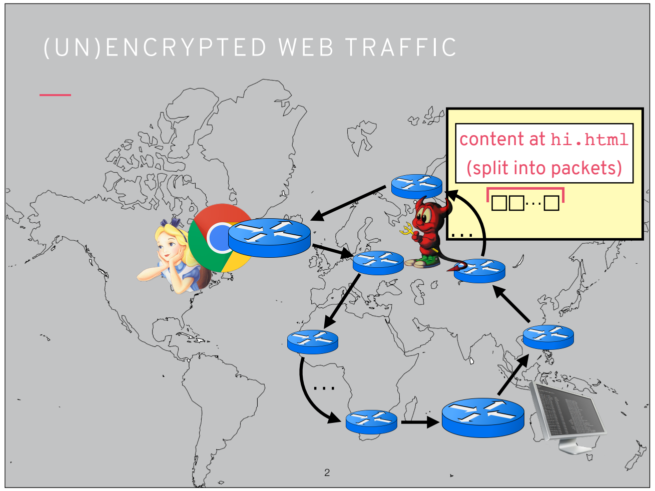
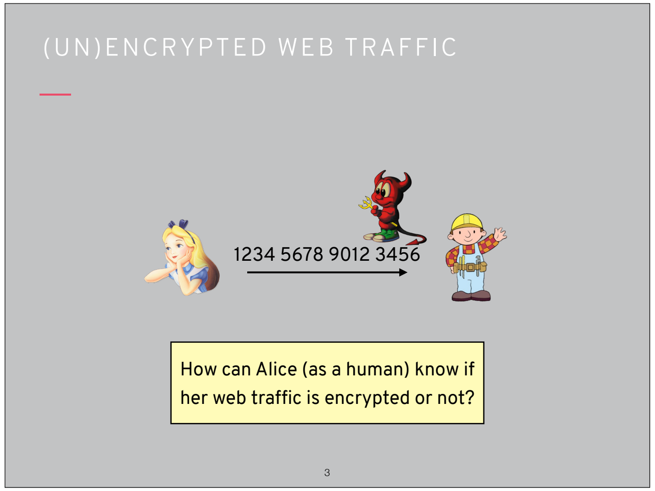
SECURITY (COMP0141): USING ENCRYPTION



(UN)ENCRYPTED WEB TRAFFIC

As we saw, adversary can spy on your traffic unless it’s encrypted

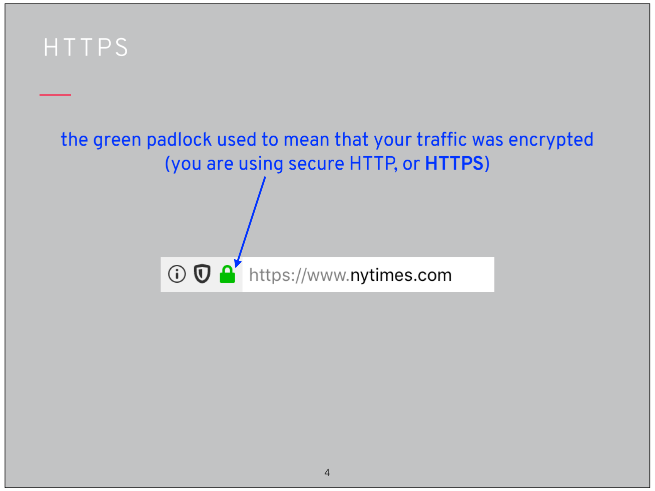


(UN)ENCRYPTED WEB TRAFFIC

1234 5678 9012 3456

How can Alice (as a human) know if her web traffic is encrypted or not?

