SWINBURNE UNIVERSITY OF TECHNOLOGY

Cryptography – Public Key Infrastructure

Lecture Twenty-three

Outline of Lecture

- Overview of how PKI can be used for different applications
- Overview of some of the weaknesses of PKI
- Some PKI products and operators

Learning goals

- You should be able to:
  - Explain how PKI can be used with emails, web transactions, VPNs and software downloads
  - Discuss some of the weaknesses of PKI and how they can be managed

Interworking of applications with PKI

- PKI can be used in the following applications
  - Email
  - messaging
  - Web access
  - VPNs
  - Digitally signed codes and files

Using PKI with email

- Sender can use PKI to
  - Digitally sign email messages
  - Encrypt email contents and attachments, protecting them from being read by online intruders
  - Usually integrated into the emailer
- Signing emails
  - email contents is hashed (MD5 or SHA) and
  - Sender uses his / her PRIVATE key to encrypt the message hash
    - The digital signature
- Encrypting emails
  - Sender obtains recipient's certificate
  - Verifies certificate
  - Uses public key contained within the certificate to encrypt the session key used to encrypt the message

Using PKI with email

- Verifying a digital signature
  - Recipient obtains the sender's certificate
  - Verifies certificate
  - Uses the public key contained within the certificate to decrypt the signature and hence the hash that it contains
  - Recipient computes the hash of the message and compares it with that in the signature
  - If the same then the signature is authenticated
- Decrypting emails
  - Recipient uses his/her private key to decrypt the email

