Lecture 7

Tuesday, 6 December 2022 13:27

defensive policies

password policies

don't share password with anyone

long passwords

not in dictionary

large-scale attacks must be profitable in expectation, not merely in particular scenarios

many attacks cannot be made profitable, even if many profitable targets exist

huge gap between possible and actual/profitable attacks

Weakest link is a failing model; it does not properly consider costs and gains

as well as uncertainty about these numbers,

competition between attackers

or attack failure for another reason than good defenses e.g. internet outage / block by ISP

does not consider scalability and convenience for the attacker

attacker wants to gain more from an attack (on average) than its cost.

actually: wants to maximize profit → expected, so certainty plays a role too

sum of effort defense

encryption in internal network may not provide security benefits in e.g. SCADA systems

but it may make troubleshooting/discovery more difficult

endpoint is more vulnerable than the cable

but, for long distances, confidentiality may sometimes be useful

authentication & integrity are necessary

the unfalsifiability of security claims is the root reason of many policy errors

exercising good judgment and being scientific is particularly difficult

things can be declared insecure by observation, but not the reverse

policy creep: policies only become more strict over time

↓

"we only add more countermeasures"

but that might introduce problems ...

↓

if there is a problem with a policy e.g. a bypass vulnerability

↓

we never remove it ...

people tend to prefer avoiding losses to acquiring equivalent gains

rejection of security advice by users

checking links costs orders of magnitude more than it prevents in phishing damages

article states; more than 2.6 minutes per year of phishing training is not economically viable