AJAN YAZILIM İÇİN BENZERSİZ KİMLİK TANIMLAMASI AR-GE RAPORU

GIYS Projesi için kullanılacak ajan kimlik bilgisinin donanım ve yazılım değişikliğinden etkilenmemesi ve oluşturulacak id için yapılan testler ve sonuçları bu raporda belirtilmiştir. Oluşturulacak olan kimlik bilgisinin referans noktasını oluşturacak methodlar Yazılımsal ve Donanımsal olmak üzere iki ana başlıkta incelenmiştir.

Donanım Kimlikleri

**/ sys / class / dmi / id / product\_uuid:** Kart üreticisi tarafından ayarlanan ve BIOS DMI bilgisinde kodlanan ana kart ürünü UUID. Bir anakartı ve sadece anakartı tanımlamak için kullanılabilir.



Kullanıcı ana kartı değiştirdiğinde değişir. Ayrıca, çoğu zaman BIOS üreticisi içine sahte seri yazar. Ayrıca,x86'ya özgüdür. Ayrıcalıklı kullanıcılar için erişim yasaktır. Bu nedenle genel kullanımı azdır.

**CPUID / EAX = 3 CPU seri numarası:** CPU üreticisi tarafından ayarlanan ve CPU çipinde kodlanan bir CPU UUID. Bir CPU'yu ve sadece bir CPU'yu tanımlamak için kullanılabilir. Kullanıcı CPU yu değiştirdği vakit değişir . Ayrıca, modern CPU'ların çoğu artık bu özelliği uygulamaz ve eski bilgisayarlar BIOS Kurulumu seçeneği ile kontrol edilebilen varsayılan olarak bu seçeneği devre dışı bırakma eğilimindedir. Ayrıca, x86'ya özgüdür. Dolayısıyla bu da çok az kullanılır.



**/ sys / class / net / \* / address:** Ağ bağdaştırıcısı üreticisi tarafından ayarlanan ve bazı ağ kartı EEPROM'da kodlanan bir veya daha fazla ağ MAC adresi. Kullanıcı ağ kartını değiştirdiğinde değişir. Ağ kartları isteğe bağlı olduğundan ve bu kimlik garanti edilmezse ve birden fazla seçim yapabileceğinizde birden fazla kullanılabilirlik olabilir. Sanal makinelerde MAC adresleri rastgele olma eğilimindedir. Bu da çok az genel kullanımdır.

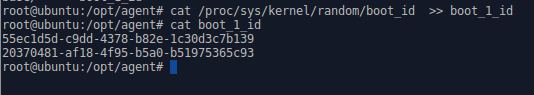


**/ sys / bus / usb / device / \* / :** USB aygıtında EEPROM olarak kodlanan çeşitli USB aygıtlarının seri numaraları. Çoğu cihazın seri numarası ayarlanmamıştır ve eğer varsa genellikle sahte olur. Kullanıcı USB donanımını değiştirir veya başka bir makineye takarsa, bu kimlikler diğer makinelerde değişebilir veya görünebilir. Bu yüzden de çok az faydası var. Birçoğu sabit diskler ve benzerleri gibi çeşitli cihazların ID\_SERIAL udev özelliği aracılığıyla bulabileceğiniz çeşitli başka donanım kimlikleri de vardır. Hepsinin ortak noktası, evrensel olarak bulunmayan, genellikle sahte verilerle doldurulmuş ve sanallaştırılmış ortamlarda rasgele olan belirli (değiştirilebilir) donanıma bağlı olmalarıdır.

**dmidecode -t 2 | grep -i vers & dmidecode -t 2 | grep -i serial :** Anakart üreticileri üretikleri anakartın versiyon kontrolünü ve yazılımsal desteğini takip etmek amacıyla versiyon numarası ve seri numarası ilave ederler. Fakat fason üretim yapan firmalar bu id leri sahte veya değer tanımlamadan piyasaya sürdükleri için bu konuda araştırmalar devam etmeketedir.

**Yazılım kimlikleri**

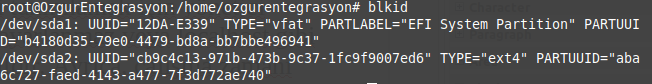
**/ proc / sys / kernel / random / boot\_id:** Her önyüklemede yeniden oluşturulan rastgele bir kimlik. Bu nedenle, yerel makinenin mevcut önyüklemesini tanımlamak için kullanılabilir. Evrensel olarak herhangi bir Linux çekirdeğinde kullanılabilir. Belirli bir önyükleme çekirdeğinde belirli bir önyükleme tanımlamanız gerekiyorsa iyi ve güvenli bir seçimdir. Ama kalıcı değildir adında da anlaşılabileceği gibi yer yeni boot da değişir.

****

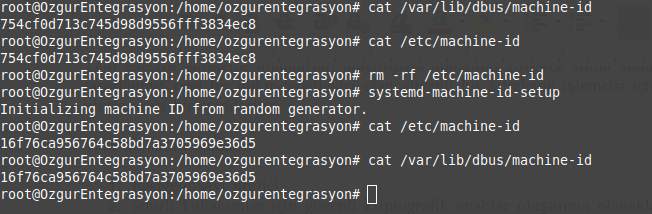
**gethostname (), / proc / sys / kernel / hostname:** Ağdaki bir makineyi tanımlamak için yönetici tarafından yapılandırılan rastgele olmayan bir kimlik. Genellikle bu ayarlanmaz veya localhost gibi bazı varsayılan değerlere ayarlanır ve hatta yerel ağda benzersiz değildir. Ayrıca,çalışma zamanı sırasında değişebilir, örneğin güncellenmiş DHCP bilgilerine göre değiştiği için. Bu nedenle, kullanıcıya sunum dışında herhangi bir şey için neredeyse tamamen yararsızdır.

