SECURE® COMPUTING

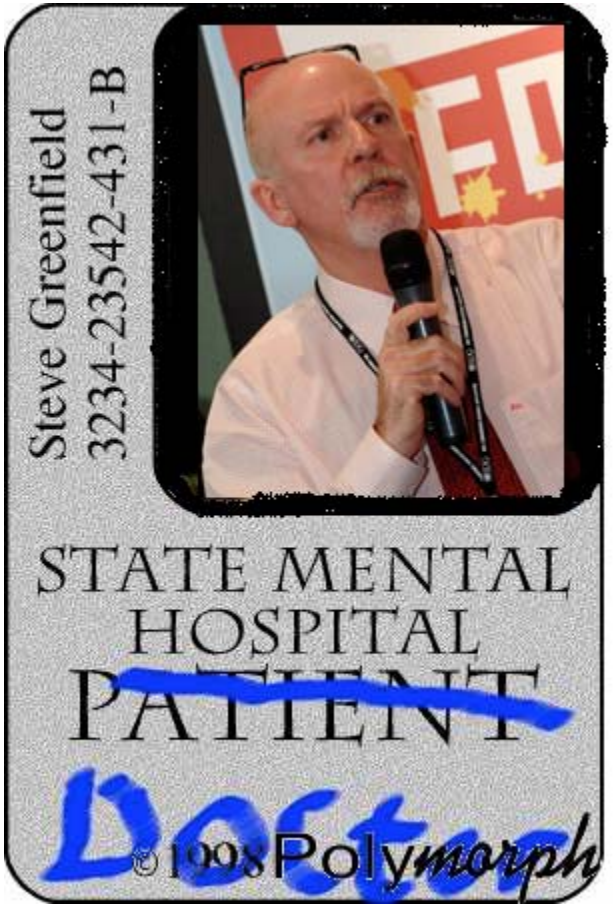
Evolution Of The Need For IAM

Evolution Of The Need For IAM

- **Identity issues are nothing new**

Who steals my purse steals trash… / But he that filches from me my good name / Robs me of that which not enriches him / And makes me poor indeed.
-William Shakespeare

