Wireless Security Issues in M-government

S. Chatzinotas, C. Costopoulou,
S. Karetsos, M. Ntaliani

Informatics Laboratory, Agricultural University of Athens

Scope

- Investigation of security gaps and considerations when designing an m-government system
- Presentation of the security architecture of the Agroportal, an m-government system designed to provide services and online information to Greek agribusinesses

Agenda

- E-government
- M-government and Security
- Mobile Security
- The Case of Agroportal
- Security Policies and Guidelines
- Conclusions

E-government

Definition

E-government is defined as the use of information and communication technologies (ICTs) in public administrations combined with organisational change and new skills in order to improve public services and democratic processes and strengthen support to public policies

E-Government

- A mean for reforming public administration
- Interactions: more efficient, easier and less costly
- Large amounts of public funds

M-Government

- Complementary element of e-government and not its substitute
- Involves the use of all kinds of wireless and mobile technologies, applications and devices for improving e-government service delivery

M-government Levels

- Government to Citizens-G2C
- Government to Businesses-G2B
- Government to Employees-G2E
- Government to Government-G2G

M-Government and Security

M-Government transactions comprise sensitive data:

- *Personal data* e.g. identity and contact details
- *Government data* e.g. record / registration numbers and certificates
- *Financial data* e.g. credit card and bank account numbers

Mobile Security

- Mobile Device
  - Small dimensions: easy to misplace, steal
  - Constantly increasing storage and processing capabilities: target for malicious programmers
- Mobile Network
  - Operates over the air medium
  - More insecure than wired lines

Mobile Devices

- Authentication
  - *Password protection* e.g. PIN code
  - *Biometrics* e.g. fingerprint reader
  - *Auto Logout*
- Authorization
  - *File Masking*
  - *Access Control Lists*
  - *Role-based Access Control*

Mobile Devices

- PIN protection is the most common mechanism
- Biometric mechanisms not yet widespread
- Little support for authorization

Mobile Networks

- Any transceiver in the radio coverage of the mobile device can capture transmitted traffic or inject its own data in the communication link
- Security vulnerabilities of some well-known wireless protocols:
  - **Bluetooth**
  - **WiFi**
  - **Cellular networks**

Mobile Networks

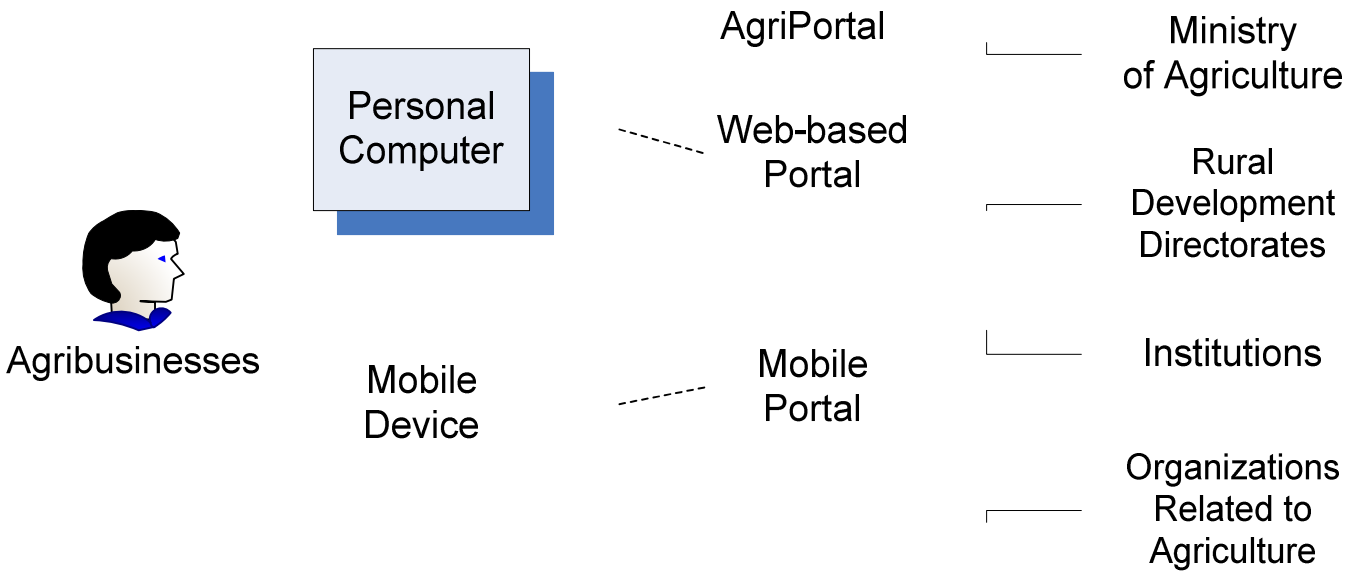
- Security Solutions for OSI layers:
  - PPTP
  - L2TP
  - IPSec
  - Mobile IP
  - SSL/TLS
  - SSH

