Samir Mody (Sophos/K7Computing)
Igor Muttik (McAfee)
Peter Ferrie (Microsoft)

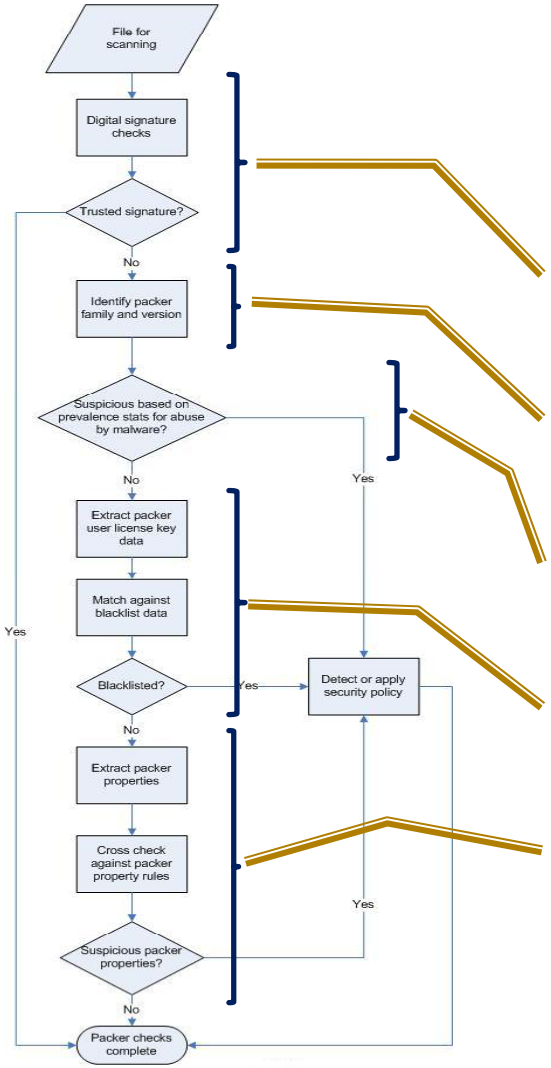
Standards and Policies on Packer Use

High-level Purpose

1. Reduce impact of legitimate packers in malware

2. Improve identification of custom packers

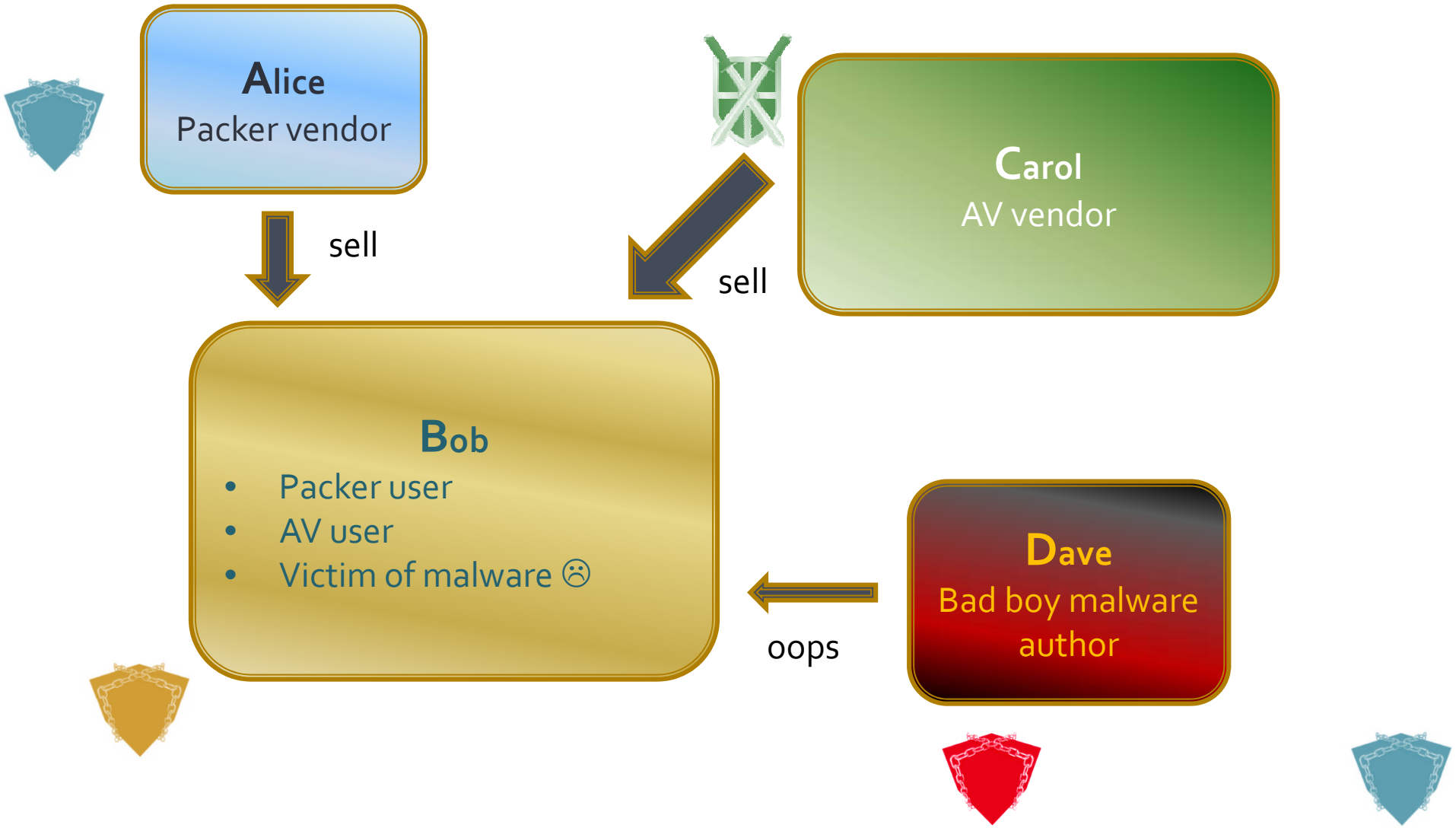
Security Vendor Checklist for Packed Files



Check:

- Digital signature
- Packer family
- Packer prevalence (malware vs clean)
- License key (alias "taggant" or "watermark") information
- Packer properties

Learn Your ABCDs



Taggants and Watermarks

What?

