6.857 Computer and Network Security November 19, 2002

Lecture Notes 21 : Tempest

Lecturer: Ron Rivest *Scribe: Giffin/Greenstadt/Plitwack/Tibbetts*

[These notes come from Fall 2001. These notes are neither sound nor complete. There is more material than is covered in lecture, and some is missing. Check your own notes for new topics brought up in 2002.]

1 Tempest

Most electronic devices produce electromagnetic radiation when they operate. Can we do anything with this radiation?

Researchers at Cambridge University (Kuhn and Anderson) set out to answer this question. They started by varying the image on a monitor, causing the electron gun to turn off and on at a specific frequency and amplitude, and played tunes on a nearby AM radio. This was a standard trick with old computers, varying the processor load to vary the amplitude/frequency.

Even this simple trick has a use. If one is able to install a virus or other malicious code into a secure facility, the code could communicate sensitive information to an outsider by using the monitors to transmit on the AM band at night for instance. An estimated 50 bits per second can be transmitted this way. In England, this could also be used to have televisions broadcast their identities to assist law enforcement searching for televisions that have not been properly registered.

A more surreptitious attack is to pick up information that is not being deliberately broadcast. In fact, Kuhn and Anderson can read text off of a screen. With most monitors of today, they can read the screen one-half to one mile away. They have built a functioning apparatus to do this.

How do you protect against this attack? There are countermeasures. Tempest fonts, also produced by Kuhn and Anderson, are one solution. These fonts look like one thing on the actual screen and another thing to remote tempest hardware.

Q: Do the fonts have a pattern?

A: Yes. Here is the trick:

> We can make a grey image for human consumption by either having solid grey, or by having varying amounts of white and black regions (pixels) at a high frequency. Humans only perceive the low frequency components of the image. Tempest is confounded by the high frequency components when they are chosen properly.

Q: Can't you just buy an LCD display?

A: They claim that LCDs are easier, not harder. You can buy a Tempest-proof monitor, but they are expensive and no one does.

Q: Tempest fonts are just a substitution cipher though, right?

A: Yeah, need to solve that problem, but certainly possible.

Q: Were these the first people to come up with this idea?

A: It's an old idea. This is the first unclassified paper on the topic. The idea of Tempest fonts is new.

Q: So an O will always look like a C?

A: Correct.

Q: But shouldn't you randomize them?

A: I suppose.

Q: Will more than one monitor cause interference?

A: I haven't tried these things. Maybe a good antenna would help. There is a lot to be done in this area.

Q: Did they publish a specification for the their receiving machine?

A: They were hand-wavy about it. But it doesn't look too hard. They talk a little bit about that. It would be good term project to build one. You would probably need more than a coat hanger and an oscilloscope though.