Owning the Enterprise

Dino A. Dai Zovi
Security Researcher
ddz@theta44.org
http://theta44.org
http://trailofbits.com

Who Am I?

- **Information security professional**
  - Experience in red teaming, penetration testing, software security: Sandia National Laboratories, @stake, Bloomberg, Matasano Security
  - Now manage information security for a technology-based finance firm
- **Independent security researcher**
  - Focus on offensive computer security in operating systems, networking, and application software
  - Regular speaker at professional, academic, and hacker security conferences like BlackHat, Microsoft BlueHat, IEEE Information Assurance, USENIX Workshop On Offensive Technologies, DEFCON and Shmoocon
  - Presentation topics have included exploiting buffer overflows, wireless client security, hardware virtualization rootkits, and hacking virtual worlds

Agenda

- Genghis Khan's Siege of Volohai
- Limitations of Internet Explorer's Protected Mode on Windows Vista
- Attacking Wireless Clients (KARMA)
- Network Access Control
- NTLM Cross-Protocol Authentication Relay
- Cloud Computing For Hackers

Bypass the Fortified Perimeter

Genghis Khan's Siege of Volohai

- Khan's army was unable to penetrate the fortified perimeter
- Khan offered to end the siege for a tribute of 1,000 cats and 10,000 swallows
- They attached bits of wool to the cats and swallows, lit the wool on fire, and they ran back to their lairs and nests, burning down the city from inside
- Don't break down the front door, climb in through an open window

Client Side Exploits

- Rise of client-side exploits follows identically
- The network perimeters have become fortified with firewalls, intrusion detection/prevent systems, hardened servers, etc.
- The cats and swallows are users' web requests and e-mails
- Compromise outbound communications, follow them back in, and take over network from the inside

Vista Will Save You

- **Vista presents some tangible security benefits**
- **Security Development Lifecycle (SDL)**
  - Results in less vulnerabilities
- **Address space layout randomization (ASLR), data execution prevention (DEP), stack protection (/GS), SafeSEH, hardened heap**
  - Vulnerabilities are impossible or difficult to reliably exploit
- **UAC notifies user when administrative actions are performed**
- **Internet Explorer runs in low-integrity "protected mode"**
  - No write access to most file system or registry locations

Protected Mode Internet Explorer

- Internet Explorer runs in low-integrity process for Internet and Intranet Zones
- Process integrity-level is a "magic" SID in token
- This means nothing across the network to pre-Vista operating systems

Protected Mode Internet Explorer

- **You wouldn't be storing user profiles or home directories on a pre-2008 server, would you?**
- **Writing a new startup item yields medium-integrity access.**
- **Calling process setup.exe will trigger auto-elevation and may trick user into allowing UAC prompt, yielding high-integrity access.**
- **Recommendations:**
  - Even with UAC, don't let users run as local administrators.
  - Move user profiles, redirected folders, and home directories onto Windows 2008 Server as soon as possible.

