2007 IEEE Symposium on Security and Privacy(SP'07)
0-7695-2848-1/07 $20.00 © 2007 IEEE

IEEE COMPUTER SOCIETY

عنوان فارسی مقاله :

آشکارسازی Trojan – تروجان - با استفاده از آثار IC

عنوان انگلیسی مقاله :

Trojan Detection using IC Fingerprinting

Dakshi Agrawal[1] Selçuk Baktır[1,2,†] Deniz Karakoyunlu[2,†] Pankaj Rohatgi[1] Berk Sunar[2,†]

2. Trojans and their Side-channel Leakage

There are several types of Trojan circuits that could infest ICs, however most Trojan circuits share some behavioral characteristics that make them useful for the attacker. All Trojan circuits need to be *stealthy*, i.e., hard to detect either from the physical appearance of the IC or during its testing and normal use. This means that the Trojan IC has to have the same physical form-factor, pin-out and *very similar* input/output behavior, i.e., for most inputs, the output of an IC with a Trojan circuit should be indistinguishable from the output of a genuine IC. In particular, if the output is a deterministic function of the input, then the Trojan IC has to output the same function for most inputs[1]. For a deterministic circuit, this essentially means that the Trojan circuit needs to monitor inputs, intermediate results, or some clock/time circuitry and wait for a trigger condition before altering the output behavior either by producing incorrect results or by causing other failures. The trigger condition has to occur with very low probability during testing or normal usage, but could be invoked more frequently by the attacker. The trigger condition may also be chosen to occur after a certain time has elapsed. For non-deterministic circuits, e.g., those involving the use of IC generated randomness, the Trojan circuit could more easily encode information in the output without detection but still needs to be very selective (possibly trigger based) in producing detectably incorrect results or causing failure.

2. Trojan و نشت از کانال جانبی

مدارهای Trojan زیادی می توانند به IC هجوم بیاورند، اما بیشتر مدارهای Trojan دارای ویژگیهای رفتاری مشابهی هستند که به واسطه آنها برای مهاجم می توانند نقش مفیدی ایفا نمایند.کلیه مدارهای Trojan می بایست پنهان مانی (stealthy) باشند ، به عبارتی آشکارسازی آنها در نتیجه ظاهر فیزیکی IC یا در طول تست و کاربرد عادی سخت و دشوار می باشد. این موضوع حاکی از آن است که Trojan IC می بایست دارای شکل فیزیکی یکسان، pin- out ، و رفتارهای ورودی/ خروجی بسیار مشابه باشند، به عبارتی برای بیشتر ورودی ها، خروجی یک IC با مدار Trojan باید از خروجی IC اصلی تمیز دانی نباشد. به ویژه، اگر خروجی را تابع تعیین کننده ورودی فرض کنیم، آنگاه، Trojan IC می بایست خروجی این تابع در بیشتر ورودی ها محسوب شود. برای مدار قطعی ، این موضوع حاکی از آن است که مدار Trojan نیازمند بازبینی ورودی ها، نتایج واسطه یا مداربندی زمان/ ساعت بوده و قبل از تغییر رفتار خروجی از طریق تولید نتایج نادرست یا بروز خطاهای دیگر، تا رسیدن به شرایط تریگر (راه انداز) صبر می کند. در طول مرحله تست یا کاربرد عادی ، شرایط تریگر بسیار کم اتفاق می افتد، اما مهاجم بیشتر اوقات از آن دفاع می کند. یکی دیگر از مواقع وقوع شرایط تریگر ، بعد از سپری شدن زمان خاص می باشد. در مورد مدارهای غیر قطعی، مثلاً مدارهایی که از حالت تصادفی ناشی از IC استفاده می کنند، مدار Trojan می تواند به راحتی اطلاعات خروجی را بدون تشخیص و آشکار سازی رمزگذاری نماید، اما در تولید نتایج نادرست آشکارشدنی یا بروز خطا (احتمالاً بر اساس تریگر) به صورت انتخابی عمل می کند .