SWINBURNE UNIVERSITY OF TECHNOLOGY

Cryptography

Lecture twenty-four

Outline of Lecture

- Hash functions
- Cryptographic protocols

Hash functions

- Hash functions map an arbitrarily sized message M to a fixed size output H(M)
  - Hashing is a one way function
  - Given a hash value H(M) it is very difficult to find M
- Collision free
  - difficult to generate two different inputs with the same hash value
  - Given M and H(M) it is very difficult to find another N (not equal to M) such that H(M) = H(N)
- Hash function output not dependent on structure or format of input
- Single bit change on average, alters half of all the bits in the hash value

MD5 code (from Schneier)

```
for each 512-bit chunk of message
    break chunk into sixteen 32-bit little-endian words w[i], 0 ≤ i ≤
15

    //Initialize hash value for this chunk:
    var int a := h0
    var int b := h1
    var int c := h2
    var int d := h3

    //Main loop:
    for i from 0 to 63
        if 0 ≤ i ≤ 15 then
            f := (b and c) or ((not b) and d)
            g := i
        else if 16 ≤ i ≤ 31
            f := (d and b) or ((not d) and c)
            g := (5×i + 1) mod 16
        else if 32 ≤ i ≤ 47
            f := b xor c xor d
            g := (3×i + 5) mod 16
        else if 48 ≤ i ≤ 63
            f := c xor (b or (not d))
            g := (7×i) mod 16
        temp := d
        d := c
        c := b
        b := b + leftrotate((a + f + k[i] + w[g]) , r[i])
        a := temp

    //Add this chunk's hash to result so far:
    h0 := h0 + a
    h1 := h1 + b
    h2 := h2 + c
    h3 := h3 + d

var int digest := h0 append h1 append h2 append h3
```

SHA-1 and successors

- Similar to MD5 but produces a 160 bit hash value
- Makes use of similar combination of logical operations and modulo arithmetic
- 160 bit hash length makes bruteforce attack difficult
- Numerous longer variations on SHA-1
  - SHA-224, SHA-256, SHA-384, SHA-512

Cryptographic protocols

- Secure Sockets Layer / Transport Layer Security (SSL/TLS)
- Internet Key Exchange (revisited)
- Pretty Good Privacy (PGP)
- Secure / Multipurpose Internet Mail Extensions (S/MIME)
- DNSSEC
- Anonymous service
- Bitcoin

SSL/TLS

- Secure Socket Layer / Transport Layer Security
- Developed by Netscape (SSL 1.0, 2.0, 3.0)
- Standardised in IETF with RFC 2246 as TLS 1.0
- SSL/TLS provides
  - Privacy
  - Authentication
  - Message integrity
- Operates at the socket layer
  - above the transport layer
  - three way handshake carried out before TLS handshake

SSL/TLS

- Application level (In Internet model) protocol
  - secure sockets
  - Requires use of specific ports
  - Specific ports are reserved for each protocol secured by TLS
    - eg HTTPS uses port 443
  - Firewalls need to open these ports
    - end to end
    - An encrypted tunnel
    - cannot proxy or NAT TLS

SSL/TLS

- Makes use of
  - Digitally signed certificates to authenticate the web server and provide the public key
  - Hashing functions to guarantee integrity of data
  - Encryption to guarantee privacy of data
- Data is encrypted between the browser and the server
- Public key encryption is used for
  - the initial handshake and
  - authenticating the server
  - exchange of symmetric keys (optionally use Diffie-Hellman)
- Symmetric key encryption is used for exchange of data
- Makes possible secure, one-off transactions

