Manyonymity: It's Who You Don't Know℠

- To Think About
  - PHP Distributed Encryption
  - What is an acceptable level of mass-market encryption?
  - How does the "average joe" fingerprint and protect their daily communication?
  - What are the true benefits of open-source vs. major company-owned encryption services?
  - What percentage of your daily digital communication is sent unencrypted?
  - How do we accelerate the adoption of PHP at the server level?

Manyonymity: In The Beginning

- What We're Going To Talk About
  - Questions & answers
  - General discussion of encryption methods, theories and apps
  - Introduction to Manyonymity
  - In-depth: Installing Manyonymity
  - Demo: configuring Manyonymity, bringing it to "GO"
  - In-depth: Maintaining Manyonymity (Admin)
  - Demo: administering Manyonymity, reports, alerts & tools
  - In depth: Using Manyonymity (Member)
  - Demo: sign-up, text encryption, fingerprinting
  - Conclusion: Review
  - Conclusion: Future

Manyonymity: By Adam Bresson

- Who I Am
  - 10+ years in computers with expertise in all PC OS's, Linux, PHP and Security
  - DEFCON 08/2000: Palm Security Talk
  - DEFCON 09/2001: PHP, Data Mining & Web Security Talk
  - DEFCON 10/2002: Consumer Media Protections (CMP) Talk
  - Started Recommendo.com, a web community devoted to What You'll Like connections between Movies, TV, Books and Music, human-based reviews
  - Started GetAnyGame.com, a web community that rents video games for the major consoles by mail and recycles your old games by helping you make money renting them on consignment

Manyonymity: You Want Answers?

- What is an acceptable level of mass-market encryption?
  - 128-bit SSL is standard in the browser and OS, we need fingerprinting, encryption and steganography
- How does the "average joe" fingerprint and protect their daily communication?
  - Use M from multiple points of access for max reliability
- What are the true benefits of open-source vs. major company-owned encryption services?
  - Open-source is expandable, solid, reliable, free-of-influence (political, etc.)
- What percentage of your daily digital communication is sent unencrypted?
  - National average=15%, strive for 50% of important info
  - How do we deem information important? Test: a leak would cause detrimental financial impact
- How do we accelerate the adoption of PHP at the server level?
  - PHP high-quality applications that are anywhere-deployable
  - PHP that pushes boundaries and innovates
  - PHP that opens new markets and propels the languages' dev

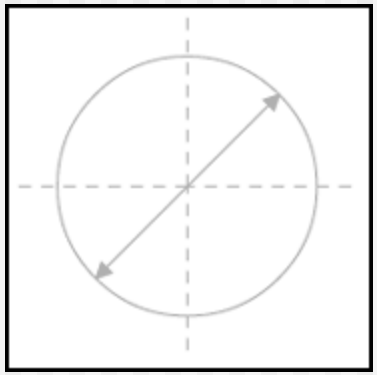
Manyonymity: General Encryption.1

- Why Use Encryption?
  - 40-bit SSL can be cracked by an Intel Pentium 266 in one hour
  - Reduce leaks of competitive company info & reduce liability
  - ITworld.com: provides authentication, integrity and accountability
  - Unencrypted records can be subpoenaed
  - Maintain file integrity over lossy TCP/IP Base64/MIME
  - Manyonymity is easy with a quick learning curve and more sophisticated features as expertise grows

Manyonymity: General Encryption.2

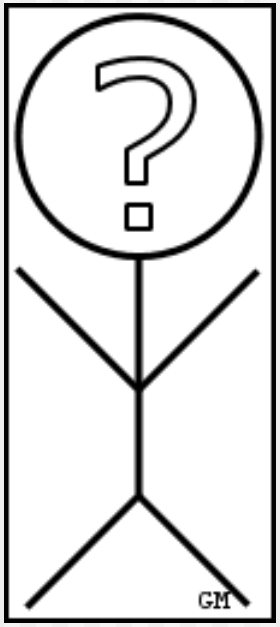
- Key Concepts
  - Algorithm: mathematical formula used to transform information
  - Fingerprinting: representing a file with a one-way key that only the unique makeup of that file would yield
  - Encryption: replacing information with a new representation of that information, often using an algorithm
  - Steganography: hiding information almost imperceptibly in a picture or other file (for example, JPEG or MP3)
  - Geometric Transformation: using geometry and its formulas to encrypt data, developing theory

