- Ensuring personal data protection while securing cyber space -

- Challenges and perspectives for the South East European Countries -
Cyber Warfare using Mobile Device as a Weapon
Agenda

• BYOD
• Mobile device – security issues
• Perimeter defense
• Mobile devices – weapon for deperimeterization
• Attack scenario – practical example
• Conclusion and open issues
BYOD

• Bring Your Own Device
• Popular
• Convenient
• Inevitable
• Dangerous (possibly)
Mobile device – security issues

• Many
  • Data on device, surveillance, access to connected accounts, privacy, ...

• Presentation focus
  • Mobile device as a stepping stone to protected network
Medieval castle

- Nothing comes in/out
  - Except through the gates
Network perimeter

- Nothing comes in/out
- Except through the firewalls
Mobile devices can “climb the walls”

- They come in/out as they (users) please
- Completely avoiding the firewalls ("deperimeterization")
Attack scenario

Outside network

Attacker

Firewall

Internal network

Secret document - available only within internal network
Attack scenario (2)

Outside network

Attacker
EvilApp.apk
or other attack on mobile device app. or OS

Internal network

Firewall

Secret document - available only within internal network

29 Oct 2014

Cyber Warfare using Mobile Devices as Weapon - Sasa Mrdovic
EvilApp.apk

• EvilApp connects back to attacker on HTTP port (80)
  • Permitted by firewall ("web surfing")
Attack scenario (4)

- Through this connection attacker has full control of mobile device
Attack scenario (5)

- including using it as a tunnel to internal network
Attack scenario (6)

• or using it to attack other PC on internal network
  • taking it completely over (no need for mob. dev.)
Conclusion

• Mobile devices are useful
• They are here to stay
• They could be used as a weapon
  • Against user and his organization
• Can we protect ourselves
  • Sure
  • But it takes some effort