





TOC

- President and Founder of encryptX Corporation
  - Over 10 million end users of encryptX desktop encryption and content management solutions
  - Corporate customers include: IBM Corporation, Nomura Securities, First Northern Bank, International Strategy & Investment Corp., Camelot Group, Kettering Medical Centers, Japan Communications Inc., States of NY and Georgia
  
- 10 Years as a Cryptologist & Computer Intelligence Analyst assigned to the National Security Agency
  
- Designed and verified trusted computer systems for DOD, FEMA, and other Federal Government agencies
  
- Ran sales and marketing for consumer information data provider (RL Polk Consumer Information Services)
  - Sold to Equifax in 2000
  
- Ran marketing strategy company that launched InterTrust Technologies (Consumer DRM market leader) into the market



# Trusted Computing System and Encryption Basics

# Trusted Computer Systems

- **Initial Standards “The Rainbow Series”**
  - Developed in the late 1970s – early 1980s at the National Security Agency
  - Series of government standards on how to build and verify trusted computer systems, networks, password management, audit, data protection
  - Classified government computer systems were built on these standards
  - Accreditation criteria for evaluating trust level of computer systems
  
- **Morphed into a series of commercial standards from the National Institutes of Standards & Technology (NIST) for commercial systems**
  - FIPS 86-1977 (DES)
  - FIPS 140-2
  - Common Criteria Certification

# Trusted Systems

- **Key foundational elements include:**
  - Identification and authentication
    - Mandatory Access Control
    - Discretionary Access Control
  - Password Management
  - Separation of Security Features from Standard Administrative Features
  - Trusted labeling of protected data objects
  - Identified and enforced security policy
    - Rules that govern what users can access which objects
  - Auditing – ability to track what actions users have taken in a tamper proof manner
  - Continuous protection
    - Throughout the system and data lifecycle
  - Encryption

# Encryption

- **Simplest trust based technique to obscure protected information**
- **Intelligible text (plaintext in crypto terms) is made unintelligible (ciphertext in crypto terms) using a secure key**
- **The security of the ciphers reside in the key length and decryption process is difficult without proper knowledge of the key.**
- **Key drivers have been**
  - Threats to Data and Information from Hackers and Malicious Users
    - Data In Motion – communicated in email, Internet
    - Data at Rest – stored data on local hard drives, file servers, etc.
  - Need for faster and more powerful cryptographic algorithms caused by Moore's law
    - Key Life Cycle – computing power advancements has increased risk in using short cryptographic keys
    - Algorithm Life Cycle – advancements in mathematical research can increase risk to existing algorithms
  - Vendor and Product Lifecycles
    - Market dynamics, mergers have eliminated/changed support for some products
      - Cylink (acquired by SafeNet)
      - RSA SecurPC file & folder encryption not supported on Windows XP
      - Cracking of Proprietary algorithms (RC4 – RC5)

# Encryption Standards

- **1977 Data Encryption Standard (DES)**
  - Developed by IBM, published as standard by National Bureau of Standards
    - Fixed  $2^{56}$  key size and  $2^{64}$  data block
    - DES Challenge Results (1977)
      - 10,000 workstations in collaboration could discover key in 140 days
    - DES Challenge Results (1999)
      - Key discovered in just over 22 hours
  
- **1998 Triple DES Published**
  - Cleartext is encrypted first time with one key, decrypted with second key, and encrypted again with third key to create ciphertext
  - X9.52 Standard
  
- **2001 Advanced Encryption Standard (AES) published**
  - Rijndael algorithm was selected in various longer key strengths
    - AES 128, 192 & 256
  - Designed to resist timing analysis, power analysis attacks
  - Low memory requirements (can be used with Smart Cards)
  
- **2005 FIPS 46-3 DES Officially Withdrawn**

# Symmetric & Asymmetric Encryption

## ■ Symmetric Approaches

- Encryption system in which the same key that is used to encrypt the data is used to decrypt the data
- Known as “Shared Secret” method
- Key is exchanged or shared with recipient “out of band” with data transmission to allow data to be decrypted
  - Phone call, separate email, etc.
- Key exchange method used is the biggest weakness
- Symmetric encryption is ideal for bulk encryption of large quantities of data

