FRENDS

Security in B2B

Sami Tähtinen
FRENDS Technology, Inc.

S-38.153 Security of Communication Protocols
January 28th, 2003

enterprise application integration platform

FRENDS

Contents

- What is B2B information exchange?
- Threats against B2B information exchange
- Ways to avoid the threats
- Conclusions

FRENDS

What is B2B information exchange?

B2B

- B2B = Business-to-Business
- Exchange of products, services, or information between businesses
- In this presentation, the definition is limited only to electronic data transfer (that may include exchange of products, services or information)

Some examples of B2B technologies

- EDI (Electronic Data Interchange)
  - Standard message format for exchanging business data
  - In use for more than 10 years
- ebXML
  - XML-based framework for exchanging business data
  - Defines messaging choreography between business processes
  - No restrictions to payload format (can be e.g. EDI)
- RosettaNet
  - Another XML-based B2B framework
  - Used by e.g. telco cluster

FRENDS

Threats against B2B information exchange

enterprise application integration platform

What makes B2B information exchange interesting to attackers?

- B2B information exchange contains valuable assets, including e.g.
  - Order information
  - Money transfers
  - Product information
- Attackers are interested in gaining financial benefits, rather than publicity
  - B2B attacks are rarely reported because of their confidential nature

B2B and Internet

- Internet is an interesting media for companies due to its economy; all businesses have access to it, and using it is almost free of charge
- B2B usage is moving from closed (expensive) to public (cheap) networks
- Usage of public networks (especially Internet) causes new requirements for B2B information exchange security

New threats

- New B2B protocols bring new challenges
- An example: ebXML registry
  - Public registry in Internet
  - Contains trading partners' information, e.g. public and bilateral Trading Partner information
  - On the other hand, may contain classified information of specific trading partners
  - Requires authentication and classification to restrict access to private data
- New protocols are (still) rarely designed with security in mind

FRENDS

Ways to avoid the threats

Cryptography

- Cryptographic tools may ensure confidentiality, integrity and partly availability of B2B messaging
- However, techniques are not enough
  - Technology is useless if people or business are not motivated to secure processes
  - Schneider's "Applied Cryptography" vs. "Secrets & Lies"

Examples of B2B security techniques

- B2B exchange protocols usually function on the top of several transfer protocols, e.g. HTTP(S), FTP, SOAP or even e-mail
- Because of this, data transfer security is often left to be decided by the parties exchanging data
- Some examples of data transfer security include
  - IPSec
  - SSL
  - PGP
  - SOAP-SEC

Examples of B2B security techniques

- Value-added Networks (VANs) may employ their own security measures in EDI
- ebXML relies heavily on XML-based security techniques such as
  - Security Assertion Markup Languagage (SAML)
  - XML Access Control Markup Language (XACML)
  - XML Digital Signature (XML DSIG)
  - XML Key Management Specification (XKMS)
  - XML Key Information Service Specification (X-KISS)
  - XML Key Registration Service Specification (X-KRSS)

FRENDS

Conclusions

Is technology enough?

- Most of attacks originate from within
  - Even if B2B messaging were completely secure, it can't stop these attacks
- As B2B messaging contains valuable assets, it is tightly observed and attacks can be found out promptly
- Who does benefit from attacks?
  - Can business afford the risk to attack?
  - May an individual gain the advantage from an attack?

The most widely used B2B protocol..

- B2B protocol that everyone uses daily
- A protocol that may be used e.g. for exchanging
  - Orders
  - Product information
  - Any business-related confidential information
- Can be encrypted and authenticated
- One of the oldest Internet protocols

..shows why B2B security is not easy

- Anyone could use PGP, but how many does?
- Company-wide rules for e-mail utilization?
- Orders, technical specifications, any confidential information is exchanged with no security measures over Internet

Questions?

sami.tahtinen@frends.com
http://www.frends.com/