKQ+yFd3Neo=; b=mpS5I9c
VJnzqN8F7h3dNT1oRSrRcs2X/xz0IxLfh/QvxsNXe43FO8n5HG9ojWNmkCe30T3T
3+y+rtfIipMZ7wtaY5kLTiPQ+ziZTneNy5c3YI9JFfDrrvzYMg4c08NXypnCh+HN
mUuVn2nzwDGzKepkIWHhKHVMql4Pf99ZBvRA=
```

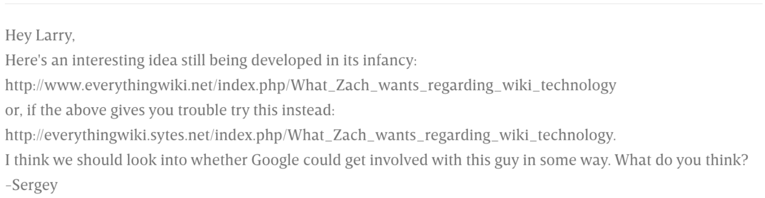
Sending an email from Google

Until 2012, Google used a 512-bit RSA modulus to sign its email.

Back then this could be factored in a matter of hours.

Sending an email from Google

Harris used this to send an email to Google founders Brin and Page from each other.



Hey Larry,

Here's an interesting idea still being developed in its infancy:

http://www.everythingwiki.net/index.php/What_Zach_wants_regarding_wiki_technology

or, if the above gives you trouble try this instead:

http://everythingwiki.sytes.net/index.php/What_Zach_wants_regarding_wiki_technology.

I think we should look into whether Google could get involved with this guy in some way. What do you think?

-Sergey

The RSA modulus was quickly updated to 2048 bits.

Speaking of digital signatures!

Certificate: file that holds public key and identifying information about owner (like `gmail.com`).

Certificates are signed by a **certificate authority**, one of a few companies that your browser trusts.

When identifying itself by proving knowledge of a secret key, the site provides a signed certificate containing its public key.

Speaking of digital signatures!

This whole system relies on people not being able to get a signed certificate for a website they do not own.

In Jan 2012, CA Trustwave admitted that it had been selling the ability to generate certificates to corporate clients.

BGP vulnerabilities

Border Gateway Protocol: how servers route internet traffic.

Each ISP has a BGP router that announces a list of IP addresses to which it can deliver information.

These are put in a giant public **routing table**.

BGP vulnerabilities

To send data to another ISP, the GBP router looks up the IP address in a routing table.

If two ISPs can deliver to the same IP address, the one with the narrowest range wins.

BGP vulnerabilities

Allows **anyone** to draw internet traffic meant for certain IPs addresses.

This traffic then gets lost: if you try to pass it on to the right IP address, it will keep bouncing back to you.

This happened when Pakistan tried to block YouTube only for its citizens but actually took it down for the whole world in 2008.

BGP attack

DefCon 2008: how to send the announcement only to some routers.

In 2013, was used to get the traffic, inspect it, then pass it on.

US government agencies and other US IP addresses were targeted.

Just for fun

The big 2021 Facebook outage happened because Facebook removed its IP addresses from BGP routing tables.

“Export-grade” cryptography

Until 1992, cryptography was on the U.S. Munitions List as auxiliary military equipment.

Cryptographic methods had to be licensed for export, and strong crypto was only licensed on a case-by-case basis.

Recall the TLS handshake

For a new connection, client sends a list of supported ciphers, and server responds with a public key for one of these ciphers.

Because clients abroad only had export-grade cryptography, servers needed weak public keys.

Some TLS clients accept a weak public key even if they asked for a strong one (OpenSSL, SecureTransport).

