James Madison University

From the SelectedWorks of George H Baker

July 21, 2008

Investigation of Stun Guns as Intentional Electromagnetic Interference (EMI) Sources

George H Baker, *James Madison University*
Ryan C Tuttle, *James Madison University*

bepress™

The Feasibility and Effectiveness of a Common Consumer Device As an Electromagnetic Interference (EMI) Source

R. C. Tuttle, G. H. Baker

College of Integrated Science & Technology

James Madison University

Harrisonburg, VA 22807, USA

Abstract – **Because the operation and control of most critical infrastructures are highly dependent on electronics, it is important to understand the vulnerability of those electronics to intentional electromagnetic interference (EMI). The possibility of interference using readily available consumer devices is a particular concern. We investigated the feasibility and effectiveness of using compact stun guns to intentionally interfere with electronic systems. Test articles included individual computers and computers networked through a central hub. 60KV and 600KV devices were used in the experiments. Results indicate that stun guns are effective in disabling digital electronic systems.**

1 INTRODUCTION

Determined malefactors have demonstrated the use of common systems as effective weapons against civilian infrastructures, e.g. commercial jetliners used as kinetic weapons and cell phones used to trigger explosive devices. This undergraduate research project investigated the possibility of using readily available stun gun devices for electro-magnetic interference with or disruption of personal computers. At present, the system effects of high power electromagnetic sources are well recognized by world scientific and military communities. Former CIA Director John Deutch has said that, "the electron is the ultimate precision-guided weapon."[1] There has been much research on the deleterious effects of pulsed voltages and currents on electronic system operation. In the course of the investigation of nuclear electromagnetic pulse (EMP) effects on electronics during the Cold War period, it became evident that garden variety, unprotected electronics would malfunction, in some cases burn out, in the presence of externally induced pulsed currents in the milliampere range. EMP and high power microwave (HPM) research have demonstrated that these effects can have serious consequences in terms of interruption or termination of critical system operation. Although military systems have been the primary concern for EMP research, it is clear that the civilian infrastructure electronic communication, processing and control systems are at least as vulnerable to disruption from intense electromagnetic environments[2].

2 STUN GUNS AS "SHOP EXPEDIENT" PULSED CURRENT SOURCES

The term "shop expedient" applies to devices that are readily available off-the-shelf or can be designed and constructed using common consumer or industrial materials. Past efforts have demonstrated development of such components from electronic components[2, 3]. The present effort explored the effectiveness of commercial "stun gun" devices for upsetting or damaging computer systems.

Stun guns are available on the open market for use as non-lethal self-defense. They are used extensively by law enforcement officers. Devices are rated by their voltage output, ranging from 60 kilovolts up to 900 kilovolts. They are relatively inexpensive with a purchase price in the $25-$600 range.

---

[1] Congressional Hearing, Intelligence and Security, Chairman Jim Saxton, Joint Economic Committee, June 17, 1997.
[2] Preliminary Study Regarding the Resistance of Critical Societal Systems to High Intensity Electromagnetic Radiation, M. Backstrom et al, Royal Swedish Defense Research Agency, Report FOA-R-97-00538-612-SE, August 1997.

Figure 1: Stun Gun Devices Showing Direct Contact and Taser designs.

The devices deliver a pulsed high-voltage, low-current output that interferes with normal nerve electrical signals to temporarily stun subjects by paralyzing muscle function. Some stun guns use compressed gas to project two needle-like probes to enable contact of individuals several meters away. These "remote contact" devices are called "Tasers." Figure 1 illustrates stun gun (panels 1 and 2) and Taser (panel 3) designs.

The circuitry within a typical stun gun design is relatively simple. A circuit example is shown in figure 2.
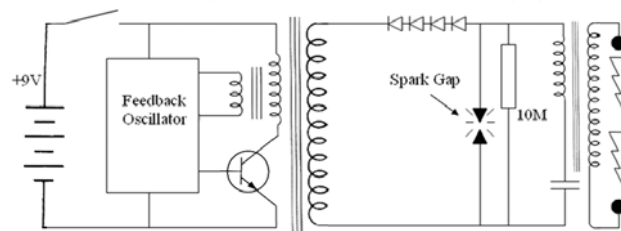

Figure 2. Example Stun Gun Circuit Schematic.

A large pulsed output voltage is produced by multiple step-up transformer stages driven by an oscillator IC. The second stage capacitor discharges through the spark gap once its breakdown voltage is exceeded yielding an exponentially decaying step function output.