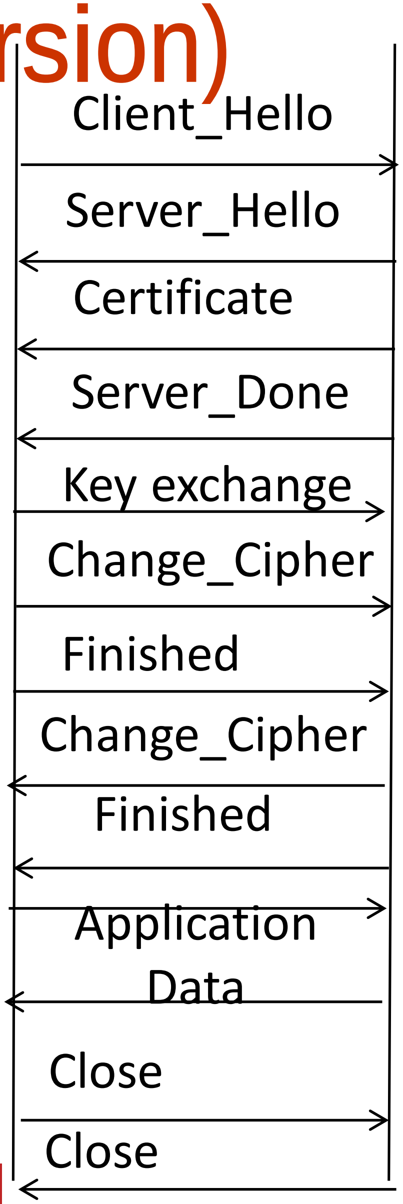
SSL/TLS handshake

- Browser and server negotiate cipher suite to use for the rest of the communication
- Browser authenticates the server
  - Server's public key is digitally signed by a trusted 3rd party
  - The browser optionally checks the signature on the server's digital certificate that contains the public key
- Browser generates a random number to be used as the basis of the session key and transmits the random number to the server encrypted with the server's public key
  - Some variants use Diffie-Hellman in this step
- The server decrypts the random number, generates the session key and communicates back to the client that data can now be transmitted

SSL/TLS handshake

- Other optional steps include the server authenticating the browser, using digital certificates
- The session key is generated using a hash of the random number and other information exchanged earlier
- Before the SSL / TLS handshake there is the TCP three way handshake to the appropriate port

SSL/TLS handshake (most common version)



Client_Hello

Server_Hello

Certificate

Server_Done

Key exchange

Change_Cipher

Finished

Change_Cipher

Finished

Application Data

Close

Close

Negotiate cipher capabilities

Send certificate to client

Random number used for key generation information (encrypted using public key)

After this communications from client encrypted

After this, communications from server encrypted

Transfer of encrypted data

Terminate connection

SSL/TLS handshake

- Negotiate cipher capabilities
  - Client sends to server a list of supported symmetric key ciphers and hash functions
  - Server selects which ones to use
- Send certificate to client
  - Server needs to guarantee to client it is who it claims to be
  - Not shown on the diagram is the client verifying the signature contained in the certificate
- Random number exchanged for key generation
  - The example shown uses RSA to share the random number used to form the symmetric key
  - There is another option that uses Diffie-Hellman

SSL/TLS handshake

- Change to cipher communications
  - Change_Cipher_Finished messages exchanged
  - From this point onwards all communications is encrypted using symmetric key cryptography
- Finished
  - Setting up the encrypted tunnel is complete
- Application Data exchanged
- Close
  - Both sides send a close message to shutdown the tunnel

TLS/SSL ports

Service	Port number	Description
https	443	Hyper-text transfer protocol
ssmtp	465	SMTP mail
snews	563	NNTP news
ssl-ldap	636	ldap directory
spop3	995	POP3 mail
ftps	990	FTP – file transfer

Internet Key Exchange (revisited)

- IKE uses a Diffie-Hellman key exchange to set up a shared session key
- Two phases
  - Phase 1 Authenticates communicating ends
  - Phase 2 Establishes Security Association
- Phase 1 has a number of different modes where information is embedded in other messages
- Most important (and simplest to understand) is the Main Mode

IKE (Main Mode)

- The Main Mode is an exchange in the first phase of IKE
- Consists of a number of exchanges of messages
- First two messages are used for negotiating the security policy for the exchange
- The next two messages are used for the Diffie-Hellman keying material exchange.
- The last two messages are used for authenticating the peers with signatures or hashes and optional certificates
  - These last two authentication messages are encrypted with the previously negotiated key and the identities of the parties are protected from eavesdroppers.

