

# Trusting unmanaged machines for remote working

Infosecurity Europe

22<sup>nd</sup> April 2008

Dr. Bernard Parsons, CTO BeCrypt

© 2008 Becrypt Limited

This document contains information which is confidential to Becrypt. This document shall only be used in connection with the Becrypt work for which it is provided. Neither the whole nor any part of this document shall be disclosed to any party without Becrypt's prior written consent.

# Outline

- ◇ Background on BeCrypt
- ◇ Flexible Remote Access: The Drivers
- ◇ Approaches to System Security
- ◇ Trusted Client Solution Overview



# BeCrypt

- ❖ Data Security – Mobile Devices
  - Laptop Encryption, Media Encryption
  - PDA Security, End-point Device Control
- ❖ Formed in the UK 2001 initial focus UK Government
  - Products approved by CESG to SECRET & above
- ❖ Growing Footprint in EU & US

# Background

- ❖ Some differences between sectors are blurring
  - Governments need more agility
  - Non-government needs & expects better protection
    - Raised awareness of vulnerabilities
    - More sophisticated attacks becoming more relevant
- ❖ Developing products across sectors requires broad stakeholder input

## A common requirement:

- ❖ To better support secure occasional remote working
  - For some organisations this means gaining greater confidence over what they already allow, e.g. webmail,
  - For others, this means better assurance before they allow anything

How do we gain trust outside controlled environment?



# Remote Working Adds Risks

Increased Risk  $\propto$

Quality Difference

(internal v external security measures)

×

Resources exposed externally

Who owns the devices?

What are the business requirements?

## Examples

- ❖ Focus on Business Continuity planning across Government and CNI.
  - Maximum flexibility with minimum risk
- ❖ Defense Department wish to support remote access
  - Insufficient budget for laptops; and,
  - Policy prohibits alternatives: you can't trust a machine you don't manage

# Examples


## ❖ US Government Department

- Potential issues around differing levels of classification on site during Emergency Response Scenarios

## ❖ Commercial Organisation

- Interest in emergency fallback solution for laptop loss / failure

# End-Point Inspection

- ❖ Typically combined with VPNs to assess state of client – patch levels etc
  - ❖ Assumes limited sophistication of attack
  - ❖ Assumes known signatures
  - ❖ Assumes trust in the user
  - ❖ Support challenges can exceed internal infrastructure
- 

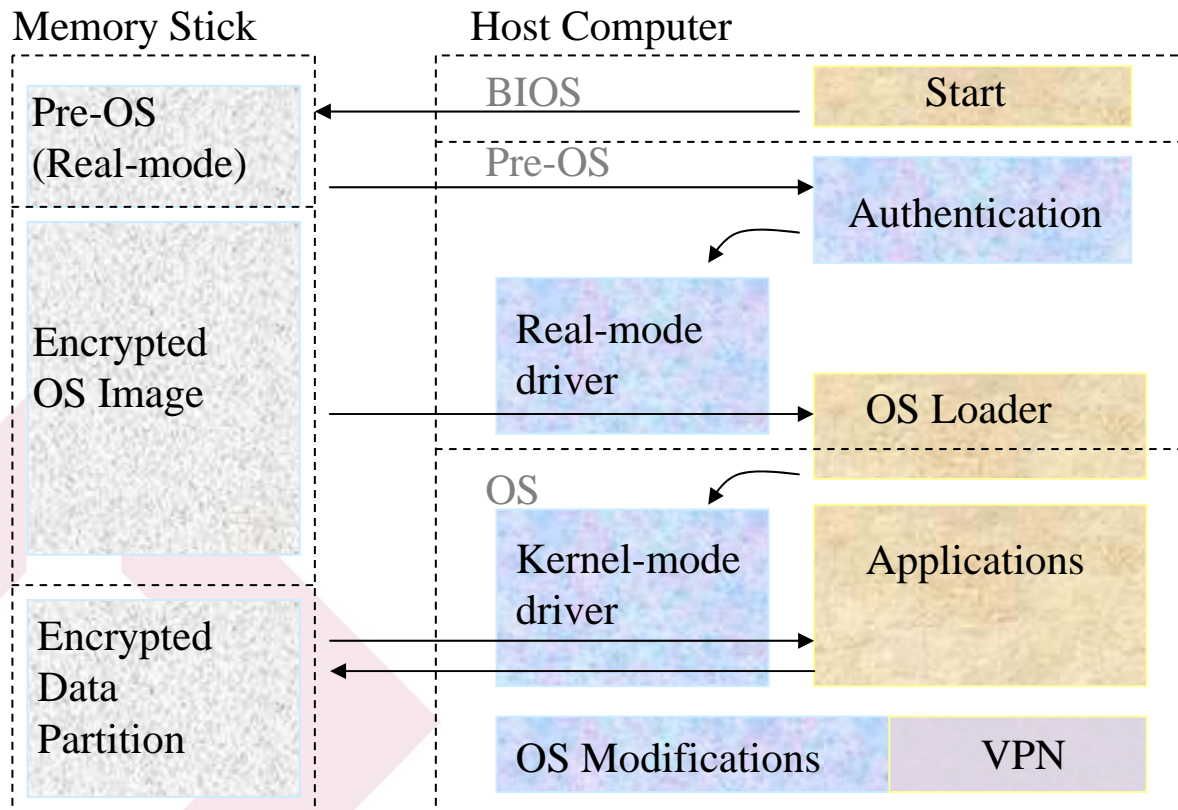
# Virtualization

- ❖ Create controlled virtualized environment “within” Host OS
- ❖ Guest OS still vulnerable to malicious software in “host” OS.
- ❖ The system could itself be virtualized, then all is lost
- ❖ May require admin privileges
- ❖ May require trust in the user
- ❖ License costs prohibit scaling

