Content control & policy based encryption

Policy based encryption

- The Policy Based Encryption (PBE) service encrypts specific emails based on a policy
- i.e. a set of rules -
  - analyzes all email, and
  - encrypt any email that matches the pre-defined conditions
- Policy Based Encryption uses the Email Content Control rules to identify which email needs to be encrypted

Policy based encryption contd…

- The Policy Based Encryption Service is managed through the same control panel that is used to manage Anti-virus and Anti-spam settings

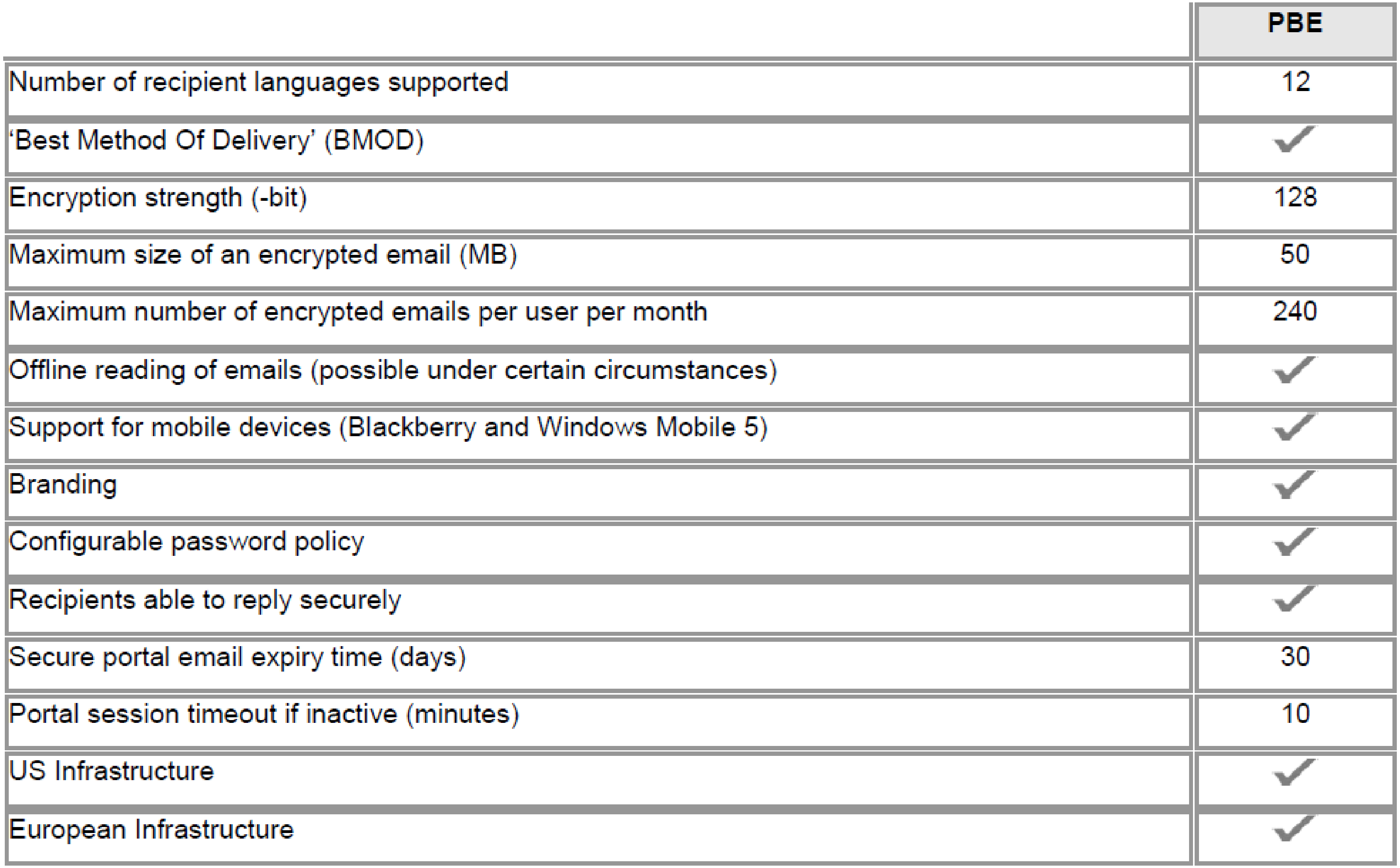
Policy Based Encryption and Email Content Control

- The Policy Based Encryption service is closely integrated with the Email Content Control service
- The rule that defines whether an email is to be encrypted is set up in the Email Content Control configuration screens in the Boundary Defense for Email Control Panel
- The encryption rule has an action to redirect any emails that meet the rules conditions to a specified encryption email address

Policy Based Encryption and Email Content Control contd…

- This email address will be sent to the administrator when the service is purchased
- This email address is used solely to process and encrypt the email

Feature summary - Example



	PBE
Number of recipient languages supported	12
‘Best Method Of Delivery’ (BMOD)	✓
Encryption strength (-bit)	128
Maximum size of an encrypted email (MB)	50
Maximum number of encrypted emails per user per month	240
Offline reading of emails (possible under certain circumstances)	✓
Support for mobile devices (Blackberry and Windows Mobile 5)	✓
Branding	✓
Configurable password policy	✓
Recipients able to reply securely	✓
Secure portal email expiry time (days)	30
Portal session timeout if inactive (minutes)	10
US Infrastructure	✓
European Infrastructure	✓

Creating an Encryption Group

- Prior to creating any encryption rules, an encryption group must be created
- This group needs to be added to each rule, as an exception in order for the mail to be forwarded to the Policy Based Encryption Gateway

Defining an Encryption Rule

- To trigger mail to be encrypted, an Email Content Control rule must be configured with an action to redirect the mail to the specified email address for the service you are using
- A rule is defined to include the specific conditions to cause email to be encrypted,
- for example, specific words contained in the header or body of the email

Defining an Encryption Rule contd…

- The Email Content Control service scans email against the rules in the order they are listed in the Control Panel portal
- If an email triggers a rule with an exit action, it is subject to that action and does not pass on to be scanned for further rules
- The redirection action for rules is an exit action
- So it is important to put encryption rules towards the bottom of the rule set, so that other rules defined to comply with the organization's acceptable usage policy are acted on first

Defining an Encryption Rule contd…

- **NOTE: If an email triggers a rule with an exit action, such as a block action higher in the rule set, the** email will not be encrypted, because the first rule, blocking the email, will take precedence.
- **NOTE: It is recommended that test groups be added to a rule initially for testing, to ensure the new** encryption performs as expected.
- This will prevent potential problems on mail flow for the entire organization.
- Test groups are created, only with valid corporate email addresses added to the rule instead non-valid email address

Example of security in E-commerce transaction

E-commerce

- Trade between two parties: where exchange is negotiated under the set of mutual acceptance conditions, so both parties emerge satisfied with result.
- Depends on whether two parties trust each other .