Pretty Good Privacy (PGP)

- PGP is a freeware electronic mail security program
  - Philip Zimmermann
- Algorithms used are
  - Can use IDEA, DES, triple-DES
    - Symmetric key algorithm
  - RSA with keys up to 2047 bits for key management and digital signatures
  - MD5, SHA-1 hash functions
- Random public keys use a probabilistic primality tester
  - initial seeds from keyboard latency

PGP key distribution

- No authorities to authenticate validity of keys
  - No specific policy to say whether or not a key is valid
- Uses a ‘web of trust’
  - Users decide who they trust and who they do not
- Every user generates and distributes his or her own public key
  - Users sign (digitally) each other’s public keys
  - Creates an interconnected community of users
- Each user keeps a collection of signed public keys in a file called a Public Key Ring
  - Each key has a legitimacy field that indicated the degree to which the particular user trusts the validity of the key, a signature trust field which signifiies how much the user trusts the signer to certify the public key of others.

S/MIME

- Secure Multipurpose Internet Mail Encoding
  - Authentication using digital signatures
  - privacy using RSA
- Uses hybrid cryptography
  - PKCS#7 standard for key exchange and digital signatures
  - Symmetric key for message encryption
    - DES, 3-DES, etc
- Different levels of certificateion
  - Class one simply links the email address to the “from” field
    - (limited in usefulness)
  - Class two identity authentication via Certificate Authority

