DEPARTMENT OF AUTOMATIC CONTROL | FACULTY OF ENGINEERING | PRESENTATION DATE 2018-06-07

THESIS Minimizing Side-Channel Attack Vulnerability via Schedule Randomization
STUDENT Nils Vreman
SUPERVISOR Martina Maggio
EXAMINER Karl-Erik Årzén

How to Avoid Your Stalker

POPULAR SCIENCE ARTICLE **Nils Vreman**

Have you ever felt like you were being watched? Afraid of falling into the same routine? Make every day feel like a brand new day with this simple trick. Try randomizing your schedule; to avoid that creeping feeling of someone stalking you.

Suppose that you are stalking a person, with one purpose in mind: robbing them. To do this, you want to gather as much information as possible about the person before you strike. After following this person around for a few weeks, you know when the person leaves her house and comes back home. You know which gym she goes to and when she is there. On her way home from the gym she always stops by the grocery store to by some food. You know exactely where she will be and when she will be there.

What you do not know is that the person has had a weird feeling for a couple of weeks, suspecting that someone has been following her every move. What could she do to avoid anyone following her? She can randomize her routine. For example, Monday and Thuesday she could workout during lunch and go to the supermarket directly after work instead. On Wednesday she could sleep in for an hour and work an hour later in the afternoon instead. This way she is keeping you, the person stalking her, confused and unaware of what she is going to do next, while she can continue doing the same things she loves to do.

The same stalker scenario happens in computation devices, especially embedded devices. As much as we enjoy the predictability of embedded devices, just as much as the person enjoys her everyday routine, it comes at a cost. Predictability makes embedded devices vulnerable to attacks.

Each embedded device has a schedule that tells it what it should do and when to do it, much like a person's everyday routine. The schedule is made up of tasks that needs to be executed for the device to work. Take for example a task that most people have: work with flextime. Each day you need to work 8 hours during your office's work hours (e.g. 7 o'clock in the morning to 7 o'clock in the evening). There are some constraints introduced by your contract that you need to work 8 hours every day, but only when the office is open. The same thing happens in an embedded device's schedule. Although, some of these constraints are relaxed, meaning there is more room for randomization than in a person's everyday routine.

In this thesis, a method has been developed which introduces as much randomness as possible into the embedded device's schedule. In a world where everything is connecting to the internet, everything needs to be secured such that a potential attacker has to fight as much as possible to attack the system. With the randomization method we introduce a line of defence to protect the information the schedule hides from attackers. In other words, you do not want your stalker to know when you are doing what. Future schedule developers might use this method to improve security in embedded devices. After all, if you want to avoid your stalker: Be spontaneous and randomize your life.