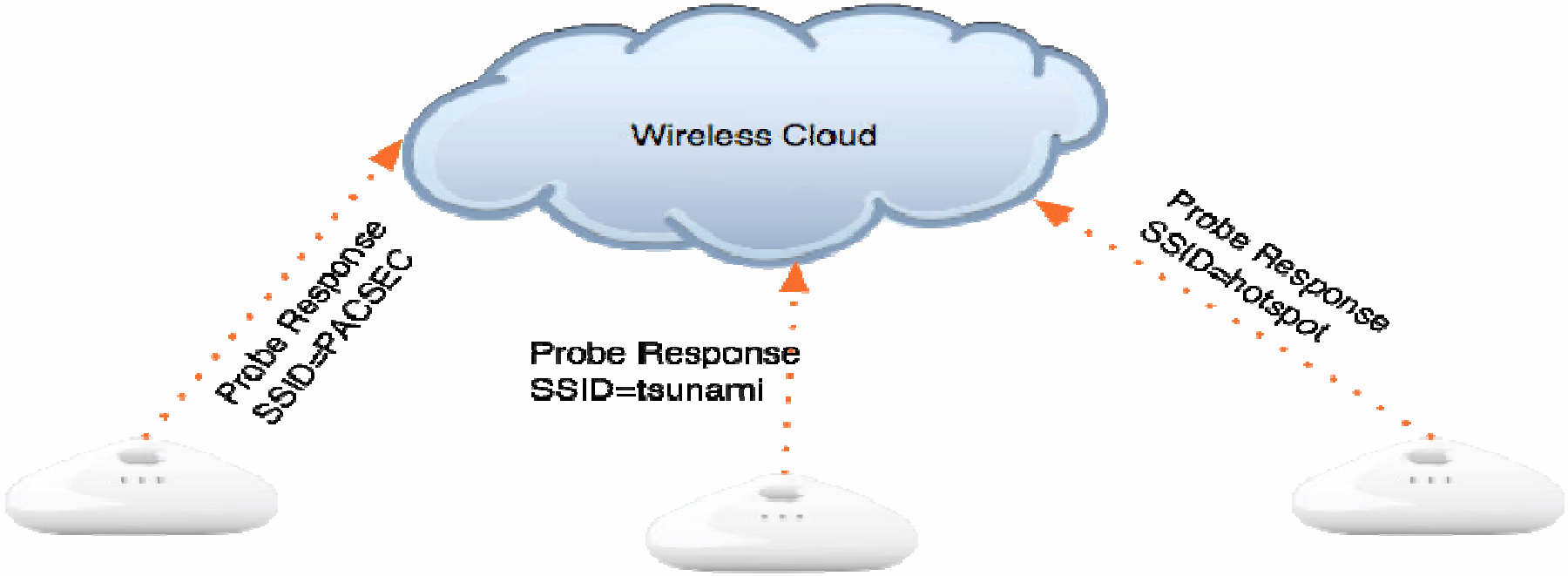
KARMA Wireless Client Attacks

- **Genghis Khan's siege of Volohai all over again**
  - Wireless network security is fortified w/ WPA2 Enterprise
  - Wireless clients still reach out looking for other networks
  - Accept client's association, compromise client, allow to rejoin secure wireless network, and attack from the inside
- **KARMA exploits several weaknesses in Windows XP wireless auto configuration**
  - Clients broadcast SSIDs in preferred networks list
  - Most-recently joined hotspots have higher precedence than the secure corporate network that was first joined a long time ago

Wireless Auto Configuration Algorithm

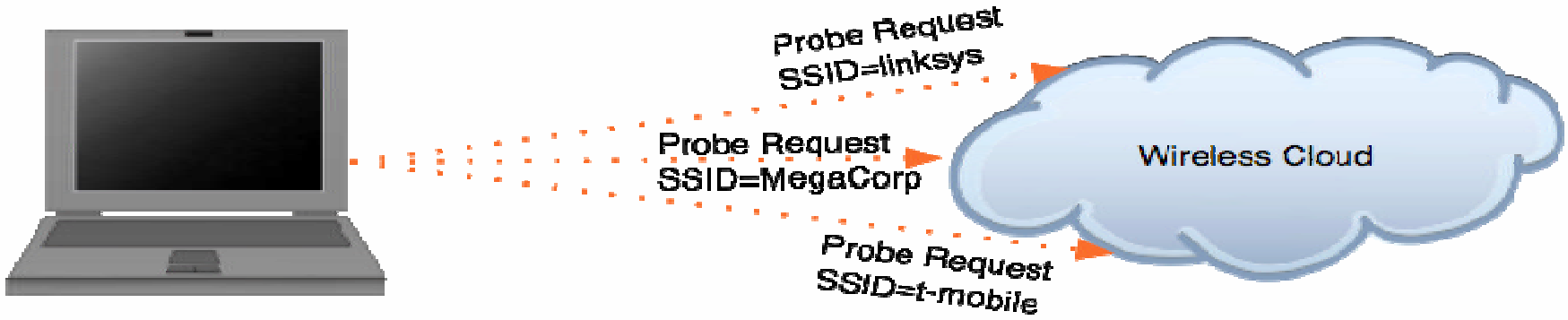
- **First, Client builds list of available networks**
  - Send broadcast Probe Request on each channel