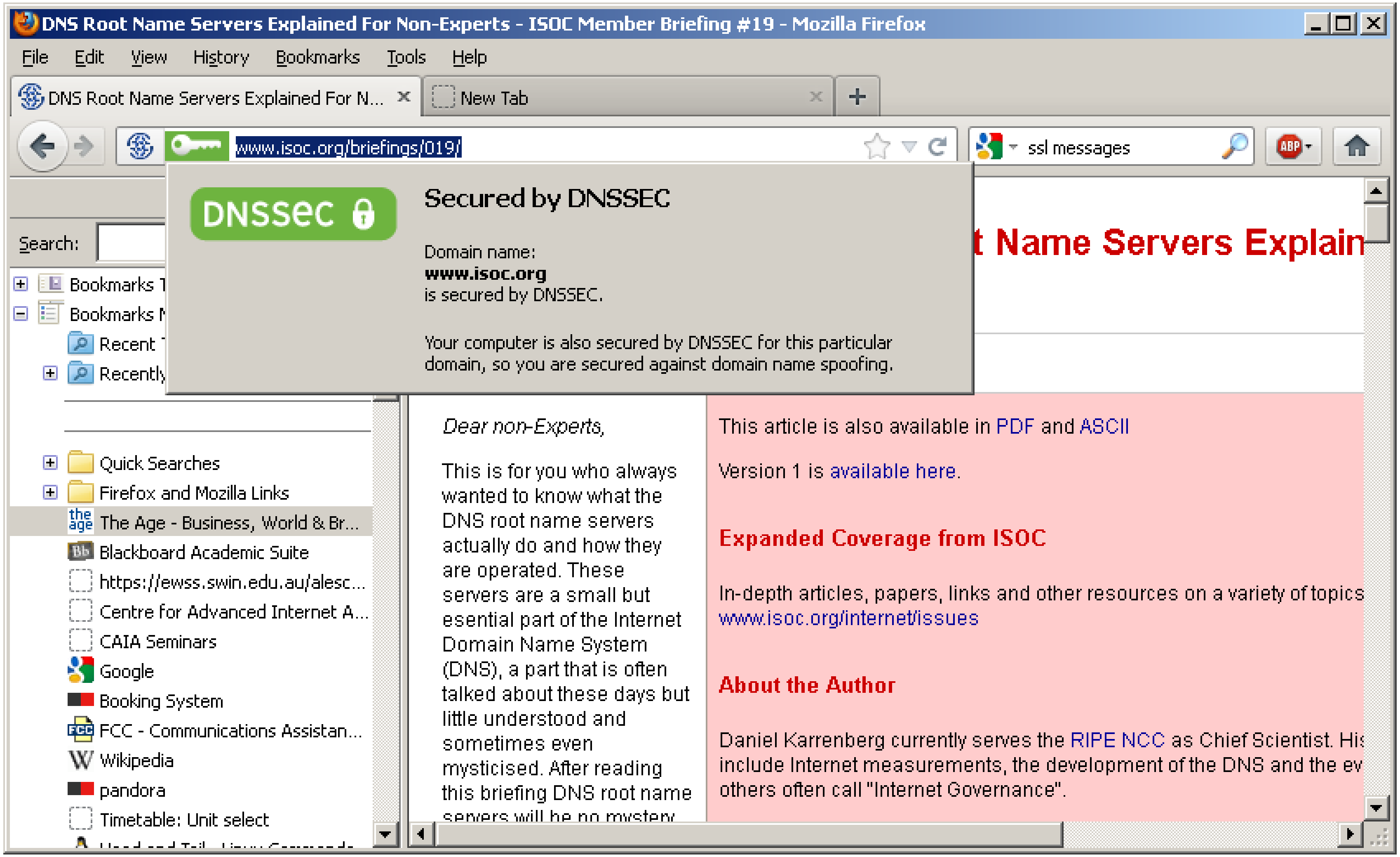
DNS Security Extensions

- The importance of DNS has increased over the past ten years
- Identity of hosts on the Internet used to be defined by their IP addresses
  - NAT extended to the carrier level has made that much less the case
  - IP addresses are now temporary tokens that are linked to an object for the duration of the transaction
  - Good discussion on the topic here
    - http://www.potaroo.net/ispcol/2015-08/gvi.html
- Much of the functionality that used to be provided by IP addressing is now being filled by fully qualified domain names
- Where identity needs to be maintained, DNS (rather than IP address) increasingly fills that role
  - Consequent increase in the importance of DNS integrity

DNS Security Extensions

- DNSSEC goal is to provide origin authentication to DNS clients (resolvers) so as to prevent forged DNS data being sent to the resolver
- All responses from the DNS Server are digitally signed
- Does not provide confidentiality, solely aimed at providing integrity
- Top level of DNS (the DNS root zone) is the Certificate Authority
  - More information as well as browser plug-ins at http://www.internetsociety.org/deploy360/dnssec/basics/

DNS Security Extension


DNS Root Name Servers Explained For Non-Experts - ISOC Member Briefing #19 - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
DNS Root Name Servers Explained For N...
New Tab
www.isoc.org/briefings/019/
ssl messages
Search:
Bookmarks T
Bookmarks M
Recent T
Recently
Quick Searches
Firefox and Mozilla Links
The Age - Business, World & Br...
Blackboard Academic Suite
https://ewss.swin.edu.au/alesc...
Centre for Advanced Internet A...
CAIA Seminars
Google
Booking System
FCC - Communications Assistan...
Wikipedia
pandora
Timetable: Unit select
DNSSEC

Secured by DNSSEC

Domain name:
www.isoc.org
is secured by DNSSEC.

Your computer is also secured by DNSSEC for this particular domain, so you are secured against domain name spoofing.

t Name Servers Explain

Dear non-Experts,

This is for you who always wanted to know what the DNS root name servers actually do and how they are operated. These servers are a small but esential part of the Internet Domain Name System (DNS), a part that is often talked about these days but little understood and sometimes even mysticised. After reading this briefing DNS root name servers will be no mystery

This article is also available in PDF and ASCII

Version 1 is available here.

