

Greenpass: Decentralized, PKI-Based Authorization for Wireless LANs

*Nicholas C. Goffee, Sung Hoon Kim, Sean Smith,
Punch Taylor, Meiyuan Zhao, John Marchesini*

**Department of Computer Science
Dartmouth College**

April 12, 2004



Motivation

Our wireless security goals

- Allow *internal* access by *authorized guests*
- Without requiring custom client software

Our PKI goals

- Move away from *centralized, name-based hierarchies*
- Accommodate *real-world trust flow*

This talk

Background

- The WPA wireless authentication standard
- Current approaches to authorization and guest access

Decentralized guest authorization

- Authorization certificates
- Modified authentication/authorization server

Delegation process

- Guest introduction
- Delegator tool
- Decentralization

Next steps

WPA authorization and guest access

WPA itself doesn't specify an authorization procedure

Centralized schemes *without* guest access

- Allow all users certified by the “right” CA
- Authenticate, then consult ACL

Centralized schemes *with* guest access

- Trust multiple CAs (with or without ACL)
- Allow unauthenticated users/guests ***outside*** the firewall

Decentralized authorization

A SPKI/SDSI authorization certificate

- Binds *authorization* → *public key**
- Can optionally allow *delegation*
- Delegation allows decentralized guest authorization

Example SPKI/SDSI certificate (unsigned)

```
(cert
  (issuer (hash md5 |BuFWyi13EpqzJtMff8DcsA==|))
  (subject (hash md5 |9WgBTLBGk6kIIvJVwZLbAg==|))
  (propagate)
  (tag (greenpass-pilot-auth))
  (valid (not-after "2004-07-02_17:43:06")))
```

WLAN authorization with SPKI/SDSI (ideal)

- User presents credential (cert) to AP
- Unfortunately, standard client software doesn't support this

Authentication/authorization procedure

RADIUS server

- Modified to look up SPKI/SDSI chain for guests

Local users

- X.509 certificates signed by local CA
- Standard EAP-TLS handshake will succeed

Guests

- RADIUS server uses EAP-TLS to extract public key
- Doesn't recognize issuer CA in guest's X.509 certificate
- Checks **certificate store** for relevant SPKI/SDSI chain
- Authorized guests get access
- Unauthorized guests are put on **restricted VLAN**

Delegation process

Guest introduces public key to delegator

- Guest connects to Web server on restricted VLAN
- Web server gets (or generates) guest's X.509 certificate
- Web server displays guest's *visual fingerprint*

Delegator signs new authorization certificate

- Delegator connects to same Web server
- Uses visual fingerprint to verify guest's identity
- Delegator generates and signs new SPKI/SDSI certificate
- Delegator signature generated by *trusted Java applet*
- Sends fresh certificate to certificate store

Greenpass: guest introduction

https://drwatson.dartmouth.edu/Greenpass/cgi- Google

Greenpass guest introduction

Thank you for introducing yourself. Your **subject ID number** is **3707**; please give this number to your delegator. Your delegator will also ask to see the **visual fingerprint** displayed below in order to verify your identity.



After your delegator has signed an **authorization certificate** granting you access to our network, you should click on the **Continue** button to install it in your web browser.*

*Your authorization certificate will be stored as a cookie within your Web browser.

[Start over](#) [Advanced](#) [Continue](#)

