Path Discovery & Validation (PD-VAL) Working Group
3 June 2004
Peter Hesse (pmhesse@geminisecurity.com)
• Overview
• Problem Description
• What is TrustEnabler?
• Our target: SSL
• How TrustEnabler Works
• More Information
• Public Key Infrastructure is a very useful technology for establishing trust in on-line transactions
  – SSL, VPN, Signed Forms, etc.
• “PKI-capable” implementations typically have concentrated on working well with simple PKIs
  – Single-CA environments
  – Trust lists of multiple CAs
  – Users directly issued by CAs, or through simple hierarchical relationships
• As this audience is quite aware, there are efforts to expand PKI relationships through cross-certification and Bridge certification authorities
  – Federal Bridge CA is the best-known example

• Typical “PKI Capable” implementations are not capable of dealing with these more complicated relationships
  – Path discovery and validation implementations are incomplete
Personally, I have been working on certification path discovery and validation efforts with the U.S. Government since 1998.

- Mostly research & development efforts
- Heavily involved in the Bridge CA technical Demonstrations 1999-2001
- Been somewhat removed for the last 2 years or so

I was surprised to see that “PKI Capable” implementations are little better now than they were in 1999!
• Typical “PKI Capable” software is capable of processing simple PKIs
  – By “simple” we’re talking about a flat hierarchy
Typical “PKI Capable” software is capable of processing simple PKIs

- By “simple” we’re talking about a flat hierarchy
- Some support use of (known) intermediate CAs
• Typical “PKI Capable” software is capable of processing simple PKIs
  – By “simple” we’re talking about a flat hierarchy
  – Some support use of (known) intermediate CAs
  – Trust lists can allow multiple simple PKIs
• If typical software is looking for that, what will it do when it sees this?
TrustEnabler provides services to improve the certification path discovery and validation of “PKI capable” products.

TrustEnabler is currently focused on providing a solution for applications that base their PKI capabilities around the technology of SSL with Mutual Authentication.

– Future TrustEnabler versions may expand the scope to other technologies.
What is TrustEnabler?

- TrustEnabler consists of three parts:
  - **TrustEnabler plugin**
    - Checks client’s digital certificate to ensure that it is trustworthy (with full certification path validation capability)
  - **TrustEnabler Explorer**
    - Explores and stores the interconnections between PKIs (provides complex certification path discovery capability)
  - **TrustEnabler Documentation**
    - Full installation and usage documentation
SSL with Mutual Authentication allows a user to authenticate to the server using a certificate and private key.

The following slides outline this process:
- Sometimes called Client Authenticated SSL
- TLS also has this capability

Also in the following slides are the impacts that the TrustEnabler software has on the process.
Client initiates a connection.
SSL Process

CLIENT

Client initiates a connection.

SERVER

Server responds with the server's certificate, a request for the client's certificate, and a list of trusted certificate issuers.
Typical implementations just send the contents of the SSL server’s trust list in this response
  - Trust lists typically don’t know anything about complex PKIs

**TrustEnabler Explorer** populates the SSL server’s trust list with other issuers it has found while exploring the PKI
  - Subordinate CA certificates
  - Cross-Certificates
  - All stored as intermediate CA certificates
SSL Process

GEMINI

**CLIENT**

- Client initiates a connection.

**SERVER**

- Server responds with the server's certificate, a request for the client's certificate, and a list of trusted certificate issuers.

- Client chooses a certificate issued by one of the trusted servers, sends the certificate and signs a challenge to authenticate to the server.
• In typical implementations, a user from another PKI will not be able to select their certificate
  – Unless their certificate issuer is stored in the SSL server’s trust list
• Since TrustEnabler Explorer populated the SSL server’s trust list with other issuers, the client can now select their own certificate and authenticate to the server
SSL Process

**CLIENT**
- Client initiates a connection.
- Client chooses a certificate issued by one of the trusted servers, sends the certificate and signs a challenge to authenticate to the server.

**SERVER**
- Server responds with the server's certificate, a request for the client's certificate, and a list of trusted certificate issuers.
- Server authenticates client and drops the connection if the client is not acceptable.
Many SSL server implementations are lacking in their certification path validation capabilities
- Some do not perform revocation checking
- Others do not check name constraints, certificate policies, etc.

The **TrustEnabler Plugin** provides full certification path validation capabilities to ensure that the certification path is truly valid before allowing the user to continue
SSL Process

**CLIENT**

- Client initiates a connection.
- Client chooses a certificate issued by one of the trusted servers, sends the certificate and signs a challenge to authenticate to the server.
- Client sends the server a session key encrypted with the server’s public key.

**SERVER**

- Server responds with the server's certificate, a request for the client’s certificate, and a list of trusted certificate issuers.
- Server authenticates client and drops the connection if the client is not acceptable.
• The TrustEnabler Explorer periodically performs path development starting from one or more trusted root certificates
  – Utilizes an LDAP/X.500 directory to find relationships
  – Future versions will support SIA/AIA extensions to find additional relationships
• The discovered certificate issuers are inserted into the SSL server’s trust list as intermediate certification authorities
• The TrustEnabler Plugin is an access control plugin which is invoked after the SSL negotiation process is completed, but before any pages are served to the client
  – Uses the DigitalNet Certificate Management Library (CML) v2.6 to perform certification path validation

• The plugin is invoked upon every request
  – Validation state is cached for a configurable amount of time to ensure responsiveness
• TrustEnabler provides a solution for enabling today’s applications to work with the current and growing Federal PKI
  – Combined solution to allow a web-based application to accept and trust certificates from non-local PKIs

• TrustEnabler is currently available for the Netscape/iPlanet/SunONE series of web servers
  – Platforms include Windows, Linux, HP, other *NIX
• For more information, contact me directly, or visit our website:
http://www.trustenabler.com

Peter Hesse, President
Gemini Security Solutions, Inc.
+1-703-934-2031
pmhesse@geminisecurity.com