Expanded Coverage from ISOC

In-depth articles, papers, links and other resources on a variety of topics
www.isoc.org/internet/issues

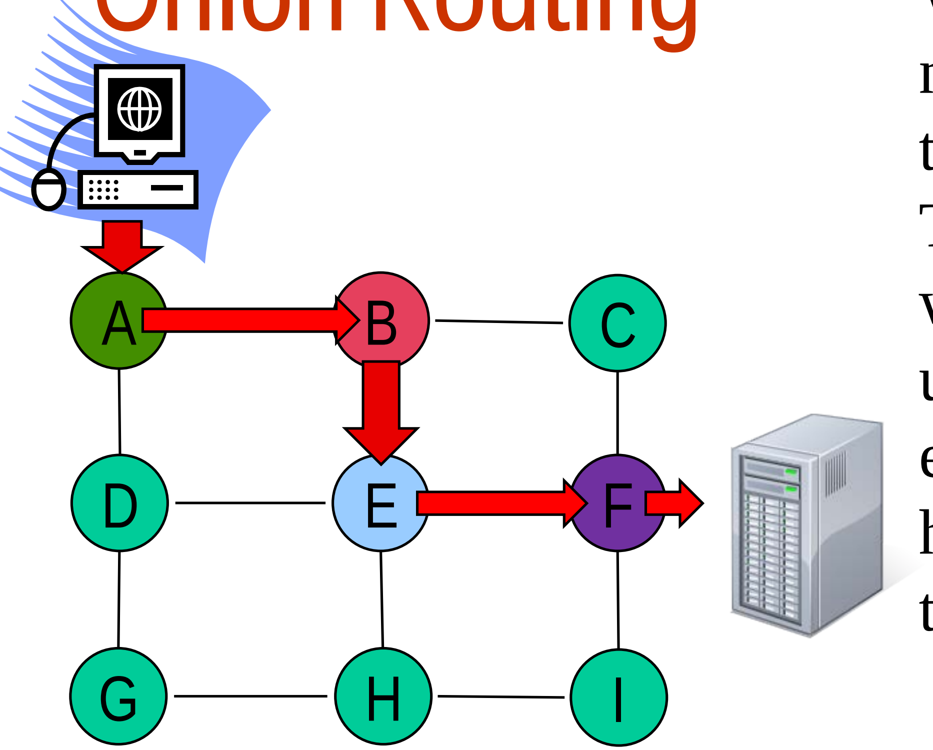
About the Author

Daniel Karrenberg currently serves the RIPE NCC as Chief Scientist. His include Internet measurements, the development of the DNS and the ev others often call "Internet Governance".