What is e-commerce

- E-commerce is a short version of the term Electronic Commerce
- transactions related to online buying and selling of products or services
- done using electronic systems such as the Internet and other computer networks
- penetration and spread of the internet has fuelled e-commerce
- Examples os e-commerce are electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems
- definition of e-commerce in modern times implies that it typically uses the World Wide Web at least at any point in the transaction's lifecycle
- Online retailers are sometimes known as e-tailers
- online retail is sometimes known as e-tail

Types of e-commerce

- B2B: E-commerce that is conducted between businesses is referred to as Business-to-business
  - (1) open to the entire public or (2) limited to a group of businesses who have been part of the specific group
  - Transaction cost reduced through reduction in
    - search costs
    - costs of processing transactions (e.g. invoices, purchase orders and payment schemes)
    - cost in trading processes
  - eliminating intermediaries and distributors
  - increase in price transparency
  - creates supply-side cost-based economies of scale

Types of e-commerce..contd…

- B2C Commerce
  - commerce between companies and consumers
  - involves customers gathering information; purchasing physical goods or information goods
  - online retailing companies such as Amazon.com, Drugstore.com, Beyond.com, Flipkart.com, Lenskart.com
  - reduces transactions costs
  - increasing consumer access to information
  - reduces market entry barriers

..Contd…

- **B2G e-commerce**
  - commerce between companies and the government
  - use of the Internet for procurement
  - licensing procedures
- **C2C e-commerce**
  - commerce between private individuals or consumers
  - online auctions
  - auctions facilitated at a portal, such as eBay, which allows online real-time bidding on items being sold in the Web;
  - peer-to-peer systems, such as the Napster model (a protocol for sharing files between users used by chat forums similar to IRC) and other file exchange and later money exchange models; and
  - classified ads at portal sites such as Excite Classifieds and eWanted (an inter-active, online marketplace where buyers and sellers can negotiate and which features "Buyer Leads & Want Ads").
  - Consumer-to-business (C2B) transactions involve reverse auctions, which empower the consumer to drive transactions.
  - There is little information on the relative size of global C2C e-commerce. However, C2C figures of popular C2C sites such as eBay and Napster indicate that this market is quite large. These sites produce millions of dollars in sales every day

M-Commerce

- buying and selling of goods and services through wireless technology
- handheld devices such as cellular telephones and personal digital assistants (PDAs) are used
- m-commerce will become the choice for digital commerce transactions
- bill payment and account reviews can all be conducted from the handheld devices
- consumers are given the ability to place and pay for orders on-the-fly
- delivery of entertainment, financial news, sports figures and traffic updates to a single mobile
- different server than that accessed by the regular online users
- allow users to book and cancel rail, flight, movie tickets through their mobile devices

Features provided by E-commerce

- Privacy : One’s information not known to others.
- Confidentiality : Secure transmission is demanded.
- Repudiation: Only if customer truly initiated the transaction, must be allowed.
- Accountability: Is it’s the user who is owner of credit card.
- Integrity : Services are available.

All these depend on the how secure are the endpoints.

Security issues of E-commerce

- **Network security** This is probably the most obvious issue for e-commerce applications, since the amount and severity of hack attacks are increasing. Fortunately, significant progress has been made in this area through firewall security products that protect against basic network-level attacks. A proper security strategy should not end here, though.

- **Identity** Since e-commerce implies trading with potentially unknown and untrusted partners, identification of trading partners can be crucial. Once again, much has been done to provide standardised methods to identify users by using certificates based on the X.509 standard. Unfortunately the deployment of these certificates for general e-commerce applications has been slow.

- **Encryption** Encryption is a key technology in e-commerce.
- **Authorisation** In order to automate trading processes, it is often required to verify more than identity. Various emerging standards such as certificates, authorization servers and the use of a database with registered users and privileges inside the application, all contribute to address the authorisation issue of who may do what.

