Email and Digital Rights Management

CS 166: Introduction to Computer Systems Security
**E-mail Transport**

- **MUA**: mail user agent, aka mail client
- **MTA**: mail transport agent, aka mail server
SMTP

• Simple Mail Transfer Protocol
  – Client connects to server
  – Client sends commands to server
  – Server acks or notifies of error
• Security issues
  – Sender not authenticated
  – Message and headers transmitted in plain text
  – Message and header integrity not protected
  – Spoofing trivial to accomplish

HELO mail.cs.brown.edu
MAIL FROM: djt@whitehouse.gov
RCPT TO: rt@cs.brown.edu
DATA
From: djt@whitehouse.gov
To: rt@cs.brown.edu
Date: March 23, 2017
Subject: Executive order
You are hereby ordered to grade all the students of CS166 class with A.
The President of the United States
What is Email Spam?

• Unsolicited email and bulk email are each acceptable
• Spam combines unsolicited and bulk
  – Forbidden by all major ISPs
  – Considered “acceptable business practice” by US Direct Marketing Association (DMA)

• In classifying email as spam, content does not matter
• US CAN-SPAM act (2004) protects commercial spam subject to requirements:
  – Opt-out mechanism
  – Sender clearly identified and subject line not deceptive
  – Adult material label in subject
Phishing

- Imitates legitimate websites
- Attempt to fraudulently acquire sensitive information (passwords, credit card numbers, etc.)
- Victim often lured to via email
- Relies on the user not inspecting page in depth
- Examples on www.phishtank.com
Phishing

• “Unicode” attack
  Instead of linking www.paypal.com, links to www.pαypal.com, where “α” is the Unicode character for the Greek “alpha.”
Falling Victim to Phishing Attacks

• **Spear Phishing**
  – Phishing attempts directed at specific individuals or companies
  – Attackers may gather personal information about their target to increase their probability of success

• **Whaling**
  – Attacks directed specifically at senior executives and other high profile targets within businesses,

• **These attacks can be difficult to detect**
Spam Conversion

• Who reads spam anyhow?
• Empirical study [Kanich+ 2008]
  – Parasitic infiltration into botnet launching spam campaigns
  – 28 conversions, yielding $3K, from 300M spam messages over 26 days
  – Spam business has small profit margin

4/2/17 Email and DRM
Blacklisting

• Spamhaus Black List (SBL)
  – Real-time database of IP addresses of verified spam sources
  – Eliminates about 10% of spam before transmission takes place
  – Formal listing and delisting procedures
  – More than 600M email users protected by SBL
Graylisting

• Spam servers typically do not resend messages after transmission errors
• Maintain database of trusted servers
• Respond with “Busy, please retry” to SMTP connection requests from servers not in database
• Server added to database if reestablishes connection
• Currently effective although simple to circumvent
Sender ID and Sender Policy Framework

- Store DNS records about servers authorized to send mail for a given domain
- Look up domain in From header to find IP address of authorized mail server
DomainKeys Identified Mail (DKIM)

- Sender’s mail server signs email to authenticate domain
- Public key of server available in DNS record

```
DomainKey-Signature: a=rsa-sha1; s=mail;
   d=example.net; c=simple; q=dns;
   b=Fg...5J

Authentication-Results: example.net
   from=bob@example.net;
   domainkeys=pass;
```
SenderID-SPF vs. DKIM

**SenderID - SPF**
- Sending MTA authentication
- Channel based
- Simple implementation
- Message integrity not protected
- Mail forwarding not supported
- Vulnerable to DNS cache poisoning
- Vulnerable to IP source spoofing

**DKIM**
- Sending MTA authentication
- Object based
- Cryptographic assurance
- Protection of message integrity
- Supports mail forwarding
- Vulnerable to DNS cache poisoning
DIGITAL RIGHTS MANAGEMENT
Digital Rights Management (DRM) is a term used for systems that restrict the use of digital media. DRM defends against the illegal altering, sharing, copying, printing, viewing of digital media. Copyright owners claim DRM is needed to prevent revenue lost from illegal distribution of their copyrighted material.
Early U.S. Copyright History

- **US Constitution, Article 1, Section 8**
  - “To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries”

- **Copyright Act of 1790**
  - "the author and authors of any map, chart, book or books already printed within these United States, being a citizen or citizens thereof....shall have the sole right and liberty of printing, reprinting, publishing and vending"
  - Citizens could patent books, charts, or maps for a period of 14 years – Could renew for another 14 years if you were alive
  - Non-citizens and works from other countries not protected
Copyright Act of 1976

