

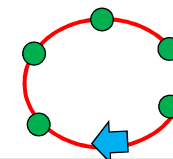
Class room exercise



Goal: need and aspects
of platform security

TASK

1. You construct a system to protect SIM lock in a mobile, 20 min:
 1. should contain architecture drawing
 2. Description of how it works
 3. How production and repair is handled
2. You analyze the solution of another group, 15 min
3. Both groups discuss what is good and bad in their solutions, 10 min



Background

- SIM lock is state stored in the phone
- SIM lock state and Info/data which operator the phone is locked to is programmed into the phone during production
- Info/data if SIM matches the programmed allow operator comes from SIM card.

- Phone: is CPU+RAM+Flash+SIM+other hardware
- Users attack hardware, on PCB but we assume one does not open chip packages.

Requirements

- 3GPP Standard: it must be possible for the user to unlock the phone. He/she gets unlock codes
- Programming of SIM lock may not delay production by more than 100ms (includes all extra time due to security for SIM lock)
- Logistical cost, e.g. due to sending code/keys must be kept small.
- Production: since it is a consumer product production must be cheap and environmental friendly (e.g. no epoxy or glue for protection allowed)

Your "enemies"

The screenshot shows the GSM UNLOCK website with a navigation bar containing 'LIFE' and 'FAQ'. Below the navigation bar are icons for 'We recommend', 'Forum', 'Tools', 'Downloads', 'Contact Us', and 'Download'. The main content area is divided into sections: 'GENERAL INFORMATION' with a list of services, 'UNLOCKS' with a list of unlocking tools, and 'Universal unlocking tools' with a list of products. The products listed are: 'Name: Honor 3000 Price: 120.00 \$', 'Name: HTC One Price: 255.00 \$', 'Name: Virgin tool box Price: 360.00 \$', and 'Name: HTC One Price: 340.00 \$'. There are also four comic-style illustrations: 'Goths', 'Vandals', 'Huns', and 'Geeks', each with a character and the text 'BRINGING CIVILIZATION TO ITS KNEES...'. The 'Geeks' illustration shows a character with a computer monitor and the text 'ACK ACK ACK ACK ACK'.



Phone hardware