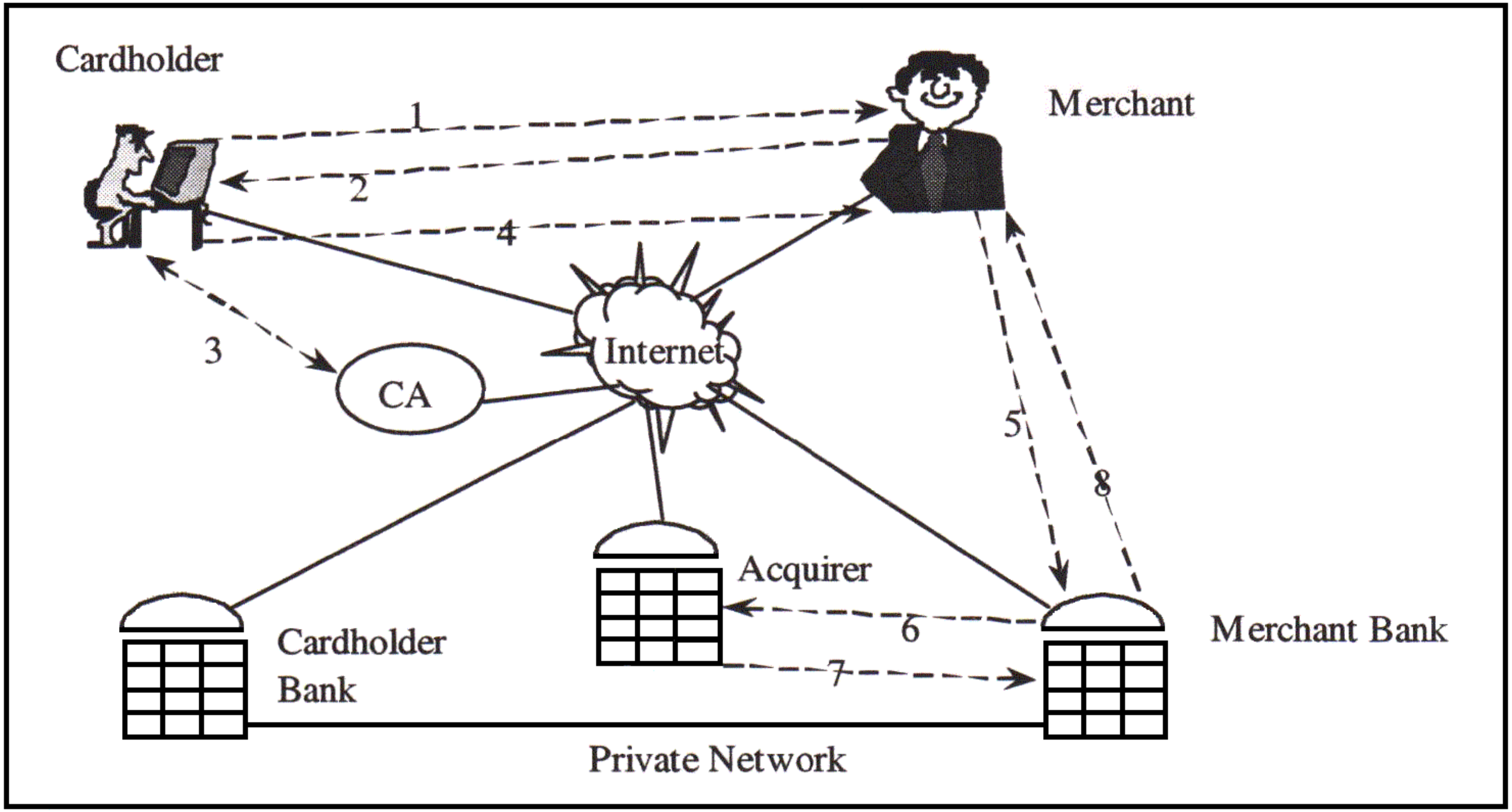
Cont’d

- **Host and application security** The protection offered by most operating systems falls short in a global networked environment. Efforts such as signed applets and signed executables are commendable, but will most probably not solve the problem of **virus and Trojan attacks**. In addition to these obvious flaws, more subtle problems such as buffer overflow attacks on certain networked applications can also lead to security compromises.

- **Transaction security** The protocols used for electronic transactions range from the primitive to the very sophisticated. Older secure protocols, for example those used in Point of Sale terminals, rely on the DES algorithm, and typically require some form of secure storage for the cryptographic keys. Many newer protocols (eg. SET) are based on public key mechanisms, but have not yet achieved widespread adoption.

- **Human error and malice** One of the most significant security problems faced by every system - no matter how secure technologically - is that trust is eventually placed in an individual. Auditing, agreements and regulatory frameworks can help, but are often too slow to react to the current demand for e-commerce.

Basic Network



Steps involved

- ***Step One***. The consumer enters an order along with their credit card information and sends it to the business.
- ***Step Two***. The business sends the consumer an invoice, their certificate and their bank’s certificate.
- ***Step Three***. The consumer acknowledges and approves this information and returns it to the business.
- ***Step Four***. The business then generates an authorization request for your credit card and sends it to their bank.
- ***Step Five***. The business’s bank then sends the credit authorization request to the Acquirer.
- ***Step Six***. The Acquirer sends an acknowledgement back to the business’s bank after receiving an acknowledgement from the consumer’s bank.
- ***Step Seven*** Once the consumer’s bank authorizes payment, the business’s bank sends an acknowledgement back to the business with the authorization number.

Different attacks

- Snooping the shopper’s computer
- Sniffing the network
- Using DDOS attacks
- Guessing passwords
- Using known OS-bugs

Simple Risks

- If URL with ’?’ separating various values, implies that the application is passing parameters to other scripts or programs. One can change these parameters and adjust the way program behaves.
- Price changed to negative number
- Buffer Overflow problems :

Do not make assumptions about user input size

Do not pass unchecked user input to shell commands

Cryptographic checksum is used to prevent unauthorized access Once the file is placed , checksum should be run on it and periodically it is run and checked with the original. To prevent false alarms, update of checksum should be a done.

Traditional to Present

- Electronic Data Interchange (EDI) has been used between business to order goods and make payment for years.
- Now-a-days SET(Secure Electronic Transmission) replaced EDI.

Verify the identity of the person

Often money flows.

Encryption Techniques

- Old symmetric key encryption: MAC(message authentication code.
- Non repudiation: By using current technologies, the signer cannot credibly deny having made his signature.

Cookies

- The primary use of cookies is to store authentication and session information, your information, and your preferences. A secondary and controversial usage of cookies is to track the activities of users.
- Temporary cookies: These cookies are valid only for the lifetime of your current session, and are deleted when you close your browser. These are usually the good type. They are mostly used to keep your session information.
- Permanent cookies: These are for a time period, specified by the site, on the shopper's computer. They recall your previous session information.
- Server-only cookies: These cookies are usually harmless, and are only used by the server that issued them.
- Third-party cookies: These are usually used for tracking purposes by a site other than the one you are visiting. Your browser or a P3P policy can filter these cookies.
- Encrypted cookies which are non-persistent are best as clear text cookie even though non-persistent , an attacker can design a proxy system between client and server to capture the required content

- SET :Secure Electronic Transaction
- S/MIME(Secure/Multipurpose Internet Mail Extensions): standard for secure e-mail which can do payment purposes.
- Cyber cash: purchasers credit card details are stored on secure PC and encrypts transactions between purchaser and internet merchants. Cyber cash is taken over by Verisign

Viruses vs. Trojan Horse

- **Viruses** Melissa ,I Love You, Resume KAK viruses have no affect on Unix as privilege access is done in Unix.
- **Trojan Horse**

  CUCme, VNCviewer, BackOrifice, Netbus -tools allow a remote user to control monitor any information on targeted PC.- Many websites www.portwolf.com/trojans.htm, www.cultdeadcow.com where one can download and play the Trojan-Horse programs.
- System admins manage huge number of workstations.
- Key stroke recorder program can also be installed at client side by attacker very easily.
- Password protection, encrypted client-server communication, PKI all go waste as the attacker will see all clear text before it gets encrypted.

Hacking tools

- I Love You virus –DDOS
- Code red worms NIDMA - as failed to install vendor patches
- Firewalls: is a hardware and software system that allows only those external users with specific characteristics to access a protected network
- Hacker tools like SMTPTunnel ICMPTunnel allow hackers to pass information through allowed ports like 80, 443
- Sniffer programs are likely to fond at end points – Encryption and switched network topologies can over come these.

Different attacks

- Access attacks - That penetrate security perimeters to steal information, DDoS attacks paralyze Internet systems by overwhelming servers, network links, and network devices (routers, firewalls, etc.) with bogus traffic. Also called as Smurf attack
- Bandwidth attacks- These DDoS attacks consume resources such as network bandwidth or equipment by overwhelming one or the other (or both) with a high volume of packets.