Wireless Auto Configuration Algorithm



- **Access Points within range respond with Probe Responses**

Wireless Auto Configuration Algorithm

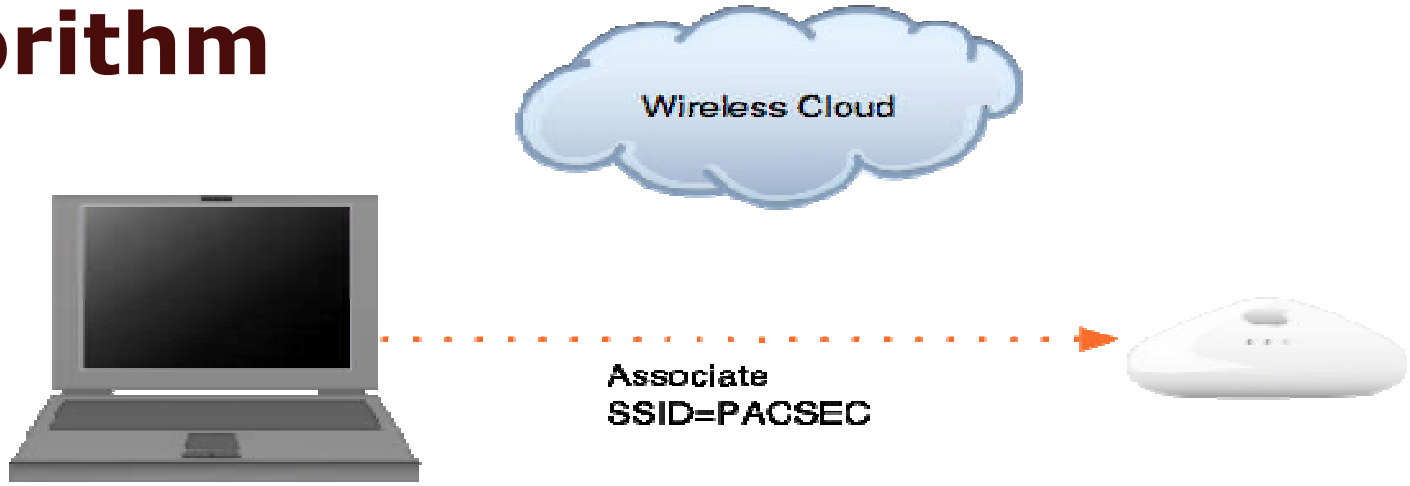


- **If Probe Responses are received for networks in preferred networks list:**
  - Connect to them in preferred networks list order
- **Otherwise, if no available networks match preferred networks:**
  - Specific Probe Requests are sent for each preferred network in case networks are “hidden”

Wireless Auto Configuration Algorithm

- **If still not associated and there is an ad-hoc network in preferred networks list, create the network and become first node**
  - Use self-assigned IP address (169.254.Y.Z)