- **Taggant**: cryptographically encrypted data based on PKI
- **Watermark**: encoded data permeating a file
  - Both specify packer family, unique packer license ID, and potentially more

Why?

- Allows blacklisting abused legitimate packers without the need to unpack

IEEE ICSG Taggant Initiative

- AV industry-packer vendor partnership
  - AV members: **AVG , CSIS SecurityGroup A/S, Damballa, ESET, IBM, K7Computing, Marvell Semiconductor, McAfee Inc., Microsoft Corporation, NovaShield, Palo Alto Networks, Panda Security, Sophos Plc, Symantec Corporation, Trend Micro Inc., Veszprog**
  - Packer partners: **Enigma, Obsidium, Oreans (Themida), VMPSoft (VMProtect)**

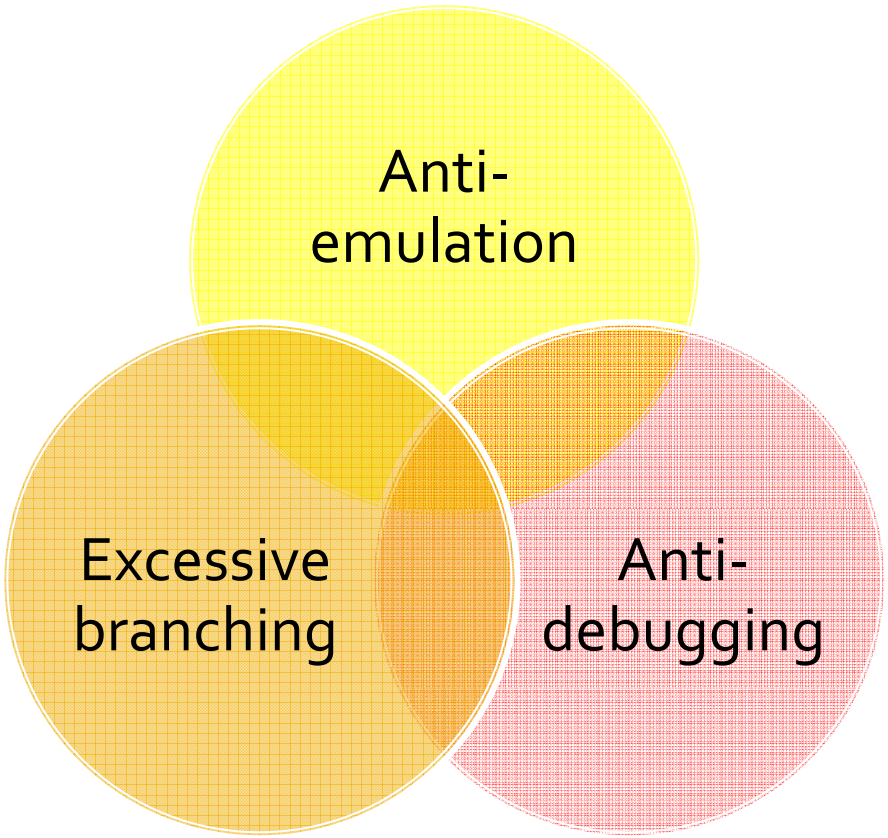
IEEE ICSG Taggant System Continued

- Sponsored technical infrastructure
  - Cryptographically secure (PKI)
  - No need to unpack
  - Compatible with digital signatures
- Sponsored administrative infrastructure
  - Managed by IEEE
  - Issuing and maintaining records of credentials
  - Addressing queries and issues

Packer Properties

- Superset of individual packer characteristics

- Potential overlaps of shared characteristics between properties



Packers on Trial

- Combinations of packer properties may be grounds for suspicion
- Suspicious packing applications may be grounds for suspicion of the packer
- Status of packers depends on:
  - Properties of the packer
  - Extent of cooperation of packer vendor
  - Prevalence of packer in legitimate applications
  - AV vendor's client base and individual security policy
- AV industry may actively promote well-behaved packers

Salient Points

- Need more comprehensive and concerted policy to deal with packer problem
- Can use digital signatures, taggants, watermarks and packer properties in decision logic on packer status
- IEEE ICSG taggant system potential
- Need cooperation of packer vendors, free packer authors and the general public

Queries

What about Free Packers?

- Difficult to blacklist outright due to high volume
- However, in general free packers are not as complex as commercial ones, i.e. most AV solutions are likely to be able to unravel free packer layers to peek inside
- Nevertheless, the IEEE ICSG scheme does incorporate a solution to accommodate applying taggants for open source or freely available packers

Examples of Packer Properties

- Polymorphic code
- Non-standard use of APIs
- Unusual structural features
- Unnecessary use of unusual instructions
- Unnecessary branching into the middle of another instruction
- Destruction of target data
- Impersonation of another packer
- Unusual transfer of execution control