Evolution Of The Need For IAM



- **The Internet has made forging identity trivial**

Evolution Of The Need For IAM

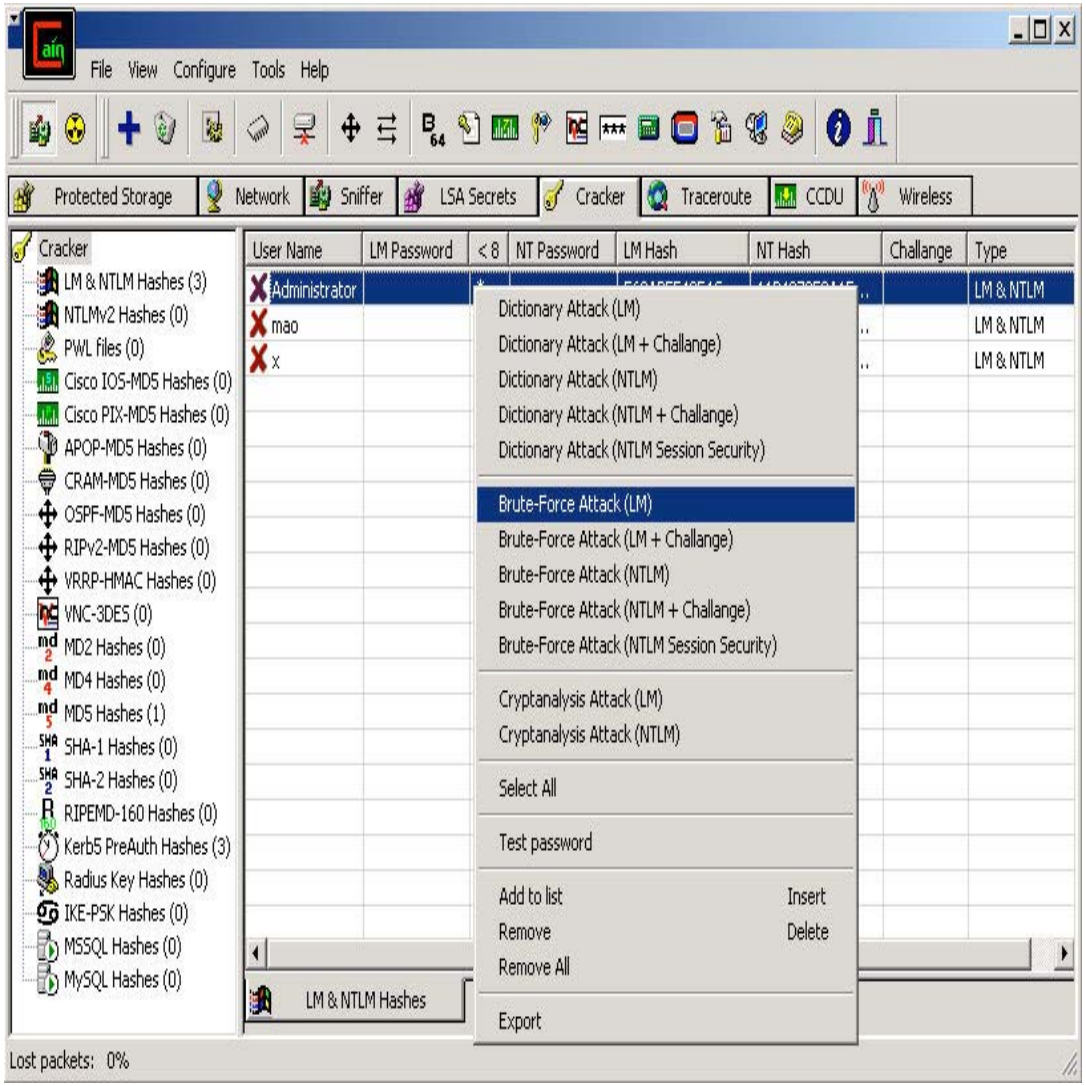
Evolution Of The Need For IAM

- **Current single factor access controls for our computers and networks have left us critically vulnerable**

- ***"There is no doubt that over time, people are going to rely less on passwords. People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure"***

Bill Gates

Evolution Of The Need For IAM



Evolution Of The Need For IAM

- **Rainbow Tables**
  - Pre computed hashes for every possible combination of letters, numbers and symbols
  - Perfect in a Windows environment
  - Has also been implemented for MD5 Hashes

Evolution Of The Need For IAM

- **Biometrics are great because they are really hard to forge: it's hard to put a false fingerprint on your finger, or make your retina look like someone else's. Some people can mimic others' voices, and Hollywood can make people's faces look like someone else, but these are specialized or expensive skills. When you see someone sign his name, you generally know it is him and not someone else.**

http://www.schneier.com/crypto-gram-9808.html

Evolution Of The Need For IAM

- **Biometrics are lousy because they are so easy to forge: it's easy to steal a biometric after the measurement is taken. In all of the applications discussed above, the verifier needs to verify not only that the biometric is accurate but that it has been input correctly. Imagine a remote system that uses face recognition as a biometric. "In order to gain authorization, take a Polaroid picture of yourself and mail it in. We'll compare the picture with the one we have in file." What are the attacks here?**

http://www.schneier.com/crypto-gram-9808.html

Evolution Of The Need For IAM

- **Compliance is not just a "legal" matter it is now a critical business function**
  - Authentication management
    - Who are you?
  - Centralized policy-based authorization management
    - What can you do?
  - Auditing and reporting
    - What did you do?

Evolution Of The Need For IAM

Management Issues

- **Decentralized Authentication & Authorization**
  - Difficult to manage across multiple servers
    - Adding a new user across multiple systems
  - Prone to error
    - To many administrators
  - Prone to privilege escalation attacks
    - Exploit the weak link
  - Slow to revoke privilege
    - Each separate system needs to be touched
  - Can the person requesting access also be the person granting access?