• Could copyright literary works, musical works, dramatic works, choreographic works, graphical works, motion pictures, and sound recordings (architectural works added in 1990)
• Copyright holders had exclusive right to reproduce, create derivative works of the original, sell, lease, or rent copies to the public, perform publicly, display publicly
• Could hold copyright for 28 years with a possible 28 year extension
• Rights of copyright holders are limited slightly by sections 107 through section 118 – Often referred to as Fair Use
Fair Use Doctrine

• When reproducing a particular work is considered fair use
  – Criticism, comment, news reporting, teaching, scholarship, research

• Four factors for determining fair use [17 U.S.C. § 106]
  1. The purpose and character of the use, including whether such use is for commercial nature or is for nonprofit educational purposes;
  2. The nature of the copyrighted work;
  3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
  4. The effect of use upon the potential market for or value of the copyrighted work
Sony vs. Universal Studios

• In the 1970s, Sony invented Betamax, a video tape recording format similar to VHS
• Could be used to record copyrighted broadcasts
• At the same time, some movie studios created Discovision which was a large disk that would disintegrate after a few plays
• In 1976 Universal Studios and Disney sued Sony for all the lost profits and tried to ban the use of Video Tape Recorders (VTR)
• District Court for the Central District of California rejected the claim on the basis that noncommercial use of VTRs was considered fair use
• Court of Appeals for the Ninth Circuit reversed the ruling and held Sony liable for aiding in copyright infringement
Sony vs. Universal Studios (cont.)

• In 1984, the Supreme Court had to decide on the issue – Is selling VTRs to the general public aid in copyright infringement of public broadcasts?

• The Supreme Court eventually ruled that “the sale of the VTR’s to the general public does not constitute contributory infringement of copyrights”
  – Concluded that most copyright holders who license there work for public broadcast would not mind having their broadcasts recorded on to a Betamax tape by viewers
  – Betamax was ruled that it fell under the Fair Use clause

• Case often referred to by future copyright lawsuits including the Napster case
Digital Millennium Copyright Act (DMCA)

- Illegal to circumvent anti-piracy measures built into software
- Unlawful to create, sell, or distribute devices that illegally copy software
- Legal to crack copyright protection to conduct encryption research, assess product interoperability, and test computer security systems
- Exceptions to nonprofit libraries, archives, and educational institutions in some cases
- ISPs are not held accountable for transmitting information resulting from their customers infringements
- Service providers are required to remove material when found
Dmitry Skylarov and Ed Felten

- Dmitry Skylarov (Elcomsoft)
  - Wrote software to remove encryption from PDF documents (legal in Russia)
  - While in the US, Skylarov was arrested and jailed for DMCA violations
  - Eventually Elcomsoft was sued and Skylarov was released

- Edward Felten (Princeton)
  - Secure Digital Music Initiative (SDMI) invited researchers to break watermark technology
  - Felten and his team succeeded and wrote paper for conference
  - SDMI and RIAA threatened legal action
  - Felten withdrew from conference and sued sued RIAA and SDMI
  - SDMI and RIAA withdrew threat
  - Felten eventually presented the paper
Copy Protection Methods

• Dongle
  – Pluggable hardware device that contains a secret value required to run the software

• Product key
  – Required to be entered by installation software
  – Online check for duplicate use
  – Hardware and OS fingerprinting to bind license to machine

• Phone activation
  – Human-to-human interaction servers as deterrent
Traitors Tracing

- A controller distributes protected content to a collection of devices
- The devices share a common symmetric key with the controller
- Each content item is encrypted with the shared key and broadcast to all the devices
- Some devices (traitors) are cloned or used to illegally copy and distribute protected content
- Problems:
  - Identifying traitors
  - Revoking traitors
Logical Key Hierarchy

• Balanced binary tree of symmetric encryption keys
• Devices associated with leaves, each holding the keys on the path to the root
• Content encrypted with the key of a node $v$ can be decrypted by all the devices in the subtree of $v$
Revocation of a Device

- If a device needs to be revoked, the keys known to this device must be changed and the new keys must be distributed.
- The distribution of new keys can be done with a logarithmic number of encrypted broadcast messages.
Encrypted Broadcasts

- Content hierarchy with various subscription packages
- Each content item is encrypted with a single symmetric key before broadcasting
- Subscriber authorized to view item must have the key to decrypt the item
- Single key per node allows computation of keys of descendant nodes
- Key distribution problem