Wireless Auto Configuration Algorithm

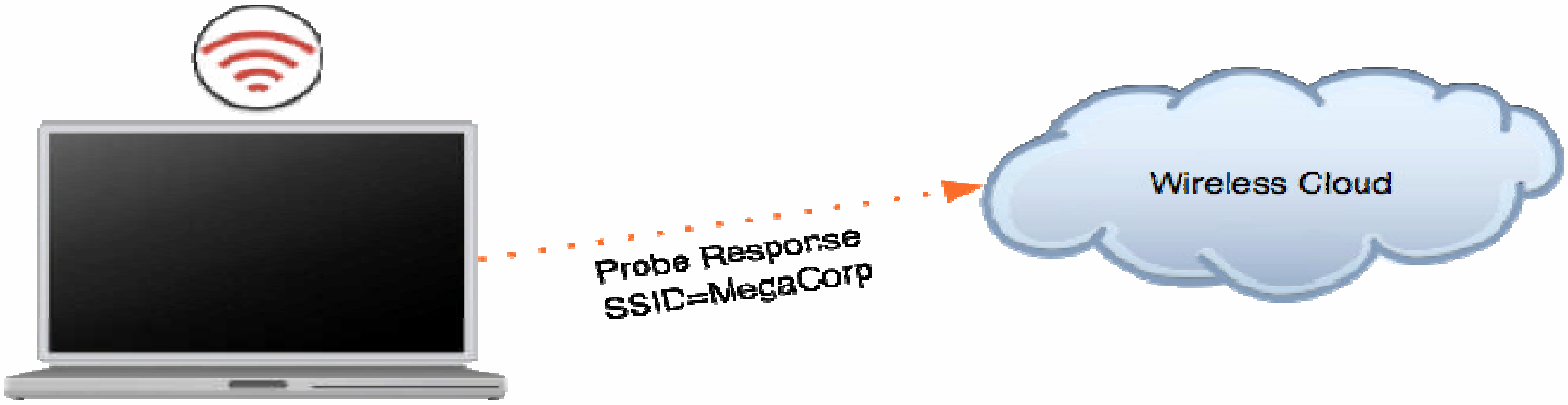


- **Finally, if "Automatically connect to non-preferred networks" is enabled (**disabled by default**), connect to networks in order they were detected**
- **Otherwise, wait for user to select a network or preferred network to appear**
  - Set card's SSID to random 32-char value, Sleep for minute, and then restart algorithm

Attacking Wireless Auto Configuration

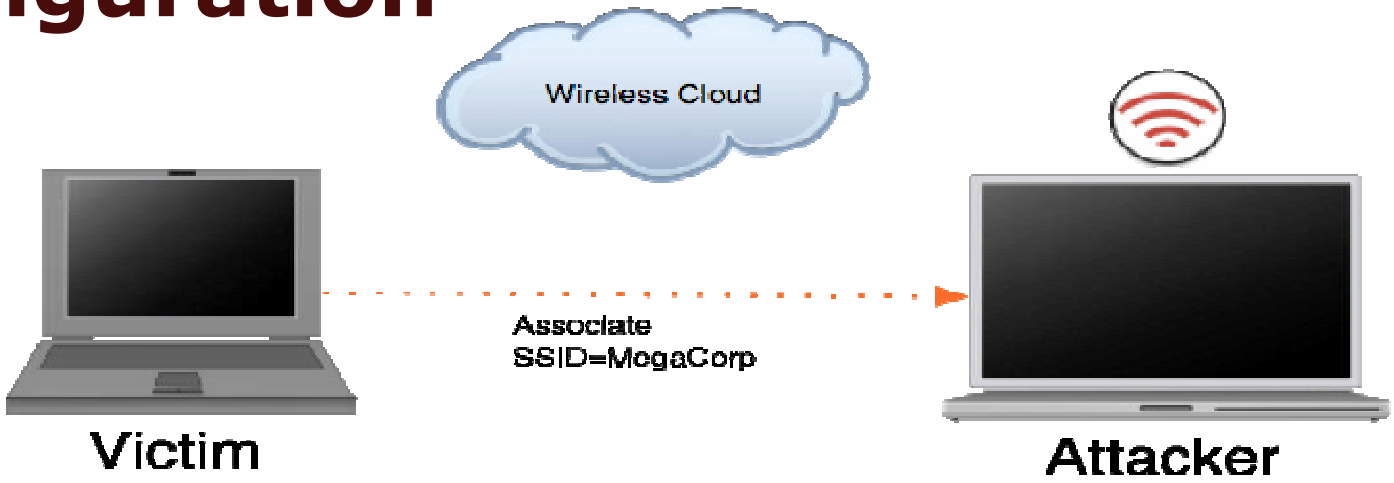
- **Attacker spoofs disassociation frame to victim**
- **Client sends broadcast and specific Probe Requests again**
  - Attacker discovers networks in Preferred Networks list (e.g. linksys, MegaCorp, t-mobile)

Attacking Wireless Auto Configuration



- **Attacker creates a rogue access point with SSID *MegaCorp***

Attacking Wireless Auto Configuration



- **Victim associates to attacker's fake network**
- **Attacker can supply hostile DHCP, DNS, …, servers**
- **Attacker is on same subnet as victim and controls DNS, all hostile web pages run in IE Local Intranet Zone**
  - Much larger attack surface with ActiveX
  - NTLM authentication is performed automatically

KARMA Current Status

- **Wireless auto configuration algorithm weaknesses addressed in:**
  - Windows Vista
  - Windows XP SP3
  - Wireless Client Update For Windows XP SP2
- **KARMA is currently not maintained, but will receive updates soon**
- **Stay tuned for KARMetasploit, BackTrack LiveCD**
- **Get KARMA at http://www.theta44.org/karma**

Wireless Client Recommendations

- **Use Vista, XP SP3, or apply Wireless Client Update For Windows XP SP2**
- **Clean out Preferred Networks List immediately after using a hotspot network**
- **Ensure that PNL has all encrypted networks in it**
- **Don’t let wireless clients connect directly to internal network or VPN onto internal network**

Network Access Control

- A security technology in search of a use case
- Are you letting non-company laptops connect to your internal network, even if they do have patches and anti-virus?
- … And you are deciding this based on a client-side agent?
- … And all hosts that fail the checks are put on the same quarantine network?