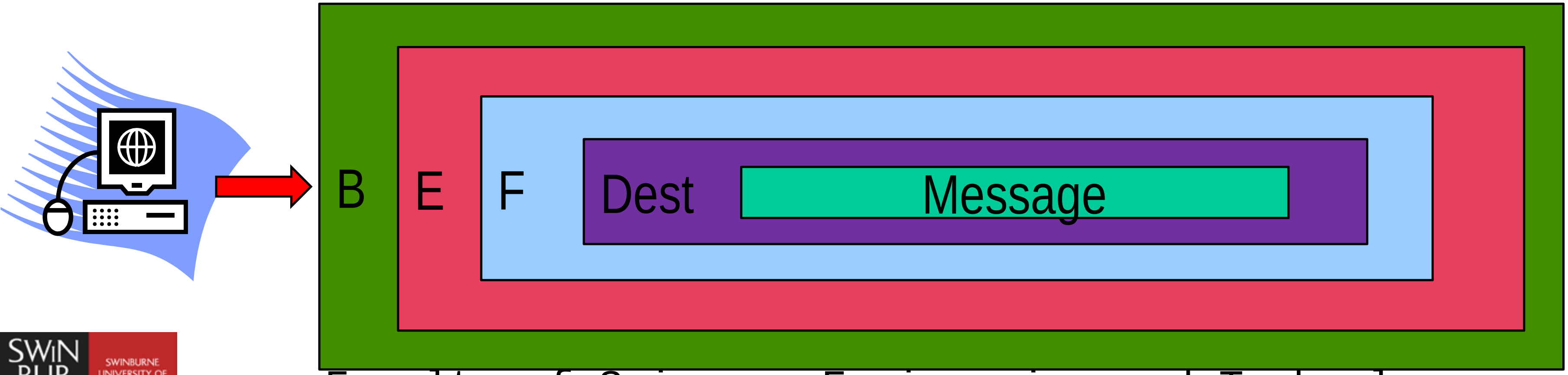
Onion Routing

- Permits anonymous communication over the Internet
- Consists of an overlay network of “Onion” Routers
  - Each onion router communicates with other onion routers via the Internet
  - Each onion router has its own public / private key pair
- When wishing to communicate across the network, a path is chosen via the onion routers
- The message is encrypted using each onion router’s public key to generate a session key
  - Layers of encryption, like an onion
- As each onion router receives a message it decrypts it, obtains the next hop information from the decrypted message and sends it to that next hop