Manyonymity: General Encryption.3



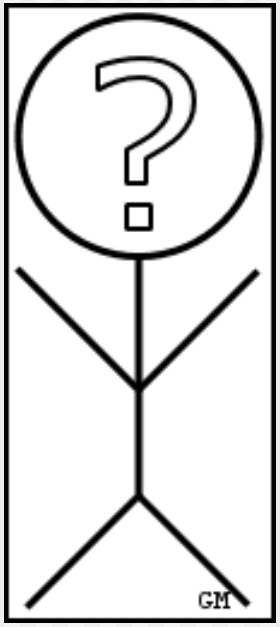
- Geometric Transformations
  - Using geometric formulas such as the area of a circle as an algorithm to generate strong, difficult-to-reverse results when encrypting
  - Example: Area Of A Circle
    - Given the area of a circle, calculate the dot density of the perimeter
    - Use the simple dot density value (100/inch) to reverse for the area
    - Area + dot density value=seed
    - Send the dot density value via email
  - Could be used with other functions and shapes, could be combined
  - Strung together like a key chain, reversible only if one knew each notch

Manyonymity: Introduction To M.1



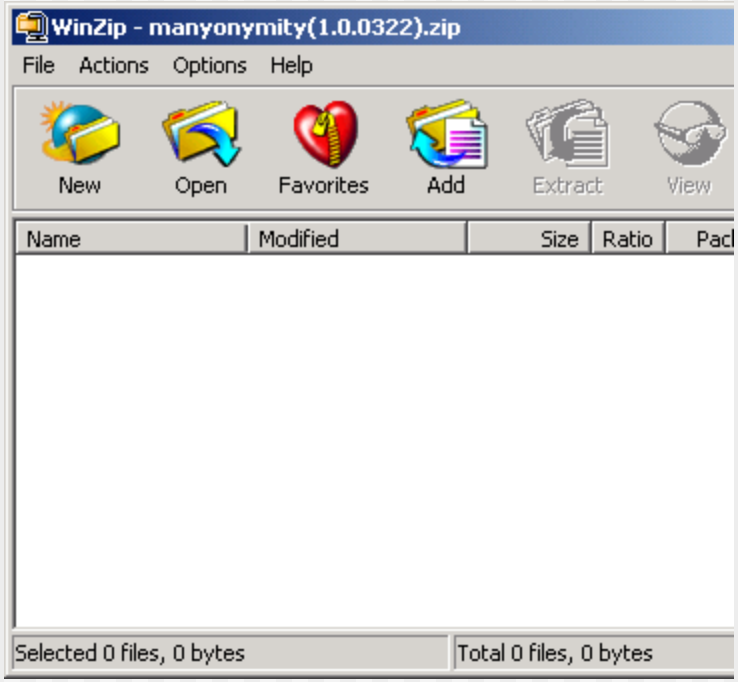
- What is Manyonymity?
  - Distributed: an encryption system with centralized server lists used to link logon information, facilitate searches and alert installations re: updates
  - Modular: add additional encryption options using secure, authenticated delivery as they become available (i.e. steganography for MP3)
  - Innovative: designed to bring encryption to everyone by making fingerprinting and encryption accessible without sacrificing the option of more sophisticated features

Manyonymity: Introduction To M.2



- Key Points
  - Easier to use than existing add-on Windows or Linux apps that compute MD5 hashes, quick email links provide one-click accessibility of verification
  - New methods of encryption ranging from simple (byte-shifting or XOR) to complex (geometric transformation or Twofish) immediately usable
  - Plugin modules allow deployments to evolve as fingerprinting and encryption methods change
  - Open-source will ensure rock-solid, smooth and fast code
  - Requirements: Apache 1.3.x, PHP 4.3.x, MySQL 4.0.x, mcrypt

