# Cyber Security

Prof V. Valli Kumari
CEO, AP INNOVATION SOCIETY
MEMBER, REAL TIME GOVERNANCE
VICE-CHAIRMAN, AP STATE COUNCIL FOR HIGHER EDUCATION

# Where the world is now

- Video

# Human Intelligence and Artificial Intelligence

- The autonomous car

# Where is automation now?

- video

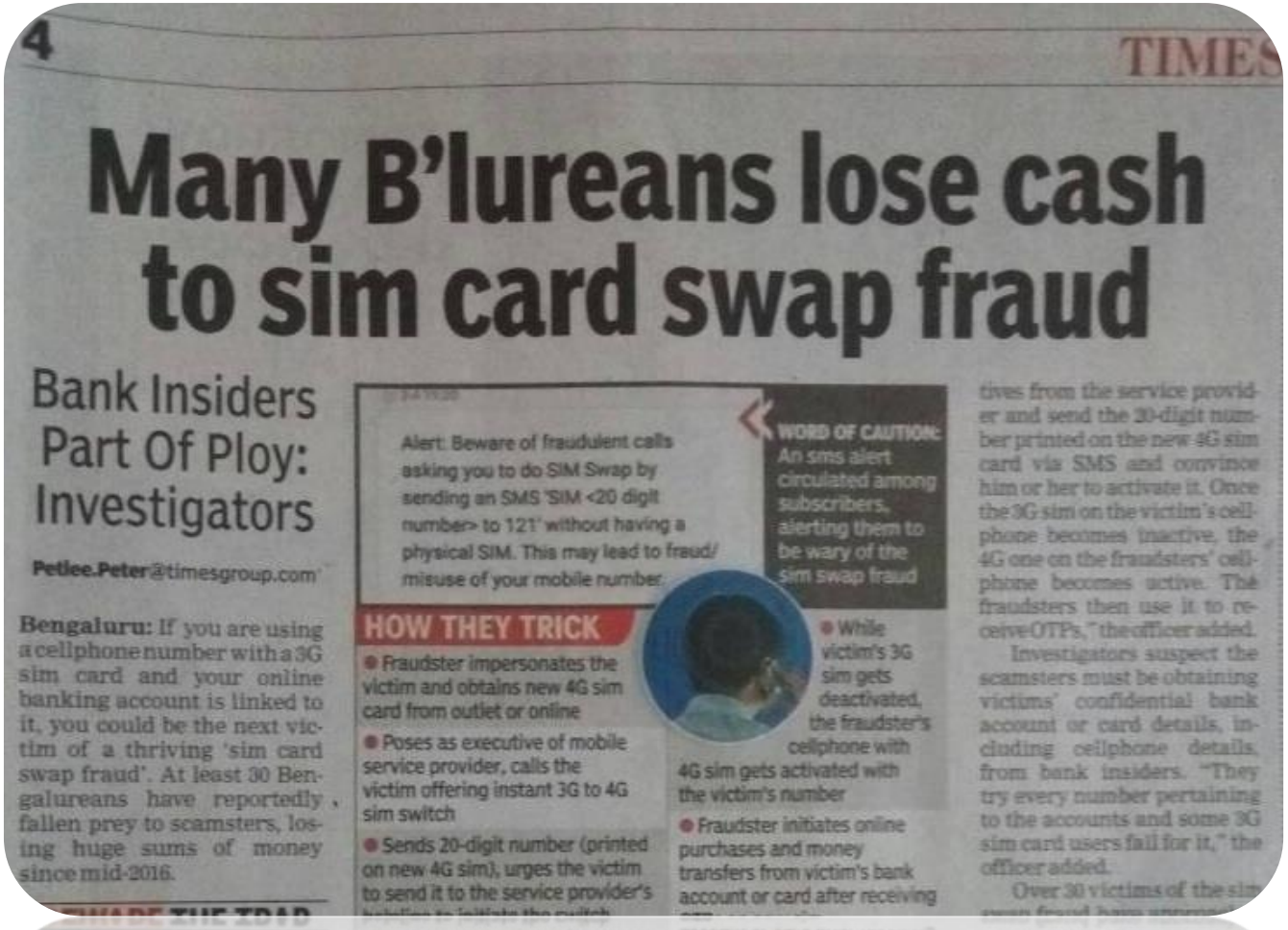
# How secure we are?

- The recent ransom ware attack

# Our Privacy?

- JanDhan, Adhaar, Mobile
- Adhaar exposed?
- Social media
  - Facebook
  - Whatsapp
- The surveillence cameras

# EXAMPLE



4

TIMES

## Many B'lureans lose cash to sim card swap fraud

### Bank Insiders Part Of Ploy: Investigators

Petlee.Peter@timesgroup.com

**Bengaluru:** If you are using a cellphone number with a 3G sim card and your online banking account is linked to it, you could be the next victim of a thriving 'sim card swap fraud'. At least 30 Bengalureans have reportedly fallen prey to scamsters, losing huge sums of money since mid-2016.

Alert: Beware of fraudulent calls asking you to do SIM Swap by sending an SMS 'SIM <20 digit number> to 121' without having a physical SIM. This may lead to fraud/ misuse of your mobile number.

