Know Thy Friends

Revisiting white-list security where black lists fail

Introduction

- When the largest security firms wrote their best practices into policy, computing resources were too slow to keep up with huge access control lists
- To provide cost-effective security, they turned increasingly to “black” lists of known offenders instead of “white” lists of trusted users

Introduction

- While the Internet has grown much larger since those days, the number of attackers has grown larger **faster**
- According to Dave Dittrich of the Honeynet project, it takes approximately 36 hours for a new Internet host to come under attack

Introduction

- As defensive measures improve in time, so do the sophistication of attacker methods
- Offenders benefit from decreasing bandwidth costs and the ensuing decreasing attack costs

Introduction

- CSI survey of 503 U.S. security professionals summary
  - 90% detected computer security breaches in the previous twelve months
  - 80% suffered financial losses due to computer security breaches
  - 40% detected system penetration from outside

Introduction

- In the harsh climate of the public Internet, it is ever more costly to identify and defend against the onslaught of malicious users
- To contrast, the number of trusted users has remained relatively unchanged for inter/intranet applications

Comparison – Black Lists

- Pro
  - Inexpensive per-entry
  - Temporary entries can inexpensively delay attackers
- Con
  - Logarithmic increase in malicious users means matching increase in number of entries and thus cost
  - Entries are hard to relate to real world

Comparison – White Lists

- Pro
  - Costs are predictable
  - Much more resilient to attackers
  - Entries are derived from real world relationships and easier to understand
- Con
  - Requires human intervention to create entry
  - Is therefore expensive per-entry

Point Comparison Summary

- Black lists are cheap and easy to create by automated processes, but quickly grow huge and become difficult to manage
- White lists are more expensive to create but easier to manage because the number of entries is so much smaller

Cost Basis

- Gartner Group estimates that one user costs about $300 per year in administration and help desk calls
- My estimates indicate that white list security incurs around 50% more help desk calls per user, which translates to another $150 per year

Cost Basis

- As accountants will undoubtedly describe, $450 per year per user is an unacceptable cost to most companies
- The Gartner Group study describes a cost reduction of greater than 50% when using automated help desk processes such as password recovery

Cost Basis

- Automated help desk and administration features can eliminate most of the additional white list incurred costs.
  - Traditional cost estimates drop from $300 to $144
  - I estimate costs for white-list based systems plummeting from $450 to $175 per year

Cost Basis

- The actual cost to a company will vary greatly based on user expertise, systemic automation and other factors
- Policy makers should seriously evaluate their current user costs and security model to see if they can simultaneously decrease their IT expenses and migrate toward the much stronger white list security model

Technology Examples

- Reliable e-mail receipt
  - Automated white-list management
  - Manual white and black list overrides
- Wireless routing
  - IPSEC/PPTP tunneling
  - 802.11x