Two stun gun models were used in this study. The first was a smaller, 60KV Pocket Guard® Model 6504. The device has dimensions of 10.4cm x 5.8cm x 3.2cm with an electrode spacing of 4.6 cm and weight of 0.126 kg (battery installed). The device may be easily concealed in a pocket. The second model was a 600KV Muscle Man® brand device of dimension 18cm x 6.0cm x 3.2cm with an electrode spacing of 4.0 cm and weighing 0.370 kg (batteries installed). The Pocket Guard® device uses one 9V battery. The Muscle Man® device uses four 9V batteries.

2.1 Source Output Measurements

Device output was measured by using voltage divider circuit interfaces to an oscilloscope. Several voltage divider schemes were tried but the circuit that provided the best impedance match, minimizing ringing, is shown in Figure 3. We were able to measure the output for the 60KV device using a Tektronix TDS 1002 scope. The 600KV device had a fault protection design that prevented it from firing into resistor loads – including the highest resistor we had available, 50 megohms.
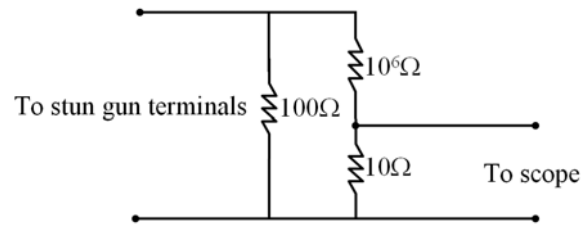
Figure 3. Voltage Divider Network for Output Recording.

The device output is a low duty cycle pulsed signal with a pulse repetition rate of 17.8/sec and corresponding period of period of 56.2 milliseconds. The pulse width at half maximum is about 2.5 microseconds. A waveform sample is included in Figure 4.
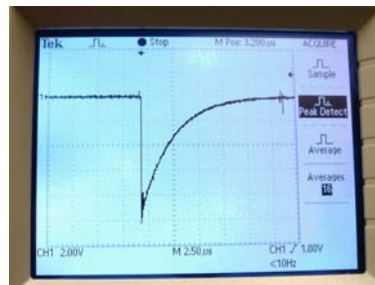

Figure 4. Stun Gun Voltage Output Trace.

2.2 Source Output Functional Fits

The pulse shape approximates a double exponential function of the form:

$$V(t) = A\left(e^{-\beta t} - e^{-\alpha t}\right)$$ (eqn. 1)

Where A is the amplitude, α is the rise rate and β is the decay rate. The Fourier transform of this function is:

$$V(\omega) = \frac{A(\alpha - \beta)/\alpha\beta}{\sqrt{\left[1 + \left(\frac{\omega}{\beta}\right)^2\right]\left[1 + \left(\frac{\omega}{\alpha}\right)^2\right]}}$$ (eqn. 2)

An α value of 0.18 x 10^6 and a β value of 8.0 x 10^6 yield reasonable approximations to the measured waveforms. A graphical overlay is presented in figure 5.
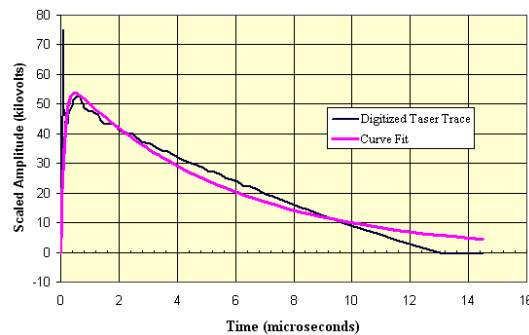
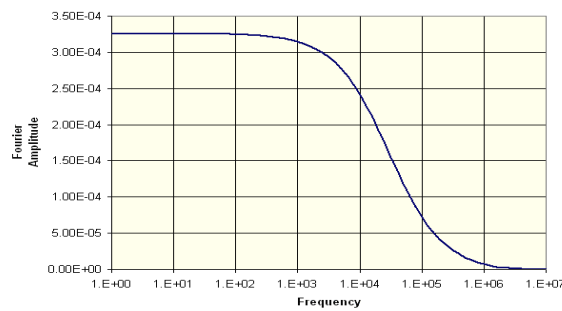

