Phishing and Mobile Phones

N. Asokan

Nokia Research Center / Helsinki University of Technology

USEC ‘07 “The Future of Phishing” panel discussion
Summary

Mobile phones ...
... will become phishing targets
... can help protect against phishing
Phishing on phones
Phishing will come to mobile phones

Cellphones becoming pocket-size banks

Access to valuable resources and services

Mobile VPN Access
Traditional social engineering by phone

(Automated) phone call or message

- “Bad things are about to happen to you; please call this premium number”

- No evidence of large scale attacks
SMS Spam, SMS Phishing

Cost of sending as a deterrent will decline
Protecting phone users will be difficult

Limited display capabilities...

Methods based on visual cues may not apply
Protecting phone users will be difficult

Limited input capabilities...

~10 key clicks to security information
Phone as an anti-phishing tool
Relevant features of mobile phones

Trusted path

- User input and output potentially difficult to spoof or intercept

Auxiliary “secure” communication channel

- *Implicit*: SMS, Cellular data
- *Explicit*: GBA (Generic Bootstrapping Architecture) 3GPP/3GPP2 standard
Mobile phone for trusted path

MP-Auth (FC ’07)
- Password entry on mobile device
- Encrypted for the server before leaving device

Personal Transaction Protocol (MeT Forum ‘02)
- Private key operations in mobile device
- Similar to PhoolProof (FC ’06)

No malware on the phone
SMS as secret channel to user

RSA NetCode-SMS, used by NZ/Aus banks

1. payment details
2. payment details
3. PIN, payment details
4. PIN, payment details
5. PIN
6. PIN
7. OK

SMS routing cannot be subverted
SMS messages remain private
No malware on the phone
SMS as authenticated channel from user

1. payment details

2. payment details

3. Nonce

4. payment details

5. OK

6. Nonce

7. OK

Internet

SMS routing cannot be subverted

SMS messages remain private

No malware on the phone
“No malware on the phone”? 

Most phones are (still) closed systems 

Security architectures for phone software platforms exist 

• J2ME security architecture 
• Symbian OS platform security
Symbian OS has platform security

• “Capability”-based security architecture
  • access to critical resources subject to permissions
    • TrustedUI, SWEEvent, MultimediaDD, ..
  • Permissions grants based on code-signing or user approval
  • Untrusted programs have no direct access to display; cannot generate input events
• Each application has a private directory
  • Can be used to store information to personalize UI
“No malware on the phone”: reasonable?

Basic OS protection mechanisms exist

But bugs in privileged software will appear

Secure hardware will help
Summary

Mobile phones ...

... will become phishing targets

... can help protect against phishing
Links

• Personal Transaction Protocol
  http://www.mobiletransaction.org/pdf/R200/specifications/MeT_PTP_v100.pdf

• Generic Bootstrapping Architecture

• Symbian OS Platform Security
  http://forum.nokia.com/main/platforms/s60/security.html