Evolution Of The Need For IAM

Reporting Issues

- **Most systems are proprietary**
  - Increases value for the vendor
  - Does not play well with others
- **No system wide view across disparate systems**
- **Lack of shared standards across vendors**
  - Industry wide problem
- **Creating reports manually is prone to error**

IAM Expectations

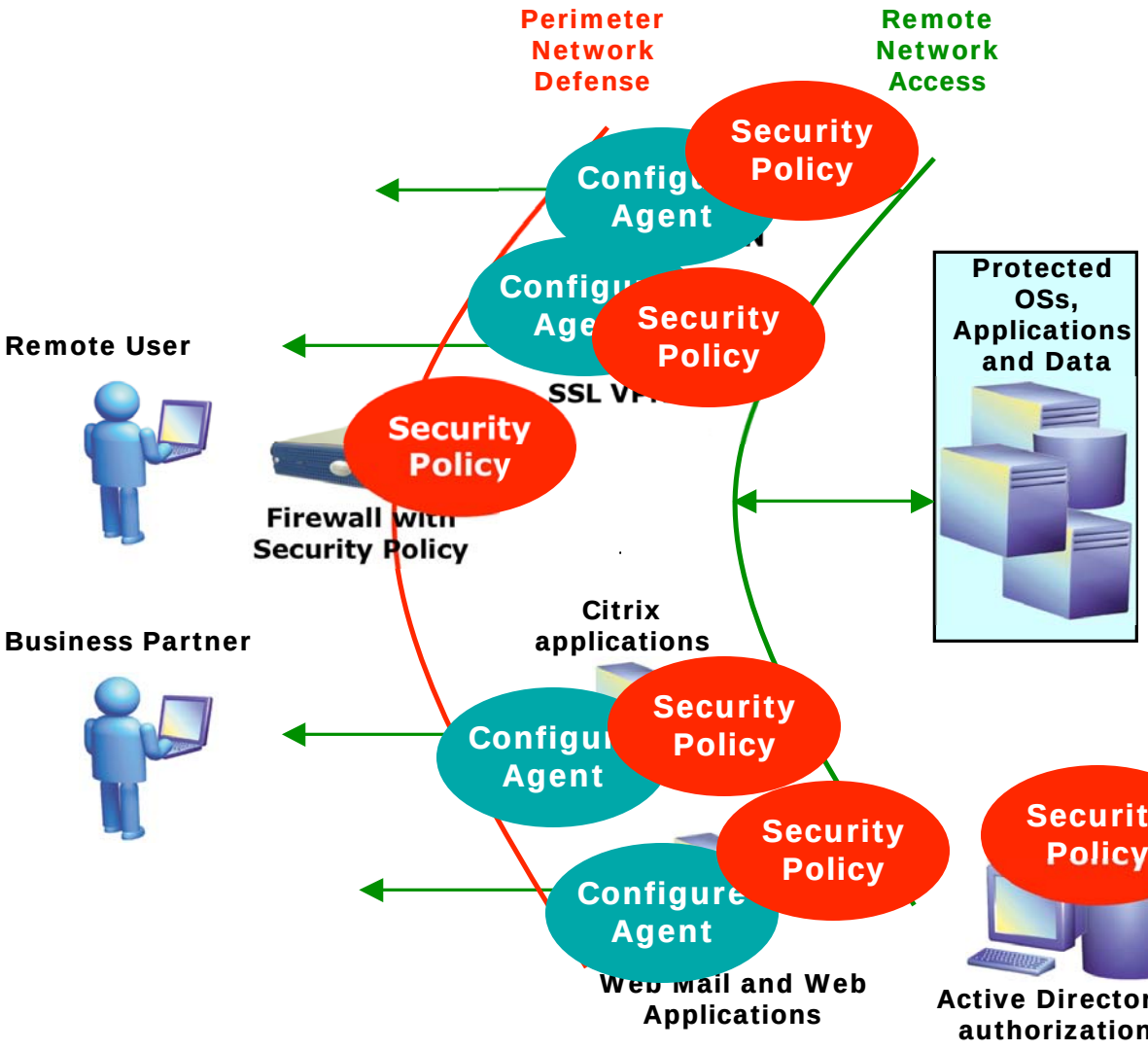
- Improved Security
- Improved Regulatory Compliance
- Better IT Department Efficiency
- Cost Reduction