Figure 5. Stun Gun Output Curve Fit

Figure 6. Fourier Transform of stun gun output curve fit

3 EXPERIMENTAL APPROACH

Tests were conducted by positioning computers on a laboratory bench top with their CPU back panels facing forward. Each computer was tested by connecting the stun gun output between a computer back panel connector pin of interest and the back panel case (ground) as illustrated in figure 6.
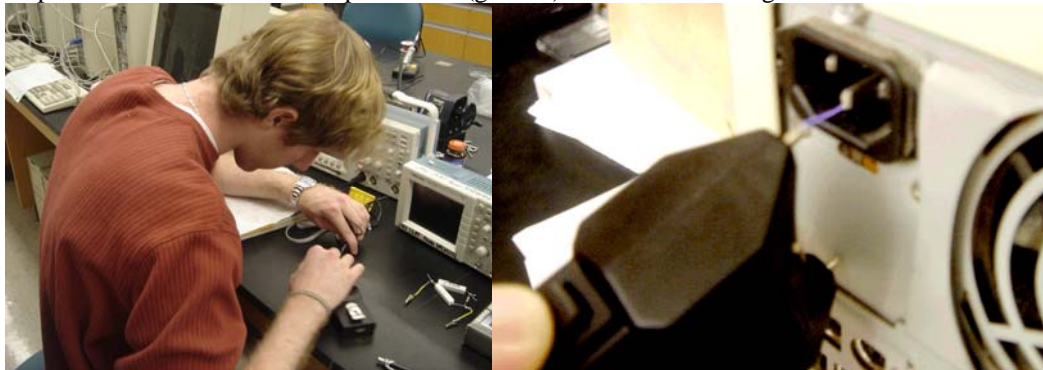

Figure 6.   Laboratory bench top setup (left panel) and injection technique (right panel).

3.1 Test Objects

Surplus computers were made available for use as test objects by James Madison University's IT division. The machines were 1998 vintage 200 MHz Dell desk top computers with basic functional components including CPU, monitor, mice and keyboards.   They each came equipped with a Windows 95 operating system. A total of eighteen computers were tested individually.

3.2 Exposure Sequence

In order to maximize information learned from each test object, we were concerned not to render a given computer inoperable on the first injection pulse. Therefore, we tested the computer injection points in the order of increasing likelihood of system function debilitation. We first ran through the injection sequence with the 60KV device. If the computer survived, we performed the injection sequence with the 600KV device.   We learned as we proceeded and adjusted the test point sequence to preserve computers for the maximum number of injection data points. The final complete test point sequence is listed in table 1. Injection ports are listed in rough order of severity of effects when pulsed.

Table 1 – Injection Sequence

Order number	Injection Point
1	Keyboard Cord Exterior
2	Mouse Cord Exterior
3	Monitor Cable Exterior
4	Power Cable Exterior
5	Audio Output Port
6	Microphone Port
7	LAN Port
8	Printer Port
9	Joystick Port
10	USB Port
11	Keyboard Port
12	Mouse Port
13	Serial Port
14	Power Port (chord disconnected)

3.3 System Effects Categories

Computer effects varied in their severity. To distinguish effects severity we developed a set of numerical rating categories. Observed system effects were recorded using the numbered categories listed in Table 2. We did not have the resources necessary to perform post-test diagnostics on the exposed computer systems other than a visual functional checkout.

Table 2. System Effects Categories

Rating Category	Effects Description
0	No effects observed during and after exposure
1	Noise or screen flicker
2	Transient upset
3	Upset leading to manual reboot
4	Manual reboot required to restore functionality.
5	Complete system failure due to permanent component(s) damage.

3.4 Experiment Results – System Effects

A total of 18 computers were tested. All computers were eventually permanently damaged (rating category 5) during the testing. Seven computers were permanently damaged by the smaller (60KV) device. The remaining computers were permanently damaged by the larger (600KV) device. Using the 60KV device, computers were permanently damaged by power port injection (5 computers), keyboard port injection (1 computer), and USB port injection (1 computer). Using the 600KV device, a wider range of port types were vulnerable. In addition to damage from injecting the power (2 computers) and keyboard(2 computers) ports , computers were permanently damaged by injecting the printer port (2 computers), USB port (2 computers), joystick port (1 computer), mouse port (1 computer), and serial port (1 computer) with the larger 600 KV device. Figure 7 provides a color-coded composite listing of experimental trials and results.

Initial Computer Ensemble

CPU Model Number/Serial Number	Keyboard Cord	Mouse Cord	Monitor Cable	Power Cable	Speaker Jack	Microphone Jack	Lan Port	Power Port (cord disconnected)	Printer Port	USB Port	Keyboard Port	Mouse Port	Serial Port
model # DCM Serial # 58KG40B	0	0	0	0	NA	NA	NA	NA	NA	NA	5	0	NA
model # MMP Serial # DZFPY	0	0	1	0	0	0	0	0	0	4	0	0	0
	0	0	0	0	0	0	0	0	5	CPD	CPD	CPD	CPD
model # DCM Serial # 6X242OB	0	0	0	1	3	1	0	1	1	4	3	0	3
	0	0	0	0	0	0	3	5	CPD	CPD	CPD	CPD	CPD
model # DCM Serial # 79CS00B	0	0	0	1	0	0	3	0	4	4	3	3	3
	0	0	0	0	1	0	NA	0	0	5	CPD	CPD	CPD
model # MMM Serial # 6JHHC	0	0	0	1	0	0	0	0	0	NA	5	CPD	CPD
	CPD	CPD	CPD	CPD	CPD	CPD	CPD	CPD	CPD	CPD	CPD	CPD	CPD
model # DCM Serial # HR1530B	0	0	0	1	0	2	0	0	4	3	4	0	3
	0	0	0	0	0	0	0	0	5	CPD	CPD	CPD	CPD