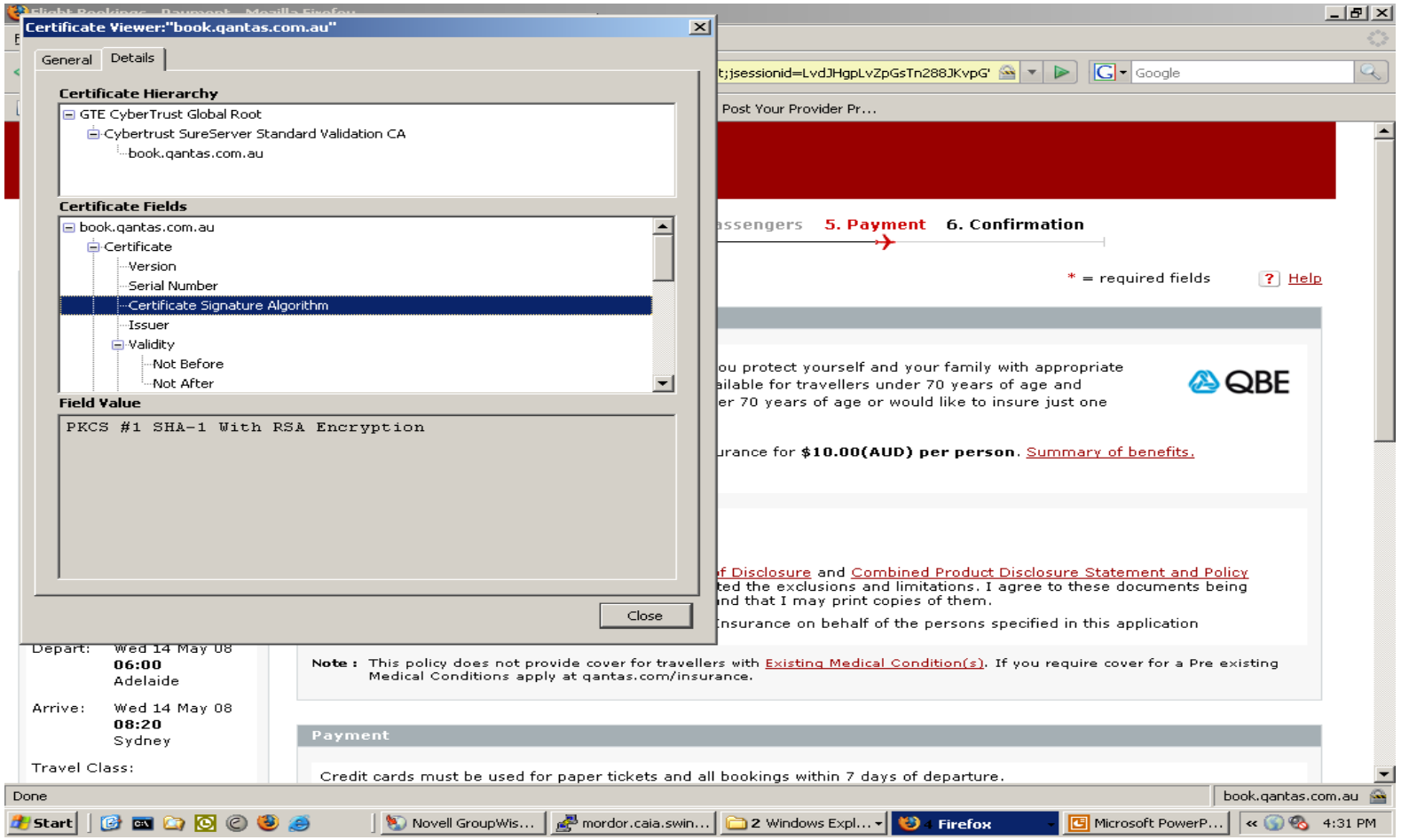
Using PKI with email

- Important issue is distributing digital certificate
- Can usually be done by
  - digitally signing an e-mail message
  - putting digital certificate in an LDAP directory service
  - Essential to verify certificate with the CA
- Private key needed to sign an email or encrypt a message
  - Important to keep private key secret
  - Smart card, USB dongle
  - Putting it on the PC is a bad idea

Using PKI with web transactions

- Server must supply its certificate to the browser
  - contains public key used for establishing secure https tunnel
- Browser verifes the server's certificate
- Server can (optionally) request and (optionally) verify the client's certificate