Network Access Control

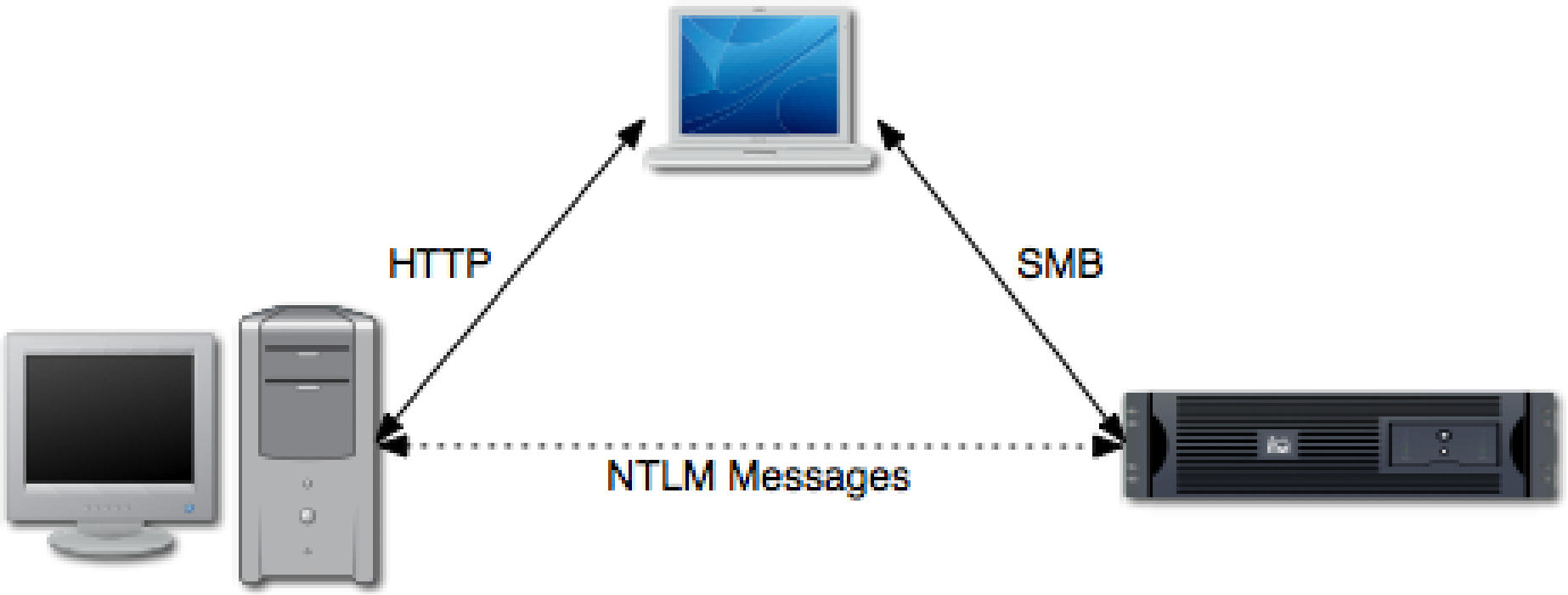
- **There is a common theme here…**
  - Deliberately fail NAC checks
  - Attack other machines in NAC quarantine network
  - They are already known to be *vulnerable*
  - Let compromised machine join secure network, attack from within
- **Recommendations**
  - Don’t let any unknown machines connect to internal network
  - Require host domain authentication at minimum
  - Use per-host isolation on quarantine network

Attack From the Inside

NTLM Authentication Protocol

- **Integrated Windows Authentication for Single-Sign-On used in SMB, HTTP, ...**
- **Challenge/Response protocol messages:**
  - Type 1: Client -> Server
    - Requested/supported feature flags
  - Type 2: Server -> Client
    - Required/supported feature flags, challenge text
  - Type 3: Client -> Server
    - Challenge-response
    - Differs among NTLMv1, NTLMv2, NTLM2 Session
- **NTLM tokens are embedded into other protocols**
- **Problem: Opaque Tokens are passed to LSASS**