Really concretely, this means if you’re entering something like your credit card number that everyone along the way can see it

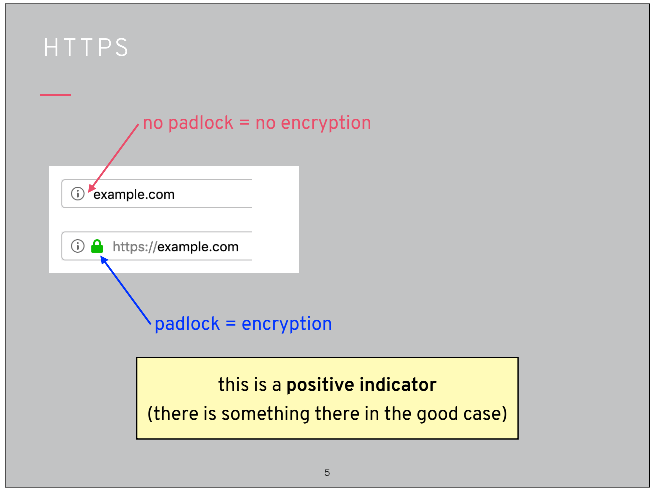


HTTPS

the green padlock used to mean that your traffic was encrypted (you are using secure HTTP, or **HTTPS**)

https://www.nytimes.com

Historically, seeing a green padlock meant your web traffic was being encrypted



HTTPS

no padlock = no encryption

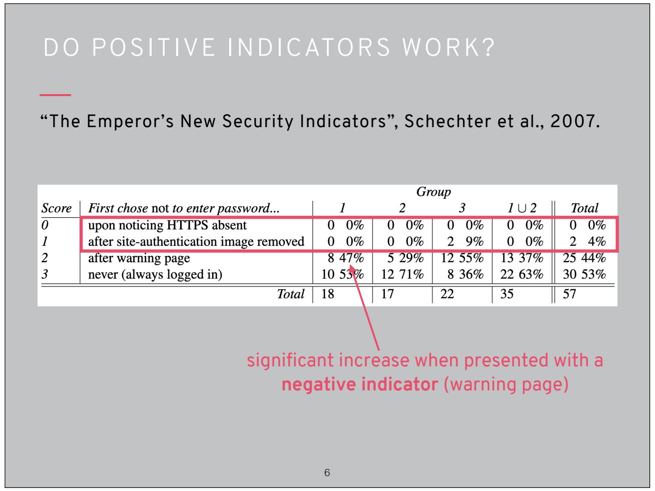
example.com

https://example.com

padlock = encryption

this is a **positive indicator**
(there is something there in the good case)

And if your web traffic wasn't encrypted, you didn't see a green padlock



DO POSITIVE INDICATORS WORK?

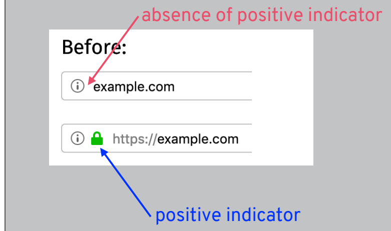
"The Emperor's New Security Indicators", Schechter et al., 2007.

		Group				
Score	*First chose* not *to enter password...*	*1*	2	*3*	*1* ∪ 2	*Total*
0	upon noticing HTTPS absent	0 0%	0 0%	0 0%	0 0%	0 0%
1	after site-authentication image removed	0 0%	0 0%	2 9%	0 0%	2 4%
2	after warning page	8 47%	5 29%	12 55%	13 37%	25 44%
3	never (always logged in)	10 53%	12 71%	8 36%	22 63%	30 53%
	Total	18	17	22	35	57

significant increase when presented with a **negative indicator** (warning page)

Positive indicators do not seem to work

BEFORE…



absence of positive indicator

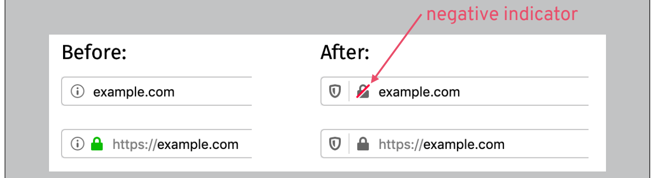
Before:

example.com

https://example.com

positive indicator

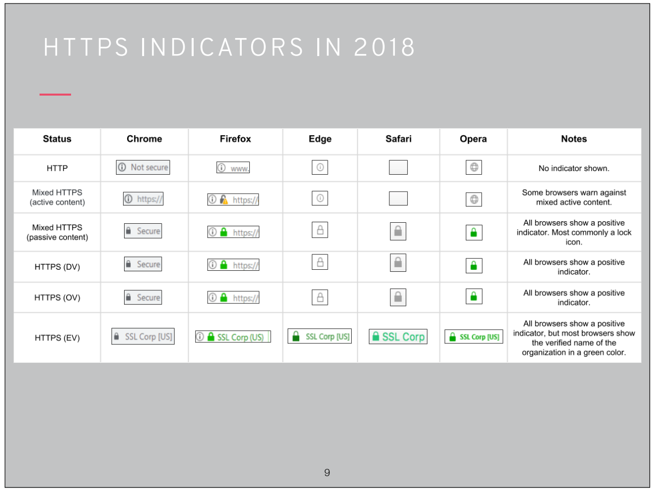
BEFORE… AND AFTER



negative indicator

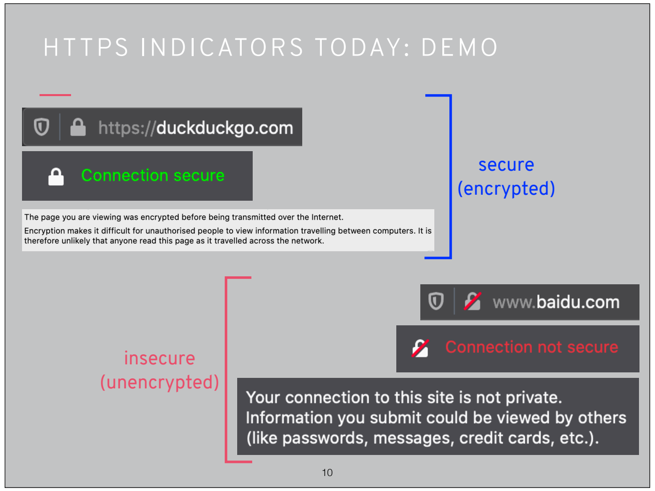
Before:	After:
example.com	example.com
https://example.com	https://example.com

As a result of these types of studies, we’ve now seen a big shift towards using negative indicators instead



HTTPS INDICATORS IN 2018

Status	Chrome	Firefox	Edge	Safari	Opera	Notes
HTTP	ⓘ Not secure	ⓘ www.	ⓘ	□	🌐	No indicator shown.
Mixed HTTPS (active content)	ⓘ https://	ⓘ 🔓⚠ https://	ⓘ	□	🌐	Some browsers warn against mixed active content.
Mixed HTTPS (passive content)	🔒 Secure	ⓘ 🔒 https://	🔒	🔒	🔒	All browsers show a positive indicator. Most commonly a lock icon.
HTTPS (DV)	🔒 Secure	ⓘ 🔒 https://	🔒	🔒	🔒	All browsers show a positive indicator.
HTTPS (OV)	🔒 Secure	ⓘ 🔒 https://	🔒	🔒	🔒	All browsers show a positive indicator.
HTTPS (EV)	🔒 SSL Corp [US]	ⓘ 🔒 SSL Corp (US)	🔒 SSL Corp [US]	🔒 SSL Corp	🔒 SSL Corp [US]	All browsers show a positive indicator, but most browsers show the verified name of the organization in a green color.



HTTPS INDICATORS TODAY: DEMO

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorised people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.

secure (encrypted)

Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).

insecure (unencrypted)

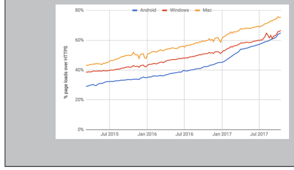
In this demo we looked at two search engines and actually clicked on the padlock to find out more information

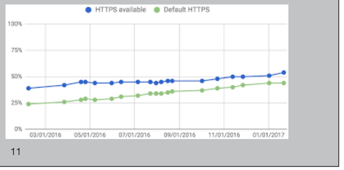
USABLE ENCRYPTION

Success story for usable security!

- Studies showed that old (positive) indicators were not usable and thus did not protect users
- As a result, browsers moved or are moving towards negative indicators instead

This was enabled by technological advances (which we'll see next week) that also made HTTPS much more widespread





QUIZ!

Please go to

`https://moodle.ucl.ac.uk/mod/quiz/view.php?id=2746845`

to take this week's quiz!