Improved Security

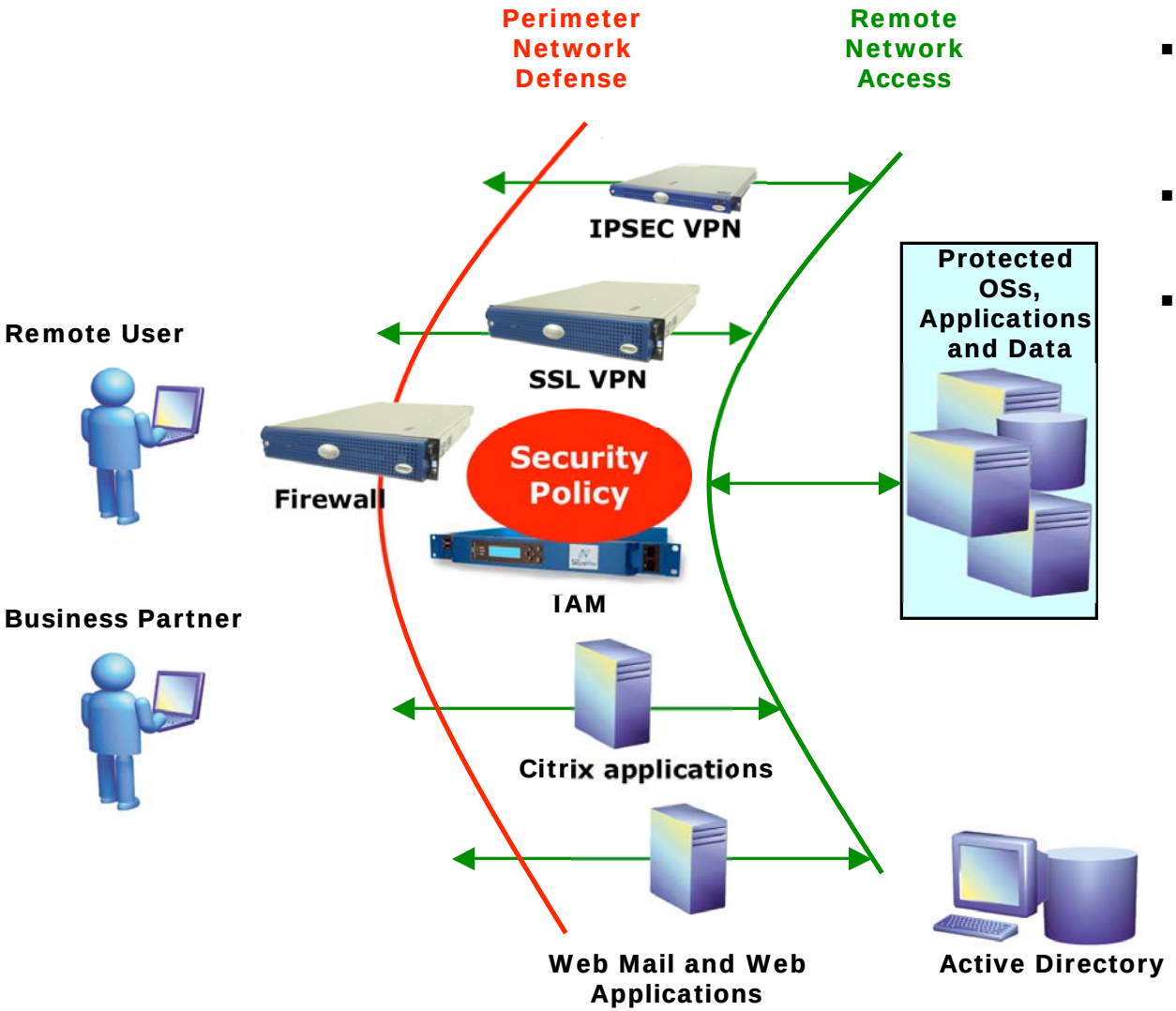
- **Two factor authentication**
  - Tokens
  - Smartcards
  - Biometrics
  - Other out of band solutions
- **Use of device can be determined by where the user is authenticating from and what the user wants to do**

Improved Security

- **Centralized policy**
  - Who can go where
  - Who can do what
  - Single point for policy management
    - Reduces errors



- Requires complex setup of many access points
- Different types of access require separate servers
- Authentication requires agent configuration
- Changes to security policy require multiple points of change



