IEEE P1735

Recommended Practice for Encryption and [Use Rights]

Management of Electronic Design Intellectual Property (IP)

John Shields
ENGINEERING MANAGER
DVT DIVISION

Mentor Graphics®

Agenda

- Scope of P1735
- Relationship to P1800 and 1076
- Progress
- Preview of Expected Major Contributions
- Version 1 Recommendation
- Security Threats
- VHDL-AMS Considerations

Why Do We Need P1735?

- LRMs use different descriptive language
  - Shared implementation technology is difficult
  - LRMs are difficult to interpret
- Users want more guidance
  - How to use it and achieve interoperability
- Early tradeoffs had unfortunate consequences
  - weak requirements in LRMs to avoid export restrictions (no longer a substantive issue)
  - Policy-free pragmas for unforeseen use cases also admitted weak semantic descriptions
- P1800/1076 are looking for this leadership

P1735 Scope

- embeddable and encapsulating markup syntaxes for design IP encryption and rights management
- recommendations for integration with other design specification formats
- use models for interoperable tool and hardware flows
- Selection of encryption and encoding algorithms and encryption key management
- description of the trust model assumed in any recommended use models
- see P1735 public home page for more info

Relationship to P1800 and 1076

- We don't replace or refactor what is already standardized
- A clearing house for issues
  - Vet issues and requests for interpretation
  - Bring LCS drafts back to the lrm working groups
- We have a liason to both groups
- IMHO, P1735 recommendations will have weight
  - strong for language neutral aspects
  - Advisory input for language specific issues

Progress

- 37 mtgs over 18 months
- Private working documents (twiki pages)
  - use cases, tool flows, focus areas below, security threats
- 4 focus areas
  - Interoperability
  - Key management
  - IP Licensing
  - Rights management
- Working group approved version 1 recommendation for basic interoperability

Interoperability

- Make it possible for production tool flows to really work
  - Pick use case, choose algorithms and convention details
  - Solve problems between tool vendors found by their customers traceable to lrm spec issues
- Basic interoperability comes before adding more features
- Goal to organize a framework for validation

Key Management

- Ignored in the current specs
  - inlined public key pragmas that the IP author has to create
  - Where do you get those keys?
  - keys are builtin to encryption tools?
- X.509 certificates with suitable conventions
  - Basis for exchange and trust management
  - Need to define reference from pragmas (owner and key name tuple)
- Work in progress
  - Secure key database?

IP Licensing

- Enforces rights management
- Additional security
- As specified, lrm feature barely keeps honest people honest
  - Unprotected function call's return value is so 80s!
- Internal licensing (optional)
  - Employ tool vendor's mechanism for IP author's use
  - Requires new legal/business deals and administration issues
  - Low bar for the small IP author with security
- External licensing (required)
  - Dynamically linked library or socket-based server
  - Use encrypted channel, provide reference implementation

Rights Management

- new pragmas, rich in detail is expected
- Who is allowed to do what with protected IP
  - Use cases – IP evaluation, tool flow restrictions
  - Some tools will be more trustworthy than others
  - Private vendor-specific rights
- VSIA contribution, but one vendor holds an underlying contribution
  - Strategy is to get the basic problems solved first and not dilute the working group too much
  - It is promised contribution and a discussion we haven't started
- 2 tool vendors have proprietary implementations

Version 1 Recommendation

- Digital envelope use case
- Defined required algorithm support
- Resolved LRM ambiguities and conflicts
- Added a version pragma for managing change in pragma definitions
- Defined default behavior for tools that produce derivatives of protected IP (e.g., synthesis)
- Meaningful milestone approved in working group that will be adopted now

Is There Anything to Worry About?

IP Protection Security Threats

- IP exposure
  - Spoofing public key used (low to guarded)
  - Theft of private key (guarded to elevated)
  - Theft of session key (low)
  - Crack session key/crack private key (low)
  - Discovery of private key in application (elevated to high)
  - Debug/dump IP from application (high to severe)
- IP overuse
  - Counterfeit licenses (low)
  - Spoofing license interface (low to guarded)
  - Cracking proxy or application (elevated to high)
  - spoofing hostid of license server (?)

