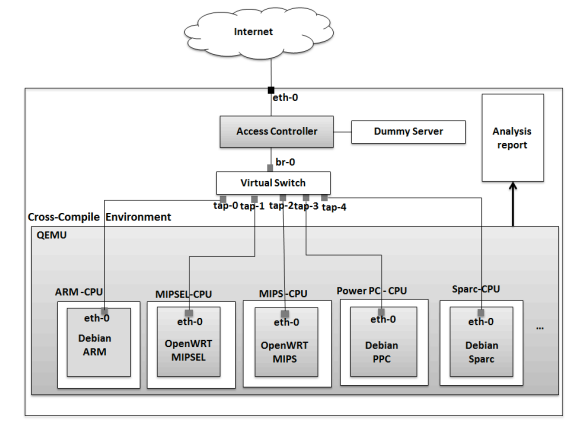
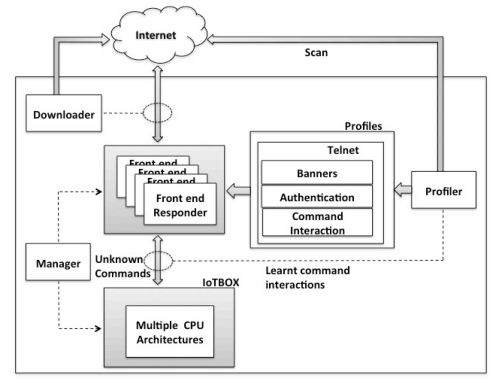
**Proje 04**

Proje : IoTPOT: IoT’nin Yükselişi Analizi:  
Yapılan Çalışma ve Öneri: İncelenen örnek bir sistemde mühendisler; IOT cihazlarına karşı artan tehditleri analiz etmişlerdir. Özellikle 2014 yılından beri IoT cihazlarını hedef alan Telnet tabanlı saldırıların arttığını göstermişler ve bundan yola çıkarak ARM, MIPS ve PPC gibi farklı CPU mimarileri üzerinde çalışan çeşitli IoT cihazlarına karşı Telnet tabanlı saldırıları çeken ve analiz eden bir IoT honeypot ve sanal alan önermişlerdir. Balküpü ve yakalanan kötü amaçlı yazılım örneklerinin gözlem sonuçlarını analiz ederek, Şu anda Telnet özellikli IoT cihazlarını hedefleyen en az 4 farklı DDoS malware ailesi olduğunu ve ailelerden birinin 9 farklı CPU mimarisi ile daha fazla aygıtı hedeflemeye hızla ilerlediğini belirtmişlerdir. IOT cihazlarının saldırılara karşı taviz vermeye açık olduğunu ve kitleler üzerindeki kötü amaçlı yazılımların hedeflerin giderek arttığını göstermişlerdir. DDoS saldırılarında aktif olarak kullanılan solucan benzeri yayılma davranışını gösteren dört kötü amaçlı yazılım ailesini tespit etmişlerdir. Gelecekte yapabilecekleri çalışma olarak da SSH gibi saldırılarla hedeflenen daha fazla protokolü desteklemek için IoTPOT’u ; Dahası, IoT aygıtlarında yaygın olan daha fazla mimari ve ortamı canlandırmak için özelliklerle  genişletmeyi planlamışlardır.  
Mimarisi: IoTBOX diye adlandırdıkları sistem, MIPS, MIPSEL, PPC, SPARC, ARM, MIPS64, sh4 ve X86 gibi 8 farklı CPU mimarisinde zararlı yazılım analizini gerçekleştirmektedir.  
  
Şekil 1. IoTBOX Yapısının Mimarisi

Farklı CPU mimarilerine sahip kötü amaçlı yazılım ikili dosyalarını çalıştırmak için çapraz derleme ortamlarına ihtiyaç duymuşlardır; bu nedenle, açık kaynak işlemci öykünücüsü olan QEMU’yu kullanarak bir CPU üzerinde ilgili platformları (OS) çalıştırmayı seçmişlerdir.  
Ardından, CPU ortamında çalıştırmak için ilgili OpenWRT platformunu kullanmışlardır. OpenWRT, gömülü aygıtlar (genellikle kablosuz yönlendiriciler) için son derece genişletilebilir bir GNU / Linux dağıtımıdır. OpenWRT’yi kurmak için, dağıtım için bir yapı sistemi olan OpenWRT Builtroot’u kullanılmakta ve Linux, BSD veya MacOSX üzerinde çalışmaktadır. IoTBOX, OpenWRT’nin yanında Debian Linux’u da desteklemektedir. Son olarak, Erişim Denetleyicisi, NAT gibi tüm ağa bağlı işlemleri ve C & C iletişimi, DNS çözünürlüğü ve DoS gibi saldırı trafiği gibi giden trafiği denetler. Dakikada en fazla 5 paket olan bazı DNS ve HTTP trafiğine izin vermek dışında, tüm giden DoS trafiği kötü amaçlı yazılımlardan engellemişlerdir. 23 / TCP taramaları, gerçekte IoTPOT olan Dummy Server’a yönlendirilir. Bu sayede Telnet üzerinden yayılımın nasıl yapılacağını izlenebilir. Analiz Raporu, toplam 24 saatlik paket izleme sonuçlarını, toplam paket sayısını, paket yakalama başlangıç zamanı ve bitiş saatini, Bayt / ısırık oranı, ortalama paket boyutu ve hızı ve her saldırı için kurban IP adresinin toplam sayısını ve ek olarak, C & C’deki komut dizelerinin özetlerini vermektedir.

IoT Honeypot (IoTPOT): Telnet tabanlı saldırılarla ilgili ön araştırmalar sonucunda, diğer IoT cihazlarını aramada ve saldırmak için tehlikeye atılmış ve yanlış kullanılmış IOT cihazlarının sayısı olduğunu görmüşlerdir. Bu saldırıları derinlemesine incelemek için, Telnet protokolünün ve çeşitli IoT cihazlarının etkileşimlerini öykünen yeni bir bal peteği olan IoTPOT’u önermişlerdir.  
  
Şekil 2. IoTPOT Yapısının Mimarisi  
Bu sistem aşağıdaki özellikleri destekleyecek şekilde tasarlanmıştır:  
• Öncelikle, saldıran müşterilerin kullanmayı seçtikleri seçenekleri desteklemeliyiz.

• İkincisi, bir saldırganın sadece bazı aygıtları tehlikeye atma konusunda uzmanlaştığı durumlarda, gerçekçi karşılama mesajı ve giriş komut istemini sağlamayı hedeflenmektedir.  
• Üçüncüsü, kimlik doğrulama etkileşimlerinde (örneğin, kullanıcı adlarının / şifrelerin dizilerinin) özellikleri gözlemlenmek istenilmektedir.  
• Son olarak, Telnet protokolünden bağımsız olarak, honeypot cihazlar arasında kötü amaçlı yazılım yakalamak için birden fazla CPU mimarisini desteklemelidir.

Nesnelerin interneti dünyası için buna benzer bir IoTpot, IoT exploiting sistem gerçekleştirilebilir.