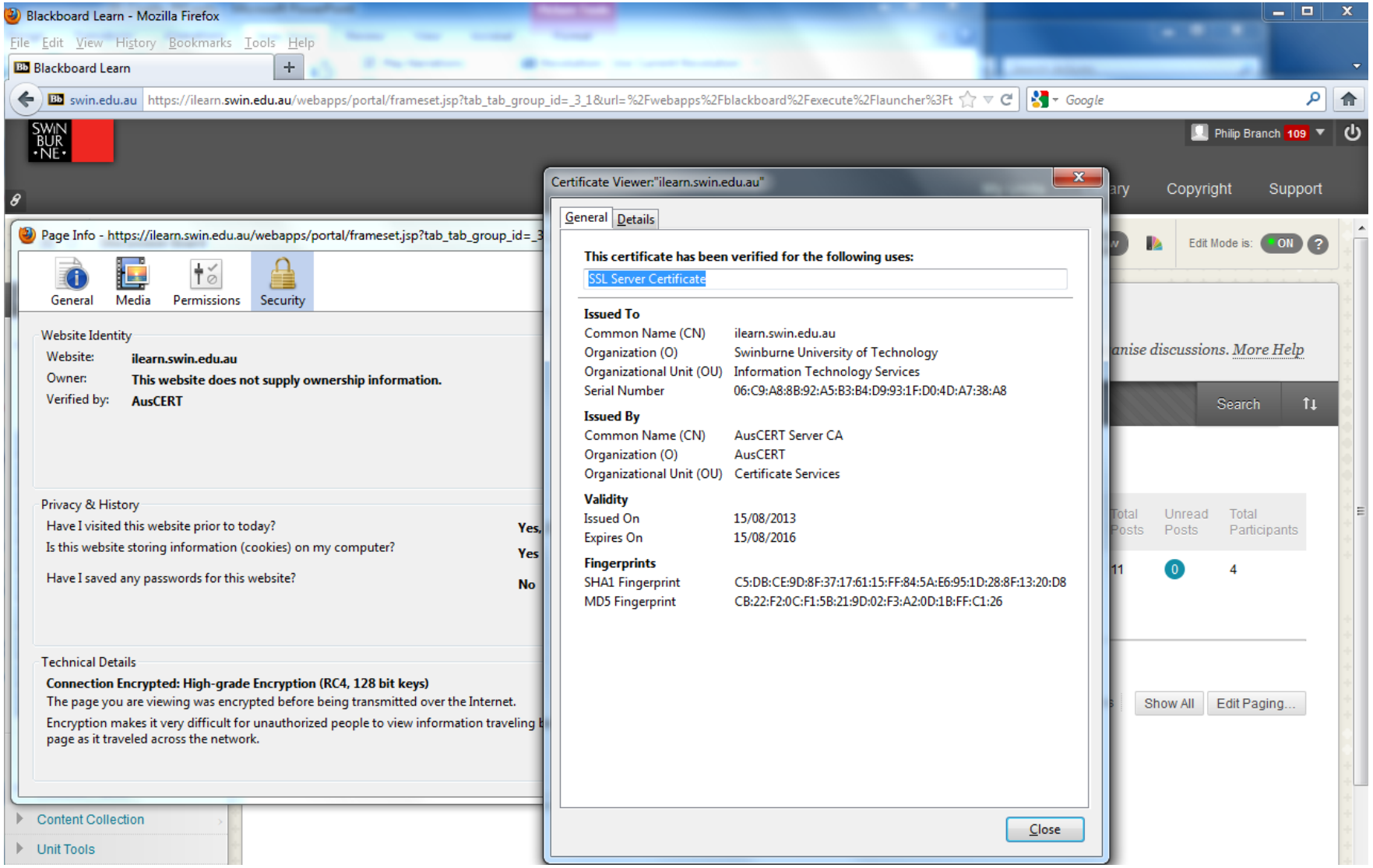
Using PKI with web transactions



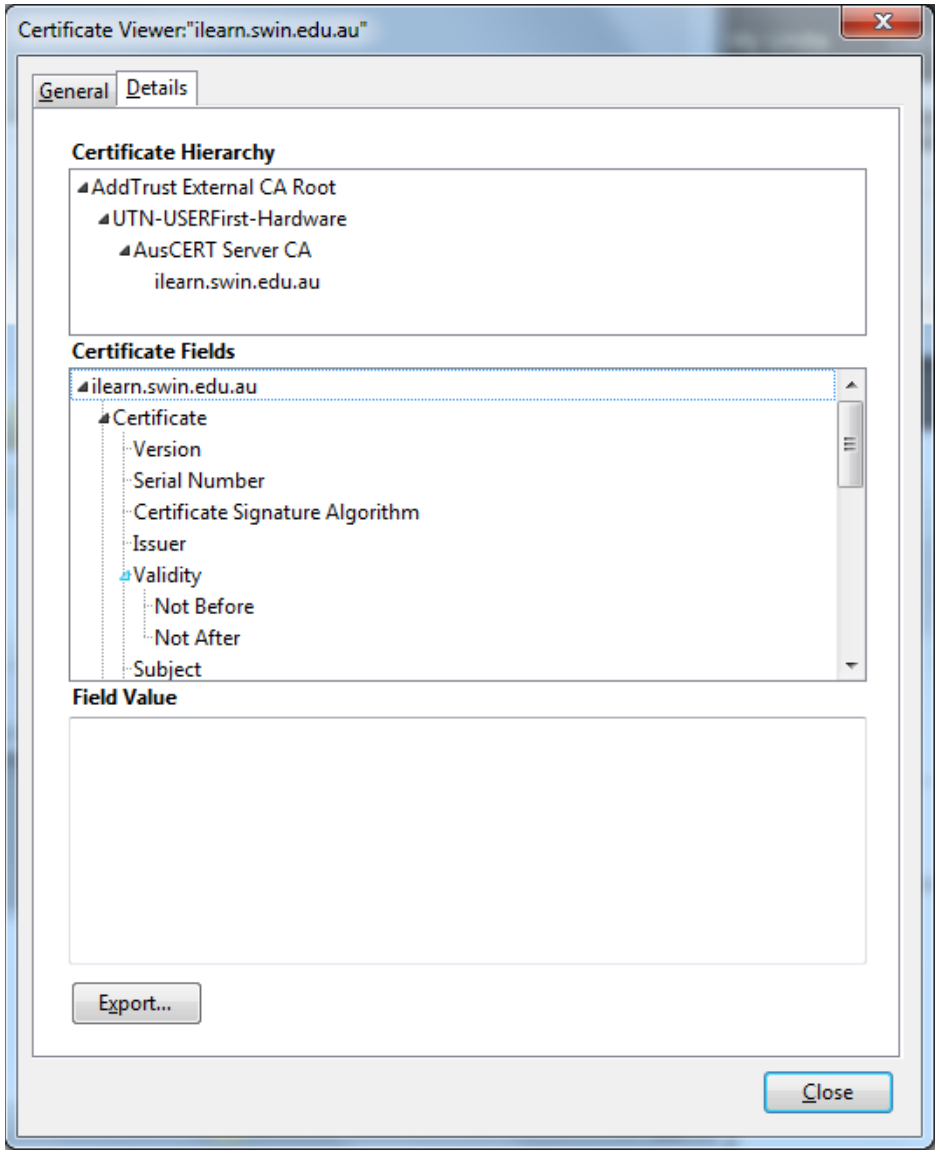
Using PKI with web transactions

- Browser verifies the certificate in the following ways
  - Checks date validity
  - Checks certification path to see that it terminates in a trusted root or intermediate certification authority
  - Optionally checks for certificate revocation

Using PKI with web transactions



Using PKI with web transactions



Question

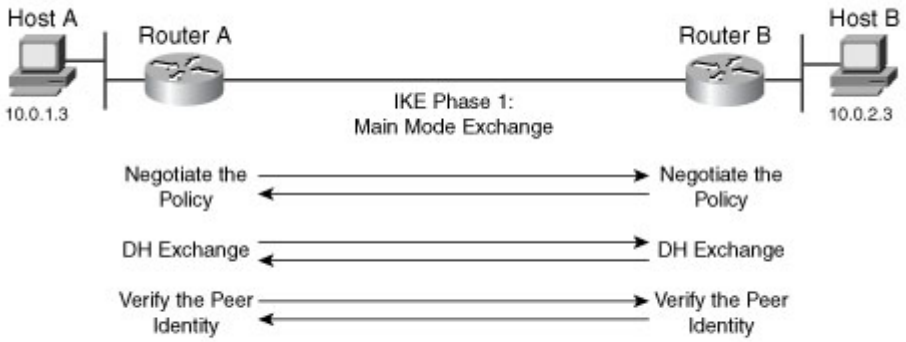
- Why when we are using sites such as Amazon.com or Qantas.com is it unnecessary for the browser to send a certificate to the server?
- Under what circumstances might it be necessary for the browser to have a certificate?

Using PKI in VPNs

- Used in Internet Key Exchange to authenticate public keys
- Certificate used to exchange public keys
- Can optionally include a certificate authentication step
- Certificate will usually be issued by whoever controls the VPN
  - Their certificate will, in turn, be signed by a root certificate authority
  - Baltimore Consulting particularly strong in this area

Using PKI in IPSec

- In IKE phase 1 (main mode exchange) there is a peer identify verification exchange
  - This can be done using pre-shared key or digital certificates
  - The certificates are often issued by a CA installed on a local router
  - (from http://ptgmedia.pearsoncmg.com/images/chap01_1587051451/elementLinks/fig22.jpg)



Using PKI to digitally sign code and files

- Often wish to load new files from the web or a local server
- How do you know that they have not been tampered with
  - may contain viruses or trojans
