A One Day Big Brother Diary

FIM, Seminar aus Netzwerke und Sicherheit:

Security Considerations in Interconnected Networks

Vortragende(r):Mag. DI. Dr. Andreas Putzinger

Marc Peter,
Macskási Csaba

Content

- Introduction
- The day (worst case)
- Technology / Prevention
- Risk Analysis
- Personal Opinion

Introduction

- Development of technology
- amount of stored personal data
- mass surveillance
- big brother
- advice on how to prevent data extrusion
- YOU are vulnerable right now

The day

- The test person gets up and...
- ...switches on the television (ip-tv)
- ...checks mails via WiFi
- ...opens the garage door (bluetooth)
- ...is caught on tape (public cameras)
- ...gets located (GPS)
- ...opens the office door (RFID)
- .. uses his phone
- ...pays via QUICK
- ...uses clear text protocols

Technology / Prevention

- Ip-Tv
- E-Mail
- Wireless LAN / Bluetooth
- GPS
- RFID
- Websites with registration / Google
- Telephone

Ip-Tv

- Ablility to send data to the service provider
- The provider sees what you see
- Customized advertisement
- P2P Ip-Tv :
  - Also clients see what you see
  - Data injection
  - Data extrusion

E-Mail

- Improved technology -> security issues
- Censoring not only by governments
- WiFi && pop3
- SMTP unencrypted
- No evidence (eavesdrop on filesystem level / network traffic)
- Mailing lists (mail visible after years)
- => use VPN || SSH || PGP

Wireless LAN / Bluetooth 1/2

- Easy to use => popular
- Insecure by design (see WEP)
- People w/o. Knowledge build networks
- Motto: “jey, it works, don't touch it” => no encryption
- Attacker can be far away (L1 unsecure)
- Aircrack / ettercap
  - Crack WEP within 2 minutes
  - Crack WPA in reasonable time

Wireless LAN / Bluetooth 2/2

- Basically any script-kiddie with a notebook and a car can eavesdrop
- Use
  - 802.1 (radius)
  - VPN-s
  - SSH tunnels
  - IDS / IPS
- Still no secure:
  - Deauthenticate clients
  - Jam frequency
  - Mdk3.0...