Manyonymity: Installing M.1



- Tips for Apache, PHP & MySQL
- Download & unzip
- Change mconfig.php options
- Test installation & register server
- Demo: configuring Manyonymity, bringing it to “GO”

Manyonymity: Installing M.2

- Tips for Apache, PHP & MySQL
  - Download latest versions of all software, watch for problems (i.e. Apache 2.x experimental w/ PHP 4)
  - Only turn on PHP options in 'php.ini-recommended' that are required, limit ext.
  - Remove all MySQL user accounts except localhost/root and add strong password
  - Set new values for max_execution_time= and memory_limit= compatible with hardware
  - Only open Apache/HTTP port 80 through firewall, watch Slashdot for recent patches

Manyonymity: Installing M.3

- Download & unzip
  - Get the latest version from M homepage [www.manyonymity.com]
  - Compatible with Linux and Windows, .tar and .zip are identical
  - Comes with modules: TCRYPT & MD5FING, must authorize!
  - Use MD5 hash to verify download
  - Unpack to www with directory structure

Manyonymity: Installing M.4

- Change mconfig.php options
  - Verify $masterserver matches M homepage
  - Set $serverroot= to your absolute URL, i.e. [www.getanygame.com/m/]
  - Create MySQL db, set db name and password
  - Set security level, see comments, recommend setting ‘H’ for high
  - Configure color scheme via hex or word color codes, i.e. ‘#FFFFFF’ or ‘black’

Manyonymity: Installing M.5

- Test installation & register server
  - Run ‘Test Installation’ tool, make changes accordingly, M won’t accept logins until ‘Test Installation’ generates (0) errors at runtime
  - Run ‘Register Server’ tool to establish your server with the Master, will add your installation and poll for availability, statistics

Manyonymity: Installing M.6

- Demo: configuring Manyonymity, bringing it to "GO"
  1. Review Apache/PHP/MySQL installation
  2. Download latest M version
  3. Unzip to www
  4. Configure options
  5. Run 'Test Installation' and 'Register Server' tools
  6. Present opening Manyonymity screen

Manyonymity:
Maintaining M (Admin).1

- Maintaining inter-server relationships
- Reports & alerts
- Adding modules
- Tools
- Demo: administering Manyonymity, reports, alerts & tools

Manyonymity: Maintaining M (Admin).2

- Maintaining inter-server relationships
  - Why?: linking Manyonymity servers ensures universal login via login forwarding, integrated searches and alerts/updates
  - Server list at M homepage communicates server status, popularity and modules (services) available
  - Don’t forget to add MD5 admin password!
  - After registering your server, run ‘Update Server Info’ after any changes from Tools to catalog your server and automatically update its listing

Manyonymity: Maintaining M (Admin).3

- Reports & alerts
  - Statistics calculated in real-time include # of active uses of each module, member signups and volume indicators
  - Reports include # & % of historical uses of each module, member detail, db consistency
  - Alerts are delivered in a “task list” format in the admin area, will highlight unperformed maintenance, updates, etc.
  - Most alerts have an associated link or action

Manyonymity: Maintaining M (Admin).4

- Adding modules
  - Get the latest module list for verified, secure modules at M homepage
  - Download a module, ‘readme.txt’, drop into the /modules directory
  - Use ‘Authorize New Module’ tool described next & demo’ed to activate
  - Verify module availability on live site

Manyonymity: Maintaining M (Admin).5

- Tools
  - Customization: News, About, Info
  - Member: Suspend, Deactivate, Email
  - Installation: Test, Register
  - Authorize New Module: choose from list, enter authcode, MD5, ready!
  - Update Server Info: will catalog your server, upload module list and verify