  The most common form of bandwidth attack is a packet-flooding attack
- Application attacks—These DDoS attacks use the expected behavior of protocols such as TCP and HTTP

  HTTP half-open and HTTP error attacks
- Blackholing describes the process of a service provider blocking all traffic destined for a targeted enterprise as far upstream as possible, sending the diverted traffic to a “black hole” where it is discarded in an effort to save the provider’s network and its other customers.

DDOS

- DDOS – success depends on inability of intermediate sites to detect, eradicate the penetration of their network
- Intermediate sites are compromised to launch DDOS against victim site.
- Source system sends a ‘ping’ packet to target. ICMP_ECHO_REQUEST packet containing source and target addresses.
- Target server if can responds gives a reply to source address listed in ‘ping’ packet. This is ICMP_ECHO_REQUEST_REPLY packet
- The original attack was called Smurf attack where source address is simply replaced with address of a host other than original sender.
- DDOS Smurf attack one step further network machines are compromised and slave daemons were installed on individual machines .These attacks are initiated only by command of the master.
- Detection & Eradication of master slave programs is solution-

  Win-trioo , TFN
- Patches should be installed.

Cont’d

- **Web site can be spoofed with a point and a click**
- SSL does not provide identity about the web site being visited
- Use a trust mark or site seal which can not be copied
- **TrustWatch® web site verification service.** TrustWatch (www.trustwatch.com) is a free toolbarand search site that helps consumers recognize whether a site has been verified and is safe for the exchange of confidential information.

Spoofing

- Spoofing
- Attackers often hide the identity of machines used to carry out an attack by falsifying the source address of the network communication
- User organizations and Internet service providers can ensure that traffic exiting an organization’s site, or entering an ISP’s network from a site, carries a source address consistent with the set of addresses for that site. Although this would still allow addresses to be spoofed within a site, it would allow tracing of attack traffic to the site from which it emanated
- They should also ensure that no traffic from "un routable addresses" are sent from their sites. This activity is often called **egress filtering**

To Overcome

- Firewalls installed can look only for particular type flavor of viruses.
- Anti virus stops only what it knows. So defensive strategies tend to be reactive rather than proactive.
- ISP’s should maintain the network integrity as high speed networks are connected with many systems.

Cont’d

- Routers, which use Access Control Lists (ACL) to filter out “undesirable” traffic, defend against DDoS attacks. And it is true that ACLs can protect against simple and known DDoS attacks, such as ping attacks, by filtering nonessential, unneeded protocols.
- Routers can also stop invalid IP address spaces, but attackers typically spoof valid IP addresses to evade detection.
- ACLs cannot block a random, spoofed SYN on port 80 of a Web server, where the spoofed source IP addresses are constantly changing.
- Unicast Reverse Path Forwarding (uRPF)- Ineffective against today’s DDoS attacks because the underlying principle of uRPF is to block outbound traffic if the IP address does not belong to the subnet which is spoofed by attacker.

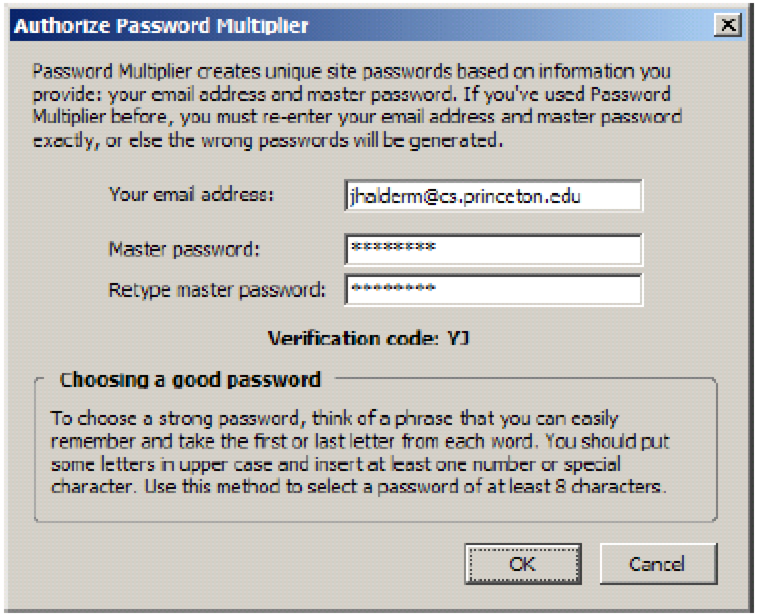
Pass words

- Resistant to brute force attack
- No simpler passwords, reusing at many sites
- Memorize one single passwd and use hash values to determine high-entropy passwords.
- let users choose their own passwds and store them somewhere safe or fixed passwds for each site that can be computed whenever needed.
- **Pwd hash** is used to provide a defense attack against phishing or spoofing

  stores passwords and other user sensitive data in encrypted database on user machine
- Lucent Personal Web Assistant (**LPWA**) operates as HTTP proxy server that user access with master username and passwd.
- Increase the computational time needed to estimate or eliminate a guess of user’s passwd by Iterated hashing

Screen Shot Of LPWA

- KDF(key ,hash, iterations)



Authorize Password Multiplier

Password Multiplier creates unique site passwords based on information you provide: your email address and master password. If you've used Password Multiplier before, you must re-enter your email address and master password exactly, or else the wrong passwords will be generated.

