TRW Enterprise Directory And Security (TEDS) Services

Overview and Lessons Learned

Vincent McCullough
vincent.mccullough@trw.com
703-345-8644

TRW Global Network

- TGN
- 130,000 users in 40 countries
  - Space & Defense 29,000 users
  - Automotive 51,000 users
- Functions
  - Information dissemination (Web sites)
  - Information acquisition (e-forms)
  - E-mail (multimedia, enclosures, etc.)
  - Discussion Groups and Chat
  - Audio/Video and Teleconferencing
- Failings
  - Used Pretty Good Privacy (PGP) PKI
    - » Manually intensive, expensive (1 hour per employee per year)
  - Insufficient security given size and global reach of TGN

What were the driving requirements for PKI?

- "Lights out" operations
  - Less than 3 minutes per year per employee
    - » Totally automated except for very special cases
  - Down from 1 hour per year for typical PKI rollout
- Transparent and Ubiquitous
  - Every person with TGN access will have a certificate
    - » Employees, consultants, retirees, etc.
  - Virtually every server will be converted to SSL
    - » Static access lists
    - » Dynamic access rules (based on user attributes)
  - Certificates used for everything
    - » From ordering supplies to filling out time cards
  - Network failure must not cause TRW shutdown

How was the Phase 1 PKI implemented?

- Centralized Certificate Authority (CA)
  - Single, central online root certificate authority (self signed)
- Automated Registration Authority (RA)
  - Designed to reduce system administration workload
  - Provides increased assurance by automating registration processes
- "Virtual" RA Officers (RAOs)
  - RAO Identity verification process automated
  - Only two dedicated RAOs needed to operate the system
- Escrow-style Key Recovery Authority (KRA)
  - Requires two company officers to recover an encryption key
    - » HR and Legal
  - Signature keys never recoverable
    - » New signature certificate issued if needed
- Replicated Directory

What kinds of certificates were used?

- **All users have a signature certificate**
  - **Prevents “holes” in security**
  - **Certificate structure is the same, from President to Mailroom**
    - » **User ID is stored on certificate**
    - » **User attributes stored in directory server (*not* on certificate)**
- **Users who need them may also have encryption certificates**
  - **Obtained by using a signature certificate**
  - **Private key escrowed for recovery by owner or other authorized user**
- **Server signature certificates**
  - **Allows server-to-server and server-to-client authentication**
  - **Enables Extranet VPN functionality**
    - » **Employee access from customer sites**
    - » **Nested security enclaves**

How did a user obtain a signature certificate?

- Employee is hired
  - Credentials checked, payroll established
  - One of the most authoritative and audited internal functions
- New employee is entered into HR database
- Employee data automatically entered into directory server
- User attempts first access to Secured Network Resource
  - Sent to splash page telling user he or she needs a certificate
  - Certificate request is performed online
- One-time PIN and Password Generated
  - Impact printed on tamper-evident package
  - Dual Delivery
    - » Password sent to home address (from HR database)
    - » PIN sent via internal mail, or email if available
  - User can also go to security office, in cases of critical timelines

TEDS PKI

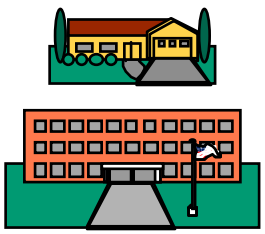
1. New employee, Alice, is entered into HR Database

2. Within 24 hours, Alice has an entry in the PKI LDAP server

3. When Alice first attempts to access any secured TRW web site, a “splash page” directs her to request certificates

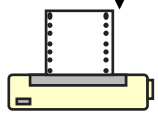
4. Alice supplies here employee number to the system which uses this number to retrieve address data from Alice’s directory record. An impact printer prints One-Time PIN and Password for Alice on tamper-evident envelopes

5. The Password is sent to Alice’s home address via U.S. postal service -- the PIN is sent to Alice’s office via internal mail

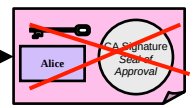


One-Time PIN

One-Time Password



6. Alice’s certificates are generated on her client, and provide only her ID, not her access privileges



7. If Alice wants to generate her certificates with a high degree of assurance,she generates certificates on a Smart Card or other hardware token

8. All certificates have the same structure -- it is the storage mechanism that determines the level of assurance

9. If Alice leaves the company, her certificate is automatically revoked and removed from the directory as a result of normal HR termination processing.

How were certificates expired and revoked?

- All certificates expire in one year
  - Users advised via email or surface mail that certificate is about to expire
  - Users return to RA website and replace expiring certificate.
    - » Authentication via expiring certificate.
- Removal of employee from HR databases deletes user certificate from directory server
  - Employment termination results in immediate loss of accesses
- CRLs generated but not used by internal web servers
  - Continued user access verified with via the directory
  - CRLs maintained for only for compatibility (if needed) with TRW partners
- Employee can revoke his or her own signature certificate
  - Then generate new signature using PIN and One-time Password scheme as before
  - No employee may have multiple signature certificates

How were private keys stored

- Private keys could be stored in one of three ways:
  - On the enterprise directory.
    - » Least secure method
      - Directory accessible to all TGN users
      - Keys are only protected by a single password.
    - » Intended for “factory floor” workers. Access to sensitive information severely limited
  - On a users PC:
    - » Better, but still vulnerable
      - Threat must have physical access to machine
      - Keys protected by login password(s), key store password
    - » Intended for average knowledge worker, greater access to sensitive data
  - On a hardware token
    - » Best, since user must possess token and know pass phrase
    - » Intended for use by those needing access to very sensitive data

What if a certificate is compromised?

- A user can revoke his or her own signature certificate and obtain a new one
  - Revoking a signature certificate requires the certificate to be revoked and a separate, long term password known only to the owner
  - Directory storage - If an employee believes somebody has “looked over his shoulder” to compromise his Password...
    - » Load the certificate and private key from LDAP server, decrypt using the storage password, then revoke certificate and request a new one
  - Hard Drive Storage - If an employee believes somebody has copied the encrypted certificate from his or her hard drive…
    - » Decrypt private key on hard drive using storage password, then revoke certificate and request new certificate
    - » Note that stolen certificate is useless without password
  - Token Storage - If an employee loses his or her hardware token…
    - » This is one of the “special cases” that uses some of those 3 minutes per employee per year
    - » Employee must contact RAO to have certificate revoked
    - » User must obtain a new token and start over (I.e., request a pin and password)

What kind of directory server used?

- **LDAP interface, but not necessarily X.500**
  - **Current X.500 does not provide for strong authentication and encryption of server**
    - » **X.500 servers may be vulnerable to insertion of phony entries**
    - » **Anticipate problem will be corrected in future versions of X.500**
- **Centralized server**
  - **Directory server will be replicated to improve network performance**
  - **Replication up-to-date within minutes, worldwide**
    - » **Replication prevents TGN outages from affecting ongoing local operations**
- **Directory server will be co-located with e-mail servers**
  - **Reduces cost of server maintenance (same personnel for both)**
  - **Establishes de facto policy for server replication**
    - » **“Wherever there’s a mail server, there’s a directory”**

Some Lessons Learned -- General

- **We are really designing two distinct systems**
  1. **Enterprise Directory**
  2. **PKI (CA, RA, KRA, etc.)**

  There are distinct lessons-learned for each of these, even though the two systems must interoperate

  - **Both systems are required to implement a good PKI**
    - » **The Directory is not the "lesser sibling" -- if anything, it's actually more important than the Certificate Authority**
    - » **Focus on the design of the Directory, and most of the the design of the PKI follows as a logical consequence**
- **Philosophical Lesson**
  - **Design decisions we made to decrease operating costs have generally had an ancillary benefit: they've tended to improve security as well**
    - » **Providing automation to decrease operator complexity has eliminated opportunities for human error in the system**
    - » **Example: PKI automation for administrators of Web servers -- keeping their job simple will reduce access control errors**

Some Lessons Learned -- Directory

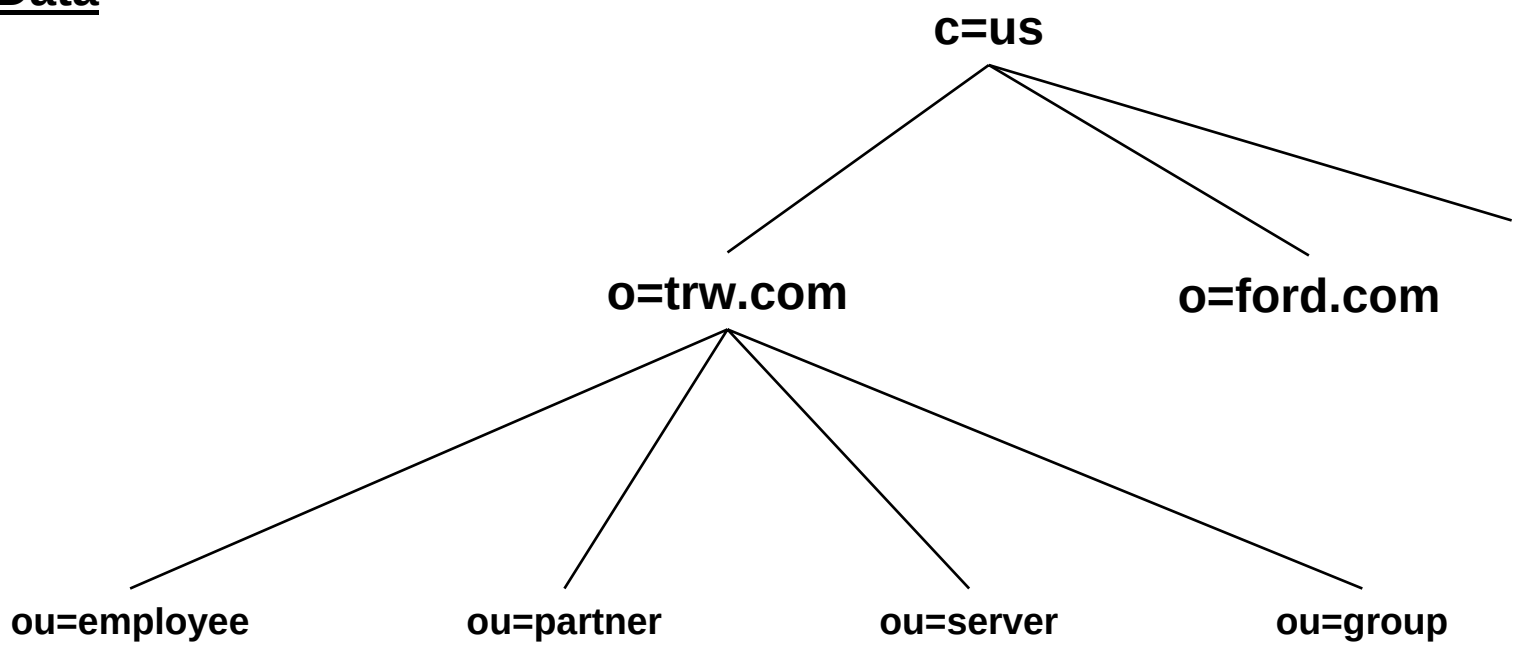
Directory Data

- **The Directory should *NOT* be an Authoritative Data Source**
  - **Unrelated, pre-existing business functions already provide authoritative information about employees, partners, servers, etc.**
  - **The directory should extract the necessary information from those functions**
    - » **Otherwise the directory administrators become data administrators.**
    - » **This increases operating costs significantly, and introduces opportunities for data integrity errors.**
  - **Lesson: If you find yourself wishing that the directory contained information that doesn't exist somewhere already, your design of the directory structure is probably more complex than it needs to be**
    - » **If the information does not already exist, then there probably isn't a real business need for that information in the PKI**

During design of the Directory structure, TRW was occasionally tempted to create directory branches or data entries that could not be extracted automatically from external sources -- we learned to view this as a warning sign that we were experiencing "requirements creep". In the end, our design uses no Directory-specific data.

Some Lessons Learned -- Directory

Directory Data



Authoritative Information Source	HR Database	Network Access Form	DNS and CA	CA
Responsible Handler	HR Manager	Employee Contact/ Sponsor	Server Administrator	Group Administrator

Some Lessons Learned -- Directory

Directory Construction

- **Keep the Hierarchy as Flat as Possible**
  - **Deep trees do not improve directory performance, they only increase administrative complexity**
  - **Embedding organizational structure is a recipe for disaster**
    - » **Organizational changes beget directory changes beget certificate changes**
    - » **Every time you reorganize, you must revoke certificates of *all* affected employees**
  - **Develop a mechanism for uniquely identifying employees and partners that is not dependent on organizational location**
    - » **Social Security Number**
    - » **Email address**
    - » **Unique ID**

Some Lessons Learned -- Directory

Directory Construction (cont)

- **When Do you Need a New Branch?**
  - **If two different branches use the same authoritative information source, then they should probably be collapsed into a single branch**
- **How Do you Populate the Directory?**
  - **Find the information providers**
  - **Negotiate an agreement with them**
    - » **Provide a business case for which the directory will actually help the information provider; e.g., TRW HR can now allow employees to use on-line forms to update personal information**
  - **Determine how frequently the information updates will occur**
  - **Determine who may see the information provided**
    - » **E.g., HR data is generally sensitive**

Some Lessons Learned -- Directory

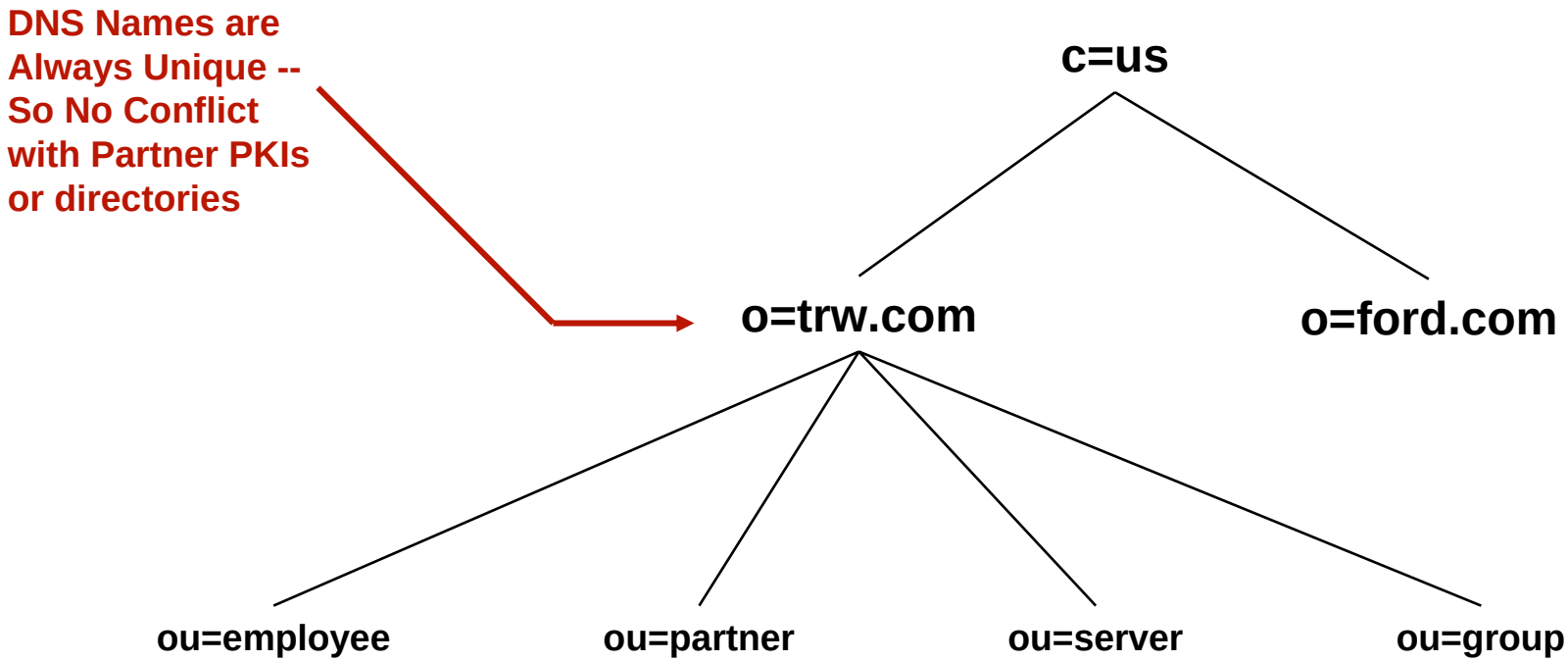
Directory Construction (cont)

- **How Do you Secure the Directory?**
  - Access to sensitive data must be strongly encrypted and authenticated
  - ***ALL*** update access must be strongly authenticated
  - Several vendors provide these capability using LDAP over SSL v3 (LDAPS)
- **How Do you Replicate the Directory?**
  - Replicate the directory to avoid performance impacts
  - Replicate the directory to reduce connectivity dependencies

Some Lessons Learned -- Directory

Directory Construction (cont)

- **DNS Names make useful Branch Names within Directories**
  - **Organization names are rarely unique, and can never be guaranteed to remain so**
  - **DNS names are already unique and well established**
    - » **E.g., TRW branch is called “trw.com”, not just “trw”**



Some Lessons Learned -- PKI

General

- Automating PKI processes is the key to
  - Reducing operational costs
  - Increasing reliability and security
  - TRW's Phase 1 PKI largely successful in this respect
- Certificates should be designed so identity rarely changes
  - Valid identity changes: change in surname, an employee becoming a partner (i.e., going to work for another contractor, agency)
  - Invalid identity changes: promotion, change in roles, reorganization
- Encryption Certificates should be distinct from signing certificates
  - Choice of encryption is not tied to identity, so encryption certificates should not be merged with signing certificates
  - Legal Issues
    - » Separate encryption certificate allows escrow for data recovery
    - » Separate signing certificate enables legal non-repudiation

Some Lessons Learned -- PKI

Security Model

- Few organizations wish to treat all data as equally sensitive.
  - Before proceeding with a PKI rollout, characterize the data that you are trying to protect
  - Then you can define your requirements for the PKI
- For example, TRW has chosen to divide data into three sensitivity levels.
  - Level 1 - Low value/sensitivity. Relatively impact from disclosure/tampering
    - » Proprietary but non-acquisition sensitive data
    - » Read/update access to basic personnel data (e.g. home address)
  - Level 2 – Moderate value/sensitivity. Substantial impact from disclosure/tampering
    - » Access to sensitive proprietary data (proposals, IR&D, etc.)
    - » Update access to payroll data by HR/payroll personnel
  - Level 3 – High value/sensitivity. Major impact from disclosure/tampering
    - » Access to enterprise and financial controls, merger and acquisition data

Some Lessons Learned -- PKI

Key Management

- Organizations may use a single set strategy for issuing and managing private keys,

-- or--

- They may use several different methods, each with its own level of assurance
- TRW's Phase 1 PKI used the first strategy, with all certificates "created equally"
  - Web servers and applications unable to assess the reliability of individual certificates
- TRW' Phase 2 PKI uses the second approach.
  - Certificates are assigned a the level of assurance is based on a combination of how registration process performed and how private key is protected.
  - Certificates are tagged to indicate the level of assurance that can be attributed to them
  - Note that this is a property of the *certificate*, not the *person*
    - » Users may upgrade certificates when needed

Some Lessons Learned -- PKI

Key Management (cont)

- **TRW Certificate Classes:**
  - **Class 2**
    - » **Certificates issued based on one-time pin and password sent directly to employee**
    - » **Private keys stored on LDAP server or personal computer**
      - **May have only one level of password only protection**
  - **Class 3**
    - » **One time PIN delivered to a human registration authority, who verifies identity before providing to employee (stronger authentication)**
    - » **Private keys must be encrypted on PC disk**
      - **Two levels of protection (access to computer, key store password)**
  - **Class 4**
    - » **Registration process is the same as for Class 3**
    - » **Private signing keys must be generated on on approved tokens**
      - **Stronger level of authentication (possession of token, knowledge of token pass phrase)**

Some Lessons Learned -- PKI

Key Management (cont)

- It should be easy for a user to revoke and replace a private key
  - If employee loses private key, he loses ability to access all systems requiring strong authentication. This may occur as a result of:
    - » Corruption of storage media
    - » Loss of token
  - Therefore, a user *must* be able to have his or her certificate (a necessary step for requesting a new certificate)
    - » Cannot revoke own certificate since the private key is needed to authenticate the revocation request
    - » Dedicated RAO may not always be readily available.
  - In TRW's Phase 2 PKI, an employee will ask manager to revoke employee certificate (using manager's certificate) so that employee can obtain new certificate
    - » Allows for rapid recovery of "lost" certificates
    - » Also allows manager to immediately terminate accesses by employees departing "under a cloud"

Some Lessons Learned -- PKI

Certificate Content

- **Pay close attention to x.509v3 “extensions”**
  - **Few are mandatory, but several “optional” extensions are actually required by client software**
  - **Key Usage**
    - » **Defines how certificate is to be used, e.g., for Digital Signature, Non-Repudiation, Key Exchange, Data Encipherment**
    - » **Required by many browsers and email clients to select appropriate certificate for authentication, signature or encryption**
  - **Enhanced Key Usage**
    - » **Further expands on how certificate will be used, e.g., Client Authentication, Secure Email, P security user**
    - » **Clients may also require this attribute in selecting certificates**
  - **CRL Distribution Points**
    - » **CA’s method for identifying where a client can look for the Certificate Revocation List**
    - » ***ABSOLUTELY CRITICAL* if certificates are to have any value**
      - **Only way for a client to determine if a certificate is still valid**

Some Lessons Learned -- PKI

Certificate Content

- X.509 Standards and usage continue to evolve, with new extensions gaining in importance
  - Authority Revocation Lists (ARLs) becoming important as CA vendors consolidate
  - New mechanisms evolving for managing trust relationships among certificate authorities
  - Improvements over in certificate revocation list management
    - » Delta CRLs
    - » On-Line Certificate Status Protocol (OCSP)
- PKI should build in ways of permitting this evolution without a great deal of pain
  - Allow users to readily revoke and reissue certificates with new properties

Lessons learned -- Performance

- **Network**
  - **Majority of hits to directory server are can be localized to LAN by replicating directory (also reduces impact of network outages)**
- **Client**
  - **Session keys are symmetric (fast)**
    - » **For Pentium-class clients, bottleneck is network, not session encryption**
  - **Public Key encryption is used only for signatures, exchange of session keys, etc.**
    - » **Generally 100 to 1,000 slower than symmetric keys**
- **Servers**
  - **COTS encryption cards (~ $1K each) eliminate all performance penalties**
  - **Without encryption cards, approximately 10-20% average performance hit for served Web pages**

Summary

- CA vendors have concentrated on the technical aspects of certificate management
  - They have not, in general, considered the impact that enterprise-wide implementations will have on operational costs
  - This is one of several reasons that PKI deployments have been "stuck in pilot mode"
- TRW recognized this problem early in it's own PKI deployment and set about remedying it
  - Focus was on decreasing operating costs while improving reliability, flexibility, security
  - TRW has filed for patent protection on many of these concepts.
- We continue to learn from our own experience in deploying our own PKI, and are developing enterprise-level strategies for dealing with the issues that we are encountering
  - The latest frontier is public key enablement
    - » The 7/10's of the iceberg that doesn't show
  - We will continue to fold this experience into products for our customers