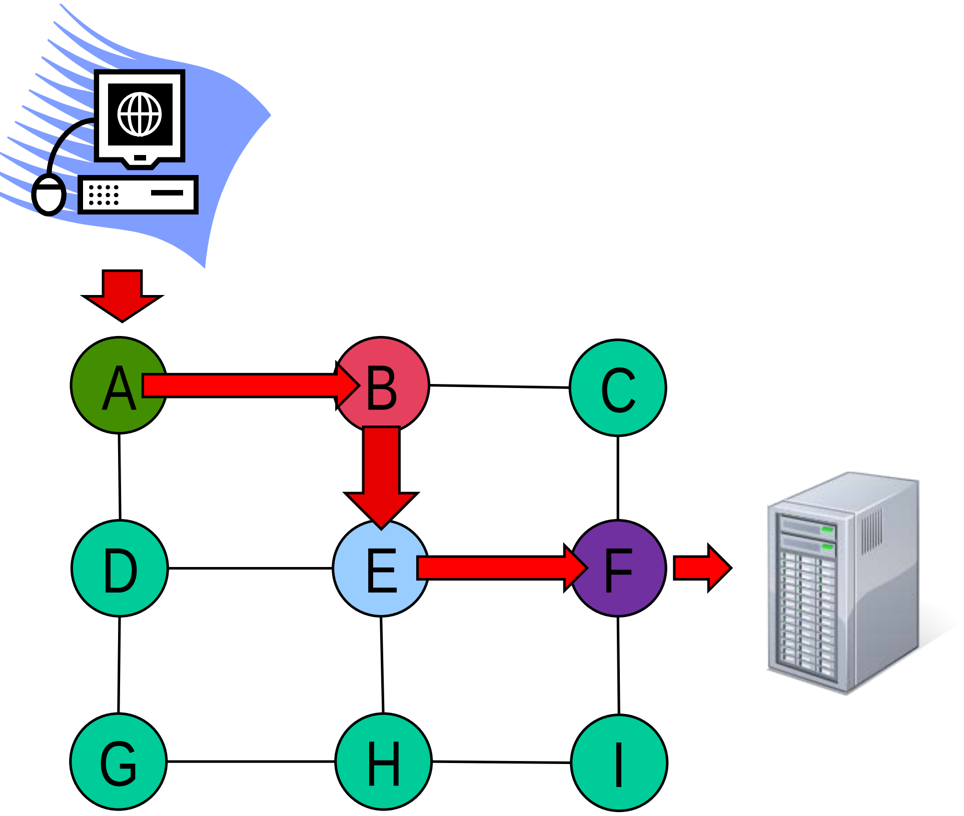
Onion Routing

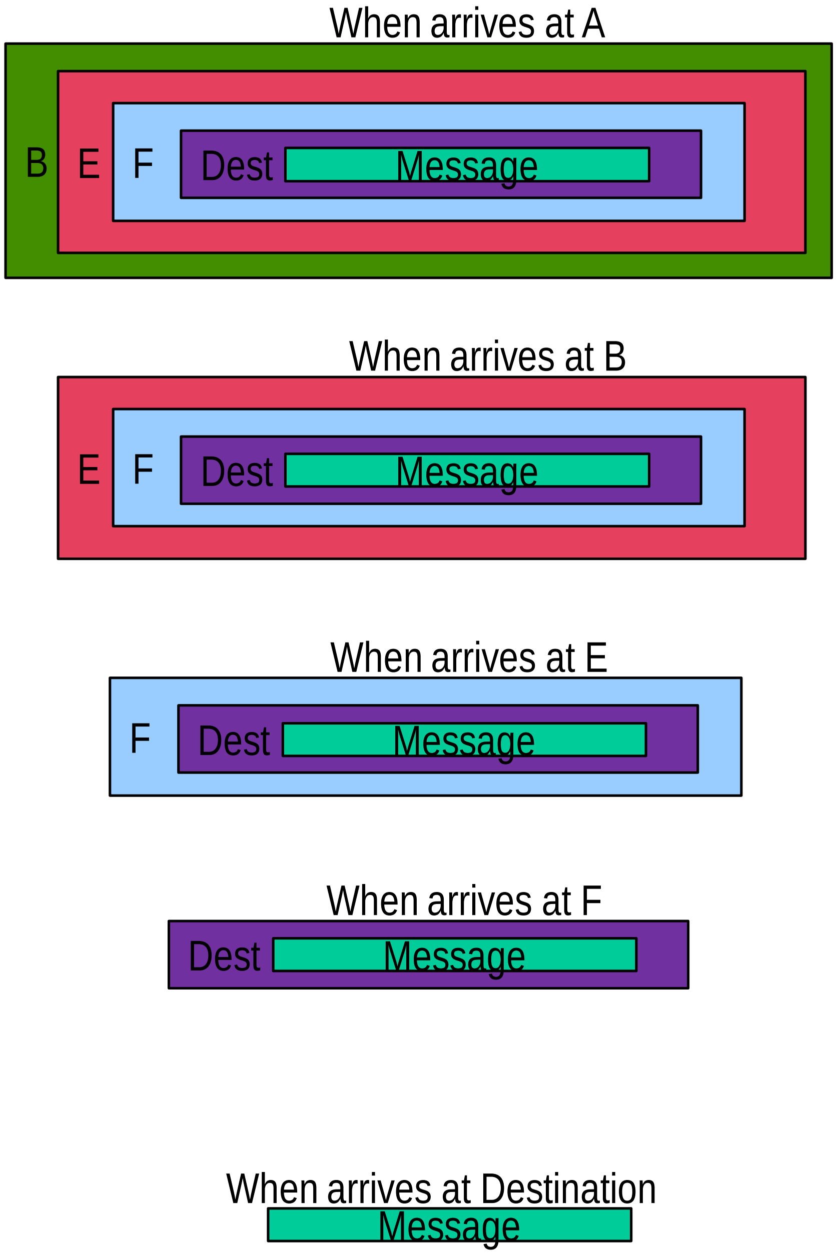


Suppose we are connected to node A We want to use a service attached to node F. Suppose our software decides to route our message via ABEF The message to be processed by F will have four layers of encryption, using each router's public key. Within each layer of encryption is the next hop and the encrypted message for the next router