## ■ Asymmetric Approaches

- Encryption system that uses two different keys – a public key known to everyone and a private key known only to the recipient of the data
  - Data is Encrypted with the Public Key of the Intended Recipient
  - Recipient Actually Decrypts the Data with a Private Key
  - Public and Private keys are a matched set
  - Extremely difficult to deduce Private Key from the Public Key
- Known as Public Key Cryptography (PKI) or Diffie-Hellman (authors)
- Best known commercial variant is RSA
- Biggest weakness is complexity in setting up, managing and finding user’s public keys for encrypting content
- Asymmetric encryption is not efficient for encrypting large quantities of data – best for short messages because it is computationally demanding
  - Recommended key length is 1024 bits

# Other Encryption Methods

## ■ Elliptical Curve Cryptography (ECC)

- Public key method – picks point on an Elliptic curve using a Random Number Generator (RNG)
- Power of algorithm allows for smaller keys – benefit in hardware constrained environments
  - ECC Key Size = 256 bits
  - RSA Key Equivalent Size = 3072 bits
- Generally used in combination with AES
  - ECC for key agreement and digital signatures
  - AES for bulk encryption of data

## ■ Identity Based Encryption (IBE)

- Public key method wherein any valid string can be used to create a public key – uses ECC methods
- Public key is created dynamically using recipient identity characteristics (e.g. email address dduncan@encryptx.com)
- Advantages are
  - Recipients don't need to have prior Public Key
  - No need to interface with Certificate Authorities (central organizations that require digital certificates and unique key publication and management processes)
- Disadvantages are
  - Need for key server that maps user identities to decryption keys
  - Authentication of the recipient to the key server to receive private key can be spoofed

# Hashes & Digital Signatures

## ■ Hashes

- One-way functions that compress arbitrary length strings into fixed short strings (message digests)
- Hash Functions can be designed using block ciphers using a secret key as a parameter along with the message that has to be hashed
- Examples - MD4, MD5, SHA-1, SHA-2, SHA-3, ....

## ■ Digital Signatures

- Proves the identity of the sender of the message
- Simplest method
  - Send a random message as plaintext and ciphertext
  - Recipient deciphers ciphertext using public key
  - If two versions match – proves that the sender was in possession of the private key
  - Only verifies the validity of the signature itself – NOT any message to which it has been attached
  - Alternative form uses a Hash function to create a message digest from a message to verify the source of the actual message
- Examples – PGP, RSA, ECC

# NIST SP 800-57 Part 1

CRYPTOGRAPHIC STRENGTH	SYMMETRIC ALGORITHM	HASH ALGORITHM	ELLIPTIC CURVE ASYMMETRIC ALGORITHM	RSA/DSA/DH ASYMMETRIC ALGORITHM
56 bits	DES	-	-	-
80 bits	3DES (2 key)	SHA-1	160 bits	1024 bits
112 bits	3DES (3 key)	SHA-224	224 bits	2048 bits
128 bits	AES-128*	SHA-256	256 bits	3072 bits
192 bits	AES-192	SHA-384	384 bits	7680 bits
256 bits	AES-256*	SHA-512	512 bits	15360 bits

- Provides general guidance and best practices for cryptography
- Recommends that comparable strength functions are used in sets
- NIST Recommends 128 Bit Key Sizes for Sensitive But Unclassified Information
- NIST Recommends 256 Bit and Above Key Size for Classified Information

- **Suite B was Announced by The National Security in February 2005**
  - New standard for information security best practices
  - Specifies matched algorithms to be used in conjunction with each other per NIST SP 800-57
  - Neither SHA-1 or DES are considered strong enough
  - Algorithms are all unclassified and exportable
  - Well suited for dual-use military and high assurance commercial implementations
  - Approved for multinational information sharing with US allies, federal, state, local agencies, Homeland Security
  - No certification standards as of yet
  - Most commercial products use mismatched cryptographic algorithms
    - Bank vault with a glass door analogy

- **US and Canadian government standard**
- **Validates claims of products using cryptography against NIST standards**
  - A form of the early Rainbow Series certification process from the NSA
  - US and Canada government purchasing agents **MUST** purchase FIPS 140-2 certified products over non-certified products
- **Multiple levels of certification**
  - Level 1 – Software and firmware encryption on non certified Operating System (software based implementations)
  - Level 2 – Adds role based authentication, tamper evidence (software and hardware combination implementations) on certified Operating Systems
  - Level 3 – Adds identity based authentication, tamper detection/response mechanisms, trusted paths (hardware based implementations)
  - Level 4 – Production grade, tamper attempt self hardening, self destruct of crypto modules (hardware based implementations)
- **Evaluation criteria includes**
  - Basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference/ electromagnetic compatibility & self-testing
- **Expensive and time consuming process**
  - Level 1 is minimum 6 months and \$100k
  - Level 3 is minimum 12 months and \$300k or more
  - Key issue is limited number of independent labs that are certified to perform evaluations



## **Advancements in Trusted Computing for the Commercial Sector – Towards Active Policy Management**

TOC



- **Most CIOs have limited understanding of the locations and users that have access to sensitive information**
  - CIO Magazine annual study reports that 2/3 of sensitive information is outside the control of the “glass house”
  
- **Information has a lifecycle – that maps to security principles**
  - Data that is new and fresh is typically more sensitive (e.g. new competitive analysis, business plans, project plans)
  - Data this is older and is in archive form is typically less sensitive
  - The author is typically fully trusted whereas users of that information may have limited rights
  
- **Encryption alone provides a false sense of security because**
  - It only enforces Mandatory Access Control – access to data through a password
  - Does not enforce Discretionary Access Control – what rights you have to access the data (e.g. can you copy, share, print)
  - Is typically point to point – not continuous protection
  - Continuous protection and Discretionary Access Control are provided by **Digital Rights Management**

# Business Problem

## “The Perfect Storm”



TOC

- Email now predominate method of business communication
- 80% sensitive data shared through email
  - IP, Financials, HR, Product Designs, Customer Data
- Distributed and Mobile
  - 2/3 all sensitive corporate data on individual user PCs
  - Financial Services
    - Distributed field agents and brokers
  - High-Tech & Manufacturing
    - Off-shore developers, channel partners

- Pharmaceutical
  - Cross-facility Intellectual Property

- Inappropriate internal email in regulated industries (e.g. brokerage firms)
- Proliferation of instant messaging & web email
- Unsecured & unsupervised collaboration with users “outside the organization”
- Contractors repurposing IP
- Attrition
- Lost or stolen laptops

- SEC/NASD 17a-4, 3010, 2711
- Sarbanes-Oxley
- HIPAA
- CA SB 1386, AB 1950

# What Threats Heighten Awareness?

## ■ Internal/Employee

- Majority of losses are not malicious
- Apathy, careless behavior
- Lack of policy enforcement, security policy education
- Repurposed IP
- Theft

## ■ External

- Breaches
- Hackers, worms, etc.
- Business partners

*Laptop stolen at university,  
over 98K SSN's exposed*

*-March 2004*

*Bank backup tapes lost  
risking 1.2M transactions*

*-Feb 2005*

*1 out of every 500 emails  
contains consumer privacy  
information* -2005 Aberdeen Report

*75% of most companies' IP  
is contained in email*

*-Enterprise Strategy Group*

- **Centralized Document Management Control Model**
  - Designed to restrict sharing and collaboration
  - Examples
    - Document Management Solutions
    - Thin Client Solutions
  - Encrypt and lock content to controlled file servers inside the glass house
  - Enforce Mandatory and Discretionary Access Controls
  - May allow some type of offline access through local client software component
  - Makes remote data access and collaboration difficult for remote/mobile users
  
- **Result = users actively try to circumvent these systems and/or complain enough that deployment is limited to niche data (e.g. financial information)**
  - “The Abstinence Method”

## ■ Point Based Protection Model

- Examples
  - Self encrypting hard drives,
  - Encrypted file systems,
  - Gateway to gateway email encryption
- Fail to address the fact that data is in motion and has many users, many localities and is communicated frequently through numerous methods
- Is not conditional based on role of user, stage of information lifecycle, Discretionary Access Control rights
- If you have the password you can do anything you want.

## ■ Result = sensitive data leaks

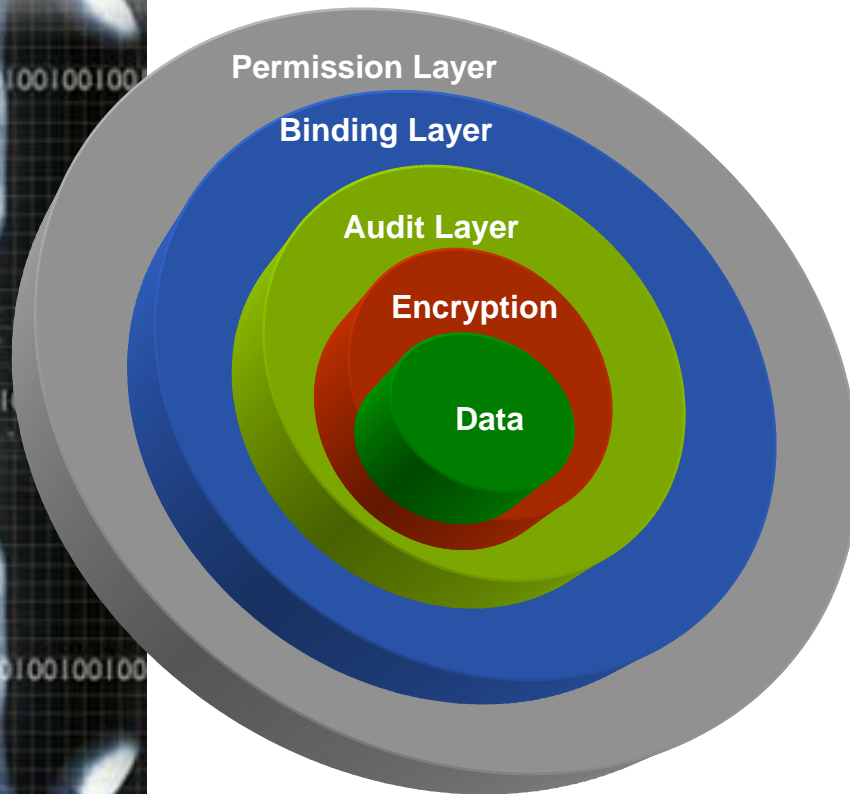
- “The Calendar Method”

# Digital Rights Management

## ■ Digital Rights Management

- The “Data Condom Method”
- Enforces Discretionary Access Control through data wrapping
  - Encapsulates data in DRM digital envelope that enforces unique DRM controls based on user, device, network, role
  - Can be used for Data in Motion and Data at Rest
- Restricts the types of operations you can perform on data and information based on your unique rights
  - Your role (executive, sales, technical support)
  - The device you are operating on (e.g. desktop, PDA, etc.)
  - Network connectivity (LAN, remote SVPN, disconnected)
  - Your role to the data (author, editor, reviewer, consumer)
  - Wrapper contains information on your unique usage rights to the information
  - Typically provides audit trail information on what operations you are performing
- Key Issue with DRM is it is difficult to set up systems and requires lots of manual updating of systems to ensure data is protected
- As a result early DRM deployments were largely confined to Publishing Industries

## Digital Rights Management Wrapper Approach



- **Optional Permission layer enforces user rights to email and attachments**
  - Can copy, decrypt, share with others, add, delete, view, print, copy, paste, time expire, restrict sharing
- **Binding layer locks email and attachments to PC**
- **Audit layer tracks user activity**
- **Encryption layer scrambles data**
  - Non-proprietary encryption algorithms are used
- **Data is not modified at all – it is encapsulated in the control mechanism**
- **As much or as little control as is specified – encryption and password only to full digital rights management**
- **Allows online and offline access to protected content**

# Addressing the Problem

## ■ Content Scanning Technology

- Scans digital information and extracts text on HDD and in electronic communications
- Parses text data chunks into individual words, phrases, numbers and patterns
- Compares data chunks to pre-defined words, phrases, patterns, numbers, that represent potential protected information
- Compares protected potential information data chunks to additional user event based information
  - User action - read, write, copy, print, email, ftp
  - User role – executive, group membership (e.g. finance)
  - Recipient – if information is being shared electronically also attempts to determine user role and organization
- **Surveillance Mode** – provides reporting and alerts to higher level authorities
- **Active Policy Management Mode** – enforces security policies over sensitive information at rest or in motion

# Active Policy Management

- **Is a broad term used to describe the ability to**
  - Automatically and persistently control digital communications and data
  - Based on organizational and regulatory compliance and organizational information security policies
  
- **According to the Radicati Group is a new generation of compliance and security technology**
  
- **Moves the industry from after the fact compliance review and surveillance to**
  - AUTOMATICALLY preventing unauthorized user data access
  - AUTOMATICALLY preventing sensitive information from being shared electronically
  - AUTOMATICALLY enforces encryption and Digital Rights Management