Your email address: jhalderm@cs.princeton.edu

Master password: *********

Retype master password: *********

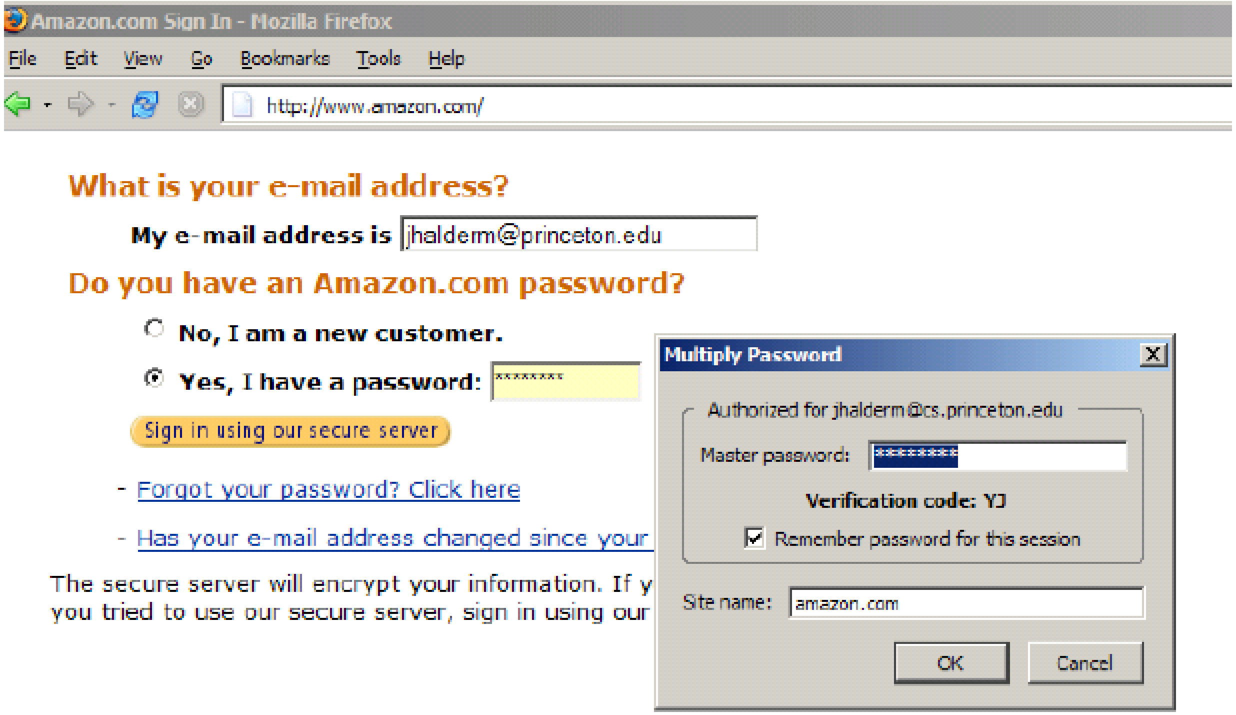
Verification code: YJ

Choosing a good password

To choose a strong password, think of a phrase that you can easily remember and take the first or last letter from each word. You should put some letters in upper case and insert at least one number or special character. Use this method to select a password of at least 8 characters.

Screen shot of LPWA usage

-


Amazon.com Sign In - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Sign in using our secure server
OK
Cancel

http://www.amazon.com/

What is your e-mail address?

My e-mail address is jhalderm@princeton.edu

Do you have an Amazon.com password?

○ No, I am a new customer.

● Yes, I have a password: ********

- Forgot your password? Click here

- Has your e-mail address changed since your

The secure server will encrypt your information. If y
you tried to use our secure server, sign in using our

Multiply Password

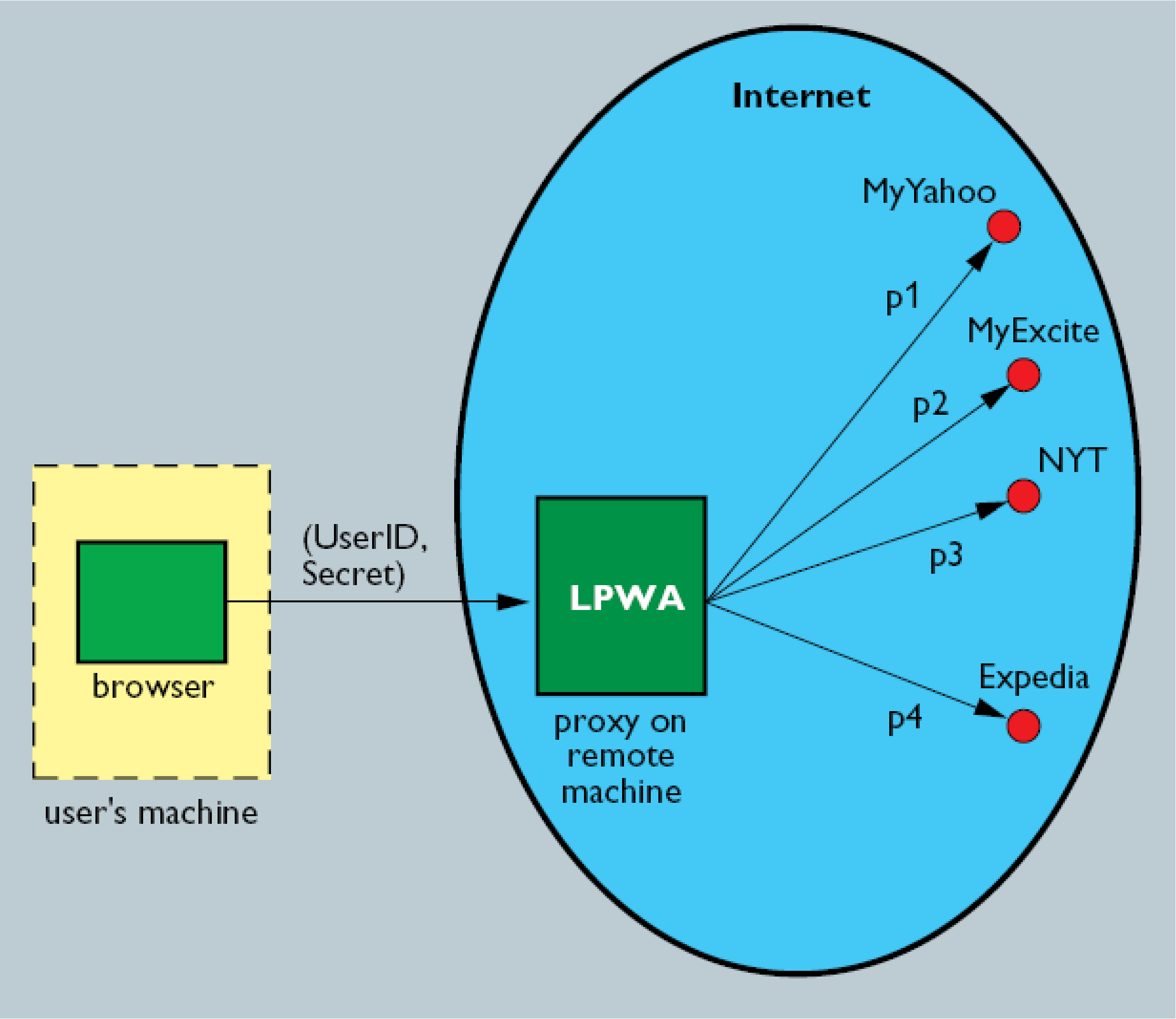
Authorized for jhalderm@cs.princeton.edu