Session Layer security for m-government

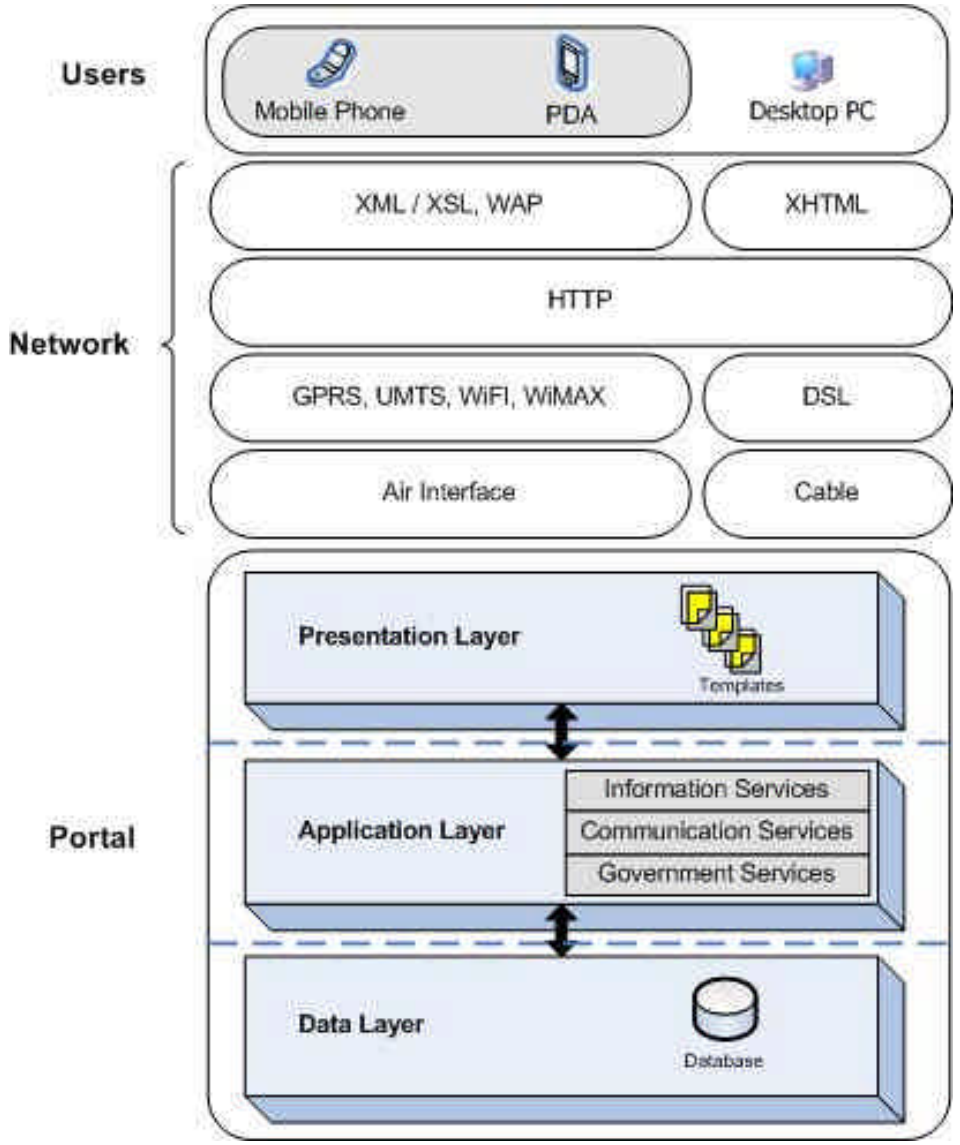
The Case of Agroportal

- Based on portal technology
- Uses open source software
- Access through PC
- Access through mobile devices