Greenpass delegation tool

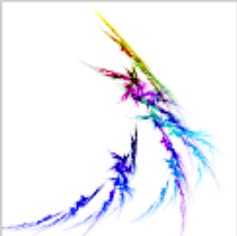

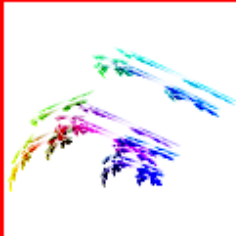
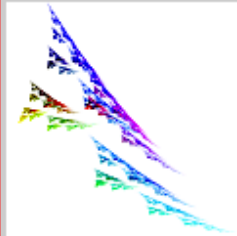
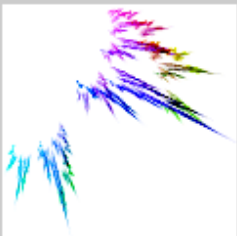
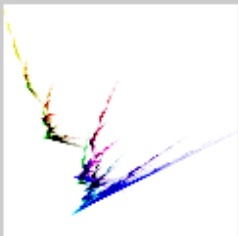
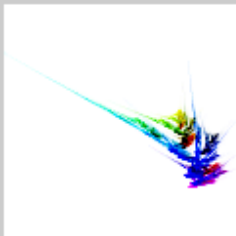
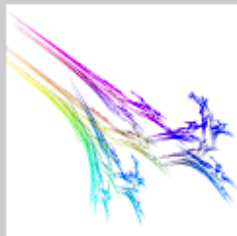
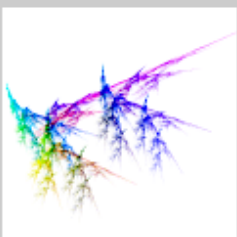
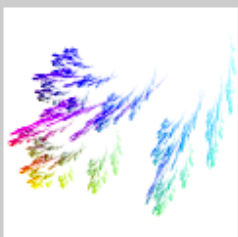
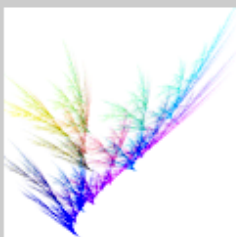
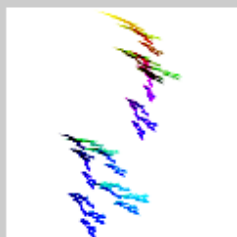
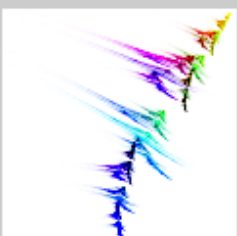
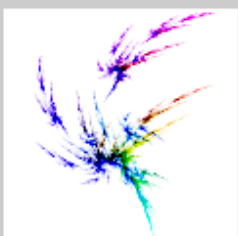
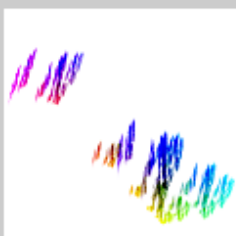
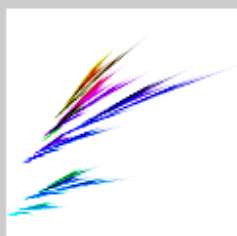
Java Applet Window

Delegation options

Valid for 2 Days

Propagate

To verify that you delegate to the correct person, please choose the visual fingerprint below that matches the fingerprint shown on your guest's screen.

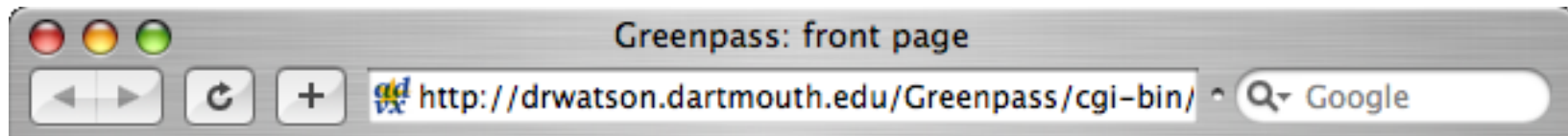
			
			
			
			

Help... Cancel Delegate!

Decentralization

Certificate store has become a short-term certificate cache

- After delegation, guest can pick up certificate chain
- Chain gets stored as a cookie on guest's machine
- Guest can use chain to reauthorize without introduction process



Greenpass front page

Your status is: REAUTHORIZED_USER

Next steps

Take off the duct tape

- Decentralize certs by using HTTP cookies (**done**)
- Move to router that can handle VLAN trunking
- Test various OS/wireless card configurations
- Move from FreeRADIUS to Cisco ACS

Try it in the real world

- Is SPKI/SDSI sufficiently expressive?
- What about SAML or PERMIS or proxy certificates or...?
- What about revocation?*

Next steps (cont'd)

Apply our tools to other settings

- VPN
- Application-level resources
- Location-sensitive policy

Try other PKI models

- Move the hybrid X.509/SPKI boundary
- No X.509 at all
- Cross-domain

Acknowledgments

Funding:

- Cisco Corporation
- Mellon Foundation
- National Science Foundation
- AT&T/Internet2
- Department of Homeland Security

Collaborators:

- Dr. Sean Smith (advisor)
- Sung Hoon Kim (RADIUS code)
- Kimmy Powell (testing, pilot)
- Meiyuan Zhao (SPKI/SDSI libraries)
- Kwang-Hyun Baek (wireless security details)
- Punch Taylor (network configuration)
- John Marchesini (black hat)