Master password: *********

Verification code: YJ

☑ Remember password for this session

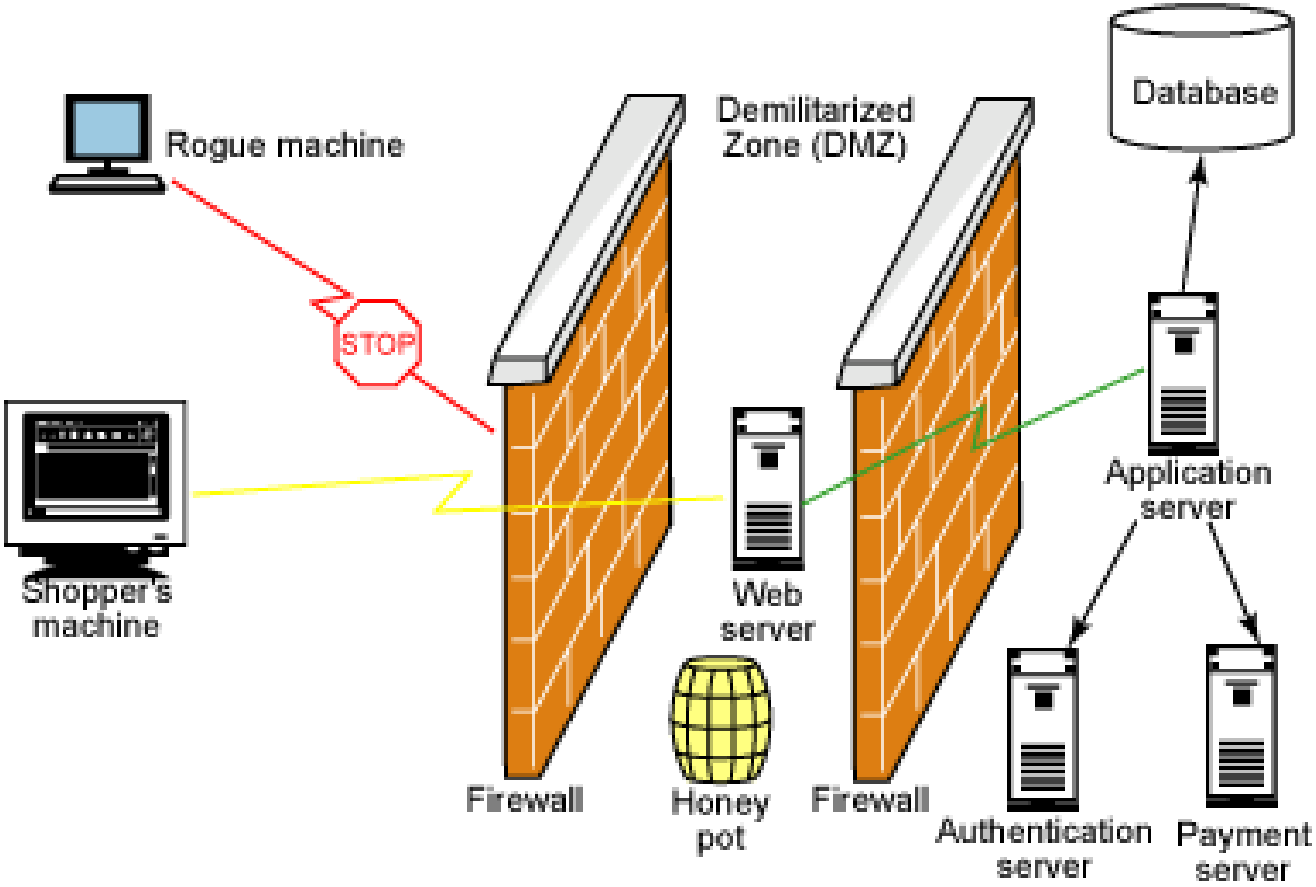
Site name: amazon.com


Internet
MyYahoo
p1
MyExcite
p2
NYT
p3
Expedia
p4
LPWA
proxy on remote machine
(UserID, Secret)
browser
user's machine