Additional Computer Ensemble

CPU Model Number/Serial Number	Keyboard Cord	Mouse Cord	Monitor Cable	Power Cable	Speaker Jack	Microphone Jack	Lan Port	Printer Port	Joystick Port	USB Port	Keyboard Port	Mouse Port	Serial Port	Power Port (cord disconnected)
model # MMS Serial # 95MVD	0	0	0	1	0	0	NA	0		0	0	0	0	0
	0	0	0	0	0	0	NA	CPD		CPD	CPD	CPD	CPD	5
model # MMS Serial # 95N6Y	0	1	1	1	1	0	NA	0		0	1	0	0	0
	0	0	0	0	1	0	NA	CPD		CPD	CPD	CPD	CPD	5
model # MMS Serial # 95NPG	0	0	1	1	0	0	NA	0		0	0	0	0	0
	0	0	0	0	0	0	NA	0		0	4	3	4	5
model # MMS Serial # 95N7X	0	0	0	1	0	0	NA	3		0	0	0	0	0
	0	0	0	0	0	0	NA	0		0	0	0	4	5
model # MMS Serial # 95NNH	0	0	0	0	0	0	NA	0		0	0	0	3	0
	0	0	0	0	0	0	NA	0		0	0	0	4	5
model # MMS Serial # 95N02	0	0	0	1	0	0	NA	0	0	0	0	0	2	0
	0	0	0	0	0	0	NA	0	0	0	0	5	CPD	CPD
model # MMS Serial # 95NCG	0	0	0	1	0	0	NA	0	0	5	CPD	CPD	CPD	0
model # MMS Serial # 95MZ7	CPD	CPD	CPD	CPD	CPD	CPD	NA	CPD	CPD	5	CPD	CPD	CPD	CPD
	0	0	0	1	0	0	NA	0	0	0	0	0	0	0
model # MMS Serial # 95MSR	0	0	0	0	0	0	NA	0	0	0	0	0	5	CPD
	CPD	CPD	CPD	CPD	CPD	CPD	NA	CPD	CPD	CPD	CPD	CPD	CPD	CPD
model # MMS Serial # 95N16	0	0	0	0	0	0	NA	0	0	0	0	0	0	0
	0	0	0	0	0	0	NA	0	0	0	4	4	4	5
model # MMS Serial # 95MYQ	0	NA	0	0	0	0	NA	0	0	0	0	NA	0	0
	0	NA	0	0	0	2	NA	0	0	0	5	NA	CPD	CPD
model # MMS Serial # 95MTK	0	0	0	0	0	0	NA	0	0	0	1	0	0	1
	0	0	0	0	0	0	NA	0	5	CPD	CPD	CPD	CPD	CPD

Key

Key
No Underline - Small Taser
Underlined Result - Big Taser
CPD = Computer Previously Destroyed
NA = Not Applicable

Effect Categories

1 noise or screen flicker
2 transient upset
3 upset leading to automatic reboot
4 manual reboot
5 permanent damage, no functionality

Figure 7: Experimental Results

4.0 CONCLUSIONS

Commercially available stun guns may be used to permanently damage personal computers. Even a small palm-size device is effective when touched to vulnerable back-panel connectors. The AC power port was the most susceptible to damage on the Dell personal computers that were tested. Other vulnerable injection points included the printer output, USB, serial I/O, joystick, and mouse ports.

Acknowledgments

References

1. Congressional Hearing, Intelligence and Security, Chairman Jim Saxton, Joint Economic Committee, June 17, 1997.
2. The Feasibility and Effectiveness of a Common Consumer Device as an Electromagnetic Interference (EMI) Source, Proceedings of the Joint International Conference on Electromagnetics in Advanced Applications, Torino, 2005.
3. Preliminary Study Regarding the Resistance of Critical Societal Systems to High Intensity Electromagnetic Radiation, M. Backstrom et al, Royal Swedish Defense Research Agency, Report FOA-R-97-00538-612-SE, August 1997