parabolic cantenna with rp-sma connection

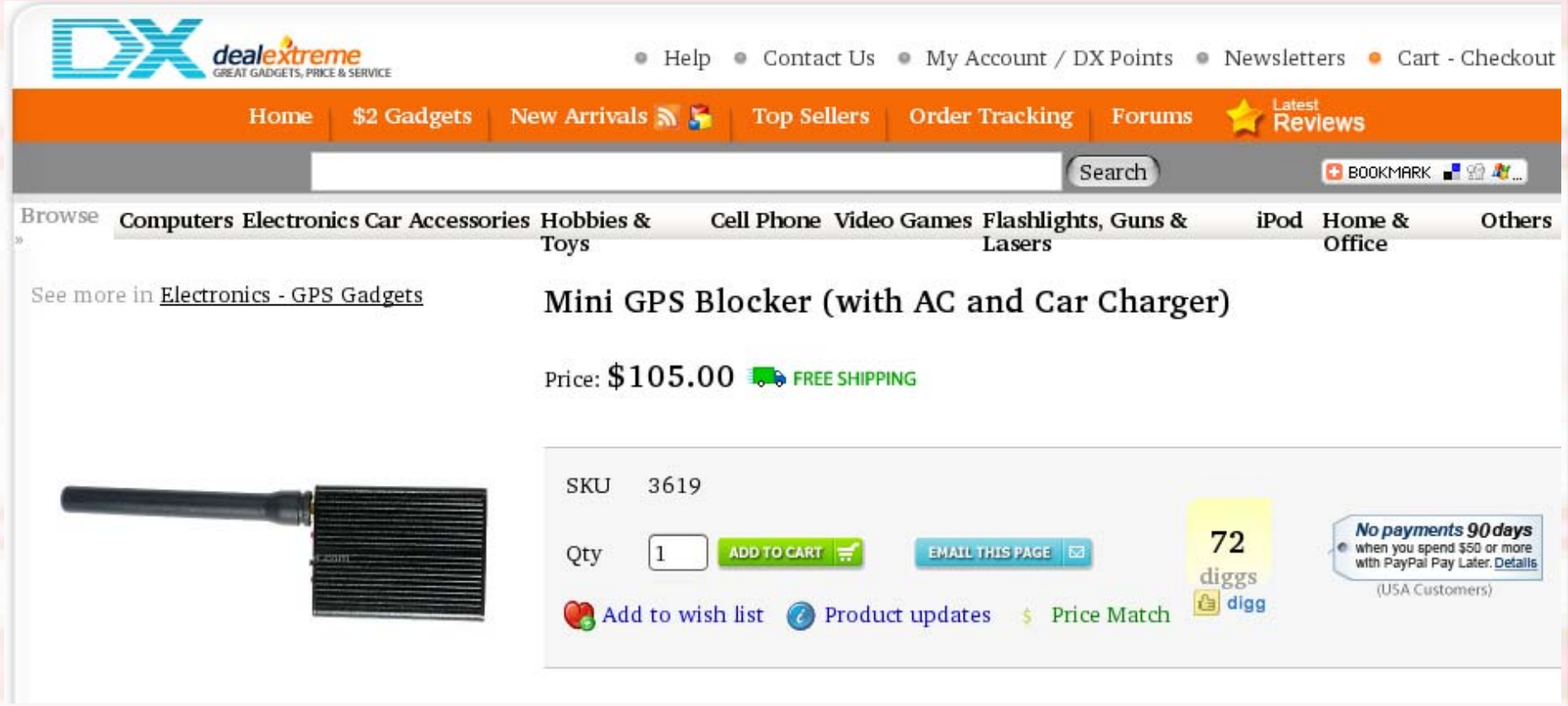
Cameras / Biometric identification

- Cameras installed in public places
- Pictures are analized
- Shape- / structure-recognition
- Face, fingerprint, iris, signature, voice
- 4 steps:
  - Picture recording
  - Normalizing, modification
  - Extraction of attributes
  - Matching
- London: you get filmed ca. 300 times/day

GPS 1/2

- Satellite based positioning system
- 24 satellites / 6 orbits
- Navigate / track vehicles
- As safe as the transmission between sender and receiver
- GPS-jammers
- Break connections
- Prevent usage of car tracking systems (anti theft)

GPS 2/2



cheap gps blocker at a Chinese website

RFID 1/2

- Transfer information over short distances
- Usage:
  - Parking tickets
  - Personal identification
  - Toll systems
  - Tracking
  - Time management systems
- Often hidden, pervasive
- Cheap reading devices (eg. in cell phones)
- Visually not detectable

RFID 2/2

- High range active devices (Piezzo-electric shoes && active RFID)
- Worst case: 2006, British passports with RFID, hacked in 48 hours
- Protect yourself:
  - Destroy chip: screwdriver, hammer, microwave (device unusable => bad)
  - Shield chip: cover chip with aluminium thinfoil

Telephone

- Since 1837
- Most connections still analogue
  - No encryption
  - Attach speaker to wire && eavesdrop
  - Cable length up to 8km. (8km insecurity)
- Early VOIP not encrypted
  - H323
  - Listen to it with VLC
- SIP is encrypted
- Mobile VOIP: traceability of the user

Risk Analysis

technology	Usage (l, m, h)	Risk (l, m, h)
Ip-TV	Low (for now)	low
E-Mail	**high**	**high**
Wireless LAN	**high**	**high**
Bluetooth	high	medium
/ biometric ide	medium	medium
GPS	Medium	low
RFID	Medium	medium
Websites	**High**	**high**
telephones	high	medium

Personal Opinion

- We are concerned about privacy issues
- In the wrong hands fatal
- If the KGB had these possibilities...
- Our advice:
  - Use only encrypted protocols
  - Tunnel unencrypted protocols
  - Never leave any evidence
    (It will be used against you.)
- “Big brother is watching you.”
  - Slogen is not made up. It is reality.

One Day Big Brother Diary

Any questions?

Thank you!