gemalto

Re-Trust meeting - Session 3

d'Annoville Jerome
Project Manager

12/20/06

Session3 - Generic Applications

Generic Applications: Criteria

- Critical
  - High value data
  - Data corruption/damage/loss cost must justify the checking penalty
- Client/server
  - Induced by the initial project architecture
- Client size
  - Avoid light-weight client
- Security
  - Sensitive data, secret, authorized access

Generic Applications: Criteria (2)

- Availability of open-source code
- PC / specific platform
- End-user attitude
  - Data to protect (!= DRM)
  - Accept control penalty
- Attack types
- Emerging
  - New security requirements

Application segments

- Mobility / Internet / Media
- Secure transaction
- Identity
- Network Security / Access Management

Generic classes of applications
Early list

- Ecommerce
- Banking
- Loyalty
- *Virtual Citizen*
- Virtual Casino
- GSM
- Transport
- *Healthcare, medical privacy*
- VoIP
- DRM
- Pay-TV
- Electronic signature
- Electronic Voting
- Governmental Records
- Medical profile access
- Tax return notification

Generic classes of applications
Augmented list

- E-commerce
- E-Banking
- Loyalty
- Virtual Citizen
- Virtual Casino
- GSM
- Transport
- Heathcare, medical privacy
- VoIP
- DRM
- Pay-TV
- Grid Computing
- Distributed firewalling/application firewalling
- Trusted TCP/IP stack
- Electronic signature
- Electronic Voting
- Governmental Records
- Medical profile access
- Tax return notification
- Collaboration tools
- Roaming authentication
- Mobile agents
- Logging
- Chatserver
- OS Security / OS update

Identity Applications

- Virtual Citizen
- Transport
- Healthcare, medical privacy
- Electronic signature
- Electronic Voting
- Governmental Records
- Medical profile access
- Tax return notification

Identity Applications

- Virtual Citizen
  - Broad term, overlap
- Transport
  - No terminal, handset
- Healthcare, medical privacy
  - Country specific
- Medical profile access
- Electronic signature
  - Standards
- Electronic Voting
- Governmental Records
  - Light-weight client
- Tax return notification
  - Cf. signature

Secure transaction

- E-commerce
- E-Banking
- Loyalty

Secure transaction

- E-commerce
  - SSL
- E-Banking
- Loyalty

Mobility / Internet / Media

- Virtual Casino
- GSM
- VoIP
- DRM
- Pay-TV

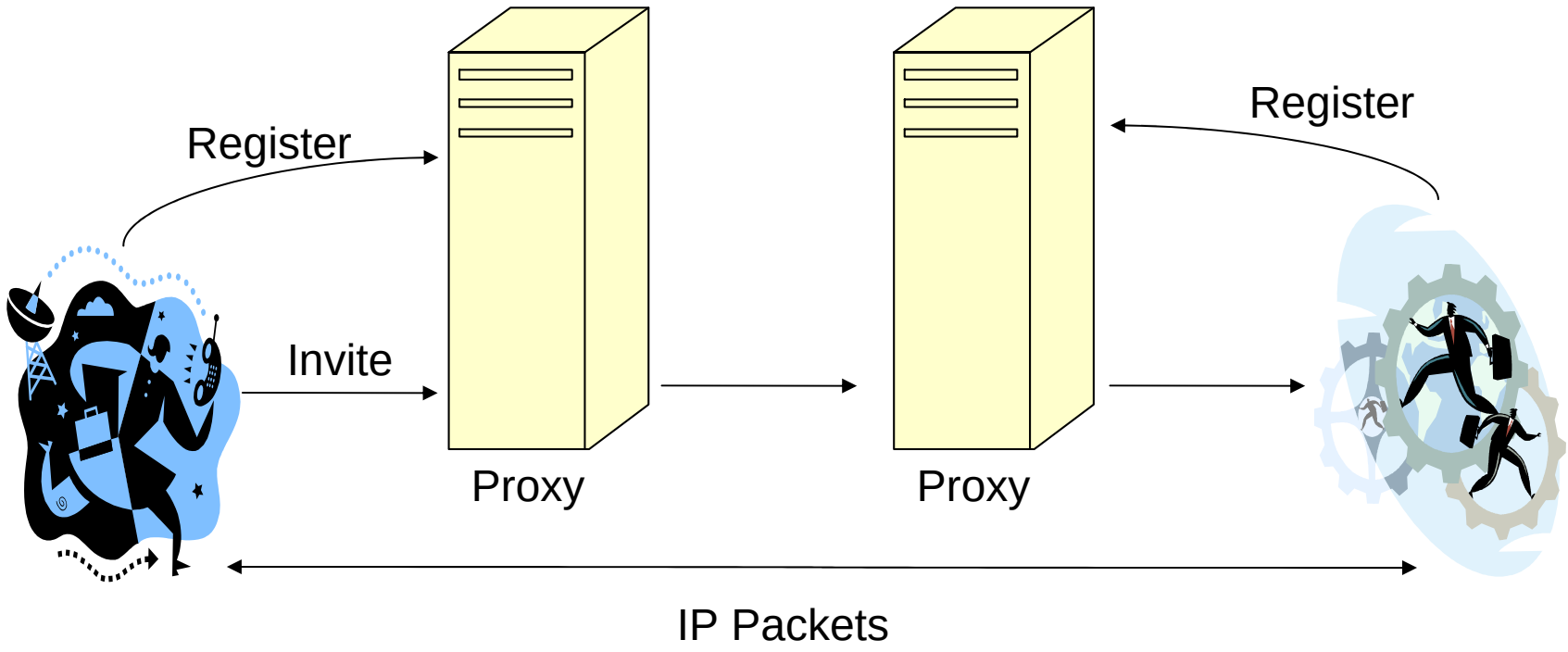
Mobility / Internet / Media

- Virtual Casino
- GSM
  - Handset
- VoIP
- DRM
  - TPM
- Pay-TV
  - Set top box

Network Security / Access Management

- Grid Computing
- Distributed firewalling/application firewalling
- Trusted TCP/IP stack
- Collaboration tools
- Roaming authentication
- Mobile agents
- Logging
- Chatserver
- OS Security / OS update

VoIP



VoIP - security

- Many possible attacks
- Authentication, integrity, privacy
- Physical layer: wifi (802.11)
- DNS service
- VoIP accessed through the network

« The more serious of the two bugs is a boundary error that exists when Skype-specific URI types like "callto://" and "skype://" are handled by the application.
This can be exploited to cause a buffer overflow and allows arbitrary code execution, according to an alert posted on the Skype Security Center »