**WORD OF CAUTION:** An sms alert circulated among subscribers, alerting them to be wary of the sim swap fraud

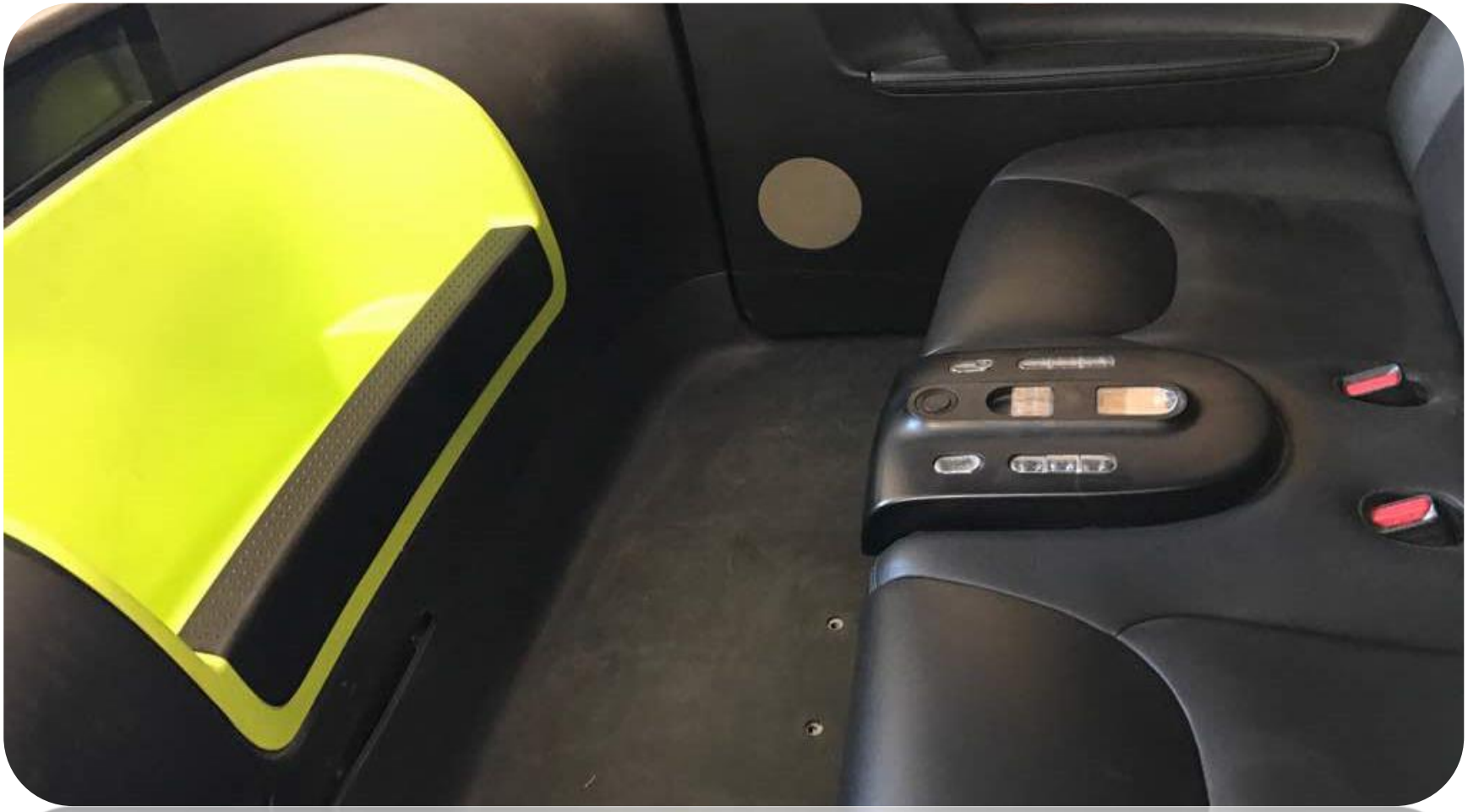
**HOW THEY TRICK**

- Fraudster impersonates the victim and obtains new 4G sim card from outlet or online
- Poses as executive of mobile service provider, calls the victim offering instant 3G to 4G sim switch
- Sends 20-digit number (printed on new 4G sim), urges the victim to send it to the service provider's
- While victim's 3G sim gets deactivated, the fraudster's cellphone with 4G sim gets activated with the victim's number
- Fraudster initiates online purchases and money transfers from victim's bank account or card after receiving

tives from the service provider and send the 20-digit number printed on the new 4G sim card via SMS and convince him or her to activate it. Once the 3G sim on the victim's cellphone becomes inactive, the 4G one on the fraudsters' cellphone becomes active. The fraudsters then use it to receive OTPs," the officer added.

Investigators suspect the scamsters must be obtaining victims' confidential bank account or card details, including cellphone details, from bank insiders. "They try every number pertaining to the accounts and some 3G sim card users fall for it," the officer added.

Over 30 victims of the sim



# Brains in palm

- The mobile and the revolution
- Palm under control of remote brains

# Security Implications

- Physical (media of propogation)
- Application
- Intermediate devices
- All layers of network
- Cloud (IAAS, PAAS, SAAS)
- Mobile /end user device

# THANK YOU