Onion Routing





When arrives at A

B | E | F | Dest | Message

When arrives at B

E | F | Dest | Message

When arrives at E

F | Dest | Message

When arrives at F

Dest | Message

When arrives at Destination

Message

Onion Routing

- As each onion router receives the message it decrypts it using its private key
- Uses public key cryptography to set up symmetric key crypto keys
  - Still layers, but after initial pass through uses symmetric key crypto
- Tor (The Onion Router) the most well known example
  - Each user runs a ‘Tor proxy’
  - Operates at the Transport layer using SOCKS
  - Used primarily for anonymous access to web services
  - Also used for access to hidden services
  - Some weaknesses – exit node information is in plain text

Anonymous peer-to-peer routing

- “Invisible Internet Project” (I2P)
- Similar idea as to Tor
  - Use of multiple layers of public keys to provide anonymity
- Differences
  - Tor operates at the transport layer while I2P operates at the network layer
  - Tor has centralised, trusted directories for determining paths whereas I2P is completely decentralised
  - I2P is designed for services that are embedded completely within the I2P network whereas Tor is (generally) used to access publicly available services

Bitcoin

- An internet currency
  - (actually some legal question as to whether a currency or a product. Products are liable for Goods and Sales Tax, currencies are not)
  - Based on the ‘Bitcoin network’
- Bitcoin network is a peer-to-peer network that records payments
- Numerous exchanges that record transactions associated with each bitcoin
  - Digitally signed
- Users ‘mine’ bitcoins
  - Find them using computational power
  - Proof of work and scarcity

Mining bitcoins

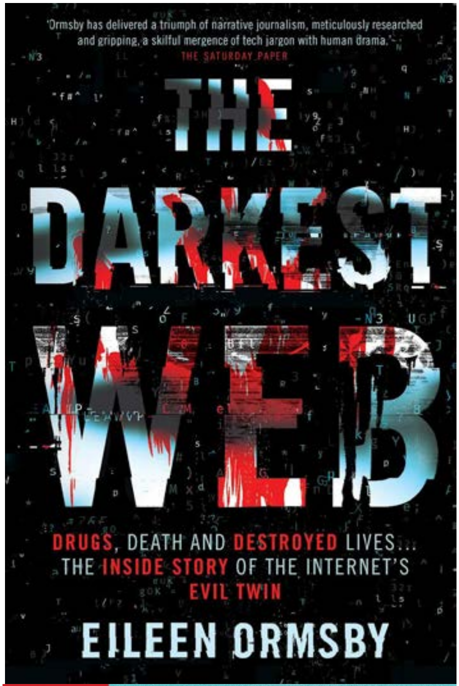
- Based on SHA-256
- Goal is to find a value that produces a SHA-256 hash value that starts with (currently) 14 zeros
  - Number of zeros varies depending on rate of production
    - Goal is to produce one solution every ten minutes (worldwide)
  - Not set by a central authority, but by aggregate number of users and level of difficulty they are prepared to accept
- Each solution is worth 25 bitcoins

Bitcoin blockchain

- Perhaps the most important contribution of Bitcoin was the idea of a blockchain
- A blockchain is a distributed transaction database
- New transactions include a hash of the previous transaction
- Fraudulent transactions, such as double spending, require hash reversal

Dark web

- Very much in the media and part of popular culture
- Not indexed by search engines
- Relies on onion routing for access (not so much I2P)
- Uses bitcoin for anonymous transactions
- Silk Road for drug purchases probably most famous
  - (Defunct – founder sentenced to three consecutive life terms in California)
- Many dubious sites advertising all sorts of horrendous ‘services’
  - Eileen Ormsby (“The Darkest Web”) believes most are scams
  - Best avoided


'Ormsby has delivered a triumph of narrative journalism, meticulously researched and gripping, a skilful mergence of tech jargon with human drama.'
THE SATURDAY PAPER
THE DARKEST WEB
DRUGS, DEATH AND DESTROYED LIVES... THE INSIDE STORY OF THE INTERNET'S EVIL TWIN
EILEEN ORMSBY

Conclusion

- Hash functions
- Protocols
- Applications of public key cryptography