****

**ID\_FS\_UUID:** udev ağacındaki belirli bir dosya sistemini tanımlayan bir kimlik. Bu dizilerin nasıl üretildiği her zaman açık değildir, ancak bu neredeyse tüm modern disk dosya sistemlerinde kullanılabilir. NFS bağlantıları veya sanal dosya sistemleri için kullanılamaz. Bununla birlikte, bu genellikle bir dosya sistemini tanımlamak için iyi biryoldur.Bununla birlikte, zayıf tanımlanmış id yapısı nedeniyle D-Bus makine kimliği genellikle tercihedilir.Biz senorya gereği disk değişimi veDisk UUID lerinin manipüle edileceğini varsayılarak bu yöntemdenvazgeçtik.

****

**Machine-id :** *machine-id dosyası,*yükleme veya önyükleme sırasında ayarlanan yerel sistemin benzersiz makine kimliğini içerir. Makine kimliği, tek satırsonu sonlu, onaltılık, 32 karakterli, küçük harfli bir kimliktir. Onaltılık koddan çözüldüğünde, bu 16 bayt / 128 bit değerine karşılık gelir. Bu kimlik tamamen sıfır olamaz. Makine kimliği genellikle sistem kurulumu veya ilk önyükleme sırasındarastgele bir kaynaktan oluşturulurve sonraki tüm önyüklemeler için sabit kalır. İsteğe bağlı olarak, durum bilgisi olmayan sistemler için, gerektiğinde erken önyükleme sırasında çalışma zamanı sırasında oluşturulur. Makine kimliği, örneğin ağ önyüklemesi yapılırken, systemd.machine\_id = çekirdek komut satırı parametresi ile veya --machine-id = seçeneğini sistemd'ye geçirerek ayarlanabilir. Bu şekilde belirtilen bir kimlik daha yüksek önceliğe sahiptir ve / etc / machine-id içinde depolanan kimlik yerine kullanılacaktır.Makine kimliği yerel veya ağ yapılandırmasına bağlıolarak veya donanım değiştirildiğinde değişmez. Bu makine kimliği, D-Bus makine kimliğiyle aynı formata ve mantığa uyar. Bu kimlik ana bilgisayarı benzersiz bir şekilde tanımlar. Machine id sistem ilk kurulum yaparken oluşturulduğu ve kolay manipüle edilebilir bi yapıda olduğu için uygun görülmemiştir.

****

Sonuç:

Yazılımsal ve Donanımsal değişiklerden etkilenmeyecek benzersiz kimlik id’si için TPM konusunda araştırmalara başlanıldı.

TPM entegre şifreleme anahtarları aracılığıyla donanımı güvence altına almak için tasarlanmış özel bir mikrodenetleyici olan güvenli bir şifreleme işlemcisi için uluslararası bir standarttır.

TPM kullanım alanları;

1. Rastgele sayı üretici
2. Sınırlı kullanımlar için güvenli kriptografik anahtar oluşturma olanakları.
3. Uzaktan kontrol: Donanım ve yazılım yapılandırmasını neredeyse unutulmaz karma anahtar özeti oluşturur.
4. Bağlama: Verileri, depolama anahtarından gelen benzersiz bir RSA anahtarı olan TPM bağlama anahtarı kullanarak şifreler.
5. Veri Korunumu: Bağlamaya benzer, ancak ek olarak verilerin şifresi çözülemesi için TPM modülünü kullanır.

TPM uygulamaları;

* 2006 yılından itibaren bir çok dizüstü bilgisayar yerleşik TPM yongasıyla birlikte satıldı. Bilgisayarlara TPM yongasını bağlamak için LPC veri yolu veya SPI veriyolu kullanılmıştır.
* Günümüz de bir çok bilgisayar üreticisi anakarta bu çipi entegre etmektedir. Ayrıca harici olarak bu çip sisteme entegre edilebilmektedir.

Linux' da kullanımı;

TPM esas olarak yazılım bileşeni tarafından, şifreleme ve şifre çözmeyi anında yapmak için kullanılan gizli bir anahtarlar içeren bir donanımdır.

TPM, esas olarak linux çekirdeği kullanan bilgisatarlarda, çekirdeğin değiştirilip değiştirilmediğini kontrol etmek için kullanılır. Ancak TPM yalnızca çekirdeğin bütünlüğünü değil, aynı zamanda tüm BIOS bileşenlerinin, önyükleyicinin ve diğer işletim sistemi bileşenlerinin bütünlüğünü de kontrol eder.

Benzersiz anahtarlara ulusal güvenliğin söz konusu olduğu durumlarda ulaşmak isteyen ülkeler, TPM kullanımını engelliyor. Hali hazırda Çin, Rusya, Beyaz Rusya ve Kazakistan'da TPM entegrasyonu yasak. Türkiye'ye ithal edilen bilgisayarlar bu çipin bulunma durumu ve yaygınlaşması hakkında araştırmalar devam etmektedir.