- Can have the code digitally signed to ensure that it hasn't been changed between production and loading on the server
- Process is to hash the file using SHA-1 or MD5
- Use a private key to sign the hash
- When the user downloads the file they
  - calculate the hash of the file
  - use the code producer's digital signature to verify their public key
  - use the public key to decode the encoded hash value
  - compare the decoded hash with the calculated hash

Ten risks of PKI

- Ellison and Schneier have identified some significant concerns with PKI. Ellison, C., Schneier, B., “Ten Risks of PKI: What you’re not being told about Public Key Infrastructure”, Computer Security Journal, Vol 26, No1, 2000
  - Who do we trust, and for what?
  - Who is using my key?
  - How secure is the verifying computer?
  - How effective is linking of identity to a public key?
  - Is the CA an authority on the contents of the certificate?
  - Is the user part of the security design?
  - Was it one CA or a CA plus an RA?
  - How did the CA identify the certificate holder?
  - How secure are the certificate practices?
  - Why use the CA process anyway?

Who do we trust, and for what?

- In particular can we trust the CA and what do we trust them to do?
  - CAs are not government bodies, they are commercial entities
  - How do we know they are properly audited?
  - How do we know they have good security procedures?
- We know that some do have good procedures and are well run. Those listed in the browser should be accredited
- The browser software will always alert the user if it encounters a certificate that it does not have the root certificate of

Who is using my private key?

