Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption
Identity on the Internet

Identifies it is trusted (Digital Certificate)

Keeps communications secure (encryption)

Bob

Eve
Authentication (Device, User, Servers, Connections, etc)

Confidentiality (Encryption)

Assurance (Integrity)

Fundamental principles
How do we know that it was really Bob who sent the data, as anyone can get Alice’s public key, and thus pretend to be Bob?
How can we tell that the message has not been tampered with?
How does Bob distribute his public key to Alice, without having to post it onto a Web site or for Bob to be on-line when Alice reads the message?
Who can we *really* trust to properly authenticate Bob? Obviously we can’t trust Bob to authenticate that he really is Bob.
Chapter 6: Digital Certificates

Introduction
Authentication Methods

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption
What to authenticate?

- Systems
- Users
- Data
- Servers

Hello. How are you? Is this okay?

Users

Devices

Data

Systems

Author: Prof Bill Buchanan
Authentication Methods

End-to-end authentication

Intermediate authentication

Where authenticated?
End-to-end. User to service. Intermediate. Part of the authentication process.
One-way server authentication. Server provides authentication to the client, such as SSL (HTTPS, FTPS, etc).

One-way client authentication. Client provides authentication to the server such as EAP-TLS in Wireless.

Mutual authentication. Client and server provide ID to authenticate each other. Examples include PEAP in wireless.
Authentication methods

- Something you have
- Something you know
- Something you are

Methods

- Iris scans
- Retina scan
- Palm prints
- Finger prints

Something you are

- Username/password
- Mother’s maiden name

Something you have

- Digital certificate
- Network/physical address
- Smart card

Something you know
Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption
How does Bob distribute his public key to Alice, without having to post it onto a Web site or for Bob to be on-line when Alice reads the message?

One method is the digital certificate which can carry the public key (and also the private key, if nesc.)

Digital certificates are a soft token of authentication, and require a trust mechanism.

Now that we need the public key to either encrypt data for a recipient, or to authenticate a sender...
Digital certificates should only be distributed with the public key.
The main certificate formats include:
- P7b. Text format
- PFX/P12. Binary
- SST. Binary

Digital certificates should only be distributed with the public key.
A. Bob creates the message.
B. Bob encrypts with Alice’s public key and sends Alice the encrypted message
C. Alice decrypts with her private key
D. Alice receives the message

Hello

H&$d.

Hello

Alice sends her digital certificate with her public key on it

Eve

Bob

Alice

Author: Prof Bill Buchanan
Bob sends his Digital certificate to authenticate himself

Bob’s private key

Encryption/Decryption

Communications Channel

Encryption/Decryption

Hello

Hash

H&$d.

Alice’s private key

Alice checks the hash using Bob’s public key from his certificate

Hash

Digital Cert.

Authentication

Author: Prof Bill Buchanan
Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption
Who do we trust to get Bob’s certificate … we can’t trust Bob, as he may be Eve… meet Trent.

Who can we trust to get the digital certificate from?
The Trusted Root CE (Trent) checks Bob’s identity and creates a certificate which he signs.

Certificate Authority (CA)
- Able to grant certificates
  Examples: Verisign, Entrust, Microsoft Trust.

Trusted root certificates are installed as a default on the machine (or installed with the user’s permission).

Alice checks the signature of the certificate to validate Bob. Both Alice and Bob trust the CA (Trent) as a third party.
Eve tricks the CA to get a certificate with Bob’s name.

Alice checks the signature of the certificate to validate Bob. Both Alice and Bob trust the CA (Trent) as a third party.

Trusted Root CA
Certificate Authority (CA)
- Able to grant certificates
Examples: Verisign, Entrust, Microsoft Trust.

Trusted root certificates are installed as a default on the machine (or installed with the user’s permission).

Eve

Alice

Author: Prof Bill Buchanan

Drawbacks of PKI
The Trusted Root CA:
- Secure email.
- Server authentication.
- Code signing.
- Driver authentication.
- Time stamping.
- Client authentication.
- IP tunnelling.
- EFS (Encrypted File System).

Levels of trust:
- Trusted Root CA - always trusted
- Intermediate CA - Can be trusted for some things
- Self signed - Can never be trusted
The two main problems with digital certificates are:

- Lack of understanding of how they work.
- They can be spoofed.

So let’s look at a few … are they real or fake?
Real or fake?