# Trusted Client

- ❖ A light-weight managed OS on bootable media
- ❖ Modify OS to:
  - Isolate from temporary host
  - Remove non-essential components
- ❖ Introduce security components to:
  - Ensure confidentiality in event of device loss
  - Protect against unauthorised use
  - Secure Network Access
    - Constrain IP Destination Addresses
    - Embed SSL/IPSEC VPN

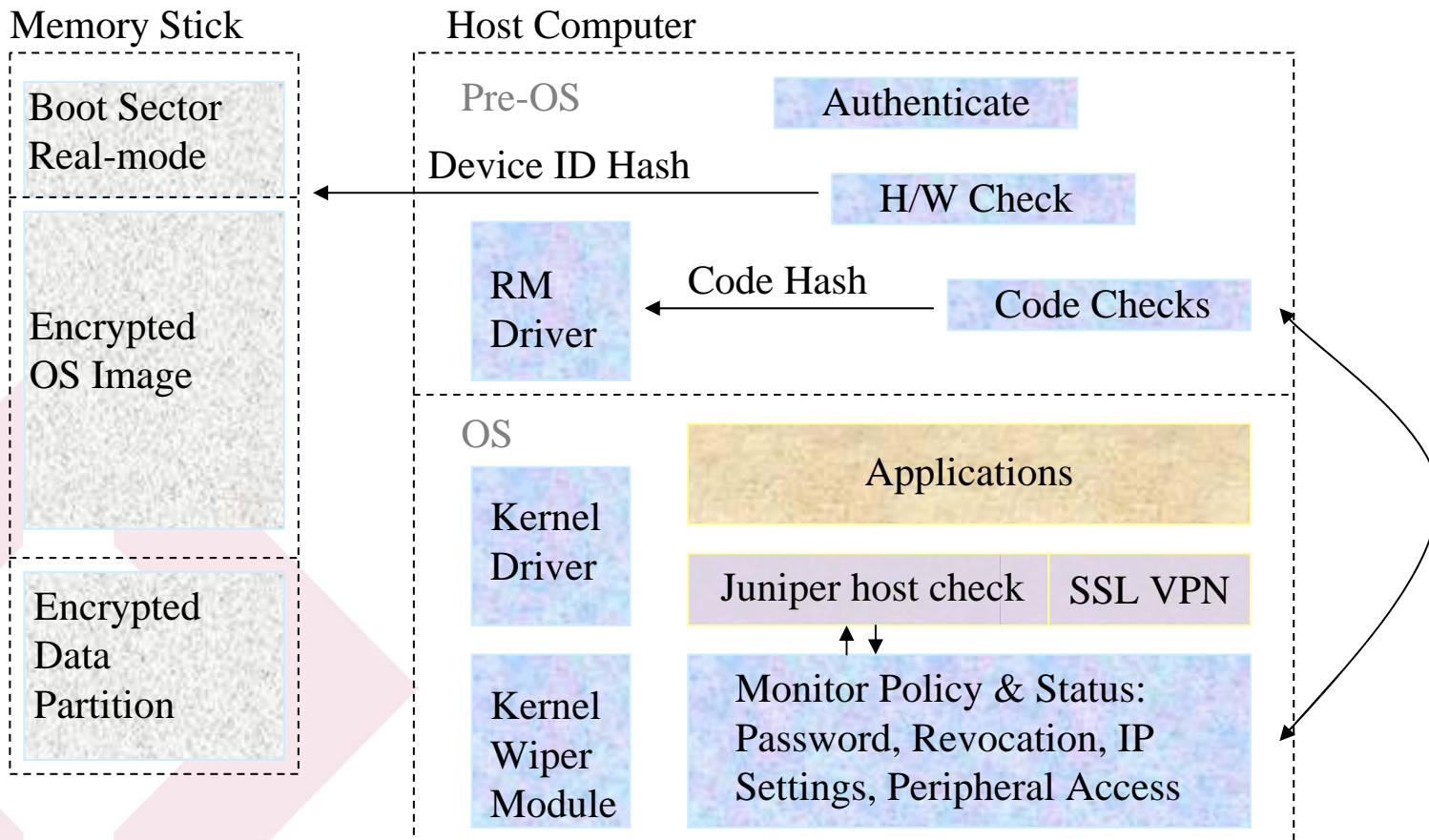
# Architectural Overview



# Threat Modelling Outcomes

- ❖ Prevent device cloning
- ❖ Monitor System Integrity
- ❖ Control self provisioning
- ❖ Allow device revocation
- ❖ Memory clean-up
- ❖ Smartcard integration (DOD/CAC FIPS 201 PIV)
- ❖ OTP Integration

# Architectural Overview



## Next Steps

- ❖ Multi-function device
  - Portable data encryption
  - OTP & Smartcard on single device
  - Customisation Tools
  - FIPS 140-2, CESSG CAPS



# Thank You

◊ Questions?



Dr. Bernard Parsons  
CTO BeCrypt Ltd  
bparsons@becrypt.com