NTLM Cross-Protocol Relay



Cross-protocol NTLM Auth Relays

- **Any protocol that supports NTLM is a potential source or target of NTLM challenges/responses**
  - SMB, MSRPC
  - HTTP, Exchange IMAP/POP3/SMTP
  - SQL Server TDS, AuthIP extensions to IPSec IKE
  - …
- **NTLMSSP messages are not bound to the hosts they are to/from**
  - Problem: Application knows target, LSASS knows password
- **Examples: jCIFS explorer servlet, Metasploit**

jCIFS Network Explorer Servlet

- **jCIFS Network Explorer Servlet browses windows network file shares using remote user's NTLM credentials**
- **Modify servlet to authenticate to hard-coded servers and hold onto connections after authentication**
- **Run servlet anywhere and inject IFRAMEs on internal blogs, wikis, sharepoints, to it**
- **This attack can also be done through remote TCP port forwards on any internal host**
  - Possible from within low-integrity IE7 process on Vista

Metasploit SMB NTLM Relay

- **Accept SMB connection from victim**
  - Receive NTLMSSP Type 1 message
- **Connect back to same host SMB port**
  - Send received Type 1 message, receive Type 2
- **Relay Type 2 to victim, receive Type 3**
  - Send received Type 3 message to authenticate as victim
- **Upload payload as EXE file**
- **Start EXE file as service using SCM RPC**
- **Requires victim to be local admin**
- **Windows XP SP2 / Server 2003 SP1 "loopback detection" is ineffective**

Cloud Computing

- **On-demand, scalable, processing and storage infrastructure from the "cloud"**
- **Popular for Facebook applications and other Web 2.0 startups**
- **Solve the user explosion problem through (sometimes automatic) dynamic horizontal scaling**
- **Examples:**
  - Amazon Web Services
  - Google App Hosting
  - 3Tera
  - Joyent

Amazon Web Services Prices

- **Amazon Elastic Compute Cloud (EC2)**
  - 1 EC2 Compute Unit @ $.10/hour (Small)
  - 4 EC2 Compute Unit @ $.40/hour (Large)
  - 8 EC2 Compute Units @ $.80/hour (Extra Large)
  - Default quota is 20 simultaneous instances
- **Amazon Simple Scalable Storage (S3)**
  - $0.15 per GB-Month of storage used
  - $0.100 per GB - all data transfer in
  - $0.170 per GB - first 10 TB / month data transfer out
  - $0.01 per 1,000 PUT, POST, or LIST requests
- **A real attacker's botnet is cheaper and faster**

Cracking Passwords for 2 Cents

- **John the Ripper cracks Windows LM hashes @ 6666K cracks/sec per 2 EC2 Compute Unit core**
- **Using 20 large instances:**
  - Alphanumeric in 4.83 minutes costs $.02
  - Alphanumeric + 16 symbols in 64 minutes costs $16.00
  - Any printable ASCII in 72 hours costs $232.00
- **Storing Rainbow tables is also cheap**
  - Alphanumeric is 703MB, $.10/month
  - Alphanumeric + 16 symbols is 7.5GB costs $1.12/mo
- **Cracking attacks also apply to Kerberos Preauthentication data**

LM/NTLM Security Recommendations

- Consider unsalted password hashes equivalent to the passwords themselves
- Disable use of LanMan hashes (LMCompatibilityLevel > 3)
- Log onto domain using UPN (*username@domain.com*) to force Kerberos
- Configure IPSec "Secure Server" policy to force client to authenticate to domain before communicating with server
- Smart Cards use stronger preauth data

Conclusions

- **Know the limitations of any security solution**
  - What does it prevent? What *doesn't* it prevent?
- **Defense in depth and diversity are key**
  - NAC at internal perimeter + hardened internal server DMZ
  - One Active Directory forest == single point of security failure
- **Maintaining a strong network perimeter is not enough**
  - Firewalls, IDS, etc are necessary, but so 2003
  - Client apps, web applications, and mobility are the new challenges
- **Cheap grid computation and storage changes attack economics drastically**
  - Can we stop using passwords yet? I want smart card SSO