Effortless Secure Wireless Enrollment

Jeff Shirley
David Evans
University of Virginia
14th USENIX Security Symposium
Solving the Enrollment Problem

- Mutual authentication between network and wireless client during enrollment
  - Enrolling temporary users
  - Visitors
- How to verify that the enrollee is the newly authorized user?
- How to verify that the wireless network is the trusted network?
Location-Limited Channels

- USB, Audio [Balfanz+, NDSS 2002]
- Visual [McCune+, Oakland 2005]
- Audio tones
  - Human evident, relatively limited range
  - Available on a wide variety of devices (laptops, PDAs, cellphones, etc.)
- Network limits enrollment to clients physically present at specific location
  - Clients connect only to network verified through the same channel
Enrollment Protocol

- Authorized user acts as intermediary
- Audio challenge-response protocol
Current Status

- Working implementation: enroll on our network!
- Distributing client software securely
  - Signed Java applet available from insecure network
- Ensuring interoperability with existing systems
  - Initial implementation of the protocol enrolls users for standard EAP-TLS authentication
- Tradeoff between reliability of audio channel and transmission speed (4 bits per second)
Questions?

Email: jshirley@cs.virginia.edu