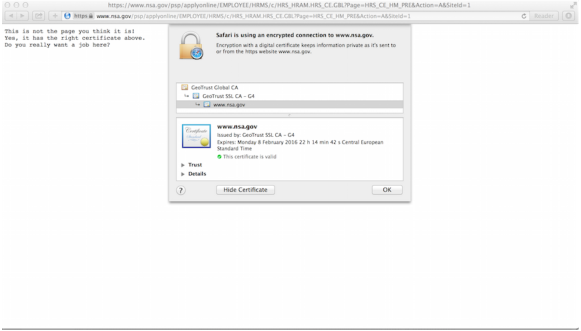
The attack

1. Client asks for strong RSA encryption.
2. Man-in-the-middle changes the message to ask for weak RSA.
3. Server responds with weak key.
4. Client accepts key due to the bug.
5. Attacker factors weak RSA modulus to decrypt the pre-master secret and recovers master secret.

Proof of concept

2015: Heninger factored 512-bit RSA in 7.5 hours for $104.

This was used to hack the NSA site.



https://www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_HM_PRE&Action=A&SiteId=1

https www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_HM_PRE&Action=A&SiteId=1

```
This is not the page you think it is!
Yes, it has the right certificate above.
Do you really want a job here?
```

Safari is using an encrypted connection to www.nsa.gov.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.nsa.gov.

GeoTrust Global CA
↳ GeoTrust SSL CA – G4
↳ www.nsa.gov

www.nsa.gov
Issued by: GeoTrust SSL CA – G4
Expires: Monday 8 February 2016 22 h 14 min 42 s Central European Standard Time
● This certificate is valid

DSA based on DLP

Person A has published their Elgamal public key:

$$a_A, \quad b_A (\equiv a_A^{k_A} \pmod{p_A}) \quad \text{and} \quad p_A.$$

Person A has also sent *m* encrypted with Person B's public key.

DSA based on DLP

To prove authenticity, Person A proves they have access to k_A:

1. They generate a random integer $0 < \ell < p_A - 1$
2. They compute $r \equiv a_A^{\ell} \pmod{p_A}$
3. They also compute $s \equiv \ell^{-1}(m + k_A r) \pmod{p_A - 1}$

The signature is (r, s), which is published.

Note that ℓ and k_A remain secret. (And only B knows m.)

DSA based on DLP

To check that A knows k_A, B computes

$$a_A^{ms^{-1}} b_A^{rs^{-1}}$$

and checks that this is equal to r.

Indeed,

$$\begin{aligned} a_A^{ms^{-1}} b_A^{rs^{-1}} &\equiv a_A^{ms^{-1}} (a_A^{k_A})^{rs^{-1}} \pmod{p_A} \\ &\equiv a_A^{s^{-1}(m+k_A r)} \pmod{p_A} \\ &\equiv a_A^{\ell} \pmod{p_A} \\ &\equiv r \pmod{p_A}. \end{aligned}$$

All that B needs is access to m, and it only works if A has used k_A.

One use of DSA

Modern game consoles are prevented from installing software that does not come from their manufacturer.

This is done by telling the console to accept software updates only from sources that give the correct signature.

2012 attack on PS3

2012: Three Musketeers obtain access to the Sony "k" value.

The public key (a, b, p) for this value was embedded in the hardware of every PS3 produced to date.

With this key PS3 could be jailbroken and made to run pirated games or any other software.

Because this affected the lowest level of security of the PS3, this could not be patched.

How could this happen?!

Sony used the same value of ℓ repeatedly.

This is easy to notice: the first parameter of the signature is

$$r \equiv a^{\ell} \pmod{p};$$

two signatures with the same r have used the same ℓ.

Just solve for ℓ

Once you receive two signatures (r, s_1), (r, s_2), recall that

$$s_i \equiv \ell^{-1}(m_i + kr) \pmod{p-1}$$

Solving for m_i we get

$$m_i \equiv s_i\ell - kr \pmod{p-1}.$$

So

$$m_1 - m_2 \equiv (s_1\ell - kr) - (s_2\ell - kr) \equiv (s_1 - s_2)\ell \pmod{p-1}.$$

And now solve for k

It is now trivial to recover k:

$$k \equiv r^{-1}(s\ell - m) \pmod{p-1}.$$

Thank you for a great three weeks!