- Who has access to my private key? How do I know it is safe?
  - It is usually located on a private computer where it can be subjected to attacks by viruses and other malicious software
  - How do I know it hasn't been hacked after hours?
  - If it's protected by a password, how hard is the password to guess?
- A very serious issue
  - Some US digital signature laws (Utah, Washington) make the owner of the key responsible for anything done with it
  - If you own a key that is stolen and used to defraud someone then you are in trouble
- Requires good practices such as strong passwords or restricting private keys to hardware tokens such as USB dongles or smart cards

How secure is the verifying computer?

- How secure is the verifying computer, the one using the public key?
  - It uses the “root” public keys in the browser to verify certificates
  - If an attacker can insert his/her root key in your browser you will accept certificates from that CA in exactly the same way as certificates from legitimate CAs
- Again, no real solution other than good business practices

How effective is linking of identity to a public key?

- Purpose of a certificate is to associate a public key with a name
  - What about when that name is a person's name? How do you know that the "John Robinson" in the certificate is the "John Robinson" you know?
- There needs to be levels of trust placed in digital certificates
  - eg Verisign has three levels of trust
    - Highest level involves multiple authentication
    - Lowest level is just your email
- Need to know what the level of trust is of the certificate

Is the CA an authority on the contents of the certificate?

- Certificates are used to link public keys to DNS names, business names and email addresses
  - Do the CAs have the expertise to check the validity of a particular application for a certificate that links a name to a key?
- Reputable CAs have Registration Authorities do this work
- The RA is an expert in validating the name to be linked to the key
- Typically the RA will be an organisation that operates in the state or country the certificate is to be issued while the CA may be an international organisation

Is the user part of the security design?

- Does the user get to check whether or not the certificate is legitimate?
  - Most serious issue here is where organisations make use of web hosting and use the web host's certificate rather than their own
- A matter of education
  - Web host companies should not allow hosted organisations to use their certificate
  - Users should always check the digital certificate before entering sensitive data into an https page

Was it one CA or a CA plus an RA?

- RA / CA model overcomes difficulty of CA not knowing enough to link name to key, but introduces additional weaknesses
  - The RA might be compromised
    - criminal, incompetent
  - There is the risk of man-in-the-middle attacks between the CA and RA
- Again no good answer other than good security policy and procedures by both the CA and RA, including frequent audits

How did the CA or RA identify the certificate holder?

- Even if the name is legitimate how does the CA know they are signing a certificate for the person or organisation that owns that name?
  - Process is usually
    - Someone emails the RA wanting bhp.com
    - The RA queries Dun and Bradstreet and finds that BHP is a legitimate business name
    - How does the RA know that the person emailing them was from BHP?
- Again, registration procedures need to be very tight. Should include some out-of-band communication initiated by the RA
  - a phone call using a number obtained from a public phone directory

How secure are certificate practices?

- Can the certificate be stolen? Can the certificate be revoked and can the revocation be recognised by the user?
- Lots of issues
  - Accessing updated CRLs
  - lifetime of certificates
  - Theft of certificates
    - procedures and informing users

Why use the CA process anyway?

- Main point of Ellison and Schneier's criticism is that PKI is being touted as a total security solution
- All PKI does is attempt to link identity to a public key
  - Not a solution to every security issue
  - Lots of questions on how well identity is linked to the key
- PKI is just one building block in making an organisation secure
- Like all the other building blocks it needs to be used with an understanding of the associated risk and how it can be used to achieve the organisation's security goals
  - Gets back to security policy

PKI deployment issues

- Need to include some discussion of PKI in the security policy
  - Will PKI be used to verify identity?
  - What systems?
  - How will interoperability be achieved?
  - Are our applications able to use PKI?
  - Are our staff able to implement and use PKI?
  - Have we developed protection against PKI attacks?

PKI products

- PKI toolkits
  - RSA, Entrust, Windows
- Certificate authorities for private certificates
  - Used by organisations to validate users accessing their services
    - banks, government departments
  - Baltimore, eSign
- Certificate authorities for public certificates
  - Used by organisations to allow users to purchase goods via their websites
    - Verisign

Conclusion

- Overview of how PKI can be used for different applications
- Overview of some of the weaknesses of PKI
- Some PKI products and operators