Lecture 1

maandag 6 februari 2023 14:45

protocol: set of rules for communication

security protocol aims to achieve a security properties
e.g. C+A

often, involves malicious parties who do not abide by protocol/expectations
untrusted channel and/or dishonest participants

secrecy

does protocol achieve secrecy?

		HTTP
WPA	TLS/SSL	TCP
	DNSSEC	DNS

verification remains necessary since we keep introducing new protocols

secrecy: prevention of unauthorized disclosure of information

weak secrecy: not be able to deduce message contents

strong secrecy: not learn anything about messages at all
including length!

authentication
- of a user
- of a message (sender)

integrity

anonymity: prevent identifying specific properties of individual events in a set

unlinkability: do not allow party to see two sessions with one party as having come from the same party

(undeniability
(non)repudiation
availability → typically not part of a protocol
fairness
privacy → too complex for this course

notation

symmetric encryption	$\langle M \rangle K$
asymmetric encryption	$\{\|M\|\} K$
cryptographic hashing	$\#(M)$
tupling	$(M_1, .., M_n)$
messages	M
nonces	N_1, N_2 assumed unguessable
keys	K_1, K_2 assumed unguessable

Dolev-Yao attacker model:
attacker controls communication medium
but cryptography is perfect

no info without key
no modification without key
perfect keys
perfect random numbers
perfect hashes

injectivity: things do not collide if they are not the same.

Dolev-Yao model is insensitive to message length
e.g. it is impossible to confuse a tuple with two log messages with a tuple with three log messages

an informal protocol narration describes the message sequence of a regular protocol run

A and B are roles for a session of the protocol

details are left implicit (e.g. whether and how correctness checks are performed, and their consequences)