Technology Examples

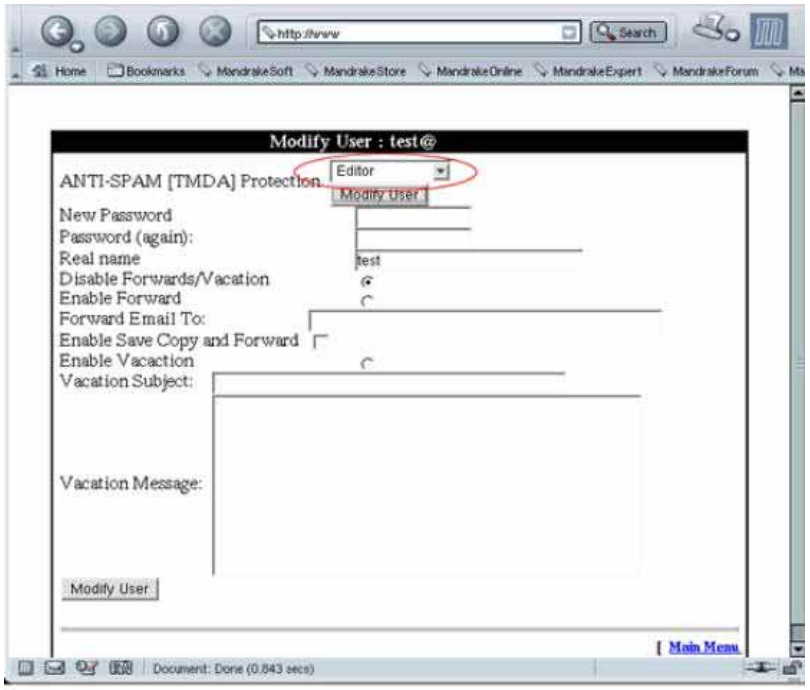
Improving E-mail Reliability

Improving e-mail reliability

- Tagged Message Delivery Agent
  - Free software
  - Allows manual white and black list e-mail addresses
  - Automatically verifies unknown senders by replying to their message
  - When used, inbound messages can minimally be guaranteed to be traceable

Improving e-mail reliability

- QAdmin-TMDA
  - Web-based e-mail account manager with direct QMail and TMDA support
  - Enables quick and easy per-account maintenance



Configuring TMDA

- The technical details are covered at http://tmda.net/
  - Configure your MTA to allow filtering
  - Insert TMDA into your mail transfer chain
  - Generate keys for each user
  - Optionally configure client software to tag outbound messages and send them through to authentication mechanism

Configuring TMDA

- Message tagging
  - To temporarily add the recipient of outbound mail to your white list, using the following lines in FILTER_OUTGOING:
    - ## use bare address and a dated envelope (to
    - ## catch bounces) with whitelisted recipients
    - to-file ~/.tmda/lists/whitelist tag envelope dated=14d from bare
    - to-file ~/.tmda/lists/wildcards tag envelope dated=14d from bare
  - This will allow a 14 day grace period without any automatic responses from TMDA to your recipients

Configuring TMDA

X-TMDA:	Outbound e-mail header
bare	Your sender address is left unchanged (ex: mary@host.net)
bare-append	Same as bare, plus adds recipients to a permanent list
dated	Tags sender address so that replies can only be received within a default timeout period (ex: mary-dated-989108708.a17f80@host.net)
dated=3m	Tags sender address so that replies can only be received within 3 months
sender	Tags sender address so that only the recipient list can reply to the message (ex: mary-sender-a17f80@host.net)

Improving e-mail reliability

- TMDA adds protection from unsolicited commercial e-mail and adds a layer of knowledge about messages received by your user base
- By automating the white list, the features are gained with extremely low cost to the company and user

Technology examples

Improving 802.11 Security

Wireless Technology Example

- 802.11 protocols are a major source of security vulnerabilities in corporate networks
- All the same, these protocols form the basis of exciting mobile workflows and are increasingly common in the office environment

Wireless routing

- The technology basis defaults to giving access to any user, often with primitive hardware address filtering using white and black lists
- This is a fundamentally difficult security system and does nothing to address the cryptography problems intrinsic to 802.11b

Wireless routing

- Transforming the black-list based security to a white-list system is a lot easier if we rely on common authentication and encryption mechanisms
- VPN tunnels are clearly the easiest solution

Wireless routing

- Step-by-step white list 802.11
  - Put a default-deny firewall between the AP and the rest of the network
  - Enable only the protocols and ports required to support your favorite VPN tunnel
  - Configure a VPN server to use your existing authentication software and position it behind the firewall

What This Means

- Network installations are attacked consistently by people trying to infiltrate black-list environments
- Black-list systems are increasingly complex and expensive
- White-list systems are relatively fixed-cost and increasingly manageable

What This Means

- Black lists are decreasingly feasible
- White lists are increasingly feasible
- The burden is on administration and management to push for ‘default deny’ policies to replace ‘default allow’ policies