

# **SOUPS Research from 2005-2009**

1. Access control
  - 1.1. Access control system adoption
  - 1.2. Access control policies
  - 1.3. Access control use by users
  - 1.4. Grid computing
  - 1.5. Information visualization
  - 1.6. Role-based access
  - 1.7. Secure group communication
  - 1.8. Setting XP file permissions
  - 1.9. Smartphone
  - 1.10. Usability
  - 1.11. Usage control and Electronic collaboration
  
2. Authentication
  - 2.1. Air traffic control systems
  - 2.2. CAPTCHA
    - 2.2.1. Video CAPTCHA
  - 2.3. Challenge questions
  - 2.4. On-screen keypad
  - 2.5. Passwords
    - 2.5.1. Alphanumeric passwords
    - 2.5.2. Eye tracking authentication
    - 2.5.3. Graphical authentication
    - 2.5.4. Password management
  - 2.6. Persona information
  - 2.7. Personal RFID tags
  - 2.8. PINs
  - 2.9. Untrustworthy environments
  
3. Biometrics
  - 3.1. Fingerprint biometrics
  
4. Cryptography
  - 4.1. Randomness generation
  - 4.2. Threshold cryptography
  - 4.3. Future decryption

5. Electronic consent and EULAs
  - 5.1. Augmenting information to understand EULAs
6. Email
  - 6.1. Attachment protection
  - 6.2. Encryption and secure email
  - 6.3. Preventing misdirected email
7. Federal Employee Personal Identity Verification (PIV) Program
  - 7.1. Threat analysis
8. Health care data
  - 8.1. Deidentifying sensitive patient data
  - 8.2. Authentication
9. Identity Management
  - 9.1. Privacy-enhanced identity management
  - 9.2. User-centered design of Identity Management Systems
10. Information Assurance
  - 10.1. Information Assurance education
11. Information disclosure
  - 11.1. Web-based information disclosure
12. Information visualization
  - 12.1. Attacking information visualization systems
13. Instant Messaging
  - 13.1. Off-the-record Messaging (OTR)
14. Intrusion Detection System
  - 14.1. Using Intrusion Detection Systems
15. Patterns
  - 15.1. Security patterns

## 16. Phishing protection

- 16.1. Anti-phishing browser enhancements
- 16.2. Anti-phishing technology
- 16.3. Anti-phishing training
- 16.4. Anti-phishing UI
- 16.5. Susceptibility

## 17. Privacy policies

- 17.1. Natural language parsing
- 17.2. Natural language policy authoring
- 17.3. P3P-enabled search engine
- 17.4. Privacy label
- 17.5. Privacy management workbench
- 17.6. Trust
- 17.7. User comprehension
- 17.8. User perception

## 18. Privacy

- 18.1. Desktop
- 18.2. Location sharing apps and privacy
- 18.3. Mobile apps
- 18.4. Online data practices
- 18.5. Online privacy
- 18.6. Online search
- 18.7. Privacy concerns
- 18.8. Privacy loss and protection
- 18.9. Privacy threats
- 18.10. Public spaces
- 18.11. Social network privacy
- 18.12. Social inferences
- 18.13. Vote verification

## 19.Security

19.1.Accessibility

19.2.Computer security

19.2.1.Desktop applications

19.2.2.Home computers

19.2.3.Laptop security

19.2.4.Personal firewalls

19.2.5.Security decision making

19.3.Context-sensitive guidance (CSG)

19.3.1.Security decisions

19.4.Home security

19.4.1.Home monitoring system

19.5.Internet Security

19.5.1.Darknets (friend-to-friend networks)

19.5.2.Unicode

19.6.IT security

19.6.1.Experience with IT security

19.6.2.Security administrators

19.7.Mobile environment

19.7.1.Software security

19.8.Security incidents

19.9.Security threats

19.10.Security visualization

19.11.Usability

19.12.Web security

19.12.1.Anonymous web browsing

19.12.2.Security design flaws

19.12.3.Web browser security

## 20.Sensitive content in texts

20.1.Sanitization

## 21.Spyware and viruses

21.1.Spyware protection

21.2.Virus protection

## 22.Trust

22.1.Browsers and trust

22.2.Collaborative environment

## 23. Ubiquitous and pervasive computing

23.1. Communication appliance

23.2. Device pairing

23.3. Home networks

23.4. Mobile coordination tool

23.5. Power-line communications