IP Protection Countermeasures

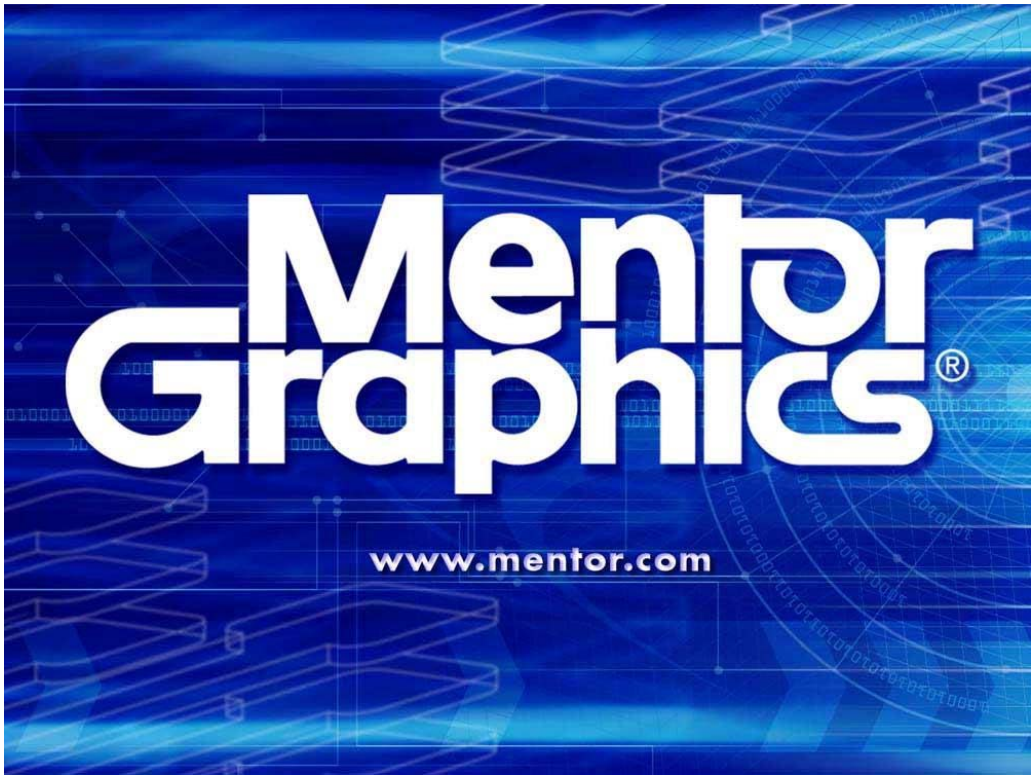
- IP exposure
  - Spoofing public key used -flow verification and signed keys
  - Theft of private key –security policies, periodic new keys
  - Theft of session key –single use of random keys
  - Crack session key/crack private key –strong algorithms
  - Discovery of private key in application
    - obfuscation and commercial protection
  - Debug/dump IP from application
    - Anti-debugger/anti tampering technology
    - Minimize decrypted IP in memory
    - Avoid decrypted IP in temp files
    - Avoid spoofable dynamic libraries

IP Protection Countermeasures

- IP overuse
  - Counterfeit licenses -FLEXnet TRL or equivalent
  - Spoofing license interface –secure comms between app and proxy
  - Cracking proxy or application –anti tampering in app and proxy
  - spoofing hostid of license server
    - enhanced hostid, EDAC anti-piracy committee

1076.1 considerations

- Take a position on 1076 and P1735 early
- Expect no one else to focus on any language specific issues
  - Visibility concerns
  - Need for unique rights
- Explore use cases with ams examples, ip providers, and users – model the supply chain
- Bring input to P1735


Mentor Graphics®
www.mentor.com