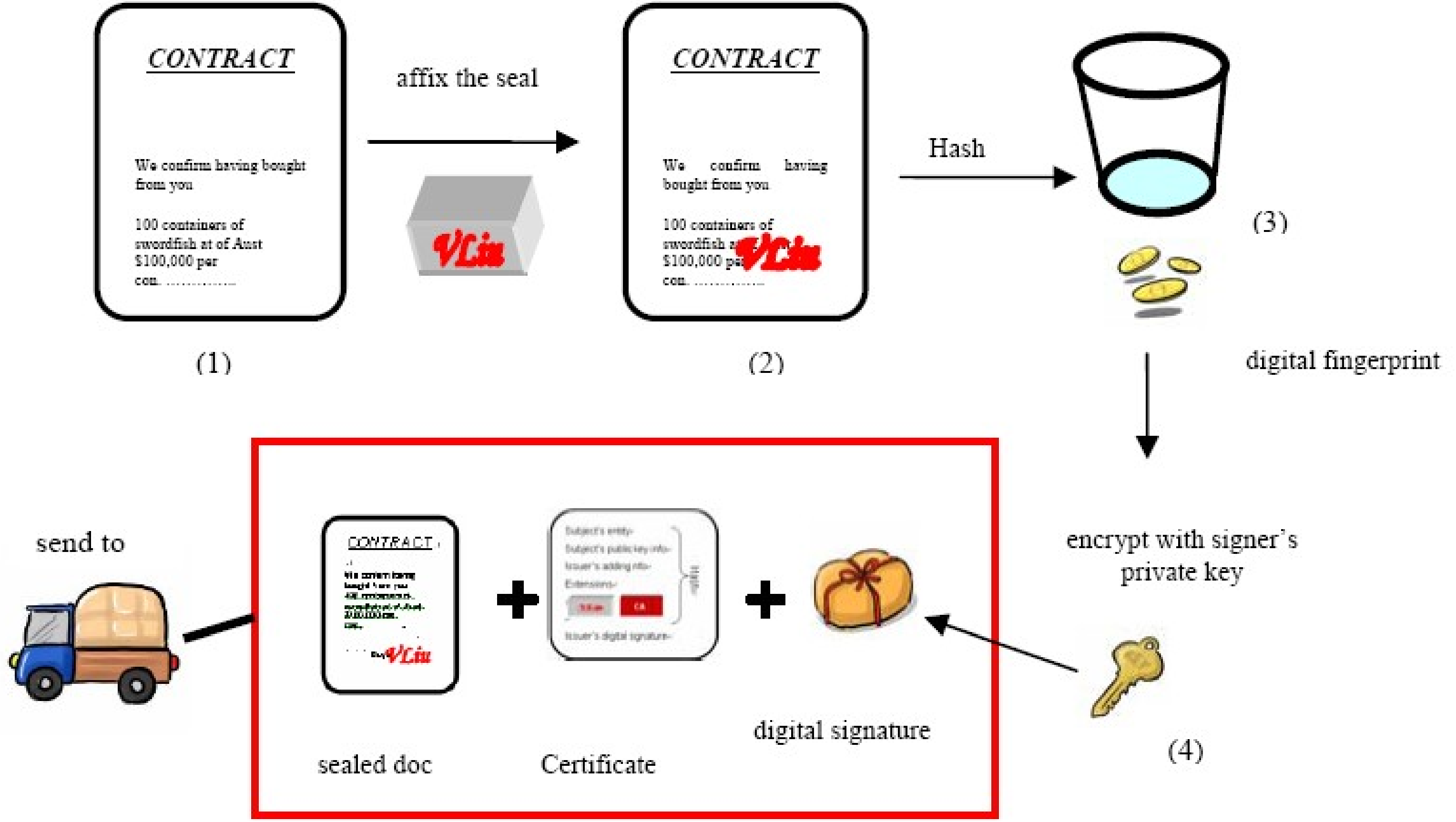
Multiple Layers of firewall

- Without robust physical and network security, sensitive corporate data is at risk of intrusion
- The use of firewalls, intrusion detection, client PC virus software, server-based virus checking and keeping all systems up to date with security patches will prevent most type of threats
- Firewalls should restrict access from the Internet and from one internal network (e.g. application servers) to another network (e.g. database).
- It’s recommended to use multiple layers of firewalls for distinctly different functional portions of the network – one for the demilitarized zone (DMZ), a second for the web server, a third for the application server and perhaps a fourth for the database layers.

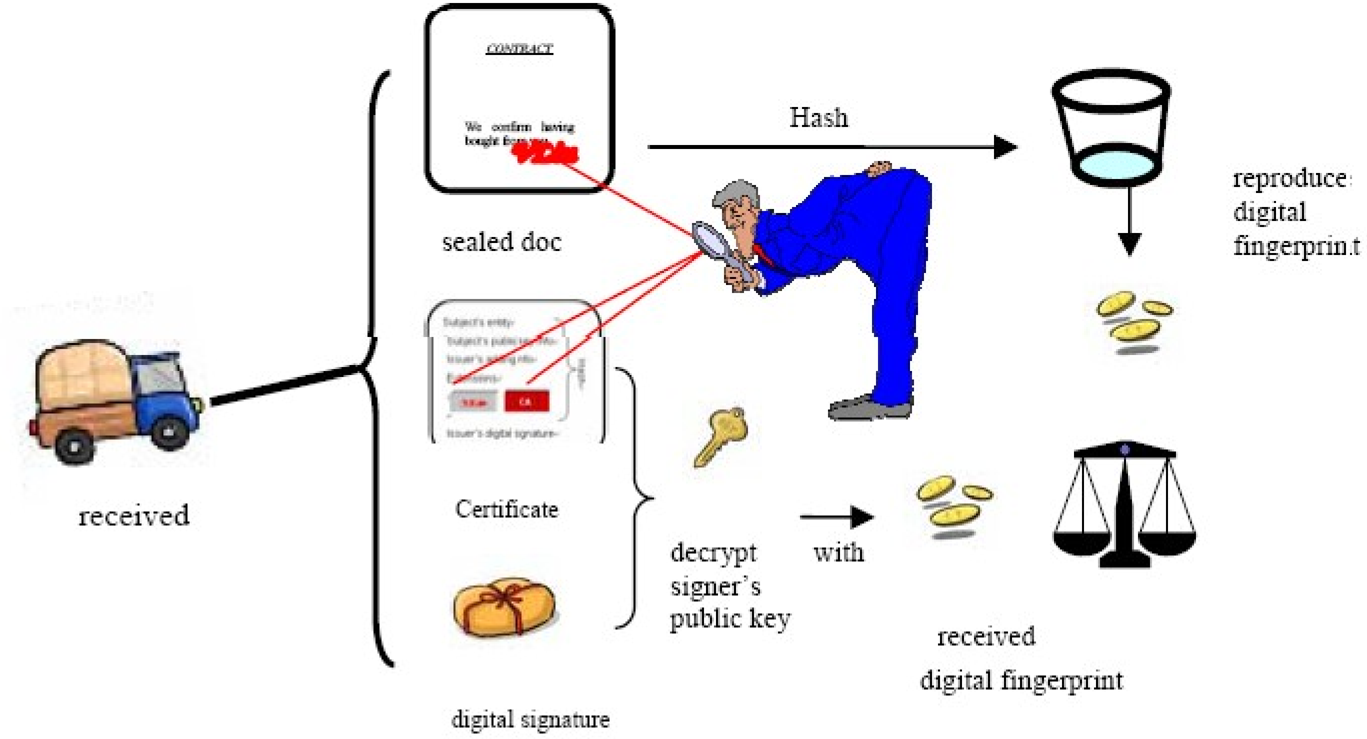
Measures for Security Installations



Signature Stripping attack


CONTRACT
We confirm having bought from you
100 containers of swordfish at of Aust $100,000 per con. …………..
(1)
affix the seal
VLiu
CONTRACT
We confirm having bought from you
100 containers of swordfish at of Aust $100,000 per con. …………..
(2)
Hash
(3)
digital fingerprint
encrypt with signer's private key
(4)
send to
CONTRACT
sealed doc
Certificate
digital signature