## Key Drivers for APM

- **The average corporate user sends & receives 60 messages per day (Radicati Group)**
- **1 in 4 outgoing emails contain content that poses a legal, financial or regulatory risk (Proofpoint May 2005 Study)**
- **Enterprise Strategy Group survey finding that 75% of company intellectual property is contained in messages and attachments sent through email systems**
- **More than 1/3 of enterprise organizations employ staff to review and analyze email for compliance**
  - 30,000 email reviewers are employed in financial services
    - Orchestria Study
- **Gartner Research predicts volume of business email will grow 25 – 30% through 2009**

## Active Policy Management (APM)

- **Enabled in next generation of compliance solutions for email, and instant messaging**
  - Automatically enforces appropriate email, IM communication and data security policies
  
- **Enabled in next generation of content scanning technologies for data on HDD, file servers, email and IM**
  
- **Reduces exposure that privacy protected data/files (e.g. transactional information, privacy information) will be compromised when used, backed up and shared**
  - Through automatic encryption and digital rights management

## APM Solutions for Data

- **Are focused on controlling access to sensitive data/files based on information security/privacy policies**
  - Encrypt data
  - Enforce digital rights
    - Edit, Read, Copy, Print, Time Expiration, Share
  - Provide audit tracking of user actions
- **Use one of 5 basic models**
  - Central document server – document management solution
  - Local PC policy driver – interacts with rules server to enforce controls over local PC & file server hosted files
  - Digital container/permission wrapper model – encapsulates protected data in digital security envelope
  - P2P – encrypted shared workspace on file server/HDD that is accessible by trusted users
  - Operating System – encrypted file system or HDD block encryption – auto encrypt content on the HDD

# APM Solutions for Email

- **Must have email SMTP gateway features**
  - Ability to redirect email, block email, auto attach pre-scribed disclaimers/warnings, auto-encrypt email before it leaves the corporate email gateway
- **Use content scanning/filtering engines**
  - Lexical analysis
  - Regular expressions
  - Document types
  - Must be able to scan all parts of email and all attachments
  - Should have ability to flag or set policy for email and attachments that cannot be scanned
  - Set scanning policy based on sender/recipient domains, groups
- **Allow multiple deployment models**
  - APM for selected users/groups (e.g. traders) or on per email domain basis
  - Surveillance monitoring (post email transmission) for other users (e.g. research analysts)
  - Variable sampling rates for reviewers assigned to different group

# APM Solution Summary

- **Email APM**
  - 3<sup>rd</sup> Generation Approach – new solutions allow email archiving, intelligent surveillance and APM controls
- **Instant Messaging APM**
  - 2<sup>nd</sup> Generation Approach – surveillance and review today after the fact – new solutions that allow interactive APM are on the horizon
- **Data APM**
  - Document Management – best for highly sensitive small pockets of protected information due to difficult access models
  - OS/HDD – best for protecting laptop contents if device is lost or stolen
  - DRM Wrapper – best for data that is being shared across networks/outside the organization with mobile/remote and external users
  - Policy Driver/Rules Server – best for internal users due to difficulty in installing drivers on host PCs

# Compliance and Security

- **Compliance and Security requirements are in conflict**
  - Need to encrypt customer specific/privacy data
  - Need to have pristine “in the clear” copies of email communications
  - How to share encrypted communications between companies that are both regulated?
  - Requires that recipient organization have the ability to decrypt the communication and archive per compliance regulations
  
- **Must have federated trust models**
  - Ability to encrypt and protected data during transmission and use
  
- **Maintain in the clear copies for compliance investigations for sender and recipient organizations**

# Trusted Computing Futures

- **Next generation security technologies must provide AUTOMATIC data and electronic communication protection through Active Policy Management features**
- **Will enforce organizational and regulatory security policies transparently and without user interaction**
  - Understanding of user action and role
- **Will integrate with compliance technologies (e.g. email archiving) and provide federated trust models to allow regulated data disclosure**
- **Will implement NSA Suite B “matched set” requirements for cryptographic primitives**
- **Will increasingly be certified using some type of standard (e.g. FIPS 140-2, Common Criteria)**
- **Cryptographic and certification standards will need to be increasingly agreed to across national boundaries**
  - To meet needs of multi-national corporations and organizations



TOC

**Questions?**