System Design



System Architecture

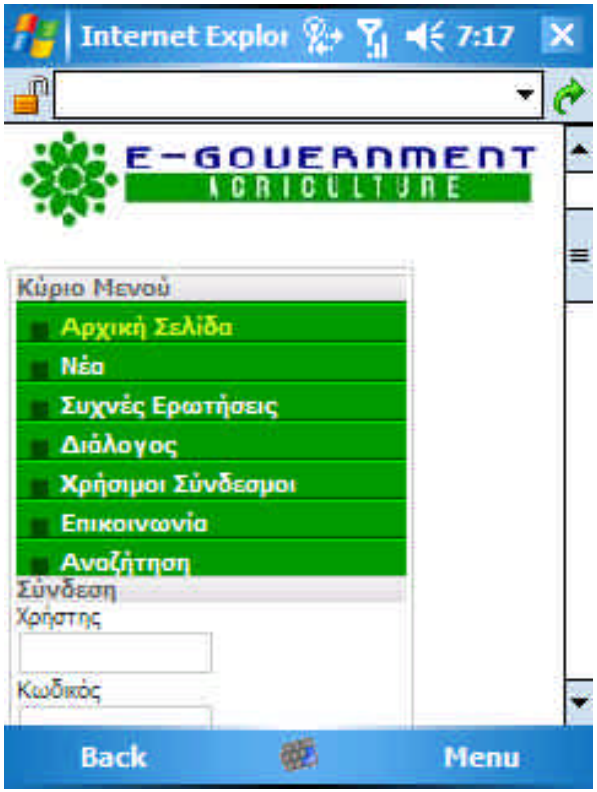


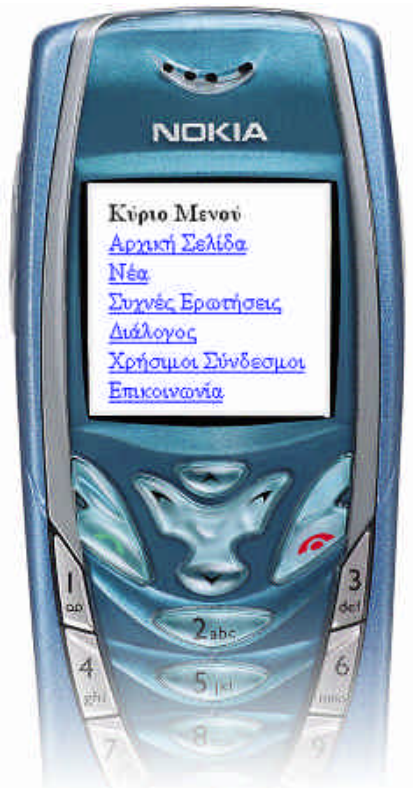
System Deployment

- Pilot implementation
  - **Information Services**
    - News, FAQs, Useful links
  - **Communication Services**
    - Synchronous (e.g. real-time chat) and asynchronous communication methods (e.g. email, forum, private messages)
  - **Government Services**
    - Submission and processing of applications, certificate issuing

System Deployment

PDA





Mobile Phone

System Deployment

http://meli.aua.gr/agroportal

Security Considerations

- Session layer security was preferred
  - Combines application transparency with wireless interface independence
  - Can survive user roaming between different wireless network infrastructures
- Application layer security could be an alternative but
  - Developmental overhead
  - Protects only a specific application

Policies and Guidelines

- SSL/TLS session layer security
- Antivirus and firewall software
- Frequent change of authentication credentials
- Sensitive information in the storage of the device should be encrypted
- Avoid sending authentication details and m-government documents over insecure connections
- Install latest security patches of the operating system
- Empower access control
- Avoid untrusted wireless network access points

Conclusions

- M-Government systems make use of sensitive information
- Mobile networks have been proven to have security vulnerabilities
- Special security considerations when designing, deploying an m-government system
- Policies to increase security awareness and eliminate social engineering attacks

Thank you for your kind attention!