PKI

Humor12.com

Certificate

Certificate Information

This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: signin.ebay.com

Issued by: VeriSign Class 3 Extended Validation SSL CA

Valid from 25/01/2007 to 25/01/2009

Learn more about certificates

Install Certificate... Issuer Statement

OK
When authenticating:

- P rof B ill B uchanan

**VeriSign Relying Party Agreement**

YOU MUST READ THIS RELYING PARTY AGREEMENT ("AGREEMENT") BEFORE VALID CERTIFICATE, USING VERSIONS ONLINE CERTIFICATE STATUS PROTOCOL ("O CSP") OR USING A VERSION OR VERSION AFFILIATE DATABASE OF CERTIFICATE REVOCATION ANY VERISIGN CERTIFICATE-RELATED INFORMATION COLLECTIVELY. VERISIGN IF NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT SUBMIT A QUERY AND DO NOT RELY ANY VERSION INFORMATION. IN CONSIDERATION OF YOUR AGREEMENT, YOU ARE ENTITLED TO USE VERSION INFORMATION AS SET FORTH HEREIN.

1. **Term of Agreement.** This Agreement becomes effective when you submit a query Certificate, or rely on any VeriSign Information in the manner set forth in the provisions here shall be applicable for as long as you use and/or rely on such VeriSign Information.

2. **Definitions.**
   - "Certificate" or "Digital Certificate" means a message that, at least, states a name or id identifies the Subscriber, contains the Subscriber’s public key, identifies the Certificate a Certificate serial number, and contains a digital signature of the issuing CA.

**Author:** Prof Bill Buchanan

**Real or fake?**
When: Prof Bill Buchanan

Real or fake?
You are about to install a certificate from a certification authority (CA) claiming to represent:

Amazon eCommerce

Windows cannot validate that the certificate is actually from "Amazon eCommerce". You should confirm its origin by contacting "Amazon eCommerce". The following number will assist you in this process:

Thumbprint (sha1): D0C30E53 98AA68C1 29BA54E3 513920F6 BEE4E388

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk.
If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

**Fake!**
The certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority’s statement for details.

**Certificate Information**

**Issued to:** *.napier.ac.uk

**Issued by:** GlobalSign Domain Validation CA

**Valid from:** 16/05/2008 to 16/05/2013

**Real or fake?**

Author: Prof Bill Buchanan
When authenticating:

- Prof Bill Buchanan

Real or fake?
Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption
Public key encryption … secret … identity … trust
Public key encryption ... secret ... identity ... trust
Public key encryption ... secret ... identity ... trust

Bob’s Private Key

Eve

Trent

MegaCorp

Allice’s Public Key

Alice’s Private Key

Alice’s Public Key

Bob’s Public Key
Public key encryption ... secret ... identity ... trust

Bob’s Private Key

Hello Alice,
Wish you were here!
- Bob

Alice’s Public Key

Alice’s Private Key

Bob’s Public Key

Eve

Trent

MegaCorp

Alice’s Public Key
Public key encryption … secret … identity … trust

Hello Alice,
Wish you were here!
- Bob
Public key encryption … secret … identity … trust

Hello Alice,
Wish you were here!
- Bob

Which key to open the message?

MegaCorp

Bob’s Private Key

Bob’s Public Key

Alice’s Public Key

Alice’s Private Key
Public key encryption ... secret ... identity ... trust

Hello Alice, Wish you were here! - Bob

Which key to open the message?

Bob’s Private Key

Alice’s Private Key

Bob’s Public Key

Alice’s Public Key

Alice’s Private Key

Trent

Eve

MegaCorp

Digital Certificate

Name: Alice
Verified: MegaCorp
Issued: 1 Dec 2013
Valid Until: 1 Jan 2015
Fingerprint: XYZABCD
Trusted For: Email, Web

MegaCorp

Alice

Allice’s Private Key

Alice’s Public Key
Public key encryption … secret … identity … trust

Bob’s Public Key

Bob’s Private Key

Eve

Trent

MegaCorp

Alice’s Public Key

Hello Alice, Wish you were here! - Bob

Which key to we open the signature with?

Alice’s Private Key
Public key encryption ... secret ... identity ... trust

Digital Certificate
Name: Bob
Issued: 1 Nov 2013
Valid From: 1 Jan 2016
Fingerprint: 12345678
Trusted For: Email, Web

Bob's Private Key

Eve

Trent

MegaCorp

Hello Alice,
Wish you were here!
- Bob

Alice's Public Key

Bob’s Public Key

Alice’s Private Key
Public key encryption ... secret ... identity ... trust

Bob’s Private Key

Bob’s Public Key

Alice’s Public Key

Alice’s Private Key

Eve

Trent

Hello Alice, Wish you were here!
- Bob

MegaCorp
Using Bob’s private key to authenticate himself.
Bob encrypts the message/hash with Alice’s public key.
Bob encrypts the message/hash with Alice’s public key.

- Message
- MD5
- Encrypted MD5
- Encrypted Content

Alice decrypts the message using her private key.

Bob's private key
Bob's public key
Alice's public key
Alice's private key
The magic private key

Bob

Bob's private key
Bob's public key

MD5

Encrypted MD5

Message

Encrypted Content

Alice

Alice's public key
Alice's private key

Alice decrypts the message

Author: Prof Bill Buchanan
Alice compares the MD5 values. If they are the same ... Bob sent the message.
Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE
http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption