# KERBEROS for MOBILE DEVICES

Zhanna Tsitkova
MIT Kerberos Consortium
November 3, 2008

Kerberos consortium
www.kerberos.org

# Constraints to Address

- Battery
- Limited memory
- Limited CPU
- Network bandwidth
- High packet loss
- High latency
- Signal strength

# Reduce memory footprint

## Lite Client – 450 K

### Was achieved

- Dead-code stripping at the link time
- Server code stripping
- Disabled PKINIT
- Disabled replay cache
- Error code strings
- MAC OS X

### Next step

- Investigate dead-code stripping on other plats
- ASN.1 disk footprint reduction

# Future Work

Reduce CPU

- Use native crypto libraries
- Optimize ASN.1

Use caching to reduce DNS traffic

Have local KDC perform cross-realm authentication

- Yokogawa Electric proposal to IETF

Improve in high-latency high-packet-loss env.

# Credential Management

## PKINIT

- Public key infrastructure
  is favored by US government
- Passwords
  typing is challenging
- Hardware accelerators
  rely on vendor's implementation

# Outreach

- Apple
- Google
- Intel
- Nokia
- Yokogawa Electrical

- MIT
- Other universities / Research labs