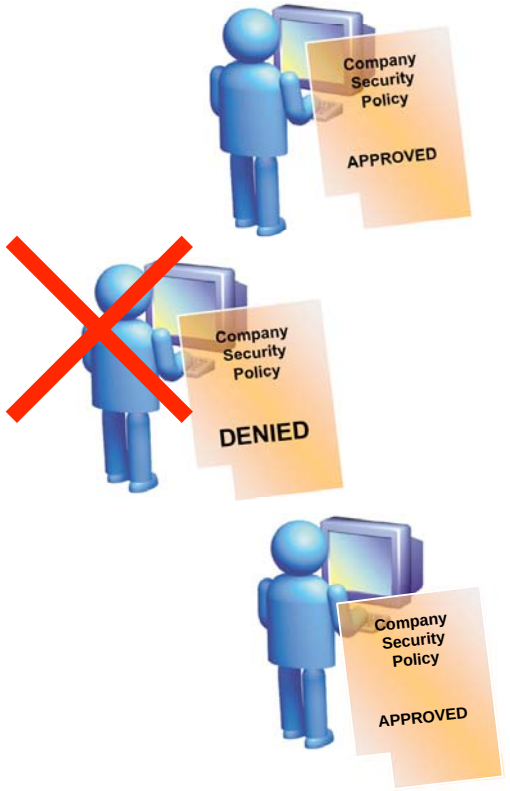
- **Host many different types of access on a single IAM solution**
- **Change policy once and you're done!**
- **Authentication works out of the box; no agents to configure**

Improved Security

- **Enforcement with Security Zones**
  - Segments the network into Security Zones
  - Access is limited to certain resources based on authority
  - Only properly identified, authorized users can access
    - Example: Mission-critical resources only accessible when connected from corporate LAN
    - Example: Remote usage may be limited, except for users with two-factor authentication
  - Security Zones require no additional reconfiguration of the network infrastructure

Improved Security

- **End point security and configuration compliance**
  - Antivirus
  - Firewall
  - Patches



Improved Security

- **Resources protected**
  - Web: HTTP, JavaScript, WebDAV, ActiveX
  - File: CIFS, NFS,DFS
  - Mail: IMAP, POP, SMTP, MAPI (MS exchange)
  - Terminal Services: Citrix, Windows, VNC
  - Host Access: Telnet, SSH, Mainframe (3270 – 5280)
  - Client/Server: All client server applications, TCP/UDP, static port, dynamic port

Improved Security

- **Deployment**
  - SSL VPN
  - IPSec VPN
  - Remote extranet
  - Department firewall
  - Intranet
  - Guest network

Improved Security

- **Meets the four "As" of Information Security**
  - Authentication
  - Authorization
  - Administration
  - Audit

Improved Regulatory Compliance

- **Rather then attempting to drill down in to each regulation we will examine a short list of common denominators across numerous regulations:**
  - Creation of new policies
  - Implementation of new processes
  - Audit trail
  - Granular reporting

Improved Regulatory Compliance

- **Creation of new policies**
  - Single policy management point simplifies policy creation and deployment
    - Change control is another serious consideration
      - It is an achievable reality in IAM but can be a nightmare without it, when working across several policy enforcement points

Improved Regulatory Compliance

- **Implementation of new processes**
  - Simplifies deployment of new processes
    - New audit processes are dramatically simplified due to centralized auditing capability of IAM
    - New business processes are dramatically simplified due to centralized authentication, authorization and access control capabilities within IAM

Improved Regulatory Compliance

- **Audit trail**
  - Audit: source IP, userID, Group, Timestamp, resource accessed (URL, destination IP,file accessed), status, bytes, referrer, authentication method, logins/logouts

Improved Regulatory Compliance

- **Logging and reporting**
  - Events: Intrusion, denied resource attempts, security alerts with SNMP traps, Syslog, FTP or SCP transfer log, custom reporting

Better IT Department Efficiency

- **Single point of policy management across all access points**
  - Greatly increases administrative efficiency
- **Depending on authentication mechanism chosen can reduce if not eliminate password resets**
  - Typically 30% of helpdesk calls are password related
- **Automated reporting**
  - Reduced administrative burden for report consolidation

Cost Reduction

- **Single point of policy management and reporting can dramatically reduce costs**
  - Consolidation of disparate access control mechanisms across multiple access points to a single device for:
    - Provisioning
    - Authentication
    - Authorization
    - Audit
- **Single Sign On / Reduced Sign On**

SECURE®
COMPUTING

Questions?

SECURE® COMPUTING

Thank You

I trust you found today's presentation both interesting and informative

paul_henry@securecomputing.com