Boardplan (.../06) — security intro (slide)

① negative goal
② segreg.

⓪ **Computer security** (Ideal)
- Bad guys (15y old, huge kerrafts?!)
- Good guys (home users, internet shops, institutes, police, ...)
- Mechanism (firewall, SSL, ..., jail, ~~...~~)
- Policy (honor code, laws, firewall rules, ...)

programming language

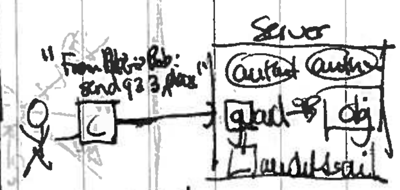
① **Real versus computer**
- Many parallels
  - cost/benefit
  - locks & police
- differences: ...
  - new opportunities
  - attacks be cheap & damage large
  - global
  - few laws

more rely on mechanisms

② **Security is difficult to attain**
- Altech/db
- Internet & Bbs didn't come with good plan
- Security is a negative goal
  - Bob cannot read file x ← harder
  - vs.
  - Bob can read file x

③ **Approach**
1) Principles & techniques
2) Safety net design approach
   - Be paranoid ⟨ economy of mech / open design
   - Be explicit
   - Design for iteration & feedback
   - Consider env & dynamics
3) Consider humans (slide)

④ **Security model**



- availability
- ~~confidentiality~~ secrecy

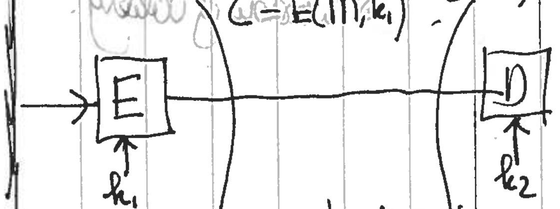
(all request; including config updates)

⑥ **Msg ~~confidentiality~~ secrecy** (closed)

(clipper chip (93)
802.11

⑦ **Open design**

$C \leftarrow E(M, k_1)$, $D(C, k_2) = M'$



$k_1 = k_2 \Rightarrow$ shared secret
$k_1 \neq k_2 \Rightarrow$ public key

locksmith

⑧ **Public key**

A: $E(M, K_{pub\,bob})$
B: $D(M, K_{priv\,bob})$

- key distribution ~~problem~~
- Ops are expensive

Attacks
1) cipher-text only — frequency, WEP
2) known-plaintext
3) chosen plaintext — ...
4) chosen ciphertext ?

S.O.S.