Manyonymity: Maintaining M (Admin).6

- Demo: administering Manyonymity, reports, alerts & tools
  1. View real-time statistics
  2. View # & % historical module report
  3. Check alerts, complete task
  4. Authorize New Module:
     1. Download from list
     2. Get authcode & enter
     3. Complete MD5 check
     4. Module ready
     5. Verify availability

Manyonymity: Using M (Member).1

- Introduction & signup
- Setting account prefs (privacy, etc.)
- Encrypting your email (text encrypt)
- Fingerprinting a file (binary MD5)
- Demo: sign-up, text encryption, fingerprinting

Manyonymity: Using M (Member).2

- Introduction & signup
  - Member accounts link encrypted content to a Member profile with account rights
  - Member security: only information required is a valid Member name, it is linked to the Member's home server
  - Members can signup at any Manyonymity server. However, login, encryption/decryption and fingerprinting are ONLY accessible through their home server

Manyonymity: Using M (Member).3

- Setting account prefs (privacy, etc.)
  - Account rights can ONLY be set on a Member's home server
  - After login, Members can access Preferences from Welcome
  - Preferences include access to services (useful for your Boss), Open/Close decryption and fingerprinting access (Member/Non-Member), Forums

Manyonymity: Using M (Member).4

- Encrypting your email (text)
  - Login to your home server
  - Choose ‘Encrypt Text’ from Welcome
  - Follow 3 Steps:
    - Choose Encryption method
    - Create or copy/paste text into window, choose Save or Display
    - If Save, M will save your encrypted text w/ your account for future decryption and present a link used to retrieve/decrypt
    - If Send, M will present your encrypted text for copy/paste into the app of your choice

Manyonymity: Using M (Member).5

- Fingerprinting a file (binary)
  - Login to your home server
  - Choose ‘Fingerprint A File’ from Welcome
  - Follow 3 Steps:
    - Choose your file
    - Enter a unique id label, choose Fingerprint
    - M will present a link used by the file recipient to match MD5 fingerprint

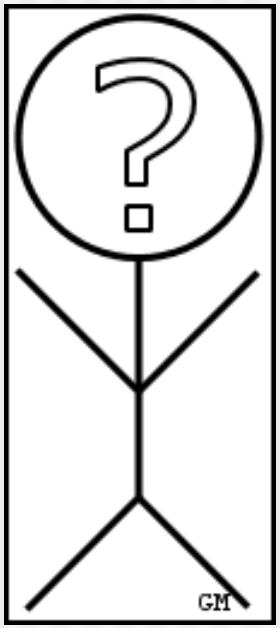
Manyonymity: Using M (Member).6

- Demo: sign-up, text encryption, fingerprinting
  1. Walkthrough sign-up and setting account prefs
  2. Demonstrate 'Encrypt Text'
     1. Watch copy/paste
     2. Discuss encryption methods
     3. Save vs. Display
  3. Demonstrate 'Fingerprint A File'
     1. Watch file size (limits)
     2. Discuss MD5 fingerprinting
     3. Open vs. Closed access

Manyonymity: Conclusion.1

- M: It's Who You Don't Know[GM]
  - Installing Manyonymity
  - Maintaining Manyonymity
  - Using Manyonymity
  - Benefits of encryption & fingerprinting
  - Manyonymity's Goal: flexible encryption, distributed geographically using PHP and always GNU GPL

Manyonymity: Conclusion.2



- Future
  - Abstract text and adapt for other languages, Unicode?
  - Additional modules such as steganography, other algorithms, auto-authorize
  - Adapt from Master/Slave model to P2P
  - Windows/Linux plugin for major email clients to automatically copy/paste
  - 100 international servers!

Manyonymity: Conclusion.3

- "dir \MANYONYMITY" on DEF CON 11 CD
  - 01-Manyonymity Presentation (ppt)
  - 02-IE link to Manyonymity homepage
  - 03-MaxCrypt (freeware)
  - 04-GRLRealHidden (freeware)
  - 05-Cleaner (freeware)