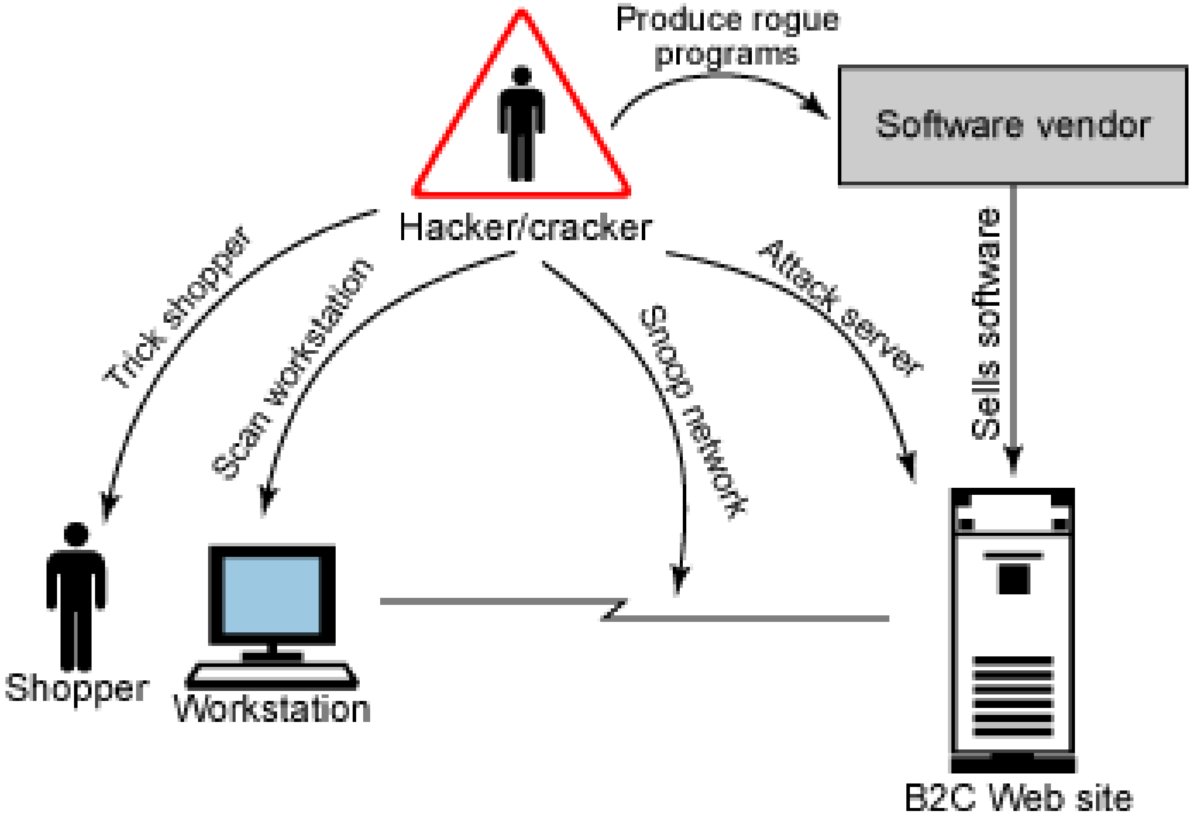
Decrypting a sealed signature Document


CONTRACT
We confirm having bought from you
sealed doc
Hash
reproduce digital fingerprin.t
received
Certificate
digital signature
decrypt with signer's public key
received digital fingerprint

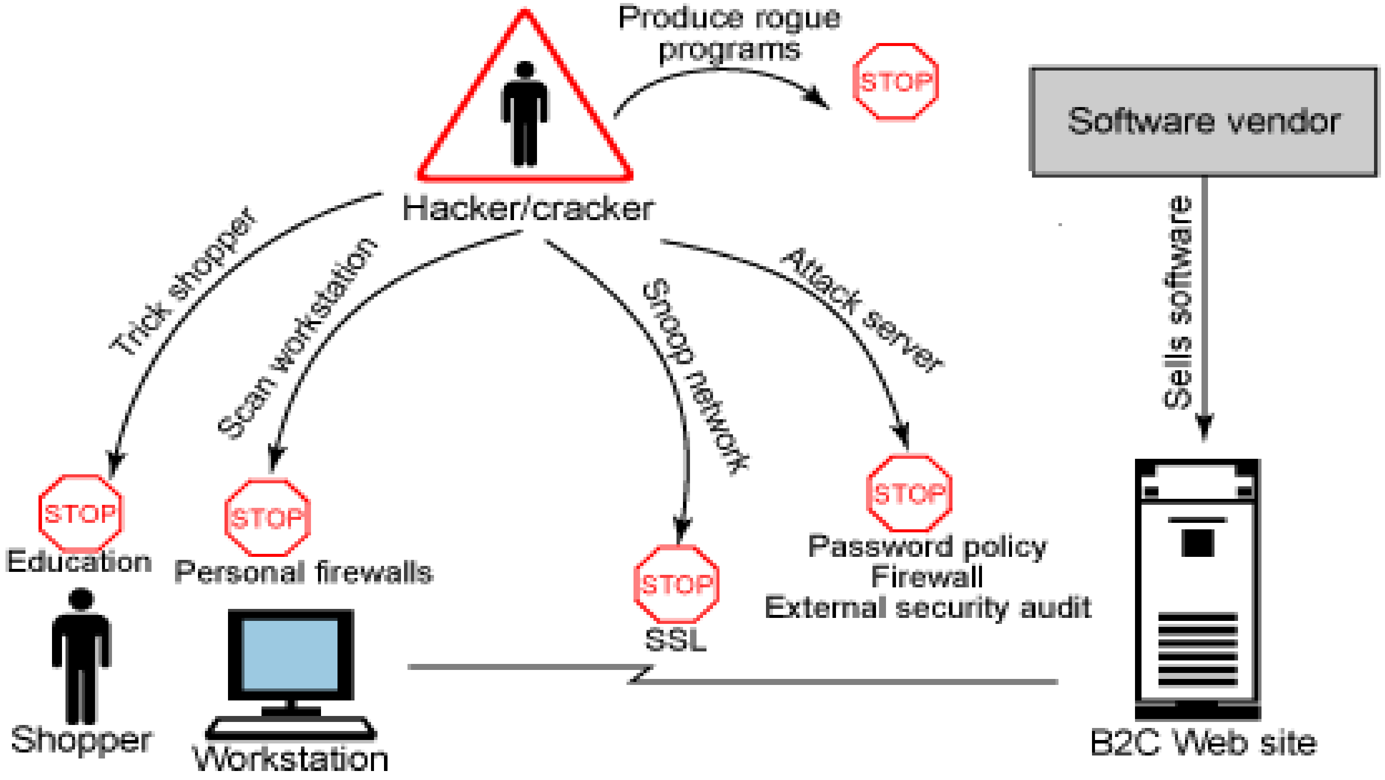
How to determine SSL sites

- In Firefox: closed lock icon on status bar, actual domain name in status bar, closed lock icon on address bar.
- XUL(XML based user interface language)
- Personalized Image but placement in a web page matters as naive users can be mislead by location
- EX: Spoofstick, spoofguard, e-bay toolbar.
- Type jacking- www.microsfot.com www.bankofvvest.com for www.bankofwest.com
- Directing users to fraudulent websites.
- Pop Up Window Attack: Where frame is placed round the site URL.
- Paypal Attack : When one is asked to provide personal details

Summary--Different stages for attack



Different measures for different stages of attacks



Communication security:

- HTTPS is used instead of http where SSL comes into play and connection is made between client and server. All traffic over this connection is encrypted.
- Digital certificates (X.509)reside on client’s machine, portability is low and specific hardware/software at seller side is needed if seller is CA.
- Biometric passwords also exits but had limitations as password change cannot be done and moreover customers may believe this act as prisoners do.

Other suggested ways

- Installing virtual private networks (VPNs) to allow secure access to critical systems for remote users.
- Time-synchronized tokens are small devices that generate a number that the user needs to enter into a web page for secure access to a network or application. Unfortunately, they are expensive.